Application Operations Management

User Guide

Issue 01

Date 2025-03-03

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 Using IAM to Grant Access to AOM

1.1 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.

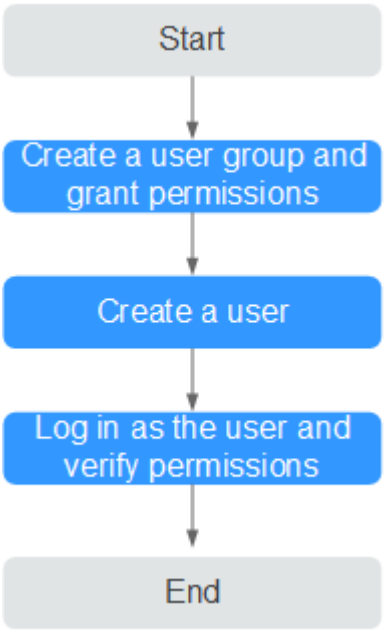
This section describes the procedure for granting permissions (see **Figure 1-1**).

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 Flow

Figure 1-1 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.

1.2 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: Create a JSON policy or edit an existing one.

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"
            ]
        }
    ]
}
```


2 Connecting to AOM

2.1 Connecting to AOM

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

Constraints

If you want to switch from the new Access Center to the old one, click **Back to Old Version** in the upper right corner.

Ingesting Metrics or Logs to AOM

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 Ingest metrics or logs based on monitored object types.

Table 2-1 Access overview

Type	Monitored Object	Data Source	Access Mode
Business access	ELB logs	Metrics	**2.3 Connecting Businesses to AOM**
	APM transactions		
Application access	Java applications	Metrics	**2.4 Connecting Applications to AOM**
Prometheus middleware access	MySQL	Metrics	**2.5.2 Connecting Middleware to AOM**
	Redis		
	Kafka		

Type	Monitored Object	Data Source	Access Mode
	Nginx		
	MongoDB		
	Consul		
	HAProxy		
	PostgreSQL		
	Elasticsearch		
	RabbitMQ		
	Other components (Custom Exporter)		
Prometheus running environment access	Cloud Container Engine (CCE) (ICAgent)	Metrics	**2.6 Connecting Running Environments to AOM**
	Cloud Container Instance (CCI)		
	Elastic Cloud Server (ECS)		

Type	Monitored Object	Data Source	Access Mode
Prometheus cloud service access	Auto Scaling, FunctionGraph, Elastic Volume Service (EVS), Cloud Backup and Recovery (CBR), Object Storage Service (OBS), Scalable File Service (SFS), SFS Turbo, Virtual Private Cloud (VPC), Elastic Load Balance (ELB), Direct Connect, Virtual Private Network (VPN), NAT Gateway, Enterprise Router, Distributed Message Service (DMS), Distributed Cache Service (DCS), API Gateway (APIG), GaussDB(for MySQL), GeminiDB, Relational Database Service (RDS), Document Database Service (DDS), Data Replication Service (DRS), ModelArts, LakeFormation, CloudTable, MapReduce Service (MRS), GaussDB(DWS), Data Lake Insight (DLI), Cloud Search Service (CSS), IoT Device Access (IoTDA), Intelligent EdgeFabric (IEF), Web Application Firewall (WAF), Cloud Bastion Host (CBH), Simple Message Notification (SMN), and Content Delivery Network (CDN)	Metrics	**2.7 Connecting Cloud Services to AOM**
Open-source monitoring system access	Common Prometheus instance	Metrics	**2.8 Connecting Open-Source System to AOM**
Prometheus API/SDK access	AOM APIs	Metrics	Through **APIs**
Custom Prometheus plug-in access	Custom Prometheus plug-ins	Metrics	**2.5.3 Connecting Custom Plug-ins to AOM**

----End

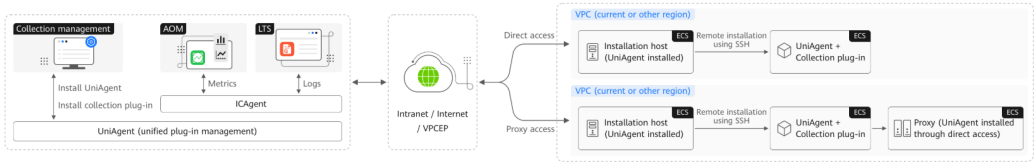
2.2 Managing Collector Base UniAgent

2.2.1 Installing UniAgents

UniAgents centrally manage the life cycle of collection plug-ins and deliver instructions (such as script delivery and execution). UniAgents do not collect data themselves. O&M data is collected by collection plug-ins. You can install collection plug-ins through the access center and create collection tasks to collect metrics.

AOM allows you to install UniAgents on cloud servers in a VPC.

Figure 2-1 Getting started



Prerequisite

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

Constraints

- For details about the Linux and Windows OSs supported by the UniAgent, see **Collection Management Restrictions**.
- To switch from the new UniAgent page to the old one, choose **Settings** > **Collection Settings** > **UniAgent Installation and Configuration** in the navigation tree on the left and click **Back to old version** in the upper right corner. To go to the **new UniAgent** page, click **Go to New Version** in the upper right corner of the **UniAgent Installation and Configuration** page.

Installation Methods

Install a UniAgent on a host manually or remotely, or by importing an Excel file. Select an installation mode based on site requirements.

Table 2-2 Installation modes

Mode	Scenario
Manual UniAgent Installation	Suitable for initial installation and single-node installation scenarios. Log in to the host where the UniAgent is to be installed and manually run the installation command. **When installing a UniAgent for the first time, you must install it manually.**

Mode	Scenario
Remote UniAgent Installation	Suitable for the scenario where UniAgents are installed in batches. Set a host where a UniAgent has been installed to be an installation host, and use it to install UniAgents on other hosts. (Enter the information about the hosts where UniAgents are to be installed on the installation page.)
UniAgent Installation by Importing an Excel File	Suitable for the scenario where UniAgents are installed in batches. Set a host where a UniAgent has been installed to be an installation host, and use it to install UniAgents on other hosts. (Import the Excel file that contains the information about the hosts where UniAgents are to be installed on the installation page.) **The Excel import function is not yet generally available. If you need this function, submit a service ticket.**

Manual UniAgent Installation

When installing a UniAgent for the first time, you must install it manually.

Step 1 Log in to the AOM 2.0 console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **UniAgent Installation and Configuration**. Then click **Install UniAgent** in the upper right corner. On the displayed page, choose **Manual**. (When you install the UniAgent for the first time, the **Manual** page is displayed by default.)

Step 4 On the **Install UniAgent** page, set parameters to install a UniAgent.

Figure 2-2 Manually installing a UniAgent

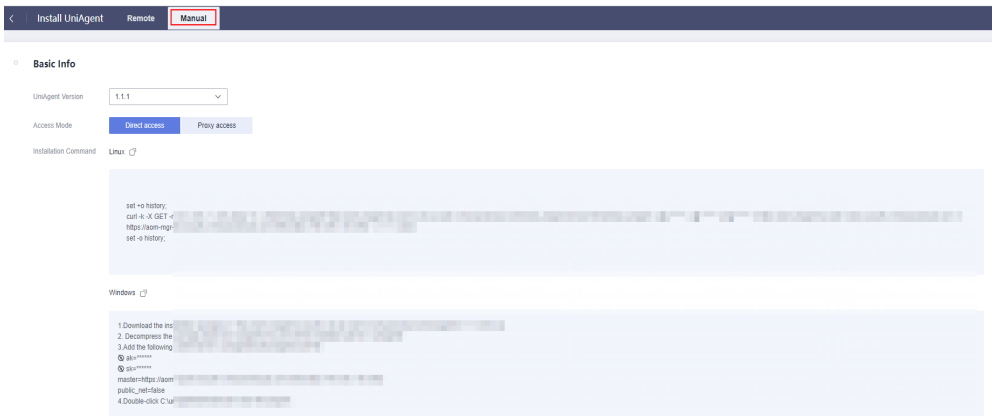


Table 2-3 Parameters for manual installation

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.0.8
Access Mode	There are 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 install the UniAgent on a host through the proxy. **You can choose Direct access (private network) and Direct access (public network) only in CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, and CN South-Guangzhou.**	Direct access (private network)
Proxy Area	Manages proxies by category. When **Access Mode** is set to **Proxy access**, you need to select or **add** a proxy area. A proxy area must contain an available proxy. This proxy must be a cloud host where a UniAgent has been installed. Also, this proxy must have been **set to be an installation host**.	Select a proxy area.

Parameter	Description	Example

Installation Command	Command for installing the UniAgent. Commands for Linux and Windows are different.
	Linux
	1. Click to copy the installation command.
	`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 -q false`
	`set -o history;`
	Windows
	1. Copy the download address (**https://aom-uniagent-*{region_name}*.obs.*{region_name}*.*{site domain name suffix}*/+uniagentd-*{version}*-win32.zip**) to the browser to download the installation package.
	{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. Enter the following configuration (obtained from the installation page) to the **C:\uniagentd\conf\uniagentd.conf** file:
	`master=https://aom-mgr-lb.xxxxxxxxxxx,https://xx.xx.xx.xx:xxxxx`
	`project_id=xxxxxxxxxxxxxx`
	`public_net=xxxx`
	4. Run **start.bat** in the **C:\uniagentd\bin** directory as the administrator.
	If you need to verify the SHA256 value of the Windows installation package, check the file downloaded from **https://aom-uniagent-*{region_name}*.obs.**
		Copy the Linux installation command.

Parameter	Description	Example
	{region_name}.{site domain name suffix}/**uniagentd-***{version}***-win32.zip.sha256**.	

Step 5 Copy the installation command and run it on the host to install the UniAgent.

- Linux host: Use a remote login tool, such as PuTTY, to log in to the target host and run the installation command copied in the **previous step** as the **root** user to install the UniAgent.
- Windows host: Log in to the target host, and download the installation package based on the installation command in the **previous step** to install the UniAgent.

Step 6 Check whether the UniAgent is displayed in the UniAgent list.

----End

Remote UniAgent Installation

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **UniAgent Installation and Configuration**. Then click **Install UniAgent** in the upper right corner.

Step 4 On the **Install UniAgent** page, choose **Remote** and set parameters to install a UniAgent. (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 2-3 Remotely installing a UniAgent

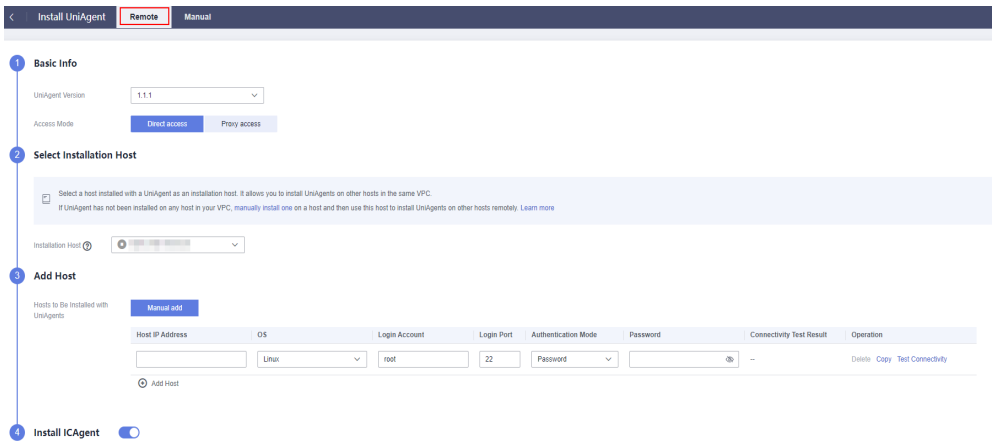
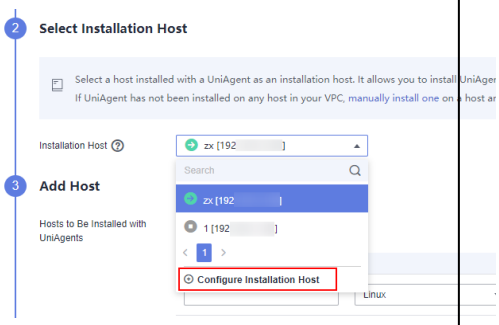


Table 2-4 Parameters for remotely installing a UniAgent

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.0.8
Access Mode	There are 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 install the UniAgent on a host through the proxy. **You can choose Direct access (private network) and Direct access (public network) only in CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, and CN South-Guangzhou.**	Direct access (private network)
Proxy Area	Manages proxies by category. When **Access Mode** is set to **Proxy access**, you need to select or **add** a proxy area. A proxy area must contain an available proxy. This proxy must be a cloud host where a UniAgent has been installed. Also, this proxy must have been **set to be an installation host**.	Select a proxy area.

Parameter	Description	Example
Installation Host	An installation host is used to execute commands for remote installation. This parameter is mandatory. To install the UniAgent remotely, ensure that the installation host does not run Windows. If no installation host has been configured, perform the following steps: 1. Select **Configure Installation Host** from the drop-down list. **Figure 2-4** 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**.	Select an installation host.

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. Add a maximum of 100 hosts: • **Host IP Address**: IP address of a host. • **OS**: operating system of the host, which can be **Linux** or **Windows**. To install the UniAgent remotely, ensure that the host does not run 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. After entering the host information, you can delete, copy, or test the connectivity of hosts in the **Operation** column. The connectivity test checks the network between the installation host and the host where the UniAgent is to be installed. The test result is displayed in the **Connectivity Test Result** column. (Windows hosts do not support connectivity tests.)	Enter the information about the hosts where UniAgents are to be installed.
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 if needed. (In some regions, you do not need to enter any AK or SK.)	-

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

----End

UniAgent Installation by Importing an Excel File

The Excel import function is not yet generally available. If you need this function, **submit a service ticket**.

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **UniAgent Installation and Configuration** and click **Install UniAgent** in the upper right corner.

Step 4 On the **Install UniAgent** page, choose **Import Excel** and set parameters to install a UniAgent. (When you install the UniAgent for the first time, the **Manual** page is displayed by default. **Import Excel** is not available.)

Figure 2-5 Installation by importing an Excel file

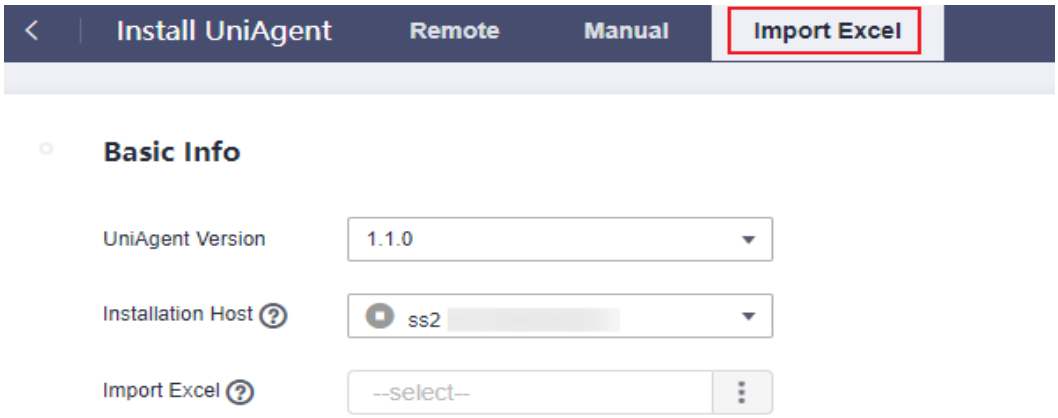
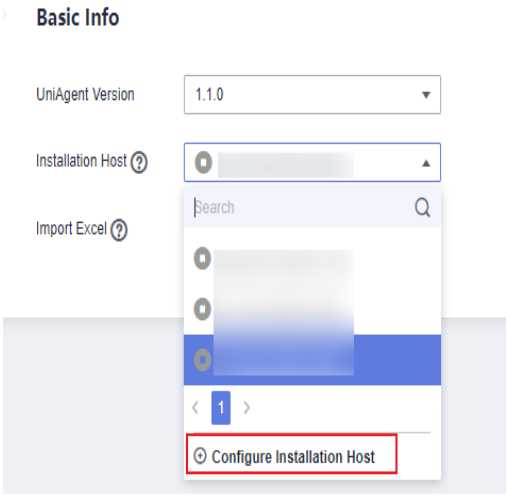
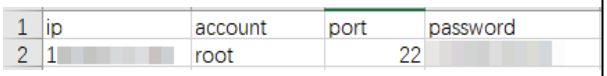


Table 2-5 Parameters for installation by importing an Excel file

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. To install the UniAgent by importing an Excel file, ensure that the installation host does not run Windows. If no installation host has been configured, perform the following steps: 1. Select **Configure Installation Host** from the drop-down list. **Figure 2-6** 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**.	Select an installation host.

Parameter	Description	Example
Import Excel	Only an **.xls** or **.xlsx** file with up to 5,000 records can be uploaded. To install the UniAgent by importing an Excel file, ensure that the host does not run Windows. Excel file example: **Figure 2-7** Configuring host information  • **ip**: IP address of the host where the UniAgent is to be installed. • **account**: account for logging in to the host. You are advised to use the **root** account to get sufficient read and write permissions. • **port**: port for accessing the host. • **password**: password for logging in to the host.	Upload the Excel file containing host information.

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

----End

Checking the UniAgent Status

On the **UniAgent Installation and Configuration** page, check the UniAgent status of the target host. For details, see **Table 2-6**.

Table 2-6 UniAgent statuses

Status	Description
Running	The UniAgent is working.
Abnormal	The UniAgent is not working. Contact technical support.
Installing	The UniAgent is being installed. The installation takes about 1 minute to complete.
Installation failed	The UniAgent fails to be installed. Uninstall the UniAgent and then reinstall it. If the installation still fails, contact technical support.

Status	Description
Not installed	The UniAgent has not been installed on the host. For a host where the UniAgent is uninstalled but it is not deleted, the UniAgent is in the **Not installed** state. You can reinstall the UniAgent or delete the host from the list.

After the UniAgent is installed on the host, ports **39338** and **39339** will be enabled to query log levels and collection tasks.

Other Operations

If needed, perform the following operations on the host where the UniAgent has been installed.

Table 2-7 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 bottom).  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. Precautions: • 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, do as follows: Choose **Cancel Installation Host** in the **Operation** column to cancel an installation host.
Changing the name of an installation host	To change the name of a configured installation host, do as follows: Click the name of the installation host. In the dialog box that is displayed, rename it.

Troubleshooting

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

2.2.2 (New) Installing UniAgents

UniAgents centrally manage the life cycle of collection plug-ins and deliver instructions (such as script delivery and execution). UniAgents do not collect data themselves. O&M data is collected by collection plug-ins. You can install collection plug-ins through the access center and create collection tasks to collect metrics.

AOM allows you to install UniAgents on ECSs or other servers in or outside the current region.

- **Current region**: Install UniAgents on the hosts in the region where the AOM console is located.
- **Outside current region**: Install UniAgents on the hosts outside the region where the AOM console is located. For example, the hosts of self-built Internet Data Centers (IDCs), of third-party cloud vendors, or in the other regions of Huawei Cloud.

Constraints

- For details about the Linux and Windows OSs supported by the UniAgent, see **Collection Management Restrictions**.
- To switch from the old UniAgent page to the new one, choose **Settings** > **Collection Settings** > **UniAgent Installation and Configuration** in the navigation tree on the left and click **Go to New Version** in the upper right corner. To go to the **old UniAgent** page, click **Back to old version** in the upper right corner of the **UniAgent Installation and Configuration** page.

Installation Methods

AOM allows you to install UniAgents on hosts in CLI mode.

Table 2-8 Installation mode

Mode	Scenario
CLI	Suitable for initial installation and single-node installation scenarios. Use a remote login tool, such as PuTTY, to log in to the host where the UniAgent is to be installed and manually run the installation command. For details, see: • **Installing UniAgent by Running Command (in Current Region)** • **Installing UniAgent by Running Command (Outside Current Region)**

Installing UniAgent by Running Command (in Current Region)

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 On the displayed page, click **Install UniAgent**.

Step 4 On the **Install UniAgent** page, set parameters to install a UniAgent.

Figure 2-8 Installing a UniAgent

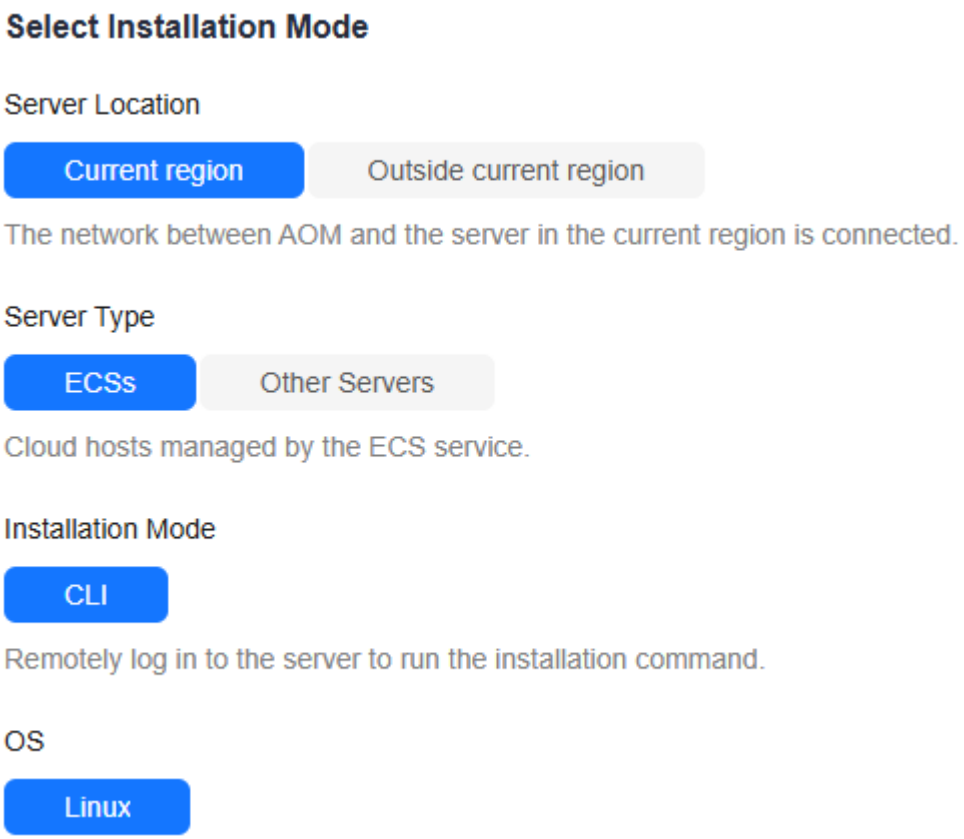


Table 2-9 Installation parameters

Parameter	Description	Example
Server Region	Select the region where the target cloud server is located. Options: • **Current region**: The network between AOM and the server in the current region is connected by default. • **Outside current region**: The cloud server is in a different region from AOM. Select a network connection solution based on site requirements.	Current region
Server Type	Options: • **ECSs**: hosts managed by the ECS service. • **Other servers**: other hosts.	ECSs
Installation Mode	Option: **CLI**. You need to remotely log in to the server to run the installation command provided on the console.	CLI
OS	Option: **Linux**.	Linux

Parameter	Description	Example
UniAgent Version	Select a UniAgent version. The latest version is selected by default.	Latest Version

Copy and Run Installation Command	1. Click **Copy** to copy the installation command.
	`set +o history;`
	`curl -k -X GET -m 20 --retry 1 --retry-delay 10 -o /tmp/install_uniagent https://aom-uniagent-**********.com/install_uniagent.sh;bash /tmp/install_uniagent -p ********** -y **********`
	`set -o history;`
	2. Use a remote login tool, such as PuTTY, to log in to the server and run the copied installation command as user **root**.
		Copy and run the installation (Linux) command.

Step 5 **Check the UniAgent status** in the UniAgent list.

----End

Installing UniAgent by Running Command (Outside Current Region)

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 On the displayed page, click **Install UniAgent**.

Step 4 On the **Install UniAgent** page, set parameters to install a UniAgent.

Figure 2-9 Installing a UniAgent

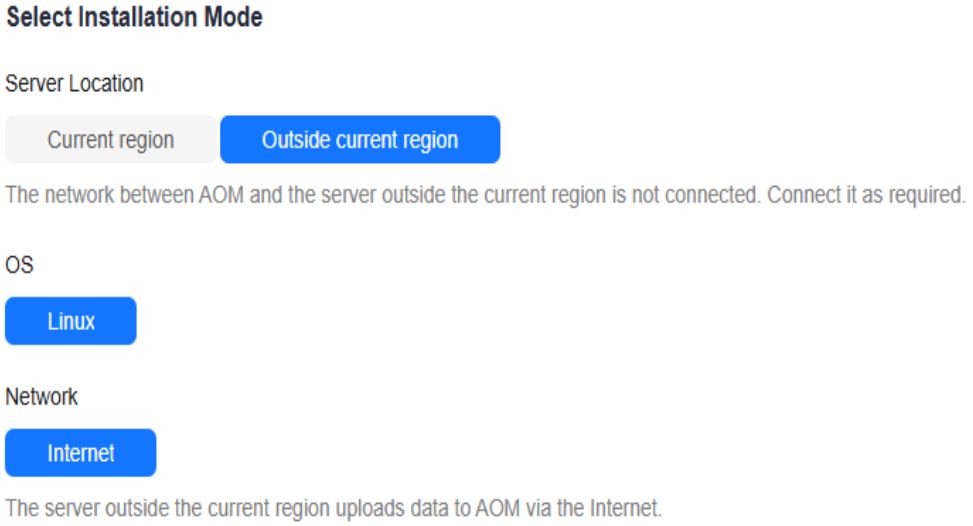


Table 2-10 Installation parameters

Parameter	Description	Example
Server Region	Select the region where the target cloud server is located. Options: • **Current region**: The network between AOM and the server in the current region is connected by default. • **Outside current region**: The cloud server is in a different region from AOM. Select a network connection solution based on site requirements.	Outside current region
OS	Option: **Linux**.	Linux
Network	Option: **Internet**. After a server outside the current region is connected to Internet, it can communicate with AOM.	Internet

Copy and Run Installation Command	1. Click **Copy** to copy the installation command.
	`set +o history;`
	`curl -k -X GET -m 20 --retry 1 --retry-delay 10 -o /tmp/install_uniagent https://aom-uniagent-**********.com/install_uniagent.sh;bash /tmp/install_uniagent -o public -p ********** -y **********`
	2. Use a remote login tool, such as PuTTY, to log in to the server and run the copied installation command as user **root**.
		Copy and run the installation (Linux) command.

Step 5 **Check the UniAgent status** in the UniAgent list.

----End

Checking the UniAgent Status

On the **UniAgent Installation and Configuration** page, check the UniAgent status of the target host. For details, see **Table 2-11**.

Table 2-11 UniAgent statuses

Status	Description
Running	The UniAgent is working.
Abnormal	The UniAgent is not working. Contact technical support.
Installing	The UniAgent is being installed. The installation takes about 1 minute to complete.

Status	Description
Installation failed	The UniAgent fails to be installed. Uninstall the UniAgent and then reinstall it. If the installation still fails, contact technical support.
Not installed	The UniAgent has not been installed on the host. For a host where the UniAgent is uninstalled but it is not deleted, the UniAgent is in the **Not installed** state. You can reinstall the UniAgent or delete the host from the list.

After the UniAgent is installed on the host, ports 39338 and 39339 will be enabled to query log levels and collection tasks.

Other Operations

If needed, perform the following operations on the host where the UniAgent has been installed.

Table 2-12 Related operations

Operation	Description
Searching for a host	In the search box above the host list, search for a host by host ID, name, or status.
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.
Sorting hosts	In the table header of the host list, click  in each column to sort hosts.  indicates the default order,  indicates the ascending order, and  indicates the descending order.

Troubleshooting

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

2.2.3 Managing UniAgents

After UniAgents are installed, you can reinstall, upgrade, uninstall, or delete them when necessary.

Constraints

- If the host where a UniAgent is installed using the **old method** runs Windows, you need to manually reinstall the UniAgent.
- UniAgents will not be automatically upgraded. Manually upgrade them if needed.
- If the host where a UniAgent is installed using the **old method** runs Windows, you need to manually uninstall the UniAgent.

Reinstalling UniAgents

Reinstall UniAgents when they are in the **Abnormal**, **Installation failed**, or **Not installed** state.

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **UniAgent Installation and Configuration**.

Step 4 Select one or more servers where UniAgents are to be reinstalled and perform the following operations:

- (Old) On the **VM Access** page, choose **UniAgent Batch Operation** > **Reinstall**. On the displayed page, **reinstall UniAgents** as prompted.
- (New) On the **UniAgent Installation and Configuration** page, switch to the **ECS** or **Other** tab page and click **Reinstall**. On the displayed page, **reinstall UniAgents** as prompted.

----End

Upgrading UniAgents

Upgrade your UniAgent to a more reliable, stable new version.

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Settings** > **Collection Settings** > **UniAgent Installation and Configuration**.

Step 3 Select one or more servers where UniAgents are to be upgraded and perform the following operations:

- (Old) On the **VM Access** page, choose **UniAgent Batch Operation** > **Upgrade**. On the displayed page, select the target version and click **OK**.
- (New) On the **UniAgent Installation and Configuration** page, switch to the **ECS** or **Other** tab page and click **Upgrade**. On the displayed page, select the target version and click **OK**.

Wait for about 1 minute until the UniAgent upgrade is complete.

----End

Uninstalling UniAgents

Uninstall UniAgents when necessary.

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Settings** > **Collection Settings** > **UniAgent Installation and Configuration**.

Step 3 Select one or more servers where UniAgents are to be uninstalled and perform the following operations:

- (Old) On the **VM Access** page, choose **UniAgent Batch Operation** > **Uninstall**. On the displayed page, click **OK**.
- (New) On the **UniAgent Installation and Configuration** page, switch to the **ECS** or **Other** tab page and click **Uninstall**. On the displayed page, click **OK**.

You can also log in to the target server as the **root** user and run the following command to uninstall the UniAgent:

bash /usr/local/uniagentd/bin/uninstall_uniagent.sh;

----End

Deleting UniAgents

Delete the UniAgents that are not used or cannot be used according to the following procedure:

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Settings** > **Collection Settings** > **UniAgent Installation and Configuration**.

Step 3 Select one or more servers where UniAgents are to be deleted and perform the following operations:

- (Old) On the **VM Access** page, choose **UniAgent Batch Operation** > **Delete**. On the displayed page, click **OK**.
- (New) On the **UniAgent Installation and Configuration** page, switch to the **Other** tab page and click **Delete**. On the displayed page, click **OK**. (Only the hosts on the **Other** tab page support UniAgent deletion.)

----End

2.2.4 Managing ICAgent Plug-ins for Hosts

AOM will support interconnection with other types of plug-ins. You can install, upgrade, uninstall, start, stop, and restart plug-ins in batches for hosts.

Currently, only ICAgents are supported. An ICAgent is a plug-in for collecting metrics and logs. ICAgent collects data at an interval of 1 minute. This interval cannot be changed.

Managing ICAgent Plug-ins in Batches

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **UniAgent Installation and Configuration**.

Step 4 Select one or more target servers 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 2-13 Plug-in operation parameters

Parameter	Description
Operation	The following batch operations are supported: install, upgrade, uninstall, start, stop, and restart. **If the ICAgent is uninstalled from a server, AOM will not collect metrics from the server. Exercise caution when performing this operation.**
Plug-in	Select the plug-in to be operated. The ICAgent of the latest version can be installed.
AK/SK	Access Key ID/Secret Access Key (AK/SK) to be entered based on your plug-in type and version. For details, see **How Do I Obtain an AK/SK**. **You need to enter an AK/SK only when installing the ICAgent of an earlier version. (If there is no text box for you to enter the AK/SK, the ICAgent of the new version has already been installed.)**

----End

2.2.5 Managing ICAgents in CCE Clusters

AOM allows you to install, upgrade, and uninstall ICAgents on hosts in purchased CCE clusters in batches.

Prerequisites

- You have bought CCE clusters and nodes. For details, see **Buying a CCE Standard/Turbo Cluster** and **Creating a Node**.

Viewing CCE Clusters

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **CCE Access**.

Step 4 Check the connected CCE clusters.

You can enter a keyword in the search box to search for your target cluster.

----End

Managing ICAgents in CCE Clusters

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **CCE Access**.

Step 4 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. 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. 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. **(Uninstalling ICAgents will cause some application O&M functions to be unavailable. Exercise caution when performing this operation.)**
  a. 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.

----End

2.2.6 Managing Host Groups

AOM is a unified platform for observability analysis. It does not provide log functions by itself. Instead, it integrates the host group management function of **Log Tank Service (LTS)**. You can perform operations on the AOM 2.0 or LTS console.

To use the host group management function on the AOM 2.0 console, **purchase LTS resources** first.

Table 2-14 Description

Function	Description	AOM 2.0 Console	LTS Console	References
Host group management	Host groups allow you to configure host log ingestion efficiently. You can add multiple hosts to a host group and associate the host group with log ingestion configurations. The ingestion configurations will then be applied to all the hosts in the host group.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane, choose **Settings** > **Collection Settings** > **Host Groups**.	1. Log in to the LTS console. 2. In the navigation pane, choose **Host Management** > **Host Groups**.	**Managing Host Groups**

- To use LTS functions on the AOM console, you need to obtain LTS permissions in advance. For details, see **Permissions**.
- AOM 2.0 also provides a new version of host group management. After you switch to the new access center, the **new host group management** page will be displayed.

2.2.7 (New) Managing Host Groups

Host groups allow you to configure host data ingestion efficiently. You can add multiple hosts to a host group and associate the host group with ingestion configurations. The ingestion configurations will then be applied to all the hosts in the host group. When there is a new host, simply add it to a host group and the host will automatically inherit the log ingestion configurations associated with the host group.

You can create host groups of the IP address and custom identifier types.

- **Host Group Type** set to **IP**: Select hosts of the IP address type and add them to the host group.
- **Host Group Type** set to **Custom Identifier**: You need to create identifiers for each host group and host. Hosts with an identifier will automatically be included in the corresponding host group sharing that identifier.

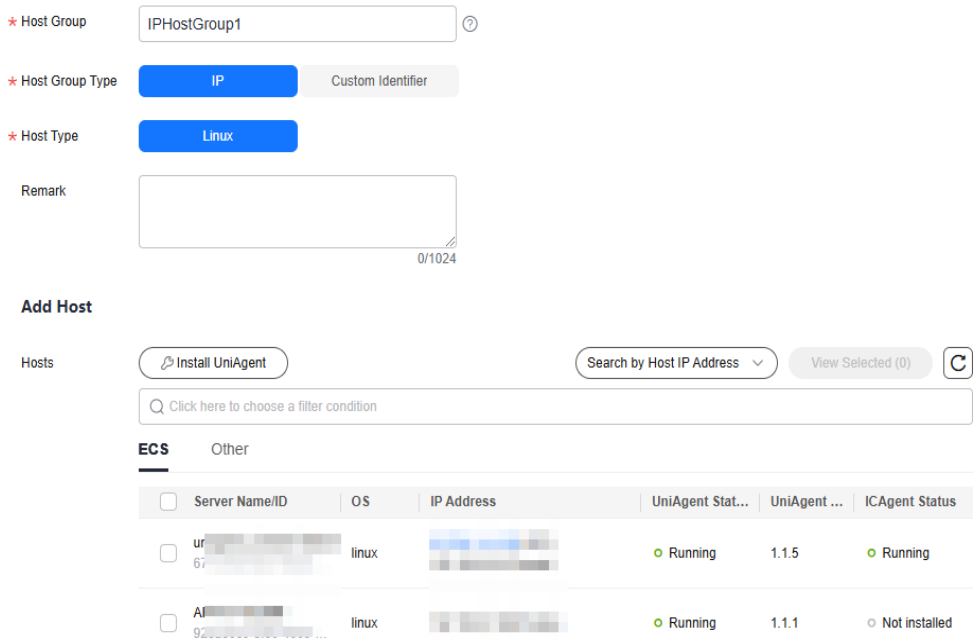
Constraints

To use the new host group management function, switch to the new access center. To go to the **old host group management** page, choose **Access** > **Access Center** in the navigation pane on the left and then click **Back to Old Version** in the upper right corner.

Creating a Host Group (IP Address)

1. Log in to the **AOM 2.0** console.
2. In the navigation pane, choose **Settings** > **Collection Settings** > **Host Groups** and click **Create Host Group** in the upper right corner.
3. In the displayed slide-out panel, enter a host group name, select **IP** for **Host Group Type**, and select a host OS (**Linux**).

   Figure 2-10 Creating an IP address host group



4. In the host list, select one or more hosts to add to the group and click **OK**.
   - You can filter hosts by host name/ID or IP address. You can also click Search by Host IP Address and enter multiple host IP addresses in the displayed search box to search.
   - If your desired hosts are not in the list, click **Install UniAgent**. On the displayed page, install UniAgents on the hosts as prompted. For details, see **2.2.2 (New) Installing UniAgents**.
   - When the selected hosts do not have UniAgent installed but have an earlier version of ICAgent installed, an upgrade prompt appears. To enable automatic UniAgent installation later, click **Upgrade** to first upgrade ICAgent to the latest version.
   - If the selected hosts do not have both UniAgent and ICAgent installed (either UniAgent or ICAgent is in the **Not installed** state), click **OK**. A dialog box will pop up, indicating the missing UniAgent or ICAgent and the number of hosts without UniAgent or ICAgent installed.
     - When selecting an ECS, click **OK** in the dialog box. The system will then issue a task for automatically installing either UniAgent or ICAgent. Otherwise, the host cannot be added to the host group.

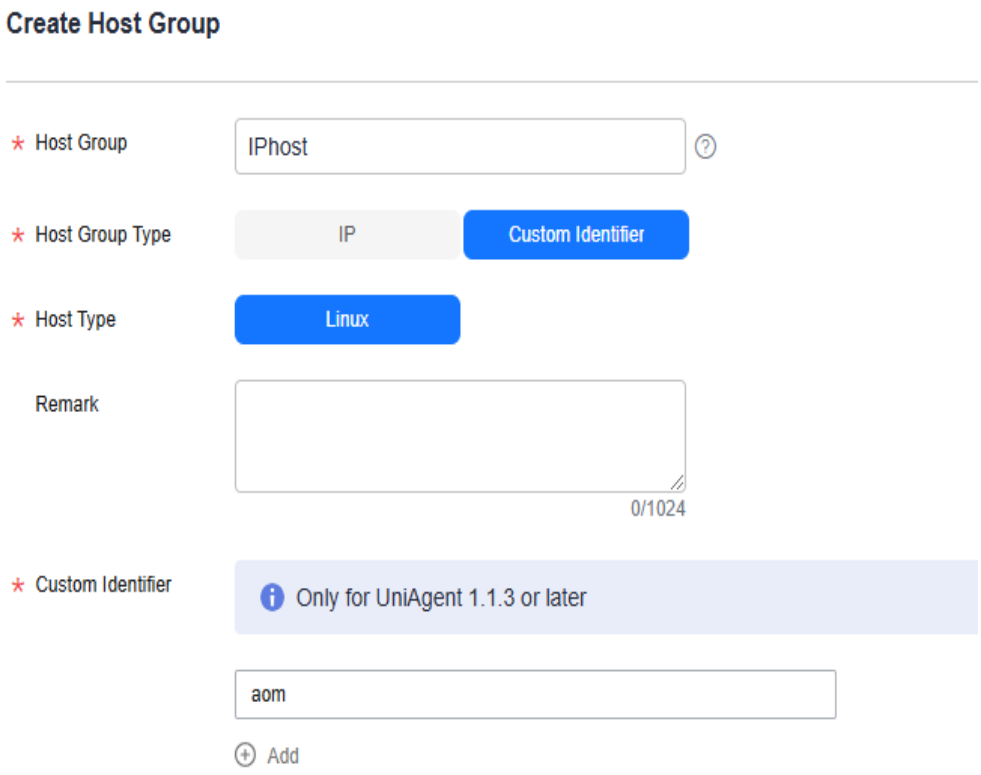
- When selecting a host of the **Other** type, manually install UniAgent and ICAgent first. Otherwise, the host cannot be added to the host group. For details, see **2.2.2 (New) Installing UniAgents**.

– Click  in the upper right corner of the host list to manually refresh the list.

Creating a Host Group (Custom Identifier)

1. Log in to the **AOM 2.0** console.
2. In the navigation pane, choose **Settings** > **Collection Settings** > **Host Groups** and click **Create Host Group** in the upper right corner.
3. In the displayed slide-out panel, enter a host group name, select **Custom Identifier** for **Host Group Type**, and select a host OS (**Linux**).

   Figure 2-11 Creating a custom identifier host group

4. Click **Add** to add a custom identifier.

   Max.: 128 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. Up to 10 custom identifiers can be added.
5. Click **OK**. After the host group is created, go to **6** to add hosts to it.
6. Log in to the host and perform the following operations as the **root** user to create the **custom_tag** file for storing host tags.

   a. Run the **cd /opt/cloud** command.

- If the **/opt/cloud** directory already exists, navigate to it and run the **mkdir lts** command to create the **lts** directory in it.
- If the **/opt/cloud** directory does not exist, run the **mkdir /opt/cloud/** command to create it, and then run the **mkdir lts** command to create the **lts** directory.

b. Run the **chmod 750 lts** command to modify the permission on the **lts** directory.

c. Run the **touch custom_tag** command in the **lts** directory to create the **custom_tag** file.

d. Run the **chmod 640 custom_tag;vi custom_tag** command to modify the **custom_tag** file permission and open the file.

e. Press **i** to enter the insert mode, enter a custom identifier, press **Esc**, enter **:wq!**, save the modification and exit.

f. Use either of the following methods to add a host to the custom identifier host group:

Table 2-15 Methods

Type	Method 1 (Recommended)	Method 2
Linux host	1. View the host identifier in the **custom_tag** file of the **/opt/cloud/lts** directory on the host. 2. On the host group configuration page, add the host identifier as the custom identifier for the host group to include the host in that group. For example, in the **custom_tag** file of the **/opt/cloud/lts** directory on the host, the identifier of the host is **test1**, and the custom identifier of the host group is set to **test1**. In this way, the host is added to the host group.	1. Configure a custom identifier before creating a host group. 2. Add the custom identifier to the **custom_tag** file in the **/opt/cloud/lts** directory of the host. The host can then be added to the specified host group. For example, if the custom identifier of the host group is set to **test** during host group creation, enter **test** in the **custom_tag** file to add the host to the host group. **If multiple custom identifiers are added, enter any custom identifier in the custom_tag file of the /opt/cloud/lts directory on the host to add the host to the host group.**

Other Operations

You can change a created host group, add hosts to or remove hosts from a host group, or associate a host group with log ingestion configurations.

Table 2-16 Operations on host groups

Operation	Procedure
Changing a host group	1. Locate the target host group and click in the **Operation** column. 2. On the displayed dialog box, modify the information such as the host group name, custom identifier, and remark. 3. Click **OK**.
Adding hosts to a host group	1. Click next to the target IP address host group. 2. Click **Add Host**. 3. In the displayed slide-out panel, all hosts that are not in the host group and run the selected OS type are displayed. Select the hosts to be added to the host group. • You can filter hosts by host name/ID or IP address. You can also click Search by Host IP Address and enter multiple host IP addresses in the displayed search box to search. • If your desired hosts are not in the list, click **Install UniAgent**. On the displayed page, install UniAgents on the hosts as prompted. For details, see **2.2.2 (New) Installing UniAgents**. 4. Click **OK**. **This operation is not supported for hosts in a custom identifier host group. To add hosts to a custom identifier host group, refer to 6.**
Removing a host from a host group	1. Click next to the target IP address host group. 2. Locate the target host and click **Remove** in the **Operation** column. 3. In the displayed dialog box, click **OK**. **This operation is not supported for hosts in a custom identifier host group.**
Removing hosts in batches	1. Locate the target host group and click next to it. 2. Select the target hosts and click **Remove** above the list. 3. Click **OK**. **This operation is not supported for hosts in a custom identifier host group.**
Viewing log ingestion rules	1. Locate the target host group and click next to it. 2. Click the **Associated Ingestion Configurations** tab to view the log ingestion rules configured for the host group. For how to configure log ingestion rules for the host group, see **3.9 Managing Metric and Log Ingestion**.

Operation	Procedure
Viewing metric access rules	1. Locate the target host group and click next to it. 2. Click the **Metric Access Rules** tab to view the metric access rules configured for the host group. For how to configure metric ingestion rules for the host group, see **3.9 Managing Metric and Log Ingestion**.
Associating a host group with an ingestion configuration	1. Locate the target host group and click next to it. 2. Click the **Associated Ingestion Configurations** tab and then click **Associate**. 3. In the displayed slide-out panel, select the target ingestion configuration. 4. Click **OK**. The associated ingestion configuration is displayed in the list.
Disassociating a host group from an ingestion configuration	1. Click the **Associated Ingestion Configurations** tab, locate the target ingestion configuration, and then click **Disassociate** in the **Operation** column. 2. Click **OK**.
Disassociating a host group from multiple ingestion configurations	1. Click the **Associated Ingestion Configurations** tab, select target ingestion configurations, and then click **Disassociate** above the list. 2. Click **OK**.
Copying host group information	Hover your cursor over a host group name to copy a host group ID.
Deleting a host group	1. Locate the target host group and click in the **Operation** column. 2. In the displayed dialog box, click **OK**.
Deleting host groups in batches	1. Select multiple host groups to be deleted and click **Delete** above the list. 2. In the displayed dialog box, click **OK**.

Operation	Procedure
Managing tags	Tag log groups as required. 1. Locate the target host group and click in the **Operation** column. 2. On the displayed page, enter a tag key and value. Precautions: • To add more tags, repeat the preceding step. • To delete a tag, locate the target host group and click  in the **Operation** column. On the displayed page, locate the target tag and click  in the **Operation** column. • A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters. • A tag key must be unique.

2.2.8 Configuring a Proxy Area and Proxy

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 is used to manage proxies by category. It consists of multiple proxies.

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 tree on the left, choose **Collection Settings** > **Proxy Areas**. The **Proxy Areas** page is displayed.

Step 4 Click **Add Proxy Area** and set proxy area parameters.

Table 2-17 Proxy area parameters

Parameter	Description	Example
Proxy Area Name	Name of a proxy area. Max.: 64	test
Network Type	Options: **Inner** and **Public**. The default value is **Inner**.	Inner

Step 5 Click **OK** to add a proxy area.

Step 6 Locate the new proxy area, click **Add Proxy**, and set proxy parameters.

Table 2-18 Proxy parameters

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 7 Click **OK**. The proxy is added.

After configuring the proxy area and proxy, perform the following operations if needed:

Table 2-19 Managing the proxy area and proxy

Operation	Description
Searching for a proxy area	Click  next to **Add Proxy Area**. Then, in the search box, enter a keyword to search for your target proxy area.
Modifying a proxy area	Hover the pointer over a proxy area and choose > **Edit**. In the dialog box that is displayed, enter a new name, select a network type, and click **OK**.
Deleting a proxy area	Hover the pointer over a proxy area and choose > **Delete**. In the dialog box that is displayed, click **Yes** to delete the proxy area.
Checking a proxy	Click a proxy area to check the proxy in it.
Modifying a proxy IP address	Click **Modify Proxy IP** in the **Operation** column of the proxy. On the page that is displayed, modify the proxy IP address.
Deleting a proxy	Click **Delete** in the **Operation** column of the proxy. In the displayed dialog box, click **OK** to delete the proxy.

----End

2.2.9 Checking Operation Logs

AOM records operation logs of tasks such as installation, upgrade, and uninstall related to UniAgent and other plug-ins. You can check the operation logs of related tasks.

Checking Operation Logs of UniAgent

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation tree on the left, choose **Collection Settings** > **Operation Logs**. On the displayed page, click the **UniAgent Logs** tab.

Step 4 Set criteria to search for historical tasks.

- Filter data by executor name.
- Filter historical tasks by date. Options: **Last hour**, **Last 6 hours**, **Last day**, **Last 3 days**, and **Custom**. You can query historical tasks of half a year at most.

Step 5 Click a task ID. On the task details page that is displayed, click **View Log** to view UniAgent operation logs.

----End

Viewing Operation Logs of Plug-ins

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation tree on the left, choose **Collection Settings** > **Operation Logs**. On the displayed page, click the **Plug-in Logs** tab.

Step 4 Set criteria to search for historical tasks.

- Filter data by executor name.
- Filter historical tasks by date. Options: **Last hour**, **Last 6 hours**, **Last day**, **Last 3 days**, and **Custom**. You can query historical tasks of half a year at most.

Step 5 Click a task ID. On the task details page that is displayed, click **View Log** in the **Operation** column to view plug-in operation logs.

----End

Other Operations

On the **Operation Logs** page, perform the operations listed in the following table if needed.

Table 2-20 Related operations

Operation	Description
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.

2.3 Connecting Businesses to AOM

AOM provides a unified entry for observability analysis of Huawei Cloud services. Through the access center, you can monitor ELB log metrics/APM transaction metrics such as the number of users and the number of orders.

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, choose **Access** > **Access Center**. (To switch from the new access center to the old one, click **Back to Old Version** in the upper right corner.)

Step 3 In the **Business** panel on the right, click the target card and perform the operations listed in the following table if needed.

Table 2-21 Connecting businesses to AOM

Card	Related Operation
ELB Logs	On the **Log Metric Rules** page, ingest ELB log metrics by referring to **Ingesting ELB Log Metrics to AOM**.
APM Transactions	On the **Connect Application** page, ingest APM transaction metrics by referring to **Connecting Agents**.

----End

Ingesting ELB Log Metrics to AOM

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.

- **Constraints:**
  - To use business monitoring, enable this function in **Menu Settings**. For details, see **14.4 Configuring AOM Menus**.
  - 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**.
- **Procedure**

  a. Log in to the **AOM 2.0** console.

  b. In the navigation pane on the left, choose either of the two following entries:

  - Entry 1: Choose **Access Center**. In the **Business** panel, click the **ELB Logs** card.
  - Entry 2: Choose **Business Monitoring (Beta)** > **Business Metrics**. Then click **Back to Old Version** in the upper right corner of the page.

  c. Click  next to **Log Metric Rules**.

  d. Set parameters to ingest ELB logs reported to LTS to AOM. For details, see **Table 2-22**.

Figure 2-12 Ingesting logs

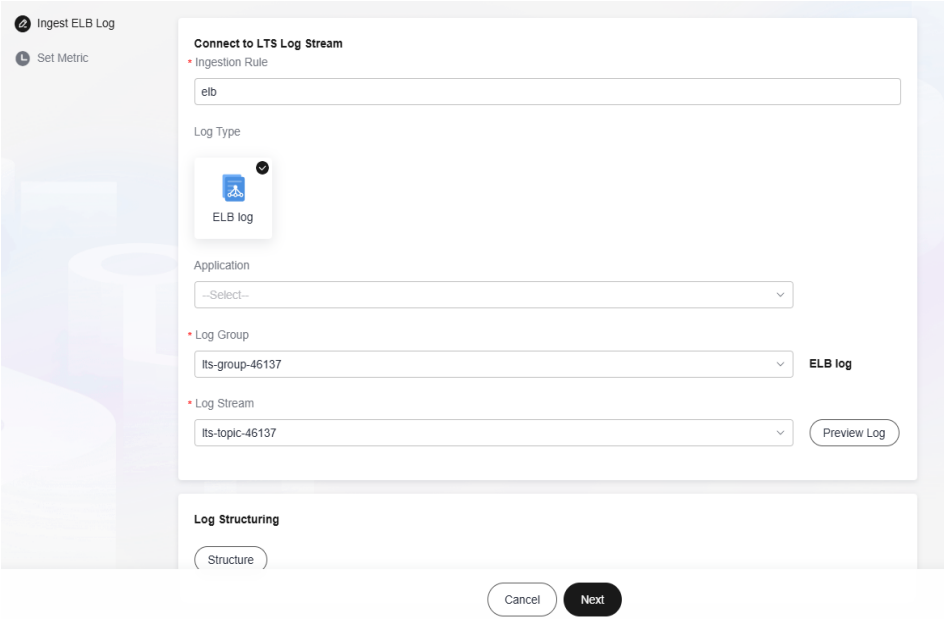


Table 2-22 Log ingestion parameters

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.

Parameter	Description
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.

e. Click **Next**.

f. Set metric information.

   i. Click **Add Metric** to add a metric for the log metric rule. For details, see **Table 2-23**.

Figure 2-13 Adding a metric

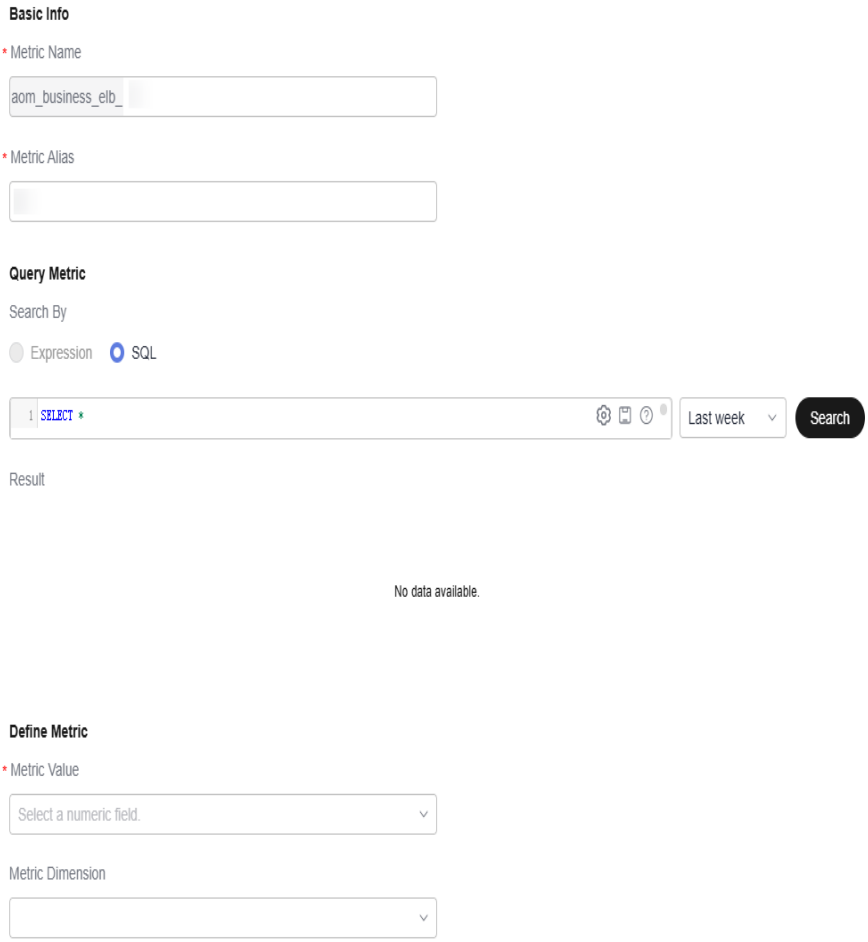


Table 2-23 Metric configuration parameters

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**.

Category	Parameter	Description
Define Metric	Metric Value	Select a value from the drop-down list. Only numeric fields can be selected.
	Metric Dimension	Select a value from the drop-down list.

ii. Click **OK**.

iii. (Optional) Click **Add Metric** to add more metrics for the rule.

g. After the configuration is complete, click **OK**.

After creating an ELB log metric rule, you can also perform the operations listed in **Table 2-24** on the **Business Monitoring (Beta)** > **Business Metrics** page (click **Back to Old Version** in the upper right corner of the page).

Table 2-24 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 **Ingesting ELB Log Metrics to AOM**.
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 **f**.
Editing a metric	1. In the log metric rule list on the left, click a rule name. 2. In the right pane, select a metric access card and click . For details, see **f**.

Operation	Description
Deleting a metric	1. In the log metric rule list on the left, click a rule name. 2. In the right pane, select a metric access card and click .
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 .

2.4 Connecting Applications to AOM

AOM provides a unified entry for observability analysis of Huawei Cloud services. Through the access center, you can ingest the traces of application components to APM for monitoring application or API performance metrics such as average request latency, error calls, and request throughput.

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, choose **Access** > **Access Center**. (To switch from the new access center to the old one, click **Back to Old Version** in the upper right corner.)

Step 3 In the **Application** panel on the right, click the target card and perform the operations listed in the following table if needed.

Table 2-25 Connecting applications to AOM

Card	Related Operation
Java	On the **Connect Application** page, ingest trace metrics related to Java applications. AOM supports quick connection to Agents to monitor Java applications. You can also install Agents for the Java applications deployed in CCE containers for monitoring. For details, see **Monitoring Java Applications Through Quick Connection to Agents** and **Monitoring Java Applications Deployed in CCE Containers by Installing Agents**.

----End

Monitoring Java Applications Through Quick Connection to Agents

AOM allows you to monitor Java applications through quick connection to Agents. Java supports enhanced Agents.

- **Prerequisites**

  The network between your host and APM is connected.

  You can run the **Telnet** command to check the network. For example, if you select region **CN-Hong Kong** and set **Access Mode** to **Enhanced Agent**, log in to the host where the application is deployed and run the **telnet 100.125.6.106:41333** command to check the network connectivity. For details about access addresses in other regions, see **Access Addresses**.

- **Procedure**

  a. Log in to the **AOM 2.0** console.

  b. In the navigation pane, choose **Access** > **Access Center**.

  c. In the **Application** panel, click the **Java** card. (In the new access center, click the **Java Component** card under the **Components** panel.)

  d. In the **Basic Info** area, select a region and an application.

  If no applications meet your requirements, create one. For details, see **Table 2-26**.

  Figure 2-14 Basic information

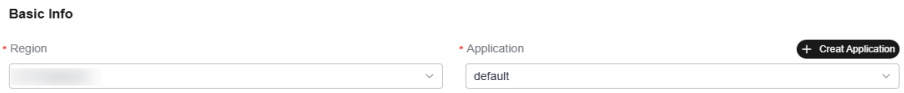
  

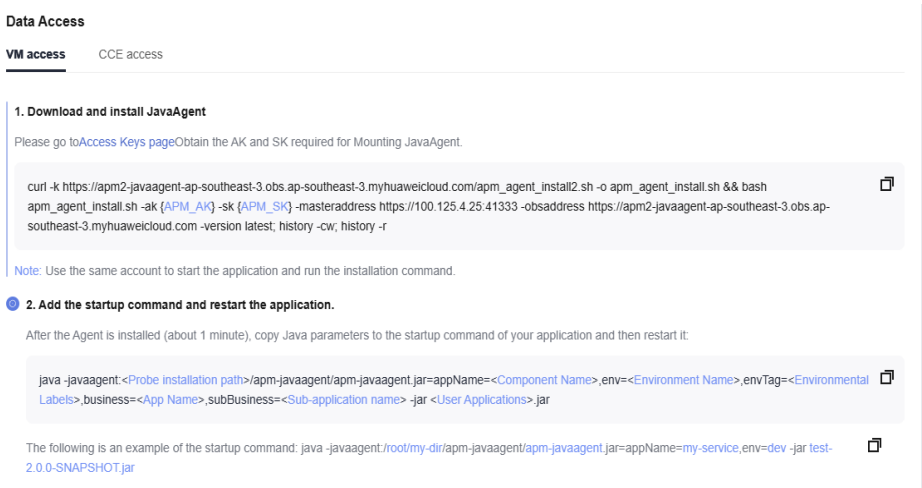
  Table 2-26 Parameters for adding an application

Parameter	Description
Application Name	Name of an application, which cannot be empty. Enter 1 to 128 characters and start with a letter. Only digits, letters, underscores (_), and hyphens (-) are allowed.
Application Alias	Application alias. The alias takes precedence over the application name to display. Enter 1 to 128 characters. Only digits, letters, underscores (_), hyphens (-), brackets, and periods (.) are allowed.
Enterprise Project	Select an enterprise project from the drop-down list. This parameter is displayed only when you use the enterprise edition.
Description	Description of the application. Enter up to 1,000 characters.

  e. (Default) Set **Access Mode** to **Enhanced Agent**.

  f. Set **Data Access** to **VM access** and ingest the data as prompted.

Figure 2-15 VM access



i. Use a remote login tool, such as PuTTY, to log in to the Linux host where the Agent is to be installed and run the copied command as the **root** user to download and install JavaAgent.

```
curl -k https://javaagent.***/apm_agent_install2.sh -o apm_agent_install.sh && bash apm_agent_install.sh -ak * -sk * -masteraddress https://**** -obsaddress https://javaagent.***.com -version latest; history -cw; history -r
```

   - **APM_AK/APM_SK**: AK and SK for installing JavaAgent. For details about how to obtain an AK and SK, see **Access Keys**. Directly copy the command for installing JavaAgent. Delete **{}** when entering **APM_AK** and **APM_SK**.
   - **master.address**: the access address of an APM Agent. For more information, see **Access Addresses**.
   - Supports dynamic configuration of AK/SK in the JavaAgent installation command and **master.address**: Assign values to environment variables **APM_MASTER_ADDRESS**, **APM_ACCESS_KEY** (**apm-ak**), and **APM_SECRET_KEY** (**apm-sk**).

ii. After installing the JavaAgent, add JVM parameters to the startup script of your application and then restart it.

Table 2-27 JVM parameters

Parameter	Description	Mandatory
Agent Installation Path	Path for installing the Agent.	Yes

Parameter	Description	Mandatory
appName	Component name, which must start with a character. Each component name must be unique under an application. A component can contain multiple environments. If there are duplicate names, use **instanceName** to distinguish them.	Yes
env	Name of an environment, where an application is deployed. A program can be deployed in different environments (such as the test or live network environment). Each environment is deployed in one region and has a unique region attribute. If this parameter is blank, the default environment will be used.	No
envTag	Environment tag for filtering environments. Different environments may share the same tag. This parameter can be left blank.	No
business	Name of an application (a global concept). Create an application before specifying this parameter. If this parameter is left blank, the default application (which is automatically created when you enable APM) will be used.	No
subBusiness	Name of a sub-application (a global concept). It is a folder under the application. This parameter can be left blank. If it is left blank, resources will be mounted to the root application. Up to three layers of sub-applications are supported. For example, for **a/b/c**, each represents one layer.	No
UserApplication	Name of a user application.	Yes

Monitoring Java Applications Deployed in CCE Containers by Installing Agents

AOM allows you to install APM Agents for Java applications deployed in CCE containers for monitoring. It enables precise problem analysis and locating, accelerate troubleshooting.

- **Prerequisites**
  - The network between your host and APM is connected.

    You can run the **Telnet** command to check the network. For example, if you select region **CN-Hong Kong** and set **Access Mode** to **Enhanced Agent**, log in to the host where the application is deployed and run the

telnet 100.125.6.106:41333 command to check the network connectivity. For details about access addresses in other regions, see **Access Addresses**.

- The endpoint of the target region has been obtained. For details, see **Regions and Endpoints**.
- The AK/SK required for installing JavaAgent has been obtained. To do so, go to the **AOM 2.0 console** and choose **APM Settings** > **Access Keys** in the navigation pane.

- **Instructions**

  You can configure performance management for Java workloads when and after the workloads are created. Agents can only be installed for Java applications deployed in CCE containers. For details, see **Configuring APM**. You are advised to install self-developed probes for applications deployed in CCE containers.

  Table 2-28 describes the parameters.

  Table 2-28 Parameters for configuring APM

Parameter	Description
Probe	Select a target probe. Options: **Disable**/**APM 2.0**.
Probe Version	Version of the probe. You are advised to select a probe version based on the CPU architecture of the node where the workload is located.
Probe Upgrade Policy	Policy for the probe upgrade. The default value is **Auto upgrade upon restart**. • **Auto upgrade upon restart**: The system downloads the probe image each time the pod is restarted. • **Manual upgrade upon restart**: If a local image is available, it will be used. If no local image is available, the system downloads the probe image.
APM Environment	Enter an APM environment name. This parameter is optional.
APM App	Select an existing APM application.
Sub-app	Enter an APM sub-application. This parameter is optional.
Access Key	The key of APM is automatically obtained. For details, see **Prerequisites**.

2.5 Connecting Middleware and Custom Plug-ins to AOM

2.5.1 Overview About Middleware and Custom Plug-in Connection to AOM

AOM provides a unified entry for observability analysis of Huawei Cloud services. Through the access center, you can quickly install Prometheus official middleware Exporters and custom plug-ins. By creating collection tasks and executing scripts, AOM can monitor middleware and custom plug-in metrics. It works with open-source Grafana for comprehensive monitoring. It helps you quickly detect and locate issues, minimizing the impact of faults on services.

To quickly connect middleware and custom plug-ins to AOM, perform the following steps:

1. Install UniAgent on your VM for installing Exporters and creating collection tasks. For details, see **2.2.1 Installing UniAgents**.
2. Create a Prometheus instance for ECS and associate it with a collection task to mark and categorize collected data. For details, see **9.2 Managing Prometheus Instances**.
3. Connect middleware and custom plug-ins to AOM. For details, see **2.5.2 Connecting Middleware to AOM** and **2.5.3 Connecting Custom Plug-ins to AOM**.
4. After middleware and custom plug-ins are connected to AOM, metrics can then be reported to AOM. You can go to the **Metric Browsing** page to query metrics.

Connecting Middleware and Custom Plug-insto AOM

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, choose **Access** > **Access Center**. (To switch from the new access center to the old one, click **Back to Old Version** in the upper right corner.)

Step 3 Click a target card under **Prometheus Middleware** or **Custom Prometheus Plug-in Access** on the right, and perform the operations listed in following table if needed.

- Middleware: You can create collection tasks and install the middleware Exporters provided by AOM to monitor middleware metrics. For details about the middleware metrics that can be monitored by AOM, see **open-source Exporters**.

Table 2-29 Connecting middleware to AOM

Card	Related Operation
MySQL	Click the **MySQL** card. On the displayed page, connect MySQL Exporter. For details, see **2.5.2.1 Ingesting MySQL Metrics to AOM**.
Redis	Click the **Redis** card. On the displayed page, connect Redis Exporter. For details, see **2.5.2.2 Ingesting Redis Metrics to AOM**.

Card	Related Operation
Kafka	Click the **Kafka** card. On the displayed page, connect Kafka Exporter. For details, see **2.5.2.3 Ingesting Kafka Metrics to AOM**.
Nginx	Click the **Nginx** card. On the displayed page, connect Nginx Exporter. For details, see **2.5.2.4 Ingesting Nginx Metrics to AOM**.
MongoDB	Click the **MongoDB** card. On the displayed page, connect MongoDB Exporter. For details, see **2.5.2.5 Ingesting MongoDB Metrics to AOM**.
Consul	Click the **Consul** card. On the displayed page, connect Consul Exporter. For details, see **2.5.2.6 Ingesting Consul Metrics to AOM**.
HAProxy	Click the **HAProxy** card. On the displayed page, connect HAProxy Exporter. For details, see **2.5.2.7 Ingesting HAProxy Metrics to AOM**.
PostgreSQL	Click the **PostgreSQL** card. On the displayed page, connect PostgreSQL Exporter. For details, see **2.5.2.8 Ingesting PostgreSQL Metrics to AOM**.
Elasticsearch	Click the **Elasticsearch** card. On the displayed page, connect Elasticsearch Exporter. For details, see **2.5.2.9 Ingesting Elasticsearch Metrics to AOM**.
RabbitMQ	Click the **RabbitMQ** card. On the displayed page, connect RabbitMQ Exporter. For details, see **2.5.2.10 Ingesting RabbitMQ Metrics to AOM**.
Other components	Click the **Other components** card. On the displayed page, connect Custom Exporter. For details, see **2.5.2.11 Ingesting Other Middleware Metrics to AOM**.

- Custom plug-in: You can create a custom plug-in based on your requirements and use it to create collection tasks for metric monitoring. For details, see **2.5.3 Connecting Custom Plug-ins to AOM**.

----End

2.5.2 Connecting Middleware to AOM

2.5.2.1 Ingesting MySQL Metrics to AOM

Create a collection task and install MySQL Exporter to monitor MySQL metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **MySQL** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **MySQL** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **MySQL** card.

Step 3 On the displayed page, set parameters by referring to the following table.

Figure 2-16 Configuring a collection task

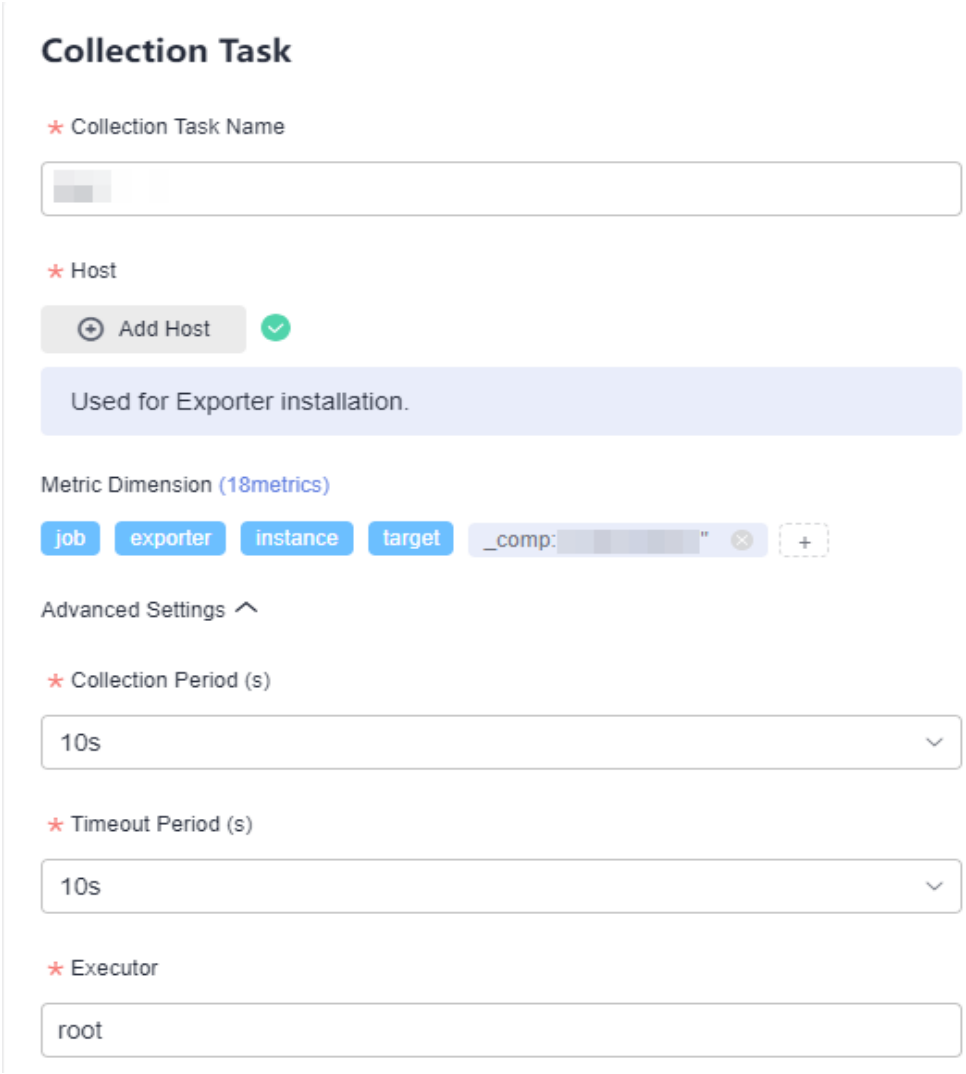


Table 2-30 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, **create one**.
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is **MYSQL**.

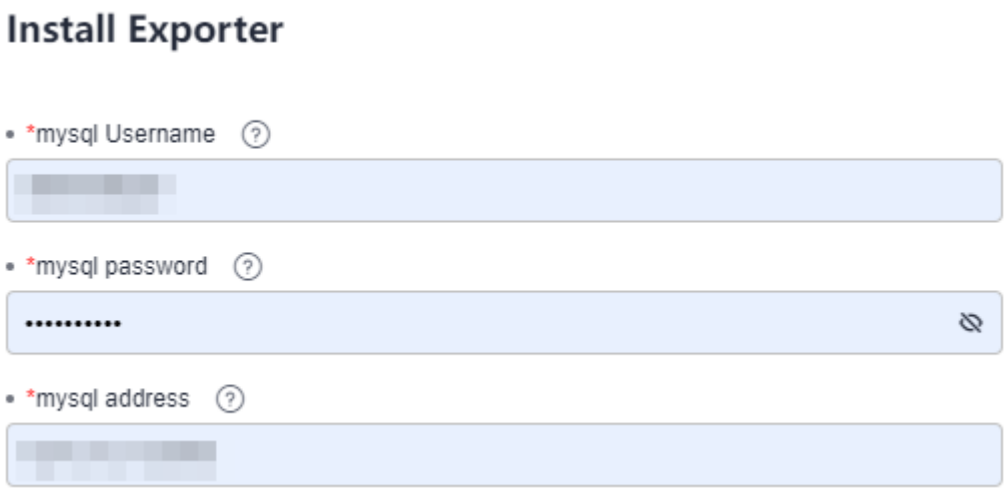
Operation	Parameter	Description
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

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

Figure 2-17 Installing Exporter



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

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

----End

2.5.2.2 Ingesting Redis Metrics to AOM

Create a collection task and install Redis Exporter to monitor Redis metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **Redis** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **Redis** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Redis** card.

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

Figure 2-18 Configuring a collection task

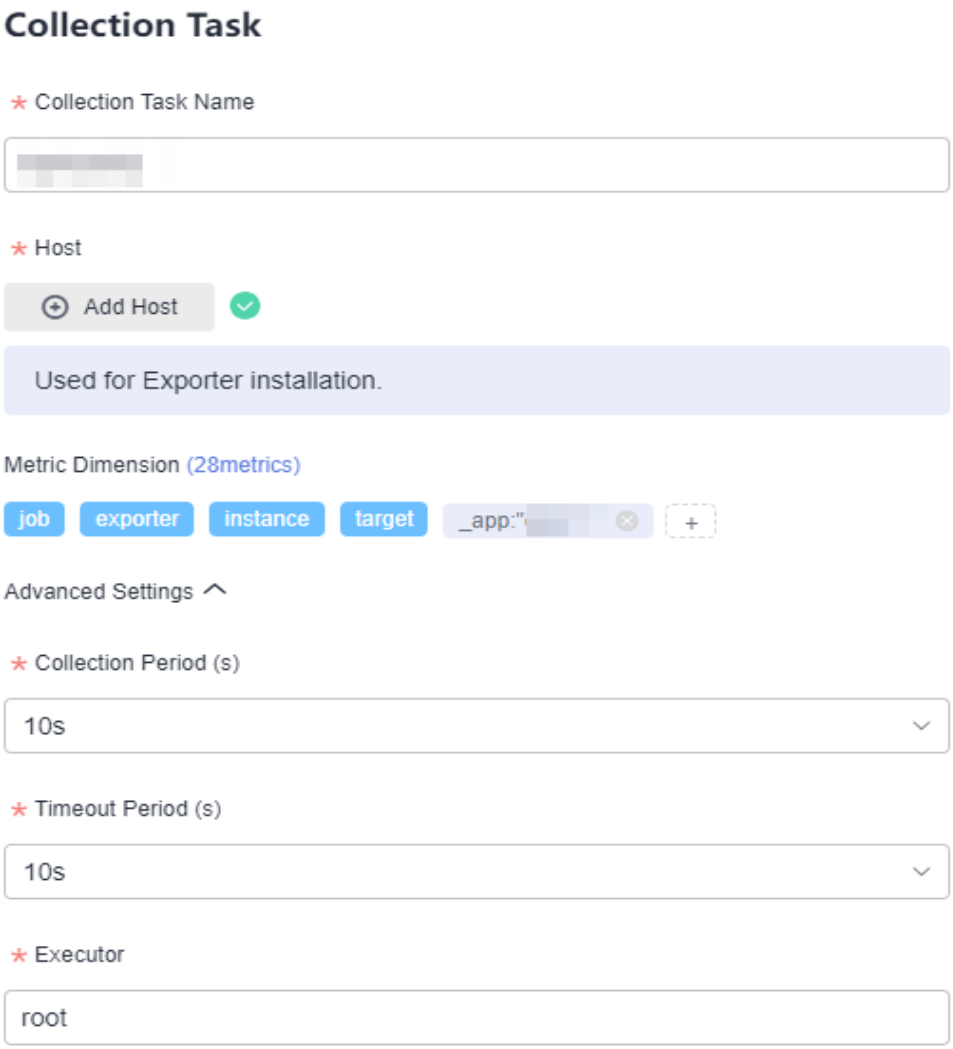


Table 2-31 Parameters for configuring a collection task

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. Only Linux is supported.
	Collection Plug-in	The default value is **REDIS**.

Operation	Parameter	Description
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

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

Figure 2-19 Installing Exporter

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

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

----End

2.5.2.3 Ingesting Kafka Metrics to AOM

Create a collection task and install Kafka Exporter to monitor Kafka metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **Kafka** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **Kafka** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Kafka** card.

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

Figure 2-20 Configuring a collection task

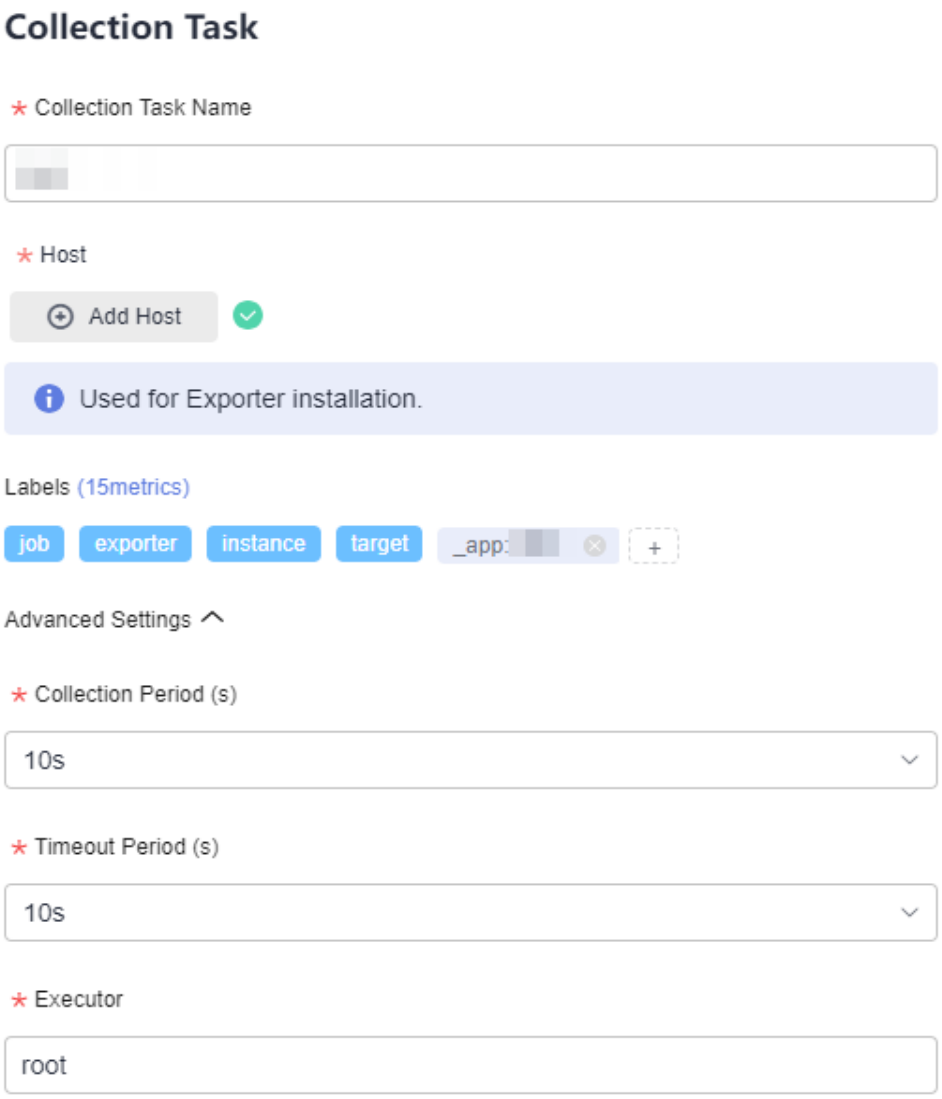


Table 2-32 Parameters for configuring a collection task

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. Only Linux is supported.
	Collection Plug-in	The default value is **KAFKA**.

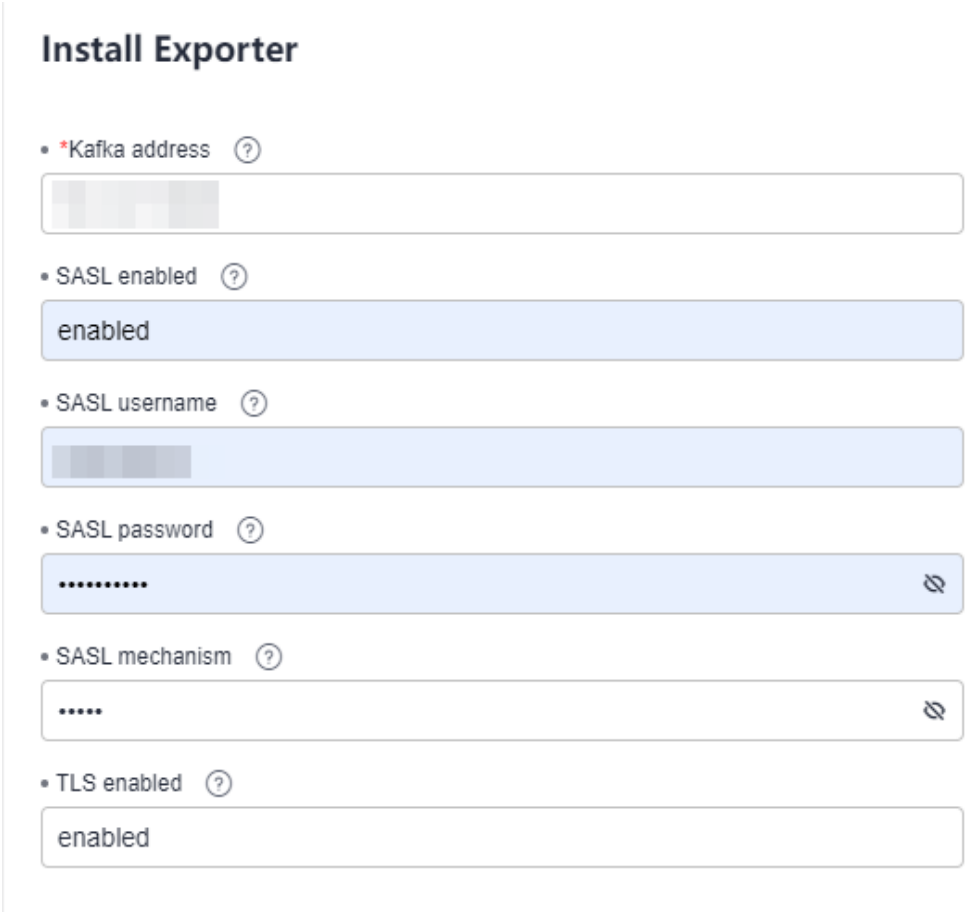
Operation	Parameter	Description
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

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

Figure 2-21 Installing Exporter



Parameter	Description
Kafka address	IP address and port number of Kafka, for example, **10.0.0.1:3306**.
SASL enabled	Whether to enable Simple Authentication and Security Layer (SASL). • **enabled**: Enable SASL. If ciphertext access has been enabled for Kafka instances, enable SASL. • **disabled**: Disable SASL. If plaintext access has been enabled for Kafka instances, disable SASL. The default value is **disabled**.
SASL username	SASL username.
SASL password	SASL password.
SASL mechanism	Enter an SASL mechanism. Options: **plain**, **scram-sha512**, and **scram-sha256**. By default, this parameter is left blank.
TLS enabled	Whether to enable Transport Layer Security (TLS) verification. • **enabled**: Enable TLS. If ciphertext access has been enabled for Kafka instances, enable TLS. • **disabled**: Disable TLS. If plaintext access has been enabled for Kafka instances, disable TLS. The default value is **TLS**.

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

----End

2.5.2.4 Ingesting Nginx Metrics to AOM

Create a collection task and install Nginx Exporter to monitor Nginx metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **Nginx** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **Nginx** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Nginx** card.

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

Figure 2-22 Configuring a collection task

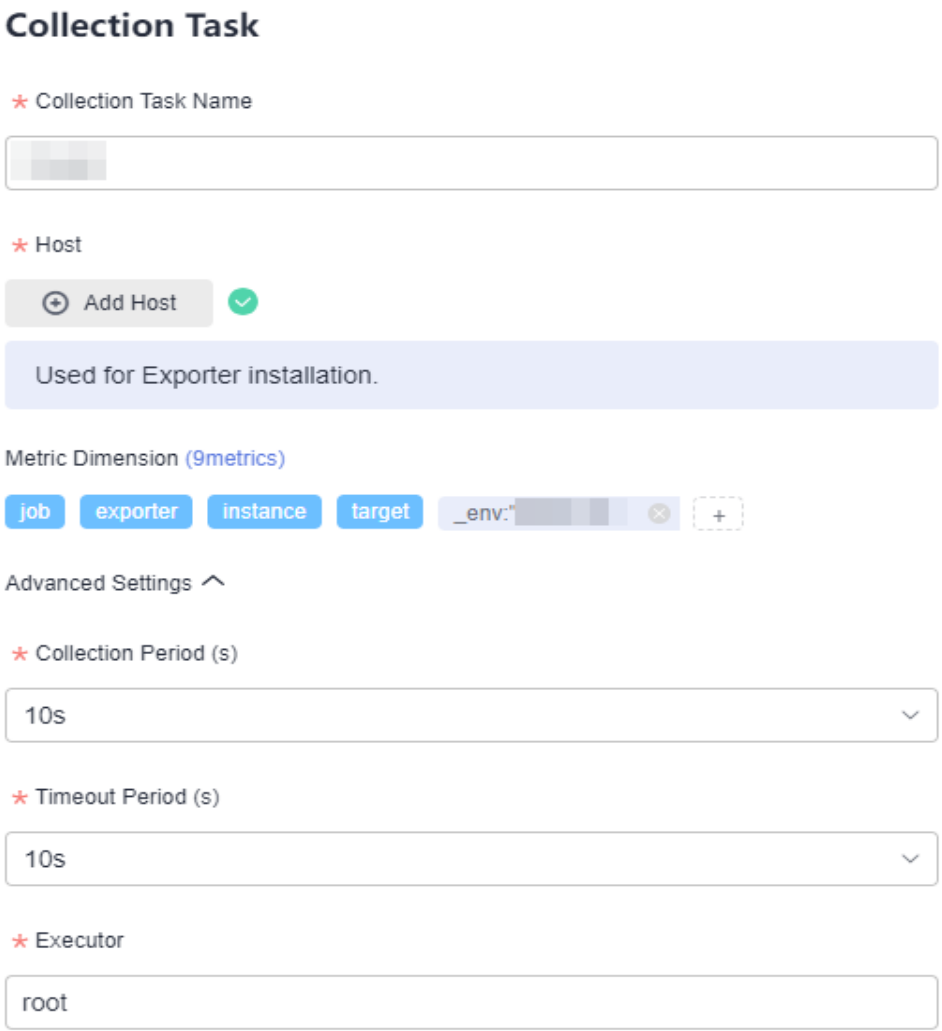


Table 2-33 Parameters for configuring a collection task

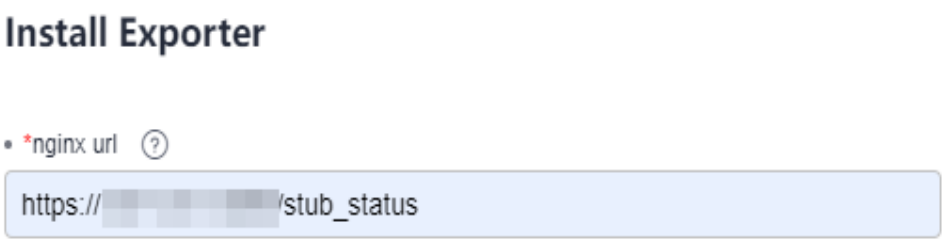
Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, **create one**.
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is **NGINX**.
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. • Search for and select a host by the host name, IP address, or Agent status. • You can click in the upper right corner to deselect the selected host. • Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.

Operation	Parameter	Description
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	● Configure the following parameters: – **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). – **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

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

Figure 2-23 Installing Exporter



Parameter	Description
Nginx URL	Nginx URL, which is in the format of "Connection address of Nginx+Nginx service status path". • Connection address of Nginx: IP address and listening port number of the Nginx service. The listening port is specified in the **nginx.conf** file. Example: **10.0.0.1:8080** • Nginx service status path: specified by the **location** parameter in the **nginx.conf** file, for example, **/stub_status**. Example: **https://10.0.0.1:8080/stub_status**

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

----End

2.5.2.5 Ingesting MongoDB Metrics to AOM

Create a collection task and install MongoDB Exporter to monitor MongoDB metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **MongoDB** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **MongoDB** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **MongoDB** card.

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

Figure 2-24 Configuring a collection task

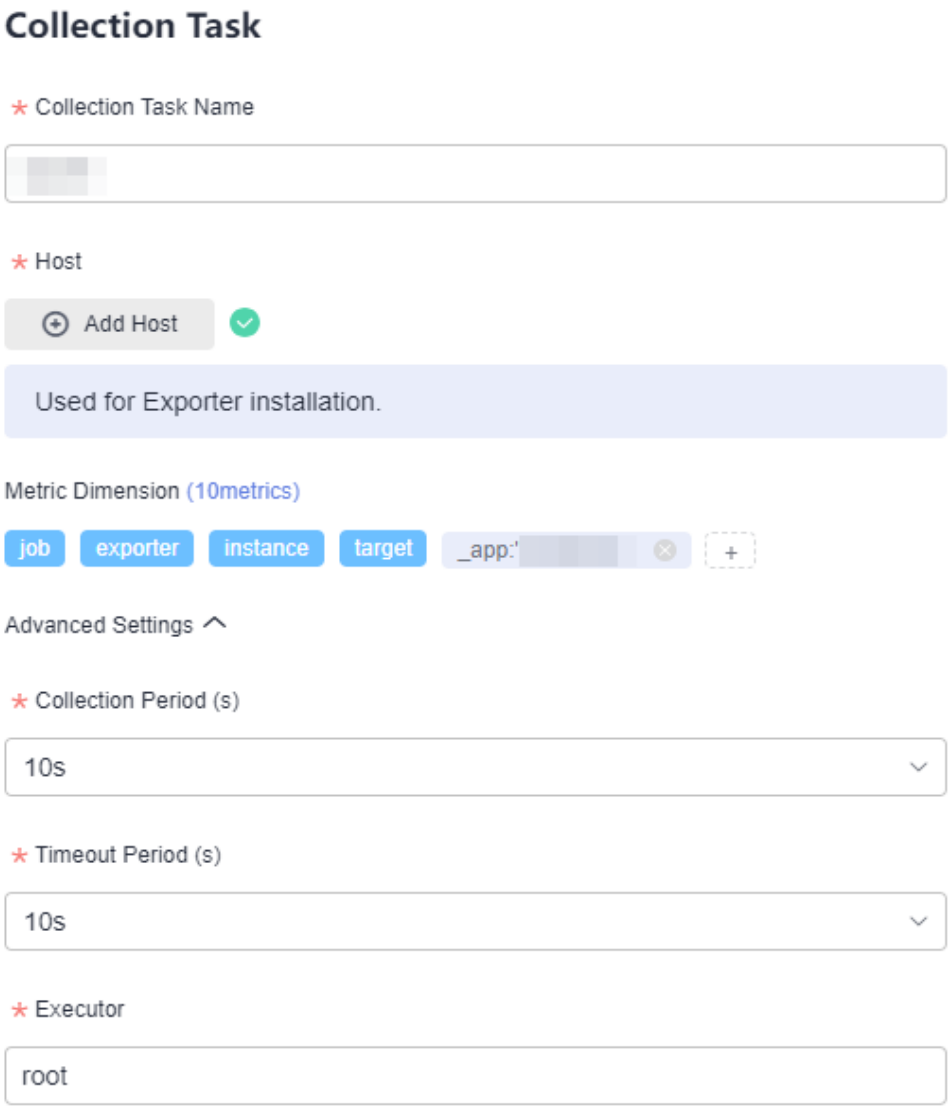


Table 2-34 Parameters for creating a collection task

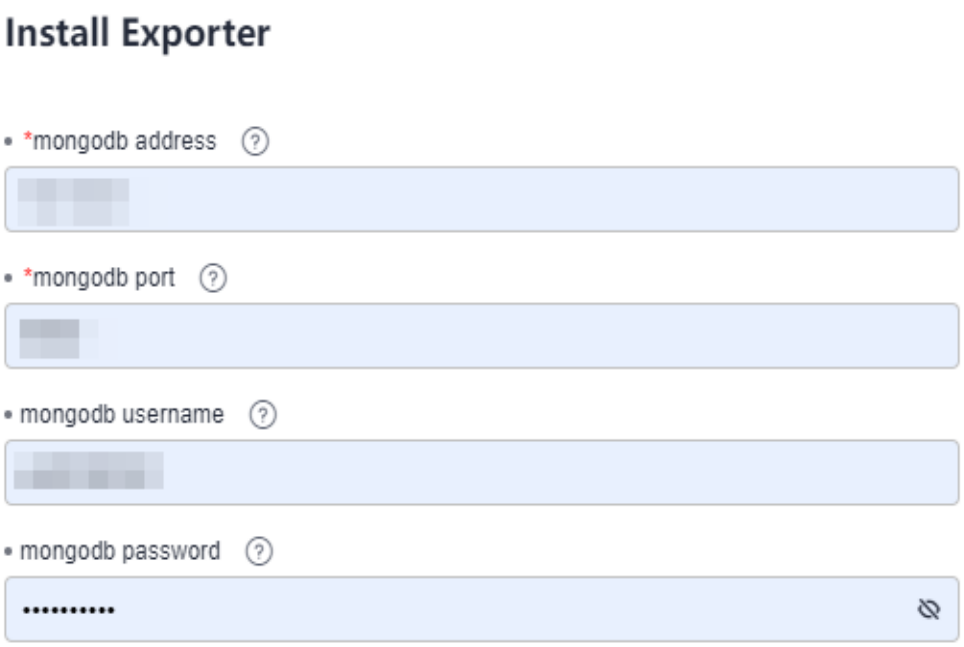
Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, **create one**.
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is **MONGODB**.
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. • Search for and select a host by the host name, IP address, or Agent status. • You can click in the upper right corner to deselect the selected host. • Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.

Operation	Parameter	Description
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: ● **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). ● **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

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

Figure 2-25 Installing Exporter



Parameter	Description
MongoDB address	IP address of MongoDB, for example, **10.0.0.1**.
MongoDB port	Port number of MongoDB, for example, **3306**.
MongoDB username	Username for logging in to MongoDB.
MongoDB password	Password for logging in to MongoDB.

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

----End

2.5.2.6 Ingesting Consul Metrics to AOM

Create a collection task and install Consul Exporter to monitor Consul metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **Consul** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **Consul** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Consul** card.

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

Figure 2-26 Configuring a collection task

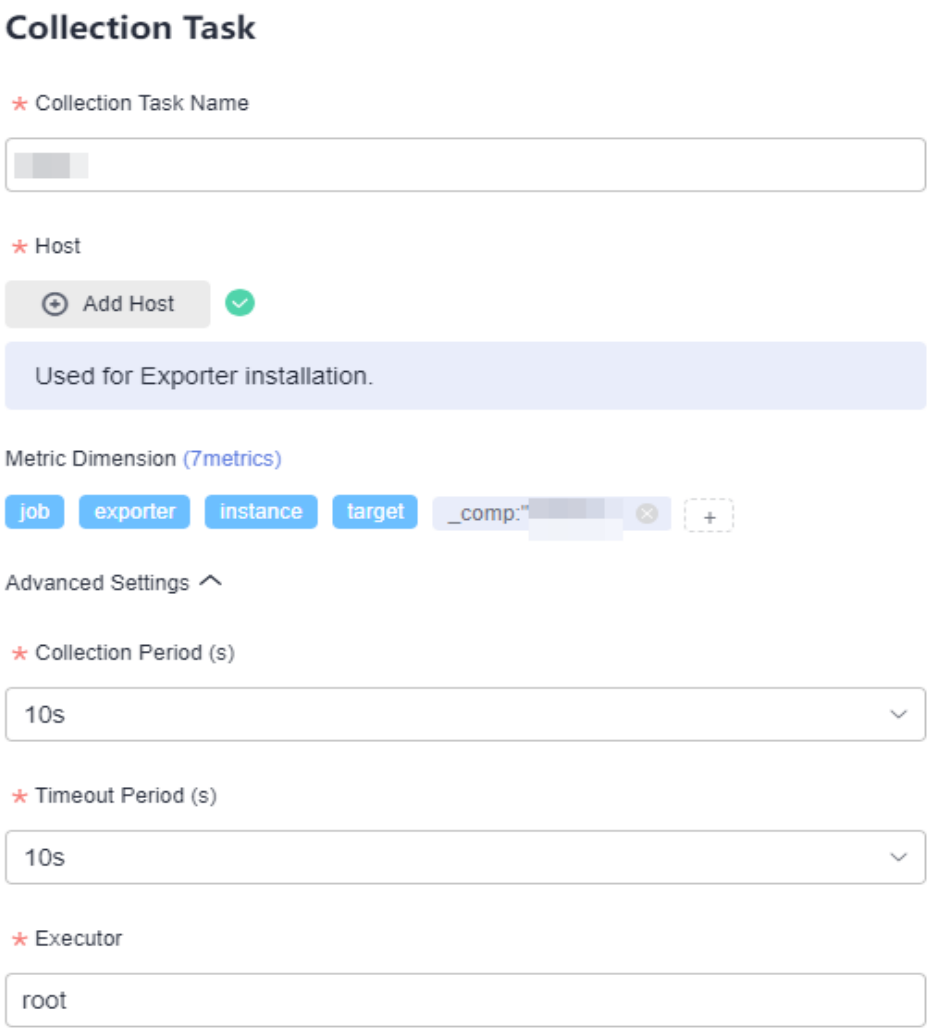


Table 2-35 Parameters for configuring a collection task

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. Only Linux is supported.
	Collection Plug-in	The default value is **CONSUL**.
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. • Search for and select a host by the host name, IP address, or Agent status. • You can click in the upper right corner to deselect the selected host. • Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.

Operation	Parameter	Description
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: ● **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). ● **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

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

Figure 2-27 Installing Exporter

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

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

----End

2.5.2.7 Ingesting HAProxy Metrics to AOM

Create a collection task and install HAProxy Exporter to monitor HAProxy metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **HAProxy** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **HAProxy** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **HAProxy** card.

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

Figure 2-28 Configuring a collection task

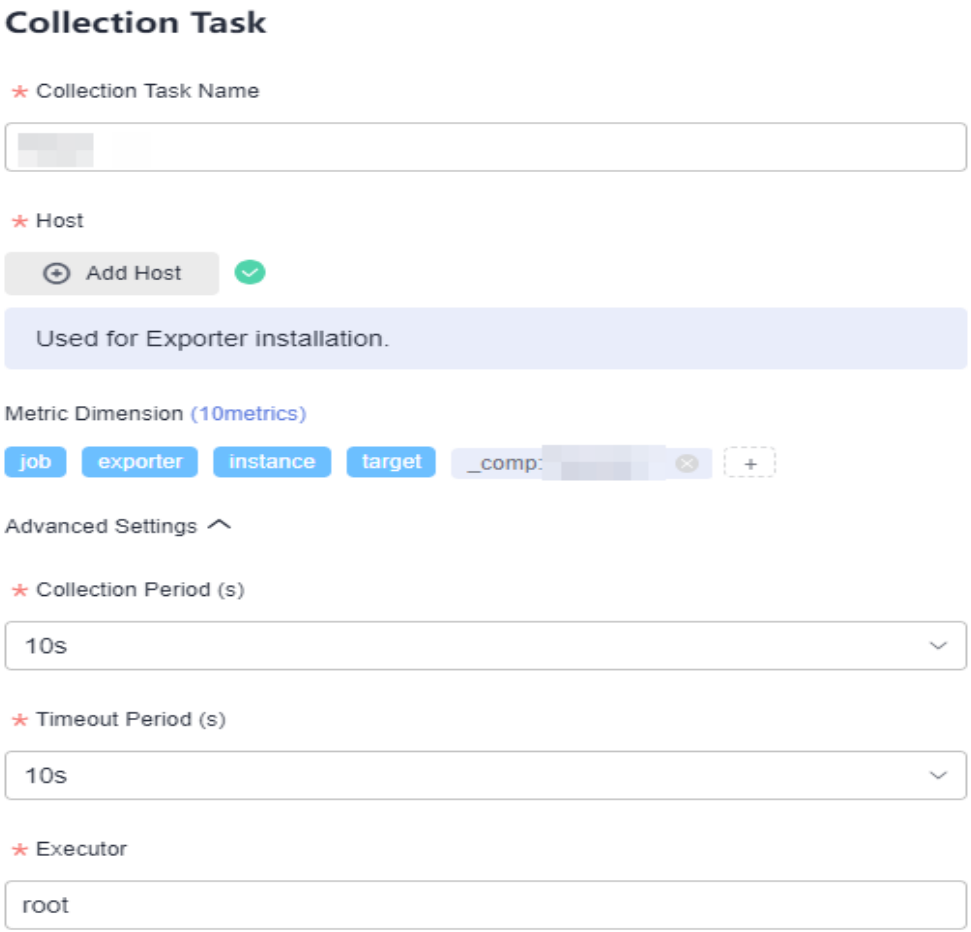


Table 2-36 Parameters for configuring a collection task

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. Only Linux is supported.
	Collection Plug-in	The default value is **HAPROXY**.

Operation	Parameter	Description
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

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

Figure 2-29 Installing Exporter

Parameter	Description
HAProxy URL	HAProxy connection address, which must be in the format of "http://*{username}*:*{password}*@*{IP address}*:*{port}*/haproxy_stats;csv". • *{username}*: username for logging in to HAProxy. • *{password}*: password for logging in to HAProxy. • *{IP}*:*{port}*: HAProxy IP address and port number, for example, **10.0.0.1:3306**. Example: **http://admin:**************@10.0.0.1:3306/haproxy_stats;csv**

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

----End

2.5.2.8 Ingesting PostgreSQL Metrics to AOM

Create a collection task and install PostgreSQL Exporter to monitor PostgreSQL metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **PostgreSQL** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **PostgreSQL** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **PostgreSQL** card.

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

Figure 2-30 Configuring a collection task

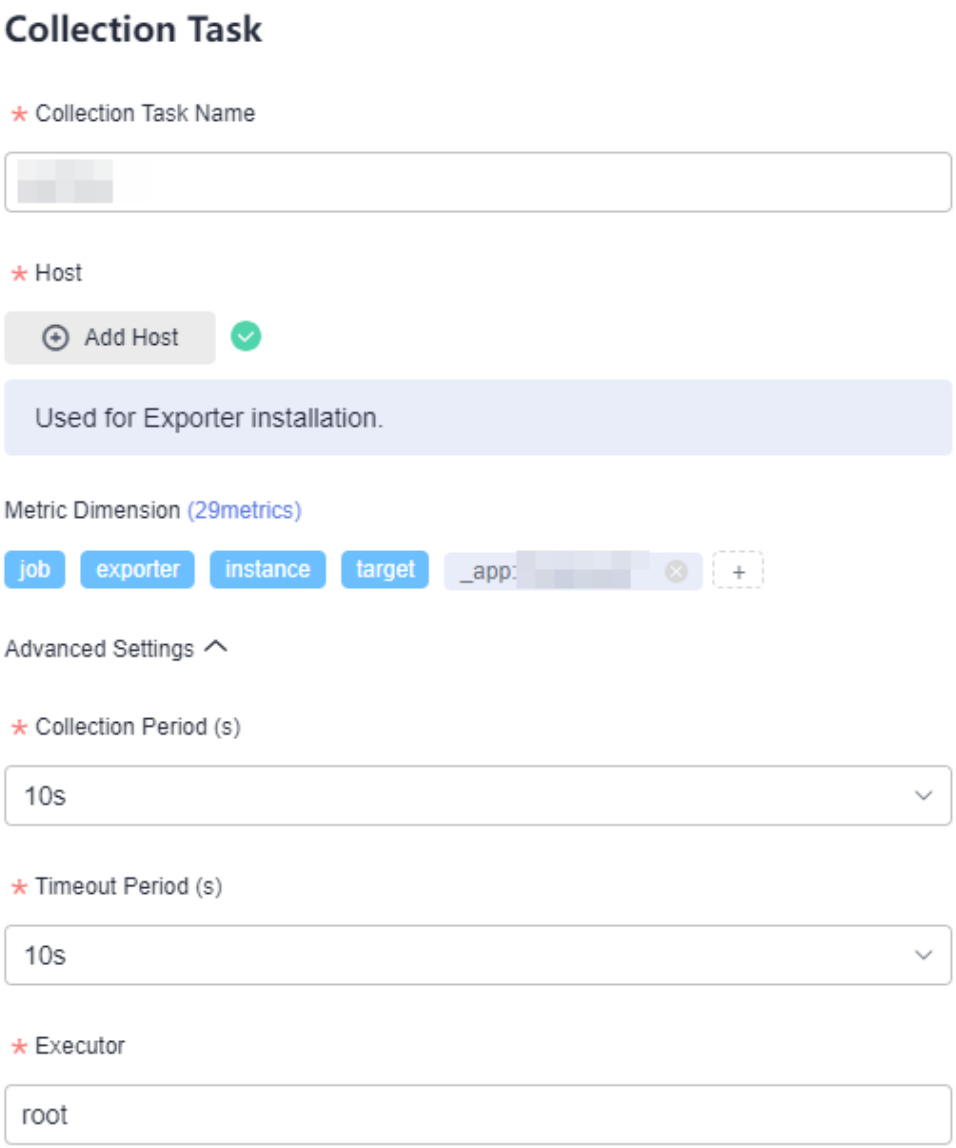


Table 2-37 Parameters for creating a collection task

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. Only Linux is supported.
	Collection Plug-in	The default value is **POSTGRESQL**.

Operation	Parameter	Description
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

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

Figure 2-31 Installing Exporter

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

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

----End

2.5.2.9 Ingesting Elasticsearch Metrics to AOM

Create a collection task and install Elasticsearch Exporter to monitor Elasticsearch metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **Elasticsearch** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **Elasticsearch** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Elasticsearch** card.

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

Figure 2-32 Configuring a collection task

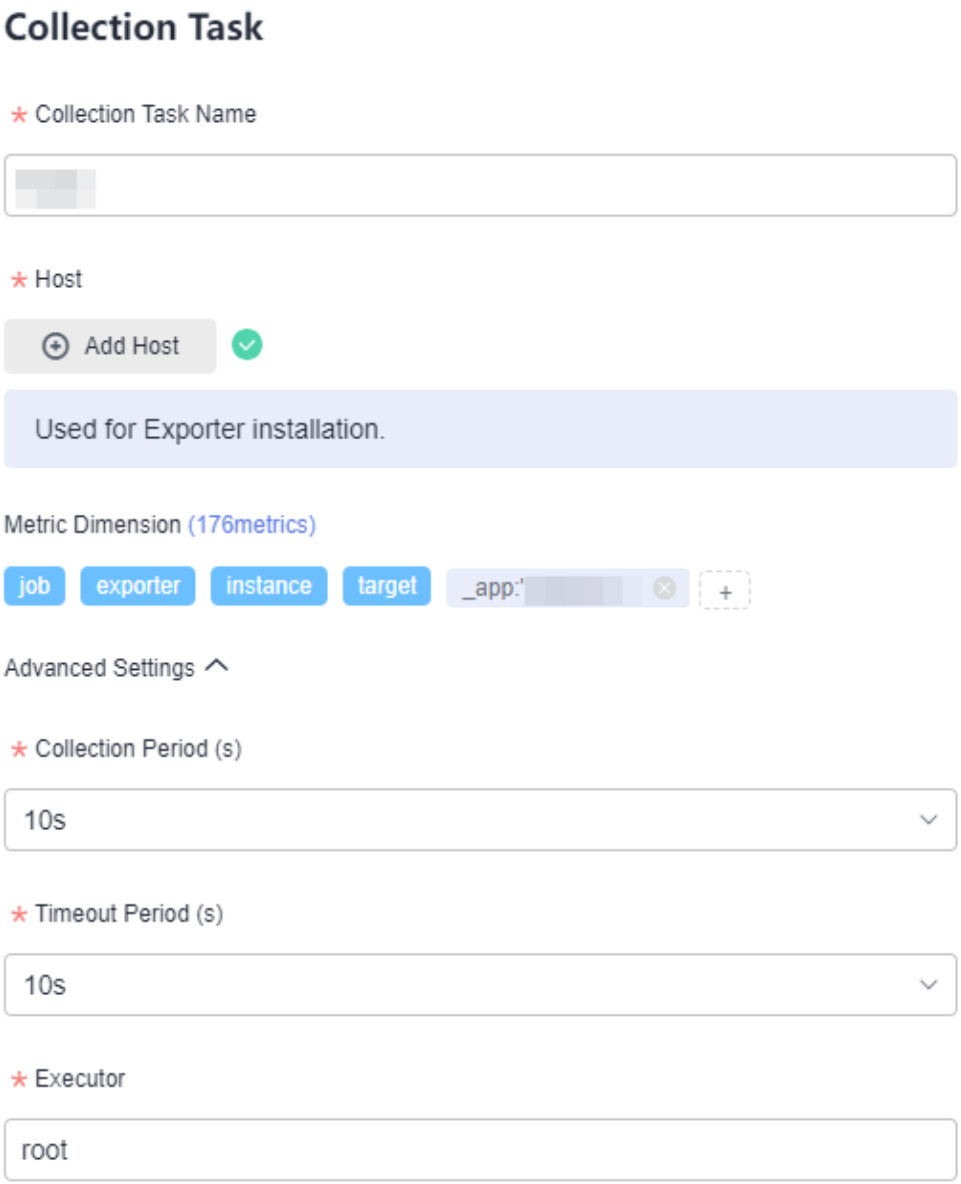


Table 2-38 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task 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. Only Linux is supported.

Operation	Parameter	Description
	Collection Plug-in	The default value is **ELASTICSEARCH**.
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

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

Figure 2-33 Installing Exporter

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

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

----End

2.5.2.10 Ingesting RabbitMQ Metrics to AOM

Create a collection task and install RabbitMQ Exporter to monitor RabbitMQ metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **RabbitMQ** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **RabbitMQ** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **RabbitMQ** card.

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

Figure 2-34 Configuring a collection task

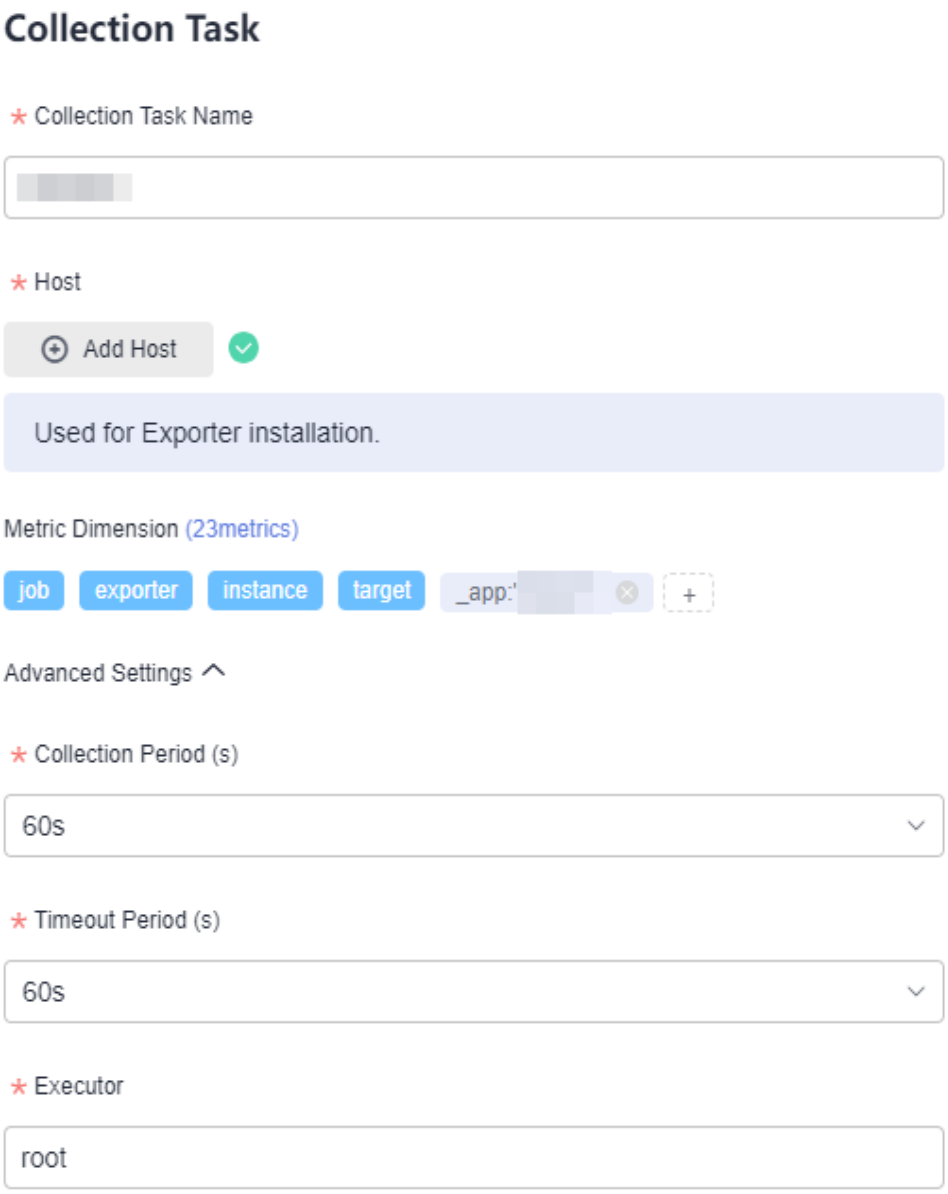


Table 2-39 Parameters for creating a collection task

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. Only Linux is supported.

Operation	Parameter	Description
	Collection Plug-in	The default value is **RABBITMQ**.
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

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

Figure 2-35 Installing Exporter

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

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

----End

2.5.2.11 Ingesting Other Middleware Metrics to AOM

If existing middleware Exporters do not meet your requirements, install your own Exporter and create a collection task to monitor middleware metrics.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **Other components** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **Other components** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Other components** card.

Step 3 On the displayed page, set parameters by referring to the following table.

Figure 2-36 Configuring a collection task

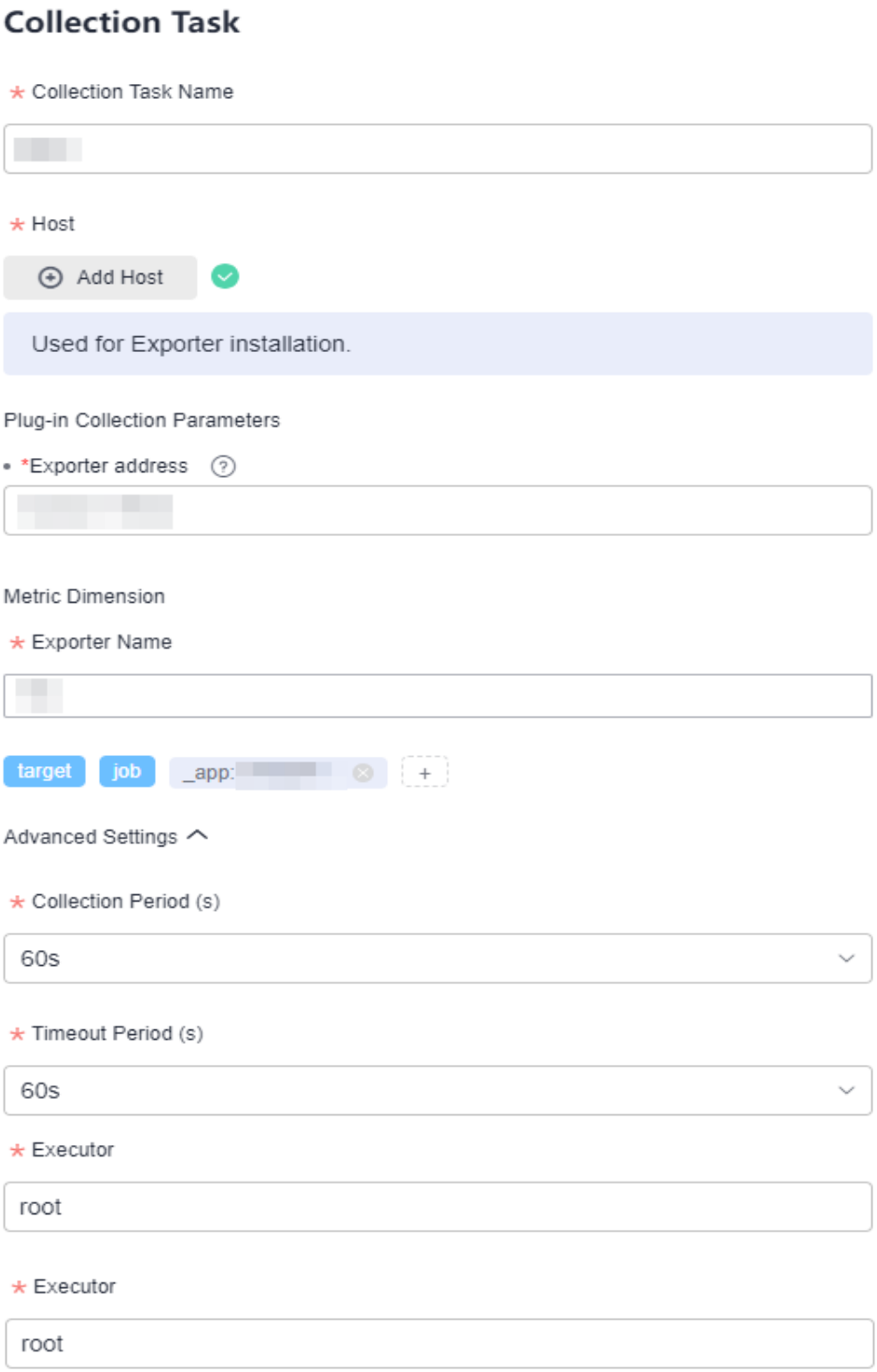


Table 2-40 Parameters for configuring a collection task

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. Only Linux is supported.
	Collection Plug-in	The default value is **CUSTOM_EXPORTER**.
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. • Search for and select a host by the host name, IP address, or Agent status. • You can click in the upper right corner to deselect the selected host. • Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Plug-in Collection Parameters	**Exporter Address**: IP address and port number of the host where Exporter is installed. The format is "IP address:Port", for example, **10.0.0.1:9100**

Operation	Parameter	Description
	Metric Dimension	**Exporter Name**: Enter an Exporter name. Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: ● **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). ● **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Click **Create**.

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

----End

2.5.3 Connecting Custom Plug-ins to AOM

Create a plug-in, specify the metrics to be reported to AOM using a script, and create a collection task. Then the specified metrics can be reported to AOM for monitoring.

Prerequisites

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

Creating a Custom Plug-in

You can create a plug-in using a custom script and create a collection task **during the connection of the custom plug-in** to report metrics to AOM.

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Access** > **Access Center** to go to the old access center. (The new access center does not support the connection of custom plug-ins. Click **Back to Old Version** in the upper right corner to switch from the new access center to the old one.)

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

Step 4 On the displayed page, set related parameters.

- Plug-in information

  Table 2-41 Plug-in parameters

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

- Set Plug-in

  Table 2-42 Plug-in configuration parameters

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

Parameter	Description

Plug-in Script	Custom plug-in script. You need to specify the metrics to be reported to AOM in this script. The script type can be **Linux** or **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`

Default Script Parameter	Default parameters of the custom plug-in script. Set default parameters for script modeling. You can also leave them empty. Rules: **$*{Parameter}***: Enter a maximum of 64 characters starting with a letter. Only letters, digits, and underscores (_) are allowed. For example, **${a_b}**. You can combine parameters as required and separate them with spaces. Max.: 250 characters.
Script Parameter	Configure the attributes of the default parameters in the custom plug-in script. You can configure the following information as required: – **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. The system automatically identifies the script parameter name based on **Default Script Parameter** you have already configured. The parameter here is grayed and cannot be configured. – **Default Value**: default value of the script parameter. – **Description**: description of the parameter. When you **configure a collection task** for the custom plug-in, script parameters are displayed based on the script parameter attributes configured here. You can configure collection based on the script parameter attributes.

Step 5 Click **Save**.

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

Table 2-43 Related operations

Operation	Description
Checking the plug-in status	Locate the target plug-in, hover the mouse pointer over the plug-in, and choose > **Version**. On the page that is displayed, check the plug-in status. • **Unreleased**: When you create a plug-in or create a plug-in version, the plug-in status is **Unreleased**. You can click the version number to edit the plug-in. • **Released**: After you click **Release** in the **Operation** column, the plug-in status changes to **Released**. You can click the version number to view the plug-in details.
Creating a version	Locate the target plug-in, hover the mouse pointer over the plug-in, and choose > **Version**. Click **Create Version**. On the displayed page, set the plug-in information. Precautions: • A maximum of five versions can be created for a plug-in. • If there is only one plug-in version, only **Copy** is available in the **Operation** column. If there is more than one plug-in, both **Copy** and **Delete** are available in the **Operation** column. You can click **Delete** to delete a plug-in version.
Modifying a plug-in	Locate the target plug-in, hover the mouse pointer over the plug-in, and choose > **Modify**. On the displayed page, modify the plug-in information.
Deleting a plug-in	Locate the target plug-in, hover the mouse pointer over the plug-in, and choose > **Delete**. On the displayed page, click **Yes** to delete the plug-in. If a collection task has been configured for a plug-in, deleting the plug-in will also delete the collection task.

----End

Connecting Custom Plug-ins to AOM

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Access** > **Access Center** to go to the old access center. (The new access center does not support the connection of custom plug-ins. Click **Back to Old Version** in the upper right corner to switch from the new access center to the old one.)

Step 3 On the collection task configuration page, set parameters by referring to the following table.

Figure 2-37 Configuring a collection task

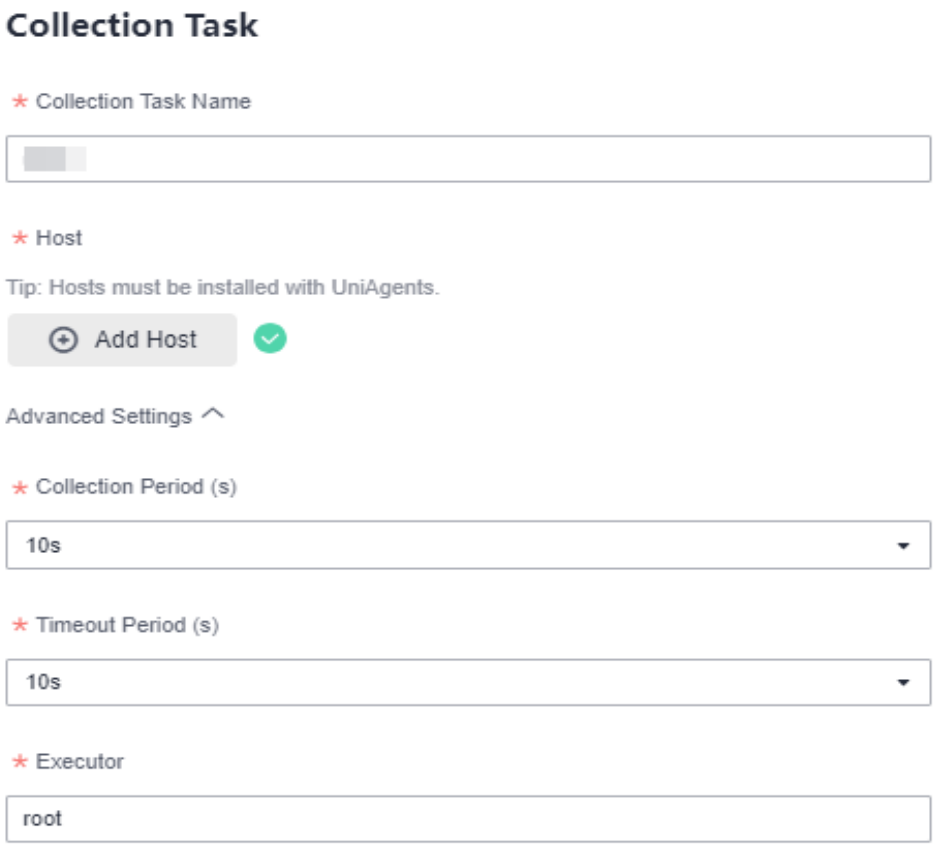


Table 2-44 Parameters for configuring a collection task

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**. For a custom plug-in, the OS is automatically selected.
	Collection Plug-in	(Default) Created custom plug-in.
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Operation	Parameter	Description
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. • Search for and select a host by the host name, IP address, or Agent status. • You can click in the upper right corner to deselect the selected host. • Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Plug-in Collection Parameters	Set parameters for the custom plug-in script. They come from the default script parameters you define when **creating a custom plug-in script**.
	Advanced Settings	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). The timeout period cannot exceed the collection period. • **Executor**: user who executes the collection task, that is, the user of the selected host. Default: **root**. Enter a username. Recommended: **root**.

Step 4 Click **Create**.

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

----End

2.5.4 Managing Middleware and Custom Plug-in Collection Tasks

After connecting middleware or custom plug-ins to AOM, you can manage the collection tasks created during the connection in the access center.

1. Log in to the **AOM 2.0** console.
2. In the navigation pane, choose **Access** > **Access Center** to go to the access center. (The new access center does not support the connection of custom plug-ins. Click **Back to Old Version** in the upper right corner to switch from the new access center to the old one. Then you can manage custom plug-in collection tasks on the old access center.)

3. On the **Prometheus Middleware** or **Custom Prometheus Plug-in Access** panel, click a plug-in card for which a collection task has been configured. The card details page is displayed.
4. On the **Collection Tasks** tab page, manage the collection tasks created for the middleware or custom plug-in. Procedure:

   Also, you can choose **Prometheus Monitoring** > **Instances** and click an instance to go to the instance details page to view or delete related collection tasks.

Table 2-45 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click  in the **Start/Stop** column of a collection task to start or stop it.
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	Click  in the **Operation** column of the target collection task. On the displayed page, change target hosts. You can only change the target hosts for the collection tasks created using custom plug-ins.
Sorting collection tasks	Click in the **Timeout Period** or **Collection Period** column to sort collection tasks. indicates the default order.  indicates the ascending order (that is, the maximum time is displayed at the bottom).  indicates the descending order (that is, the maximum time is displayed at the top).
Copying a collection task	Click  in the **Operation** column of a collection task. On the displayed page, modify parameters as required.
Modifying a collection task	Choose > **Modify** in the **Operation** column of the target collection task. On the displayed page, modify parameters as required. • Modifying a custom plug-in collection task: The plug-in version and collection task details can be modified. • Modifying a middleware collection task: Only metric dimensions can be modified.
Deleting a collection task	Locate a collection task and choose  > **Delete** in the **Operation** column. On the displayed page, confirm the deletion.

2.6 Connecting Running Environments to AOM

AOM provides a unified entry for observability analysis of Huawei Cloud services. Through the access center, you can connect running environments to AOM. This function enables CCE and CCI container metrics and ECS metrics to be reported to AOM.

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, choose **Access** > **Access Center**. (To switch from the new access center to the old one, click **Back to Old Version** in the upper right corner.)

Step 3 In the **Prometheus Running Environments** panel on the right, click the target card and perform the operations listed in the following table if needed.

Table 2-46 Connecting Prometheus running environments to AOM

Card	Related Operation
Cloud Container Engine (CCE) (ICAgent)	Uses ICAgent to collect CCE cluster metrics. By default, ICAgent is installed when you purchase a CCE cluster and node. ICAgent automatically reports CCE cluster metrics to AOM. Click the **Cloud Container Engine (CCE) (ICAgent)** card to view the CCE cluster metrics that can be ingested. For details about the CCE cluster metrics that are reported to AOM, see **Basic Metrics: VM Metrics**. To use Prometheus to collect CCE cluster metrics and report them to AOM, see **9.4 Using Prometheus Monitoring to Monitor CCE Cluster Metrics**.
Cloud Container Instance (CCI)	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 CCI metrics that can be ingested. For details about the CCI metrics that are reported to AOM, see **Basic Metrics: VM Metrics**.
Elastic Cloud Server (ECS)	Click the **Elastic Cloud Server (ECS)** card. In the displayed dialog box, install the Node Exporter provided by Prometheus. The information and running metrics of Linux hosts can then be collected. For details, see **Connecting ECSs to AOM**.

----End

Connecting ECSs to AOM

Node Exporter is provided by Prometheus to collect information about Linux hosts, including the CPU, memory, load, file system, and network. You can install Node Exporter on an ECS and create a collection task. Related metrics can then be reported to AOM.

- **Constraints**

  A host supports only one Node Exporter.

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

Step 1 Log in to the **AOM 2.0** console.

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

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

Step 4 On the **Procedure** tab page of the **Elastic Cloud Server (ECS)** dialog box, perform the installation as prompted.

1. Select a target Prometheus instance for ECS from the drop-down list.
2. Install Node Exporter: Select one or more hosts where Node Exporter is to be installed.

Step 5 Click **Install** to install Node Exporter.

- After the installation is complete, use UniAgent to create a collection task. Node Exporter can then collect host metrics. For the metrics collected by Node Exporter, see **Basic Metrics: Node Exporter Metrics**. By default, both the values of **Metric Collection Interval (s)** and **Metric Collection Timeout (s)** are **60**. The two values cannot be changed.
- You can also perform the following operations on the **Collection Tasks** tab page under **Elastic Cloud Server (ECS)**.

Table 2-47 Related operations

Operation	Description
Searching for a collection task	You can search for collection tasks by collection task, collection status, host IP address, or host name.
Refreshing a collection task	Click  in the upper right corner of the collection task list to obtain the latest information.
Deleting a collection task	Click **Delete** in the **Operation** column.

Operation	Description
Starting or stopping a collection task	Click the button in the **Start/Stop** column of a collection task to start or stop it.

----End

2.7 Connecting Cloud Services to AOM

AOM provides a unified entry for observability analysis of Huawei Cloud services. Through the access center, you can connect cloud services to AOM. Cloud service metrics (such as CPU/memory usage) can then be reported to AOM.

To quickly connect cloud services to AOM, perform the following steps:

1. Create a Prometheus instance for cloud services. This instance is used to store collected data. For details, see **Creating a Prometheus Instance for Cloud Services**.
2. Connect cloud services to AOM. For details, see **Connecting Cloud Services to AOM**.
3. After cloud services are connected to AOM, their metrics can be reported to AOM.
   - You can go to the **Metric Browsing** page to query metrics.
   - For some cloud services connected to AOM, you can view their information on the **Cloud Service Monitoring** page.

Constraints

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

Creating a Prometheus Instance for Cloud Services

Step 1 Log in to the **AOM 2.0** console.

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

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

Table 2-48 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 Cloud Services**.

Step 4 Click **OK**.

----End

Connecting Cloud Services to AOM

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest cloud service metrics:

- Method 1:
  a. Choose **Access** > **Access Center**. The **Access Center** page is displayed. (To switch from the new access center to the old one, click **Back to Old Version** in the upper right corner.)
  b. Click the cloud service to be connected on the **Prometheus Cloud Services** panel.
- Method 2:
  a. Choose **Prometheus Monitoring** > **Instances** and then click a target Prometheus instance.
  b. In the **Unconnected Cloud Services** area, click the cloud service to be connected.

Table 2-49 Cloud service card

Card	Description
Auto Scaling, FunctionGraph, Elastic Volume Service (EVS), Cloud Backup and Recovery (CBR), Object Storage Service (OBS), Scalable File Service (SFS), SFS Turbo, Virtual Private Cloud (VPC), Elastic Load Balance (ELB), Direct Connect, Virtual Private Network (VPN), NAT Gateway, Enterprise Router, Distributed Message Service (DMS), Distributed Cache Service (DCS), API Gateway (APIG), GaussDB(for MySQL), GeminiDB, Relational Database Service (RDS), Document Database Service (DDS), Data Replication Service (DRS), ModelArts, LakeFormation, CloudTable, MapReduce Service (MRS), GaussDB(DWS), Data Lake Insight (DLI), Cloud Search Service (CSS), IoT Device Access (IoTDA), Intelligent EdgeFabric (IEF), Web Application Firewall (WAF), Cloud Bastion Host (CBH), Simple Message Notification (SMN), and Content Delivery Network (CDN)	• ModelArts automatically reports metrics to AOM as ready-to-use data. No manual configuration is required. For details about ModelArts metrics, see **Basic Metrics: ModelArts Metrics**. • IoTDA automatically reports metrics to AOM as ready-to-use data. No manual configuration is required. For details about IoTDA metrics, see **Basic Metrics: IoTDA Metrics**. • Intelligent EdgeFabric (IEF) automatically reports metrics to AOM as ready-to-use data. No manual configuration is required. For details about IEF metrics, see **Basic Metrics: IEF Metrics**. • For other cloud services, ingest their metrics to AOM by referring to **3**. For details about cloud service metrics, see **Cloud Service Metrics**.

Step 3 In the displayed dialog box, set information about the cloud service.

Table 2-50 Connecting a cloud service

Parameter	Description
Select Prometheus Instance for Cloud Services	Select the **Prometheus instance** for metric ingestion. • Enterprise Project – Connecting cloud services on the **Cloud Service Connection** page of the Prometheus instance details page: By default, the enterprise project is the same as that selected during the **creation of the Prometheus instance for cloud services**. This option is grayed and cannot be changed. – Connecting cloud services through the access center: Select a required enterprise project from the drop-down list. If the existing enterprise projects cannot meet your requirements, create one by referring to **Creating an Enterprise Project**. • Prometheus Instance for Cloud Services – Connecting cloud services on the **Cloud Service Connection** page of the Prometheus instance details page: By default, the value of this parameter is set to the **target Prometheus instance** selected in **1**. This option is grayed here and cannot be changed. – Connecting cloud services through the access center: By default, the value of this parameter is the Prometheus instance for cloud services under your selected enterprise project. If there is no such a Prometheus instance, create one.
(Optional) Connect Cloud Service Tags	Whether to connect cloud service tags. Tags are used for aggregation and association. If the existing tags cannot meet your requirements, click **Go to Tag Management Service (TMS)** to **add tags**.
Auto Sync	Whether to enable automatic synchronization of cloud service tags. • Enable: The addition and modification of cloud service tags are synchronized to the ingestion configuration. This function is enabled by default. • Disable: The addition and modification of cloud service tags are not synchronized to the ingestion configuration.

Step 4 Click **Connect Now**.

----End

Other Operations

You can also perform the operations listed in **Table 2-51** on the **Cloud Service Connection** page of the Prometheus instance for cloud services.

Table 2-51 Related operations

Operation	Description
Searching for cloud services	On the **Cloud Service Connection** page, enter a keyword in the search box to search for a cloud service.
Disconnecting cloud services	On the **Cloud Service Connection** page, click a target cloud service. In the displayed dialog box, click **Disconnect Cloud Service**.
Checking or modifying tag configurations of connected cloud services	On the **Cloud Service Connection** page, click a cloud service under **Connected Cloud Services** to change cloud service tag settings. For details, see **Table 2-50**.

2.8 Connecting Open-Source System to AOM

AOM provides a unified entry for observability analysis of Huawei Cloud services. Through the access center, you can create a common Prometheus instance to connect the open-source monitoring system to AOM.

Scenario

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

Creating a Common Prometheus Instance

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, use either of the following methods to create a common Prometheus instance:

- Method 1:
  a. Choose **Access** > **Access Center**. The **Access Center** page is displayed. (To switch from the new access center to the old one, click **Back to Old Version** in the upper right corner.)
  b. In the **Open-Source Monitoring** panel, click the **Common Prometheus instance** card.
- Method 2:

  Choose **Prometheus Monitoring** > **Instances**, and click **Add Prometheus Instance**.

Step 3 In the displayed dialog box, set an instance name, enterprise project, and instance type.

Table 2-52 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 **Common Prometheus Instance**.

Step 4 Click **OK**.

----End

2.9 Managing Log Ingestion

AOM is a unified platform for observability analysis. It does not provide log functions by itself. Instead, it uses the access management function of **Log Tank Service (LTS)**. You can perform operations on the AOM 2.0 or LTS console.

Constraints

- To use the access management function on the AOM 2.0 console, **purchase LTS resources** first.
- To use LTS functions on the AOM console, you need to obtain LTS permissions in advance. For details, see **Permissions**.

Table 2-53 Function description

Function	Description	AOM 2.0 Console	LTS Console	References
Access management	Logs can be ingested through ICAgents, cloud services, APIs, and SDKs. After logs are ingested, they are displayed in a simple and orderly manner on the console and can be queried easily.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane on the left, choose **Access** > **Access Management**.	1. Log in to the LTS console. 2. In the navigation pane on the left, choose **Access** > **Access Management**.	**Log Ingestion**

3 (New) Connecting to AOM

3.1 AOM Access Overview

AOM provides a unified entry for observability analysis of Huawei Cloud services. Through the new access center, you can quickly ingest metrics to AOM, logs to LTS, and traces to APM. After the ingestion is complete, you can view resource/application running status, metric usage, logs, and traces on the **metric browsing** and **log management** pages.

Constraints

If the old Access Center is displayed, click **Experience the new version** in the upper right corner.

Ingesting Metrics, Logs, or Traces to AOM

Step 1 Log in to the **AOM 2.0** console.

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

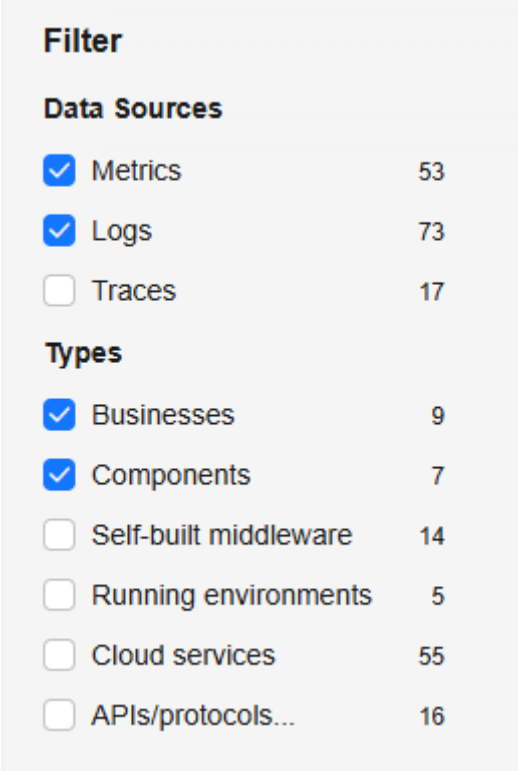
Step 3 Click **Experience the new version** in the upper right corner of the page. The new access center is displayed.

The **Recommended** area displays six popular cards. They will be automatically updated to the six cards you have recently used.

Step 4 Set criteria to quickly query the metrics, logs, or traces to be ingested.

- Filter: Filter content by data source or type.

Figure 3-1 Filter



- Attribute filtering: Click the search box and search for content by keyword, data source, or type. You can also enter a keyword to search.

Figure 3-2 Search through the search box

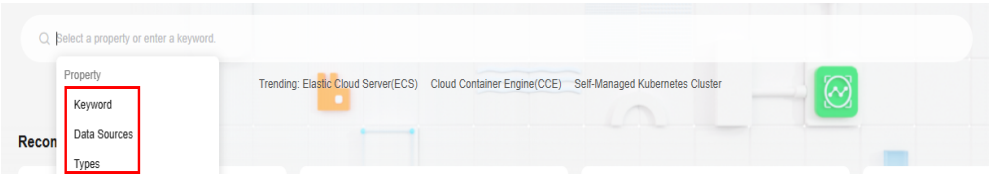


Table 3-1 Access overview

Type	Monitored Object (Card)	Data Source	Access Mode
Businesses	Web & H5	Logs/ Metrics/ Traces	3.3 Connecting Businesses to AOM
	Android App		
	iOS App		
	WeChat		
	Alipay		
	DingTalk		
	Baidu		

Type	Monitored Object (Card)	Data Source	Access Mode
	Quick Applets		
	Business Monitoring (Log-based)		
Components	Java Component	Logs/Traces	3.4 Connecting Components to AOM
	GO Component		
	Python Component		
	Node.js Component		
	PHP Component		
	.NET Component		
	C++ Component		
Self-built middleware	MySQL	Logs/ Metrics	3.5.1 Overview About Middleware Connection to AOM
	Redis		
	Kafka		
	Nginx		
	MongoDB		
	Consul		
	HAProxy		
	PostgreSQL		
	Elasticsearch		
	RabbitMQ		
	ZooKeeper		
	IIS		
	DNS		
	Flink		
Running environments	Elastic Cloud Server (ECS)	Logs/ Metrics	3.6 Connecting Running Environments to AOM
	Bare Metal Server (BMS)		
	Cloud Container Engine (CCE)		

Type	Monitored Object (Card)	Data Source	Access Mode
	Cloud Container Instance (CCI)		
	Self-Managed Kubernetes Cluster		

Type	Monitored Object (Card)	Data Source	Access Mode
Cloud services	AOM, API Gateway (APIG), Astro Zero, Bare Metal Server (BMS), Cloud Bastion Host (CBH), Cloud Container Engine (CCE), Content Delivery Network (CDN), Cloud Firewall (CFW), Cloud Trace Service (CTS), Distributed Cache Service (DCS), Document Database Service (DDS), Anti-DDoS Service (AAD), Distributed Message Service (DMS) for Kafka, Data Replication Service (DRS), Data Warehouse Service (DWS), Elastic Cloud Server (ECS), Elastic Load Balance (ELB), Enterprise Router, FunctionGraph, GaussDB, Graph Engine Service (GES), GaussDB(for MySQL), GeminiDB Redis, GeminiDB Mongo, GeminiDB Cassandra, Huawei HiLens (HiLens), IoT Device Access (IoTDA), ModelArts, MapReduce Service (MRS), Relational Database Service (RDS) for MySQL, RDS for PostgreSQL, RDS for SQL Server, ROMA Connect, Live, Simple Message Notification (SMN),	Logs	**3.7 Connecting Cloud Services to AOM**

Type	Monitored Object (Card)	Data Source	Access Mode
	SecMaster, ServiceStage-container application logs, ServiceStage-cloud host logs, Virtual Private Cloud (VPC), and Web Application Firewall (WAF)		
	Auto Scaling, APIG (Dedicated), CBH, BMS, Cloud Backup and Recovery (CBR), CloudTable, CDN, Cloud Search Service (CSS), Direct Connect, DCS, DDS, Data Lake Insight (DLI), DMS for Kafka, DRS, DWS, ELB, Enterprise Router, Elastic Volume Service (EVS), FunctionGraph, GaussDB(for MySQL), GeminiDB, IoTDA, Intelligent EdgeFabric (IEF), ModelArts, MRS, NAT Gateway, Object Storage Service (OBS), RDS for MySQL, RDS for PostgreSQL, RDS for SQL Server, LakeFormation, SMN, Scalable File Service (SFS), SFS Turbo, VPC, Virtual Private Network (VPN), and WAF	Metrics	
APIs/ protocols...	AOM APIs	Logs/ Metrics/ Traces	**3.8 Ingesting Data to AOM Using Open-Source APIs and Protocols**
	LTS APIs		
	APM APIs		

Type	Monitored Object (Card)	Data Source	Access Mode
	Common Prometheus Instance		
	Kafka Protocol		
	OpenTelemetry		
	SkyWalking		
	Syslog Protocol		
	Flume		
	Beats		
	Logstash		
	SNMP Protocol		
	Java SDK (log4j2)		
	Logback SDK		
	Cross-Account Ingestion - Log Stream Mapping		
	Custom Prometheus Metrics		

Step 5 Hover the pointer over the card and click the blue text to check LTS documents or ingest metrics and traces.

- Click **Ingest Metric (AOM)** or **Ingest Trace (APM)** to quickly ingest metrics or traces.
- Click **Ingest Log (LTS)** on **Ingest Log (LTS) Details** to quickly ingest logs or click **Details** to check documents related to log ingestion.

----End

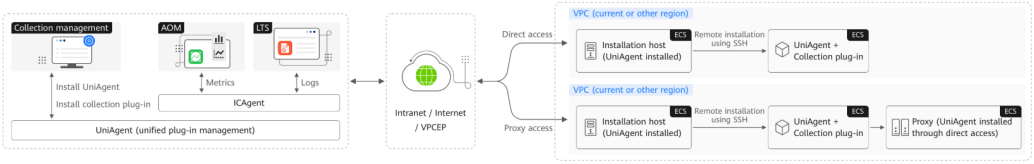
3.2 Managing Collector Base UniAgent

3.2.1 Installing UniAgents

UniAgents centrally manage the life cycle of collection plug-ins and deliver instructions (such as script delivery and execution). UniAgents do not collect data themselves. O&M data is collected by collection plug-ins. You can install collection plug-ins through the access center and create collection tasks to collect metrics.

AOM allows you to install UniAgents on cloud servers in a VPC.

Figure 3-3 Getting started



Prerequisite

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

Constraints

- For details about the Linux and Windows OSs supported by the UniAgent, see **Collection Management Restrictions**.
- To switch from the new UniAgent page to the old one, choose **Settings** > **Collection Settings** > **UniAgent Installation and Configuration** in the navigation tree on the left and click **Back to old version** in the upper right corner. To go to the **new UniAgent** page, click **Go to New Version** in the upper right corner of the **UniAgent Installation and Configuration** page.

Installation Methods

Install a UniAgent on a host manually or remotely, or by importing an Excel file. Select an installation mode based on site requirements.

Table 3-2 Installation modes

Mode	Scenario
Manual UniAgent Installation	Suitable for initial installation and single-node installation scenarios. Log in to the host where the UniAgent is to be installed and manually run the installation command. **When installing a UniAgent for the first time, you must install it manually.**
Remote UniAgent Installation	Suitable for the scenario where UniAgents are installed in batches. Set a host where a UniAgent has been installed to be an installation host, and use it to install UniAgents on other hosts. (Enter the information about the hosts where UniAgents are to be installed on the installation page.)
UniAgent Installation by Importing an Excel File	Suitable for the scenario where UniAgents are installed in batches. Set a host where a UniAgent has been installed to be an installation host, and use it to install UniAgents on other hosts. (Import the Excel file that contains the information about the hosts where UniAgents are to be installed on the installation page.) **The Excel import function is not yet generally available. If you need this function, submit a service ticket.**

Manual UniAgent Installation

When installing a UniAgent for the first time, you must install it manually.

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **UniAgent Installation and Configuration**. Then click **Install UniAgent** in the upper right corner. On the displayed page, choose **Manual**. (When you install the UniAgent for the first time, the **Manual** page is displayed by default.)

Step 4 On the **Install UniAgent** page, set parameters to install a UniAgent.

Figure 3-4 Manually installing a UniAgent

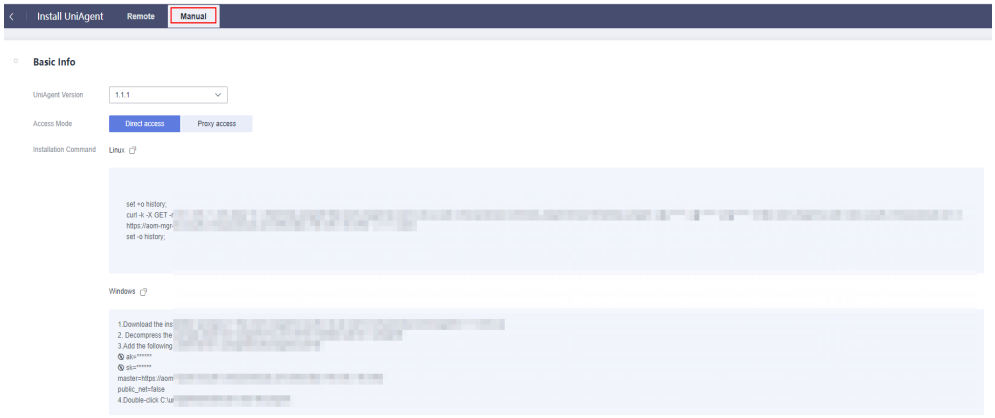


Table 3-3 Parameters for manual installation

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.0.8
Access Mode	There are 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 install the UniAgent on a host through the proxy. **You can choose Direct access (private network) and Direct access (public network) only in CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, and CN South-Guangzhou.**	Direct access (private network)

Parameter	Description	Example
Proxy Area	Manages proxies by category. When **Access Mode** is set to **Proxy access**, you need to select or **add** a proxy area. A proxy area must contain an available proxy. This proxy must be a cloud host where a UniAgent has been installed. Also, this proxy must have been **set to be an installation host**.	Select a proxy area.

Parameter	Description	Example

Installation Command	Command for installing the UniAgent. Commands for Linux and Windows are different.
	Linux
	1. Click to copy the installation command.
	`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 -q false`
	`set -o history;`
	Windows
	1. Copy the download address (**https://aom-uniagent-*{region_name}*.obs.*{region_name}*.*{site domain name suffix}*/+uniagentd-*{version}*-win32.zip**) to the browser to download the installation package.
	{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. Enter the following configuration (obtained from the installation page) to the **C:\uniagentd\conf\uniagentd.conf** file:
	`master=https://aom-mgr-lb.xxxxxxxxxxx,https://xx.xx.xx.xx:xxxxx`
	`project_id=xxxxxxxxxxxxxx`
	`public_net=xxxx`
	4. Run **start.bat** in the **C:\uniagentd\bin** directory as the administrator.
	If you need to verify the SHA256 value of the Windows installation package, check the file downloaded from **https://aom-uniagent-*{region_name}*.obs.**
		Copy the Linux installation command.

Parameter	Description	Example
	{region_name}.{site domain name suffix}/**uniagentd-***{version}***-win32.zip.sha256**.	

Step 5 Copy the installation command and run it on the host to install the UniAgent.

- Linux host: Use a remote login tool, such as PuTTY, to log in to the target host and run the installation command copied in the **previous step** as the **root** user to install the UniAgent.
- Windows host: Log in to the target host, and download the installation package based on the installation command in the **previous step** to install the UniAgent.

Step 6 Check whether the UniAgent is displayed in the UniAgent list.

----End

Remote UniAgent Installation

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **UniAgent Installation and Configuration**. Then click **Install UniAgent** in the upper right corner.

Step 4 On the **Install UniAgent** page, choose **Remote** and set parameters to install a UniAgent. (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 3-5 Remotely installing a UniAgent

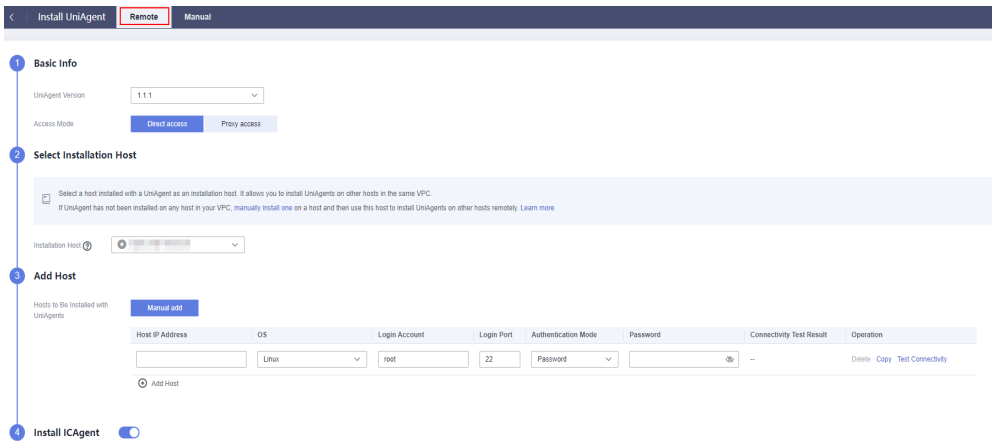
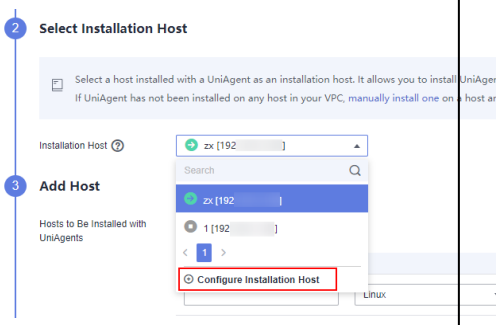


Table 3-4 Parameters for remotely installing a UniAgent

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.0.8
Access Mode	There are 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 install the UniAgent on a host through the proxy. **You can choose Direct access (private network) and Direct access (public network) only in CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, and CN South-Guangzhou.**	Direct access (private network)
Proxy Area	Manages proxies by category. When **Access Mode** is set to **Proxy access**, you need to select or **add** a proxy area. A proxy area must contain an available proxy. This proxy must be a cloud host where a UniAgent has been installed. Also, this proxy must have been **set to be an installation host**.	Select a proxy area.

Parameter	Description	Example
Installation Host	An installation host is used to execute commands for remote installation. This parameter is mandatory. To install the UniAgent remotely, ensure that the installation host does not run Windows. If no installation host has been configured, perform the following steps: 1. Select **Configure Installation Host** from the drop-down list. **Figure 3-6** 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**.	Select an installation host.

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. Add a maximum of 100 hosts: • **Host IP Address**: IP address of a host. • **OS**: operating system of the host, which can be **Linux** or **Windows**. To install the UniAgent remotely, ensure that the host does not run 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. After entering the host information, you can delete, copy, or test the connectivity of hosts in the **Operation** column. The connectivity test checks the network between the installation host and the host where the UniAgent is to be installed. The test result is displayed in the **Connectivity Test Result** column. (Windows hosts do not support connectivity tests.)	Enter the information about the hosts where UniAgents are to be installed.
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 if needed. (In some regions, you do not need to enter any AK or SK.)	-

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

----End

UniAgent Installation by Importing an Excel File

The Excel import function is not yet generally available. If you need this function, **submit a service ticket**.

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **UniAgent Installation and Configuration** and click **Install UniAgent** in the upper right corner.

Step 4 On the **Install UniAgent** page, choose **Import Excel** and set parameters to install a UniAgent. (When you install the UniAgent for the first time, the **Manual** page is displayed by default. **Import Excel** is not available.)

Figure 3-7 Installation by importing an Excel file

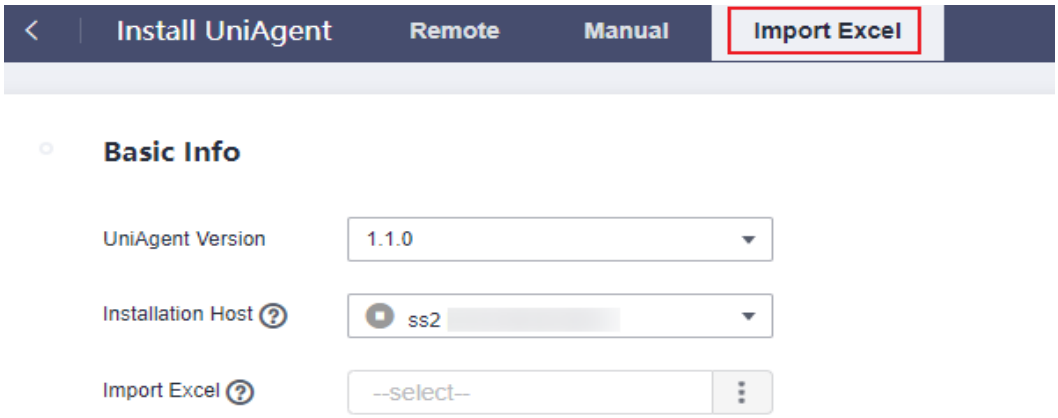
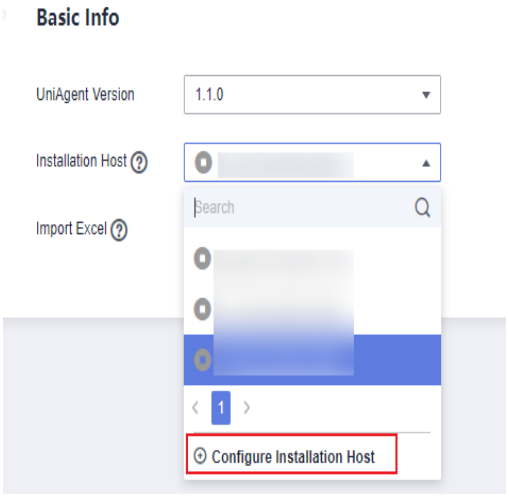
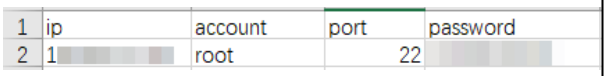


Table 3-5 Parameters for installation by importing an Excel file

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. To install the UniAgent by importing an Excel file, ensure that the installation host does not run Windows. If no installation host has been configured, perform the following steps: 1. Select **Configure Installation Host** from the drop-down list. **Figure 3-8** 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**.	Select an installation host.

Parameter	Description	Example
Import Excel	Only an **.xls** or **.xlsx** file with up to 5,000 records can be uploaded. To install the UniAgent by importing an Excel file, ensure that the host does not run Windows. Excel file example: **Figure 3-9** Configuring host information  • **ip**: IP address of the host where the UniAgent is to be installed. • **account**: account for logging in to the host. You are advised to use the **root** account to get sufficient read and write permissions. • **port**: port for accessing the host. • **password**: password for logging in to the host.	Upload the Excel file containing host information.

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

----End

Checking the UniAgent Status

On the **UniAgent Installation and Configuration** page, check the UniAgent status of the target host. For details, see **Table 3-6**.

Table 3-6 UniAgent statuses

Status	Description
Running	The UniAgent is working.
Abnormal	The UniAgent is not working. Contact technical support.
Installing	The UniAgent is being installed. The installation takes about 1 minute to complete.
Installation failed	The UniAgent fails to be installed. Uninstall the UniAgent and then reinstall it. If the installation still fails, contact technical support.

Status	Description
Not installed	The UniAgent has not been installed on the host. For a host where the UniAgent is uninstalled but it is not deleted, the UniAgent is in the **Not installed** state. You can reinstall the UniAgent or delete the host from the list.

After the UniAgent is installed on the host, ports **39338** and **39339** will be enabled to query log levels and collection tasks.

Other Operations

If needed, perform the following operations on the host where the UniAgent has been installed.

Table 3-7 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 bottom).  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. Precautions: • 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, do as follows: Choose **Cancel Installation Host** in the **Operation** column to cancel an installation host.
Changing the name of an installation host	To change the name of a configured installation host, do as follows: Click the name of the installation host. In the dialog box that is displayed, rename it.

Troubleshooting

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

3.2.2 (New) Installing UniAgents

UniAgents centrally manage the life cycle of collection plug-ins and deliver instructions (such as script delivery and execution). UniAgents do not collect data themselves. O&M data is collected by collection plug-ins. You can install collection plug-ins through the access center and create collection tasks to collect metrics.

AOM allows you to install UniAgents on ECSs or other servers in or outside the current region.

- **Current region**: Install UniAgents on the hosts in the region where the AOM console is located.
- **Outside current region**: Install UniAgents on the hosts outside the region where the AOM console is located. For example, the hosts of self-built Internet Data Centers (IDCs), of third-party cloud vendors, or in the other regions of Huawei Cloud.

Constraints

- For details about the Linux and Windows OSs supported by the UniAgent, see **Collection Management Restrictions**.
- To switch from the old UniAgent page to the new one, choose **Settings** > **Collection Settings** > **UniAgent Installation and Configuration** in the navigation tree on the left and click **Go to New Version** in the upper right corner. To go to the **old UniAgent** page, click **Back to old version** in the upper right corner of the **UniAgent Installation and Configuration** page.

Installation Methods

AOM allows you to install UniAgents on hosts in CLI mode.

Table 3-8 Installation mode

Mode	Scenario
CLI	Suitable for initial installation and single-node installation scenarios. Use a remote login tool, such as PuTTY, to log in to the host where the UniAgent is to be installed and manually run the installation command. For details, see: • **Installing UniAgent by Running Command (in Current Region)** • **Installing UniAgent by Running Command (Outside Current Region)**

Installing UniAgent by Running Command (in Current Region)

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 On the displayed page, click **Install UniAgent**.

Step 4 On the **Install UniAgent** page, set parameters to install a UniAgent.

Figure 3-10 Installing a UniAgent

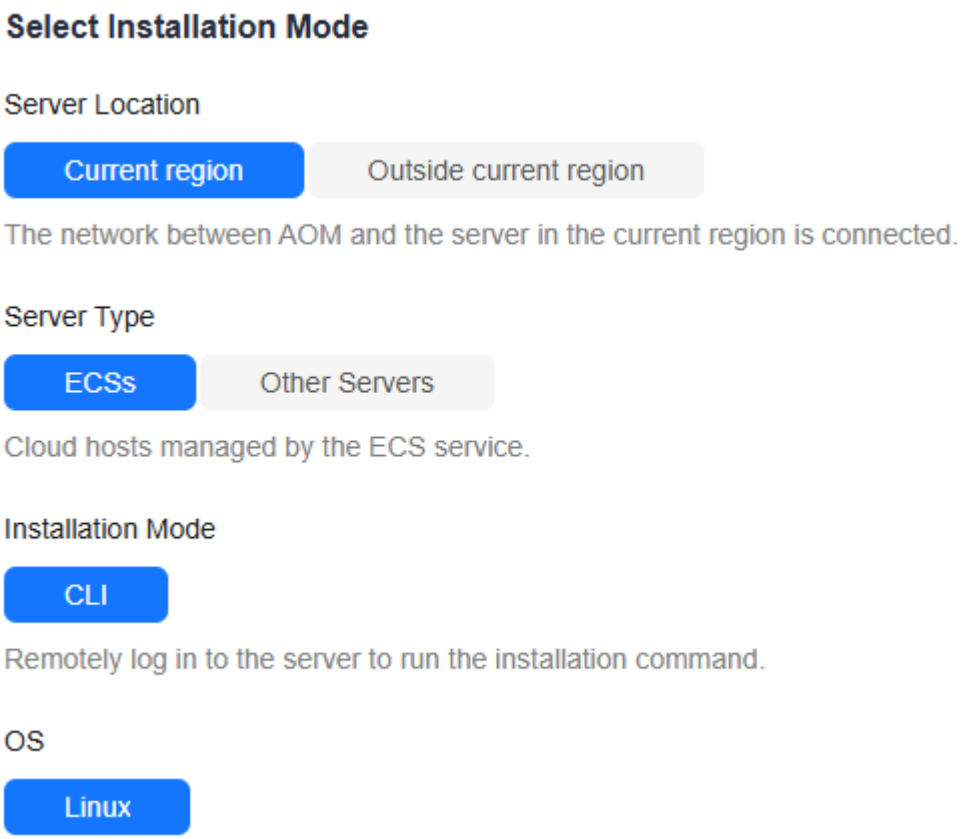


Table 3-9 Installation parameters

Parameter	Description	Example
Server Region	Select the region where the target cloud server is located. Options: • **Current region**: The network between AOM and the server in the current region is connected by default. • **Outside current region**: The cloud server is in a different region from AOM. Select a network connection solution based on site requirements.	Current region
Server Type	Options: • **ECSs**: hosts managed by the ECS service. • **Other servers**: other hosts.	ECSs
Installation Mode	Option: **CLI**. You need to remotely log in to the server to run the installation command provided on the console.	CLI
OS	Option: **Linux**.	Linux

Parameter	Description	Example
UniAgent Version	Select a UniAgent version. The latest version is selected by default.	Latest Version

Copy and Run Installation Command	1. Click **Copy** to copy the installation command.
	`set +o history;`
	`curl -k -X GET -m 20 --retry 1 --retry-delay 10 -o /tmp/install_uniagent https://aom-uniagent-**********.com/install_uniagent.sh;bash /tmp/install_uniagent -p ********** -y **********`
	`set -o history;`
	2. Use a remote login tool, such as PuTTY, to log in to the server and run the copied installation command as user **root**.
		Copy and run the installation (Linux) command.

Step 5 **Check the UniAgent status** in the UniAgent list.

----End

Installing UniAgent by Running Command (Outside Current Region)

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 On the displayed page, click **Install UniAgent**.

Step 4 On the **Install UniAgent** page, set parameters to install a UniAgent.

Figure 3-11 Installing a UniAgent

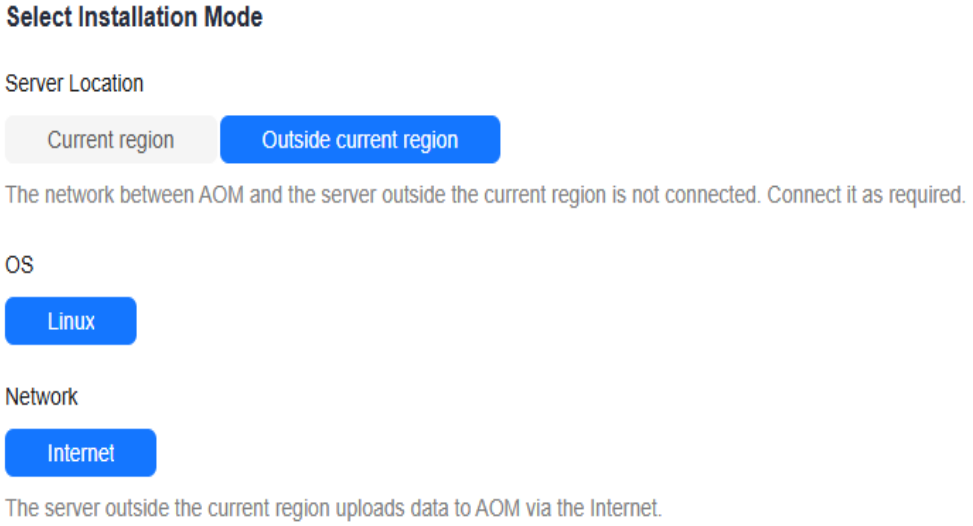


Table 3-10 Installation parameters

Parameter	Description	Example
Server Region	Select the region where the target cloud server is located. Options: • **Current region**: The network between AOM and the server in the current region is connected by default. • **Outside current region**: The cloud server is in a different region from AOM. Select a network connection solution based on site requirements.	Outside current region
OS	Option: **Linux**.	Linux
Network	Option: **Internet**. After a server outside the current region is connected to Internet, it can communicate with AOM.	Internet

Copy and Run Installation Command	1. Click **Copy** to copy the installation command.
	`set +o history;`
	`curl -k -X GET -m 20 --retry 1 --retry-delay 10 -o /tmp/install_uniagent https://aom-uniagent-**********.com/install_uniagent.sh;bash /tmp/install_uniagent -o public -p ********** -y **********`
	2. Use a remote login tool, such as PuTTY, to log in to the server and run the copied installation command as user **root**.
		Copy and run the installation (Linux) command.

Step 5 **Check the UniAgent status** in the UniAgent list.

----End

Checking the UniAgent Status

On the **UniAgent Installation and Configuration** page, check the UniAgent status of the target host. For details, see **Table 3-11**.

Table 3-11 UniAgent statuses

Status	Description
Running	The UniAgent is working.
Abnormal	The UniAgent is not working. Contact technical support.
Installing	The UniAgent is being installed. The installation takes about 1 minute to complete.

Status	Description
Installation failed	The UniAgent fails to be installed. Uninstall the UniAgent and then reinstall it. If the installation still fails, contact technical support.
Not installed	The UniAgent has not been installed on the host. For a host where the UniAgent is uninstalled but it is not deleted, the UniAgent is in the **Not installed** state. You can reinstall the UniAgent or delete the host from the list.

After the UniAgent is installed on the host, ports 39338 and 39339 will be enabled to query log levels and collection tasks.

Other Operations

If needed, perform the following operations on the host where the UniAgent has been installed.

Table 3-12 Related operations

Operation	Description
Searching for a host	In the search box above the host list, search for a host by host ID, name, or status.
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.
Sorting hosts	In the table header of the host list, click in each column to sort hosts. indicates the default order, indicates the ascending order, and indicates the descending order.

Troubleshooting

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

3.2.3 Managing UniAgents

After UniAgents are installed, you can reinstall, upgrade, uninstall, or delete them when necessary.

Constraints

- If the host where a UniAgent is installed using the **old method** runs Windows, you need to manually reinstall the UniAgent.
- UniAgents will not be automatically upgraded. Manually upgrade them if needed.
- If the host where a UniAgent is installed using the **old method** runs Windows, you need to manually uninstall the UniAgent.

Reinstalling UniAgents

Reinstall UniAgents when they are in the **Abnormal**, **Installation failed**, or **Not installed** state.

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **UniAgent Installation and Configuration**.

Step 4 Select one or more servers where UniAgents are to be reinstalled and perform the following operations:

- (Old) On the **VM Access** page, choose **UniAgent Batch Operation** > **Reinstall**. On the displayed page, **reinstall UniAgents** as prompted.
- (New) On the **UniAgent Installation and Configuration** page, switch to the **ECS** or **Other** tab page and click **Reinstall**. On the displayed page, **reinstall UniAgents** as prompted.

----End

Upgrading UniAgents

Upgrade your UniAgent to a more reliable, stable new version.

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Settings** > **Collection Settings** > **UniAgent Installation and Configuration**.

Step 3 Select one or more servers where UniAgents are to be upgraded and perform the following operations:

- (Old) On the **VM Access** page, choose **UniAgent Batch Operation** > **Upgrade**. On the displayed page, select the target version and click **OK**.
- (New) On the **UniAgent Installation and Configuration** page, switch to the **ECS** or **Other** tab page and click **Upgrade**. On the displayed page, select the target version and click **OK**.

Wait for about 1 minute until the UniAgent upgrade is complete.

----End

Uninstalling UniAgents

Uninstall UniAgents when necessary.

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Settings** > **Collection Settings** > **UniAgent Installation and Configuration**.

Step 3 Select one or more servers where UniAgents are to be uninstalled and perform the following operations:

- (Old) On the **VM Access** page, choose **UniAgent Batch Operation** > **Uninstall**. On the displayed page, click **OK**.
- (New) On the **UniAgent Installation and Configuration** page, switch to the **ECS** or **Other** tab page and click **Uninstall**. On the displayed page, click **OK**.

You can also log in to the target server as the **root** user and run the following command to uninstall the UniAgent:

bash /usr/local/uniagentd/bin/uninstall_uniagent.sh;

----End

Deleting UniAgents

Delete the UniAgents that are not used or cannot be used according to the following procedure:

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Settings** > **Collection Settings** > **UniAgent Installation and Configuration**.

Step 3 Select one or more servers where UniAgents are to be deleted and perform the following operations:

- (Old) On the **VM Access** page, choose **UniAgent Batch Operation** > **Delete**. On the displayed page, click **OK**.
- (New) On the **UniAgent Installation and Configuration** page, switch to the **Other** tab page and click **Delete**. On the displayed page, click **OK**. (Only the hosts on the **Other** tab page support UniAgent deletion.)

----End

3.2.4 Managing ICAgent Plug-ins for Hosts

AOM will support interconnection with other types of plug-ins. You can install, upgrade, uninstall, start, stop, and restart plug-ins in batches for hosts.

Currently, only ICAgents are supported. An ICAgent is a plug-in for collecting metrics and logs. ICAgent collects data at an interval of 1 minute. This interval cannot be changed.

Managing ICAgent Plug-ins in Batches

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **UniAgent Installation and Configuration**.

Step 4 Select one or more target servers 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 3-13 Plug-in operation parameters

Parameter	Description
Operation	The following batch operations are supported: install, upgrade, uninstall, start, stop, and restart. **If the ICAgent is uninstalled from a server, AOM will not collect metrics from the server. Exercise caution when performing this operation.**
Plug-in	Select the plug-in to be operated. The ICAgent of the latest version can be installed.
AK/SK	Access Key ID/Secret Access Key (AK/SK) to be entered based on your plug-in type and version. For details, see **How Do I Obtain an AK/SK**. **You need to enter an AK/SK only when installing the ICAgent of an earlier version. (If there is no text box for you to enter the AK/SK, the ICAgent of the new version has already been installed.)**

----End

3.2.5 Managing ICAgents in CCE Clusters

AOM allows you to install, upgrade, and uninstall ICAgents on hosts in purchased CCE clusters in batches.

Prerequisites

- You have bought CCE clusters and nodes. For details, see **Buying a CCE Standard/Turbo Cluster** and **Creating a Node**.

Viewing CCE Clusters

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **CCE Access**.

Step 4 Check the connected CCE clusters.

You can enter a keyword in the search box to search for your target cluster.

----End

Managing ICAgents in CCE Clusters

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Collection Settings** > **CCE Access**.

Step 4 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. 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. 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. **(Uninstalling ICAgents will cause some application O&M functions to be unavailable. Exercise caution when performing this operation.)**
  a. 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.

----End

3.2.6 Managing Host Groups

AOM is a unified platform for observability analysis. It does not provide log functions by itself. Instead, it integrates the host group management function of **Log Tank Service (LTS)**. You can perform operations on the AOM 2.0 or LTS console.

To use the host group management function on the AOM 2.0 console, **purchase LTS resources** first.

Table 3-14 Description

Function	Description	AOM 2.0 Console	LTS Console	References
Host group management	Host groups allow you to configure host log ingestion efficiently. You can add multiple hosts to a host group and associate the host group with log ingestion configurations. The ingestion configurations will then be applied to all the hosts in the host group.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane, choose **Settings** > **Collection Settings** > **Host Groups**.	1. Log in to the LTS console. 2. In the navigation pane, choose **Host Management** > **Host Groups**.	**Managing Host Groups**

- To use LTS functions on the AOM console, you need to obtain LTS permissions in advance. For details, see **Permissions**.
- AOM 2.0 also provides a new version of host group management. After you switch to the new access center, the **new host group management** page will be displayed.

3.2.7 (New) Managing Host Groups

Host groups allow you to configure host data ingestion efficiently. You can add multiple hosts to a host group and associate the host group with ingestion configurations. The ingestion configurations will then be applied to all the hosts in the host group. When there is a new host, simply add it to a host group and the host will automatically inherit the log ingestion configurations associated with the host group.

You can create host groups of the IP address and custom identifier types.

- **Host Group Type** set to **IP**: Select hosts of the IP address type and add them to the host group.
- **Host Group Type** set to **Custom Identifier**: You need to create identifiers for each host group and host. Hosts with an identifier will automatically be included in the corresponding host group sharing that identifier.

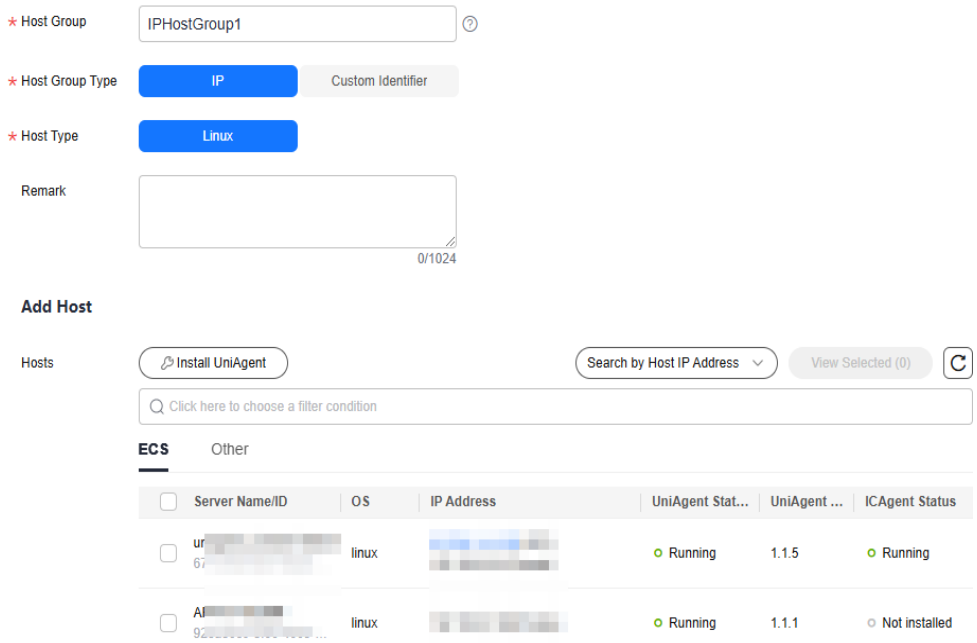
Constraints

To use the new host group management function, switch to the new access center. To go to the **old host group management** page, choose **Access** > **Access Center** in the navigation pane on the left and then click **Back to Old Version** in the upper right corner.

Creating a Host Group (IP Address)

1. Log in to the **AOM 2.0** console.
2. In the navigation pane, choose **Settings** > **Collection Settings** > **Host Groups** and click **Create Host Group** in the upper right corner.
3. In the displayed slide-out panel, enter a host group name, select **IP** for **Host Group Type**, and select a host OS (**Linux**).

   Figure 3-12 Creating an IP address host group



4. In the host list, select one or more hosts to add to the group and click **OK**.
   - You can filter hosts by host name/ID or IP address. You can also click 

     and enter multiple host IP addresses in the displayed search box to search.
   - If your desired hosts are not in the list, click **Install UniAgent**. On the displayed page, install UniAgents on the hosts as prompted. For details, see **2.2.2 (New) Installing UniAgents**.
   - When the selected hosts do not have UniAgent installed but have an earlier version of ICAgent installed, an upgrade prompt appears. To enable automatic UniAgent installation later, click **Upgrade** to first upgrade ICAgent to the latest version.
   - If the selected hosts do not have both UniAgent and ICAgent installed (either UniAgent or ICAgent is in the **Not installed** state), click **OK**. A dialog box will pop up, indicating the missing UniAgent or ICAgent and the number of hosts without UniAgent or ICAgent installed.
     - When selecting an ECS, click **OK** in the dialog box. The system will then issue a task for automatically installing either UniAgent or ICAgent. Otherwise, the host cannot be added to the host group.

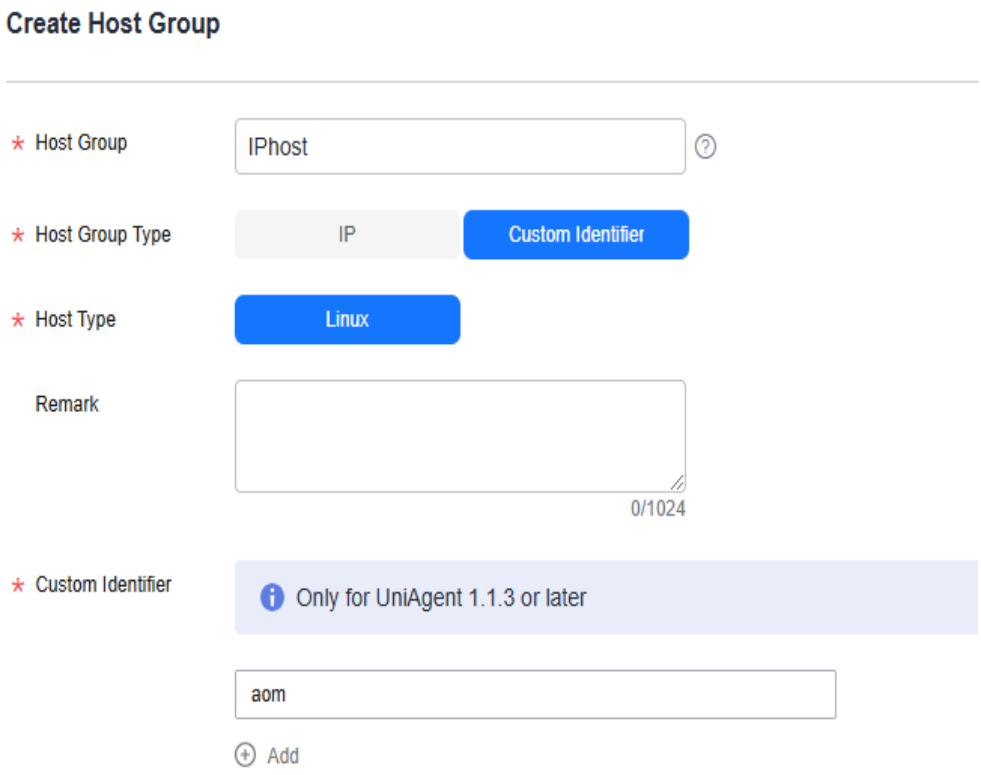
- When selecting a host of the **Other** type, manually install UniAgent and ICAgent first. Otherwise, the host cannot be added to the host group. For details, see **2.2.2 (New) Installing UniAgents**.

– Click  in the upper right corner of the host list to manually refresh the list.

Creating a Host Group (Custom Identifier)

1. Log in to the **AOM 2.0** console.
2. In the navigation pane, choose **Settings** > **Collection Settings** > **Host Groups** and click **Create Host Group** in the upper right corner.
3. In the displayed slide-out panel, enter a host group name, select **Custom Identifier** for **Host Group Type**, and select a host OS (**Linux**).

   Figure 3-13 Creating a custom identifier host group

4. Click **Add** to add a custom identifier.

   Max.: 128 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. Up to 10 custom identifiers can be added.
5. Click **OK**. After the host group is created, go to **6** to add hosts to it.
6. Log in to the host and perform the following operations as the **root** user to create the **custom_tag** file for storing host tags.

   a. Run the **cd /opt/cloud** command.

- If the **/opt/cloud** directory already exists, navigate to it and run the **mkdir lts** command to create the **lts** directory in it.
- If the **/opt/cloud** directory does not exist, run the **mkdir /opt/cloud/** command to create it, and then run the **mkdir lts** command to create the **lts** directory.

b. Run the **chmod 750 lts** command to modify the permission on the **lts** directory.

c. Run the **touch custom_tag** command in the **lts** directory to create the **custom_tag** file.

d. Run the **chmod 640 custom_tag;vi custom_tag** command to modify the **custom_tag** file permission and open the file.

e. Press **i** to enter the insert mode, enter a custom identifier, press **Esc**, enter **:wq!**, save the modification and exit.

f. Use either of the following methods to add a host to the custom identifier host group:

Table 3-15 Methods

Type	Method 1 (Recommended)	Method 2
Linux host	1. View the host identifier in the **custom_tag** file of the **/opt/cloud/lts** directory on the host. 2. On the host group configuration page, add the host identifier as the custom identifier for the host group to include the host in that group. For example, in the **custom_tag** file of the **/opt/cloud/lts** directory on the host, the identifier of the host is **test1**, and the custom identifier of the host group is set to **test1**. In this way, the host is added to the host group.	1. Configure a custom identifier before creating a host group. 2. Add the custom identifier to the **custom_tag** file in the **/opt/cloud/lts** directory of the host. The host can then be added to the specified host group. For example, if the custom identifier of the host group is set to **test** during host group creation, enter **test** in the **custom_tag** file to add the host to the host group. **If multiple custom identifiers are added, enter any custom identifier in the custom_tag file of the /opt/cloud/lts directory on the host to add the host to the host group.**

Other Operations

You can change a created host group, add hosts to or remove hosts from a host group, or associate a host group with log ingestion configurations.

Table 3-16 Operations on host groups

Operation	Procedure
Changing a host group	1. Locate the target host group and click in the **Operation** column. 2. On the displayed dialog box, modify the information such as the host group name, custom identifier, and remark. 3. Click **OK**.
Adding hosts to a host group	1. Click next to the target IP address host group. 2. Click **Add Host**. 3. In the displayed slide-out panel, all hosts that are not in the host group and run the selected OS type are displayed. Select the hosts to be added to the host group. • You can filter hosts by host name/ID or IP address. You can also click Search by Host IP Address and enter multiple host IP addresses in the displayed search box to search. • If your desired hosts are not in the list, click **Install UniAgent**. On the displayed page, install UniAgents on the hosts as prompted. For details, see **2.2.2 (New) Installing UniAgents**. 4. Click **OK**. **This operation is not supported for hosts in a custom identifier host group. To add hosts to a custom identifier host group, refer to 6.**
Removing a host from a host group	1. Click next to the target IP address host group. 2. Locate the target host and click **Remove** in the **Operation** column. 3. In the displayed dialog box, click **OK**. **This operation is not supported for hosts in a custom identifier host group.**
Removing hosts in batches	1. Locate the target host group and click next to it. 2. Select the target hosts and click **Remove** above the list. 3. Click **OK**. **This operation is not supported for hosts in a custom identifier host group.**
Viewing log ingestion rules	1. Locate the target host group and click next to it. 2. Click the **Associated Ingestion Configurations** tab to view the log ingestion rules configured for the host group. For how to configure log ingestion rules for the host group, see **3.9 Managing Metric and Log Ingestion**.

Operation	Procedure
Viewing metric access rules	1. Locate the target host group and click next to it. 2. Click the **Metric Access Rules** tab to view the metric access rules configured for the host group. For how to configure metric ingestion rules for the host group, see **3.9 Managing Metric and Log Ingestion**.
Associating a host group with an ingestion configuration	1. Locate the target host group and click next to it. 2. Click the **Associated Ingestion Configurations** tab and then click **Associate**. 3. In the displayed slide-out panel, select the target ingestion configuration. 4. Click **OK**. The associated ingestion configuration is displayed in the list.
Disassociating a host group from an ingestion configuration	1. Click the **Associated Ingestion Configurations** tab, locate the target ingestion configuration, and then click **Disassociate** in the **Operation** column. 2. Click **OK**.
Disassociating a host group from multiple ingestion configurations	1. Click the **Associated Ingestion Configurations** tab, select target ingestion configurations, and then click **Disassociate** above the list. 2. Click **OK**.
Copying host group information	Hover your cursor over a host group name to copy a host group ID.
Deleting a host group	1. Locate the target host group and click in the **Operation** column. 2. In the displayed dialog box, click **OK**.
Deleting host groups in batches	1. Select multiple host groups to be deleted and click **Delete** above the list. 2. In the displayed dialog box, click **OK**.

Operation	Procedure
Managing tags	Tag log groups as required. 1. Locate the target host group and click in the **Operation** column. 2. On the displayed page, enter a tag key and value. Precautions: • To add more tags, repeat the preceding step. • To delete a tag, locate the target host group and click  in the **Operation** column. On the displayed page, locate the target tag and click  in the **Operation** column. • A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters. • A tag key must be unique.

3.2.8 Configuring a Proxy Area and Proxy

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 is used to manage proxies by category. It consists of multiple proxies.

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 tree on the left, choose **Collection Settings** > **Proxy Areas**. The **Proxy Areas** page is displayed.

Step 4 Click **Add Proxy Area** and set proxy area parameters.

Table 3-17 Proxy area parameters

Parameter	Description	Example
Proxy Area Name	Name of a proxy area. Max.: 64	test
Network Type	Options: **Inner** and **Public**. The default value is **Inner**.	Inner

Step 5 Click **OK** to add a proxy area.

Step 6 Locate the new proxy area, click **Add Proxy**, and set proxy parameters.

Table 3-18 Proxy parameters

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 7 Click **OK**. The proxy is added.

After configuring the proxy area and proxy, perform the following operations if needed:

Table 3-19 Managing the proxy area and proxy

Operation	Description
Searching for a proxy area	Click  next to **Add Proxy Area**. Then, in the search box, enter a keyword to search for your target proxy area.
Modifying a proxy area	Hover the pointer over a proxy area and choose > **Edit**. In the dialog box that is displayed, enter a new name, select a network type, and click **OK**.
Deleting a proxy area	Hover the pointer over a proxy area and choose > **Delete**. In the dialog box that is displayed, click **Yes** to delete the proxy area.
Checking a proxy	Click a proxy area to check the proxy in it.
Modifying a proxy IP address	Click **Modify Proxy IP** in the **Operation** column of the proxy. On the page that is displayed, modify the proxy IP address.
Deleting a proxy	Click **Delete** in the **Operation** column of the proxy. In the displayed dialog box, click **OK** to delete the proxy.

----End

3.2.9 Checking Operation Logs

AOM records operation logs of tasks such as installation, upgrade, and uninstall related to UniAgent and other plug-ins. You can check the operation logs of related tasks.

Checking Operation Logs of UniAgent

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation tree on the left, choose **Collection Settings** > **Operation Logs**. On the displayed page, click the **UniAgent Logs** tab.

Step 4 Set criteria to search for historical tasks.

- Filter data by executor name.
- Filter historical tasks by date. Options: **Last hour**, **Last 6 hours**, **Last day**, **Last 3 days**, and **Custom**. You can query historical tasks of half a year at most.

Step 5 Click a task ID. On the task details page that is displayed, click **View Log** to view UniAgent operation logs.

----End

Viewing Operation Logs of Plug-ins

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation tree on the left, choose **Collection Settings** > **Operation Logs**. On the displayed page, click the **Plug-in Logs** tab.

Step 4 Set criteria to search for historical tasks.

- Filter data by executor name.
- Filter historical tasks by date. Options: **Last hour**, **Last 6 hours**, **Last day**, **Last 3 days**, and **Custom**. You can query historical tasks of half a year at most.

Step 5 Click a task ID. On the task details page that is displayed, click **View Log** in the **Operation** column to view plug-in operation logs.

----End

Other Operations

On the **Operation Logs** page, perform the operations listed in the following table if needed.

Table 3-20 Related operations

Operation	Description
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.

3.3 Connecting Businesses to AOM

AOM provides a unified entry for observability analysis of Huawei Cloud services. Through the access center, you can ingest the traces of applets (such as web & HTML5, Android, iOS, Alipay, DingTalk, and Baidu) into APM, check documents to learn how to ingest business logs into LTS, and extract LTS log data as metrics and ingest the metrics into AOM for unified management.

Connecting the Business Layer to AOM

Step 1 Log in to the **AOM 2.0** console.

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

If the old Access Center is displayed, click **Experience the new version** in the upper right corner.

Step 3 Select the check box next to **Businesses** under **Types** to filter out business cards.

Step 4 Click **Ingest Trace (APM)**, **Ingest Metric (AOM)**, and **Ingest Log (LTS) Details** on the card to quickly ingest traces, configure log metric ingestion rules, and check documents related to log ingestion, respectively.

- **Ingest Log (LTS) Details**: AOM provides an entry for ingesting business logs to LTS. By clicking **Ingest Log (LTS) Details**, you can check the documents related to log ingestion. You can ingest logs according to the documents.
- **Ingest Trace (APM)**: AOM provides an entry for ingesting business traces to APM. By clicking **Ingest Trace (APM)**, you can quickly ingest business traces.
- **Ingest Metric (AOM)**: AOM extracts log data reported to LTS as metrics for unified management. You can click **Ingest Metric (AOM)** on the **Business Monitoring (Log-based)** card to quickly create log metric ingestion rules and extract log data reported to LTS as metrics for unified management.

Table 3-21 Connecting businesses to AOM

Card	Related Operation
Web & H5	Obtain metrics, traces, and logs for web & HTML5 apps.
Android App	Obtain metrics, traces, and logs for Android apps.
iOS App	Obtain metrics, traces, and logs for iOS apps.
WeChat	Obtain metrics, traces, and logs of WeChat.
Alipay	Obtain metrics, traces, and logs of Alipay.
DingTalk	Obtain metrics, traces, and logs of DingTalk.
Baidu	Obtain metrics, traces, and logs of Baidu.
Quick applets	Obtain metrics, traces, and logs of quick applets.
Business monitoring (log-based)	You can create log metric rules to extract log data reported to LTS as metrics and monitor them on the metric browsing and dashboard pages.

----End

3.4 Connecting Components to AOM

AOM provides a unified entry for observability analysis of Huawei Cloud services. Through the access center, you can ingest the traces of components such as Java, Go, Python, Node.js, PHP, .NET, and C++ into APM. You can also check documents to learn how to ingest component logs into LTS.

Procedure

Step 1 Log in to the **AOM 2.0** console.

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

If the old Access Center is displayed, click **Experience the new version** in the upper right corner.

Step 3 Select the check box next to **Components** under **Types** to filter out component cards.

Step 4 Click **Ingest Log (LTS) Details** to learn how to ingest logs or click **Ingest Trace (APM)** to quickly ingest traces.

- **Ingest Log (LTS) Details**: AOM provides an entry for ingesting component logs to LTS. By clicking **Ingest Log (LTS) Details**, you can check the documents related to log ingestion. You can ingest logs according to the documents.
- **Ingest Trace (APM)**: AOM provides an entry for ingesting component traces to APM. By clicking **Ingest Trace (APM)**, you can quickly ingest component traces.

Table 3-22 Connecting components to AOM

Card	Related Operation
Java component	Obtain metrics, traces, and logs for Java applications. For details, see **Ingesting Traces of Java Components (APM)**.

----End

3.5 Connecting Middleware to AOM

3.5.1 Overview About Middleware Connection to AOM

AOM provides a unified entry for observability analysis of Huawei Cloud services. Through the access center, you can ingest the metrics of self-built middleware such as MySQL, Redis, and Kafka into AOM, and check documents related to log ingestion.

Procedure

Step 1 Log in to the **AOM 2.0** console.

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

If the old Access Center is displayed, click **Experience the new version** in the upper right corner.

Step 3 Select **Self-built middleware** under **Types** to filter out your target middleware card.

Step 4 Click **Ingest Metric (AOM)** to quickly ingest middleware metrics to AOM or click **Ingest Log (LTS) Details** to check documents related to log ingestion.

- **Ingest Metric (AOM)**: AOM enables quick installation and configuration for **self-built middleware**. By creating collection tasks and executing plug-in scripts, Prometheus monitoring can monitor reported middleware metrics. It works with AOM and open-source Grafana to provide one-stop, comprehensive monitoring, helping you quickly detect and locate faults and reduce their impact on services. For details about the metrics that can be monitored by AOM, see **open-source Exporters**.

  To quickly ingest middleware metrics to AOM, perform the following steps:

  a. Install UniAgent on your VM for installing Exporters and creating collection tasks. For details, see **3.2.1 Installing UniAgents**.

  b. Create a Prometheus instance for ECS and associate it with a collection task to mark and categorize collected data. For details, see **9.2 Managing Prometheus Instances**.

  c. Connect middleware to AOM. For details, see **3.5.2 Ingesting MySQL Metrics to AOM**.

  d. After middleware is connected to AOM, their metrics can be reported to AOM. You can go to the **Metric Browsing** page to query metrics.

- **Ingest Log (LTS)**: AOM provides an entry for ingesting middleware logs to LTS. By clicking **Ingest Log (LTS) Details**, you can check the documents related to log ingestion. You can ingest logs according to the documents.

Table 3-23 Connecting self-built middleware to AOM

Card	Related Operation
MySQL	A stable, efficient relational database for heavy data volumes. Used for website and application development. For details, see **Ingesting MySQL Metrics to AOM**.
Redis	In-memory storage system for multiple data structure types. Used as a database, cache, and message broker. For details, see **Ingesting Redis Metrics to AOM**.
Kafka	Distributed stream processing platform with high throughput and low latency. Used for real-time data processing and log aggregation. For details, see **Ingesting Kafka Metrics to AOM**.
Nginx	A high-performance HTTP/reverse proxy server for 50,000 concurrent requests. Reduces memory consumption. For details, see **Ingesting Nginx Metrics to AOM**.
MongoDB	High-performance, open-source NoSQL database for document storage and flexible data models. For details, see **Ingesting MongoDB Metrics to AOM**.
Consul	Open-source distributed service discovery and configuration management, supporting multiple data centers and strong consistency. For details, see **Ingesting Consul Metrics to AOM**.
HAProxy	High-performance TCP/HTTP reverse proxy load balancer with high concurrency and flexible configuration for high service availability. For details, see **Ingesting HAProxy Metrics to AOM**.
PostgreSQL	A powerful, open source object-relational database system for complex queries and customization. For details, see **Ingesting PostgreSQL Metrics to AOM**.
Elasticsearch	Distributed full-text search engine with PB-level data storage and real-time retrieval. Used for full-text search, analysis, and monitoring. For details, see **Ingesting Elasticsearch Metrics to AOM**.
RabbitMQ	Collect RabbitMQ monitoring data. For details, see **3.5.11 Ingesting RabbitMQ Metrics to AOM**.
ZooKeeper	Distributed coordination service with leader election, configuration management, and distributed locks to ensure data consistency.

Card	Related Operation
IIS	Internet Information Services (IIS) is a part of Windows Server and provides web applications and services such as HTML, ASP.NET, and PHP for clients on networks. It supports protocols such as HTTP and provides high performance, stability, and scalability.
DNS	Translates domain names into IP addresses and supports load balancing to speed up network access.
Flink	Distributed real-time compute engine with bounded and unbounded data streams processing, efficient memory performance, and exactly-once semantics.

----End

3.5.2 Ingesting MySQL Metrics to AOM

Create a collection task and install MySQL Exporter to monitor MySQL metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **MySQL** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **MySQL** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **MySQL** card.

Step 3 On the displayed page, set parameters by referring to the following table.

Figure 3-14 Configuring a collection task

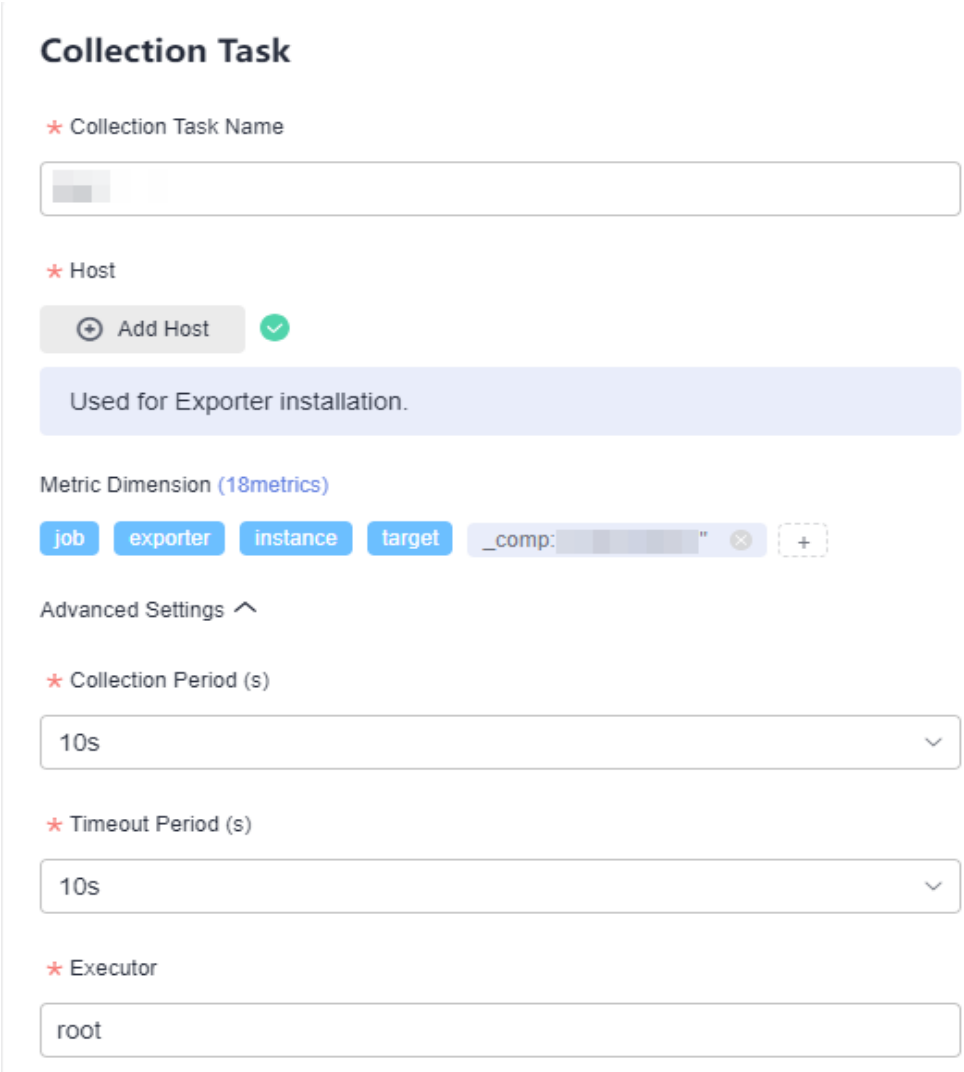


Table 3-24 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, **create one**.
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is **MYSQL**.

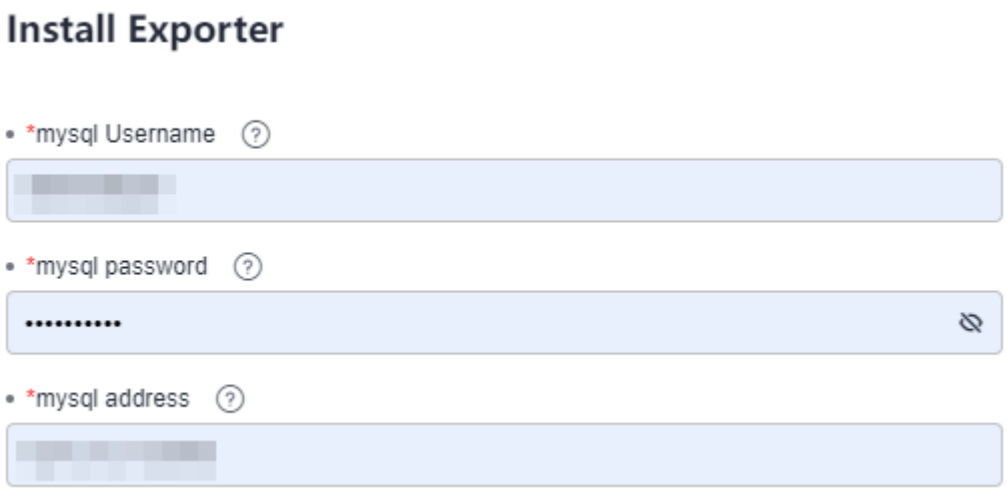
Operation	Parameter	Description
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

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

Figure 3-15 Installing Exporter



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

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

----End

3.5.3 Ingesting Redis Metrics to AOM

Create a collection task and install Redis Exporter to monitor Redis metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **Redis** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **Redis** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Redis** card.

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

Figure 3-16 Configuring a collection task

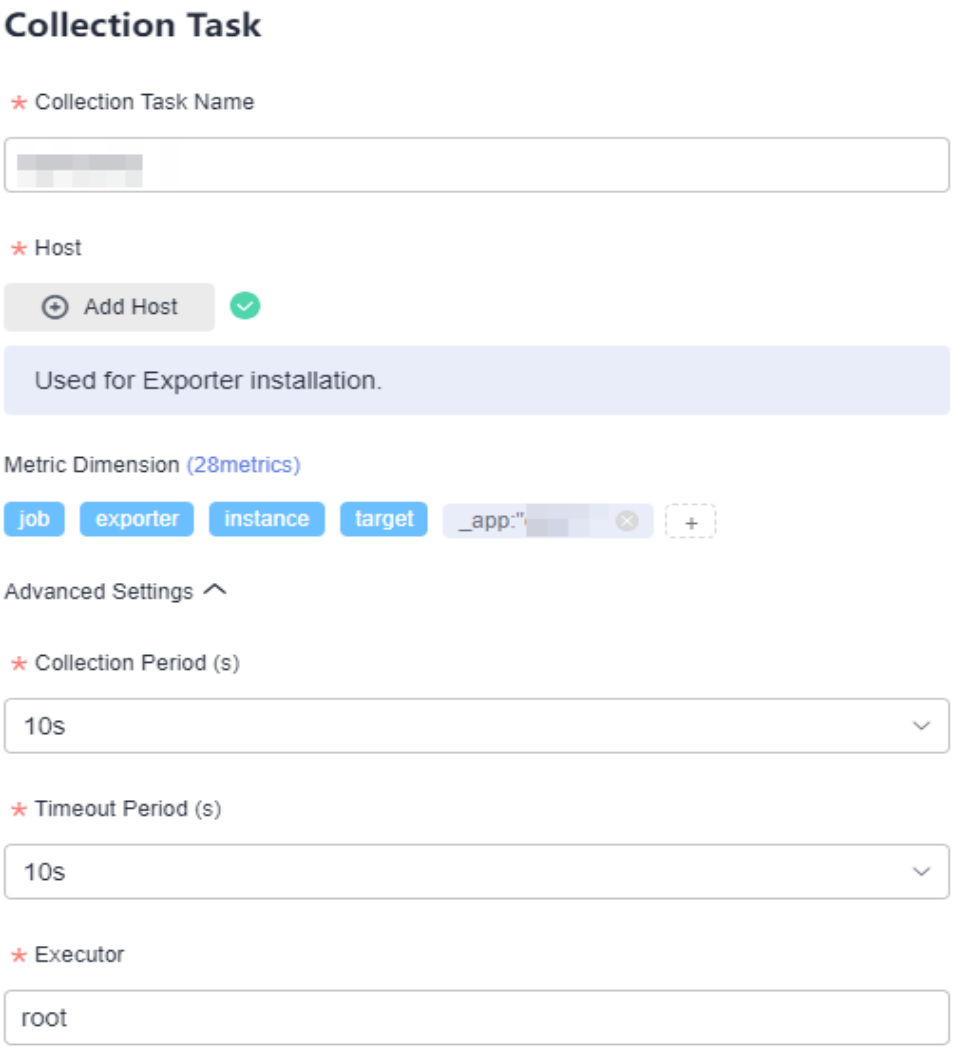


Table 3-25 Parameters for configuring a collection task

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. Only Linux is supported.
	Collection Plug-in	The default value is **REDIS**.

Operation	Parameter	Description
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

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

Figure 3-17 Installing Exporter

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

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

----End

3.5.4 Ingesting Kafka Metrics to AOM

Create a collection task and install Kafka Exporter to monitor Kafka metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **Kafka** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **Kafka** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Kafka** card.

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

Figure 3-18 Configuring a collection task

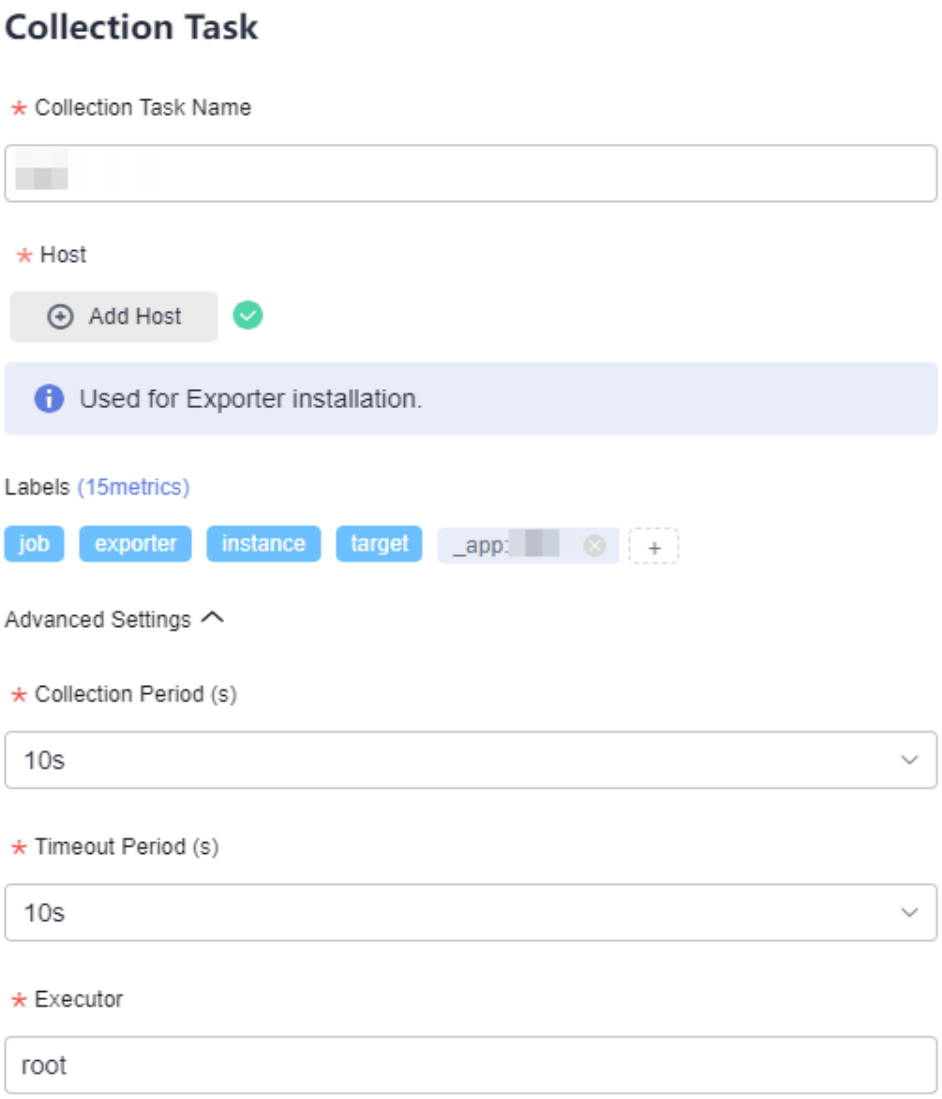


Table 3-26 Parameters for configuring a collection task

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. Only Linux is supported.
	Collection Plug-in	The default value is **KAFKA**.

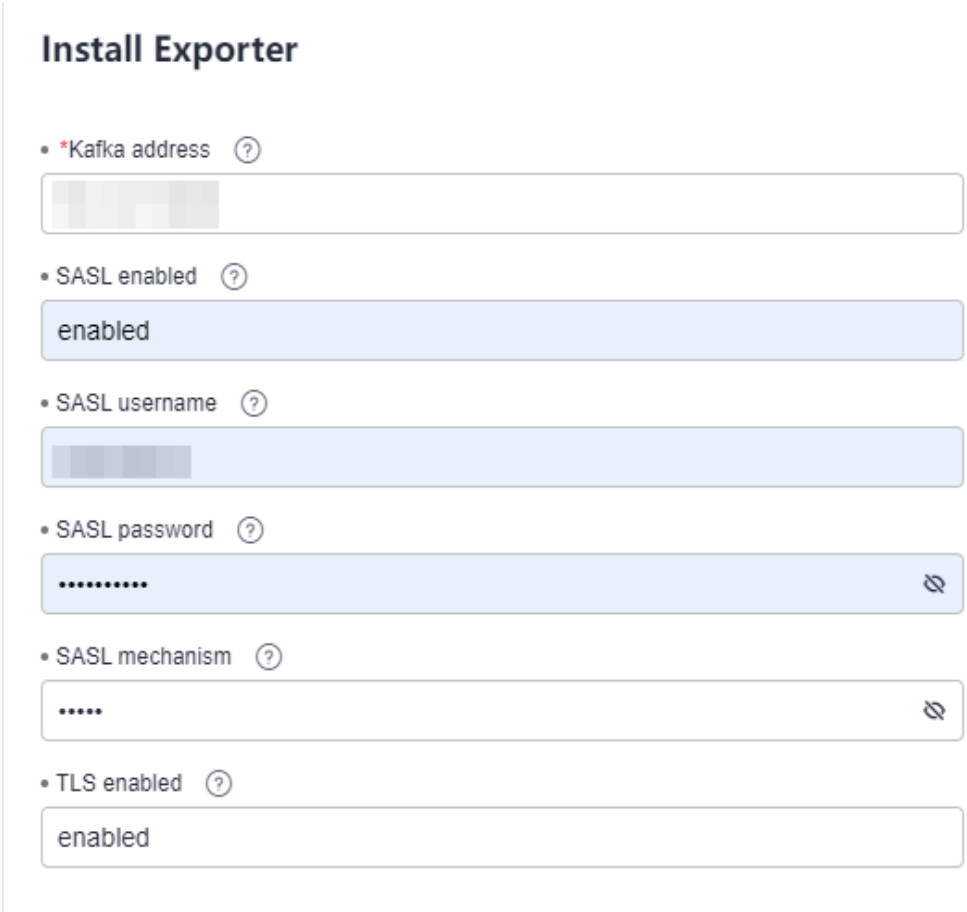
Operation	Parameter	Description
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

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

Figure 3-19 Installing Exporter



Parameter	Description
Kafka address	IP address and port number of Kafka, for example, **10.0.0.1:3306**.
SASL enabled	Whether to enable Simple Authentication and Security Layer (SASL). • **enabled**: Enable SASL. If ciphertext access has been enabled for Kafka instances, enable SASL. • **disabled**: Disable SASL. If plaintext access has been enabled for Kafka instances, disable SASL. The default value is **disabled**.
SASL username	SASL username.
SASL password	SASL password.
SASL mechanism	Enter an SASL mechanism. Options: **plain**, **scram-sha512**, and **scram-sha256**. By default, this parameter is left blank.
TLS enabled	Whether to enable Transport Layer Security (TLS) verification. • **enabled**: Enable TLS. If ciphertext access has been enabled for Kafka instances, enable TLS. • **disabled**: Disable TLS. If plaintext access has been enabled for Kafka instances, disable TLS. The default value is **TLS**.

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

----End

3.5.5 Ingesting Nginx Metrics to AOM

Create a collection task and install Nginx Exporter to monitor Nginx metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **Nginx** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **Nginx** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Nginx** card.

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

Figure 3-20 Configuring a collection task

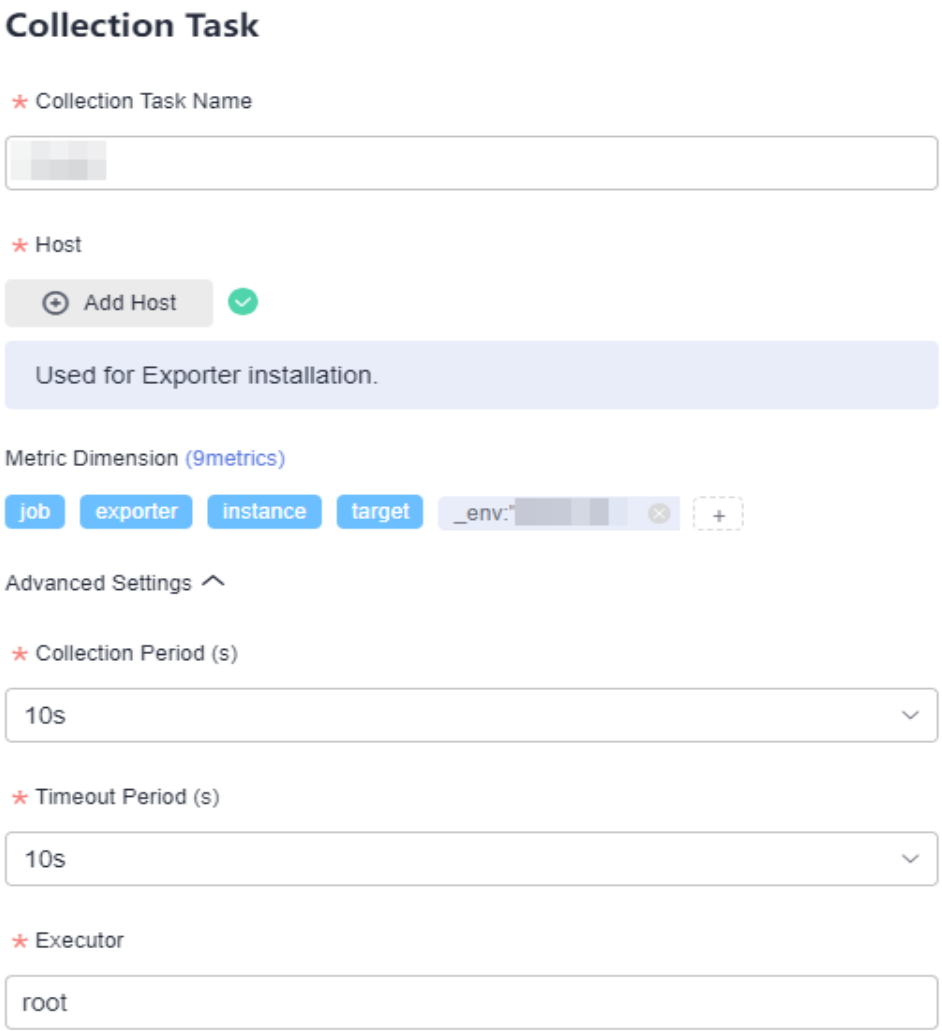


Table 3-27 Parameters for configuring a collection task

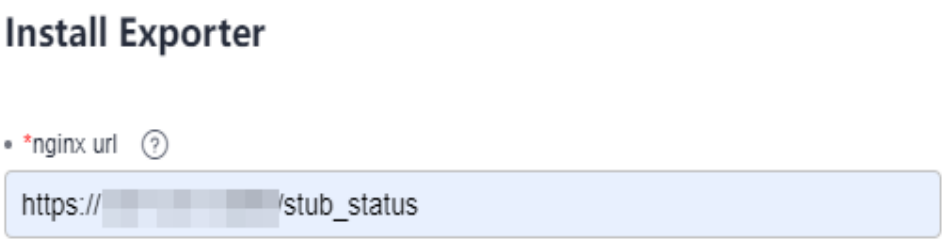
Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, **create one**.
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is **NGINX**.
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. • Search for and select a host by the host name, IP address, or Agent status. • You can click in the upper right corner to deselect the selected host. • Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.

Operation	Parameter	Description
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	● Configure the following parameters: – **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). – **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

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

Figure 3-21 Installing Exporter



Parameter	Description
Nginx URL	Nginx URL, which is in the format of "Connection address of Nginx+Nginx service status path". • Connection address of Nginx: IP address and listening port number of the Nginx service. The listening port is specified in the **nginx.conf** file. Example: **10.0.0.1:8080** • Nginx service status path: specified by the **location** parameter in the **nginx.conf** file, for example, **/stub_status**. Example: **https://10.0.0.1:8080/stub_status**

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

----End

3.5.6 Ingesting MongoDB Metrics to AOM

Create a collection task and install MongoDB Exporter to monitor MongoDB metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **MongoDB** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **MongoDB** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **MongoDB** card.

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

Figure 3-22 Configuring a collection task

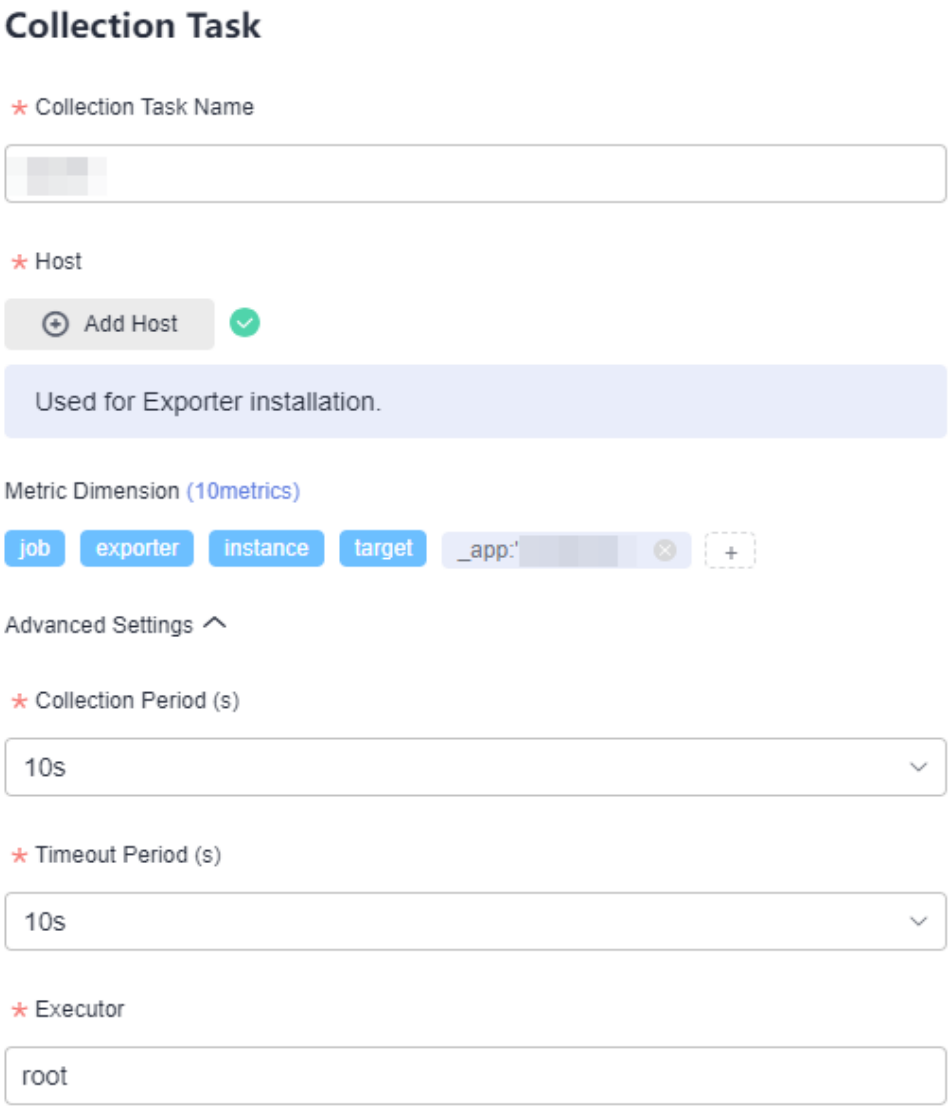


Table 3-28 Parameters for creating a collection task

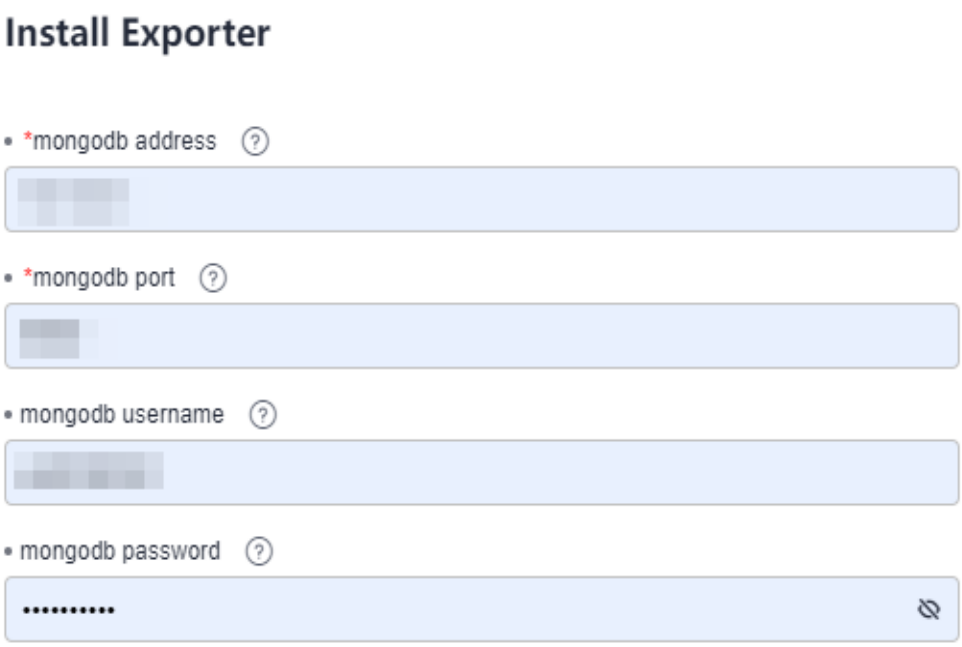
Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, **create one**.
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is **MONGODB**.
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. • Search for and select a host by the host name, IP address, or Agent status. • You can click in the upper right corner to deselect the selected host. • Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.

Operation	Parameter	Description
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: ● **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). ● **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

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

Figure 3-23 Installing Exporter



Parameter	Description
MongoDB address	IP address of MongoDB, for example, **10.0.0.1**.
MongoDB port	Port number of MongoDB, for example, **3306**.
MongoDB username	Username for logging in to MongoDB.
MongoDB password	Password for logging in to MongoDB.

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

----End

3.5.7 Ingesting Consul Metrics to AOM

Create a collection task and install Consul Exporter to monitor Consul metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **Consul** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **Consul** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Consul** card.

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

Figure 3-24 Configuring a collection task

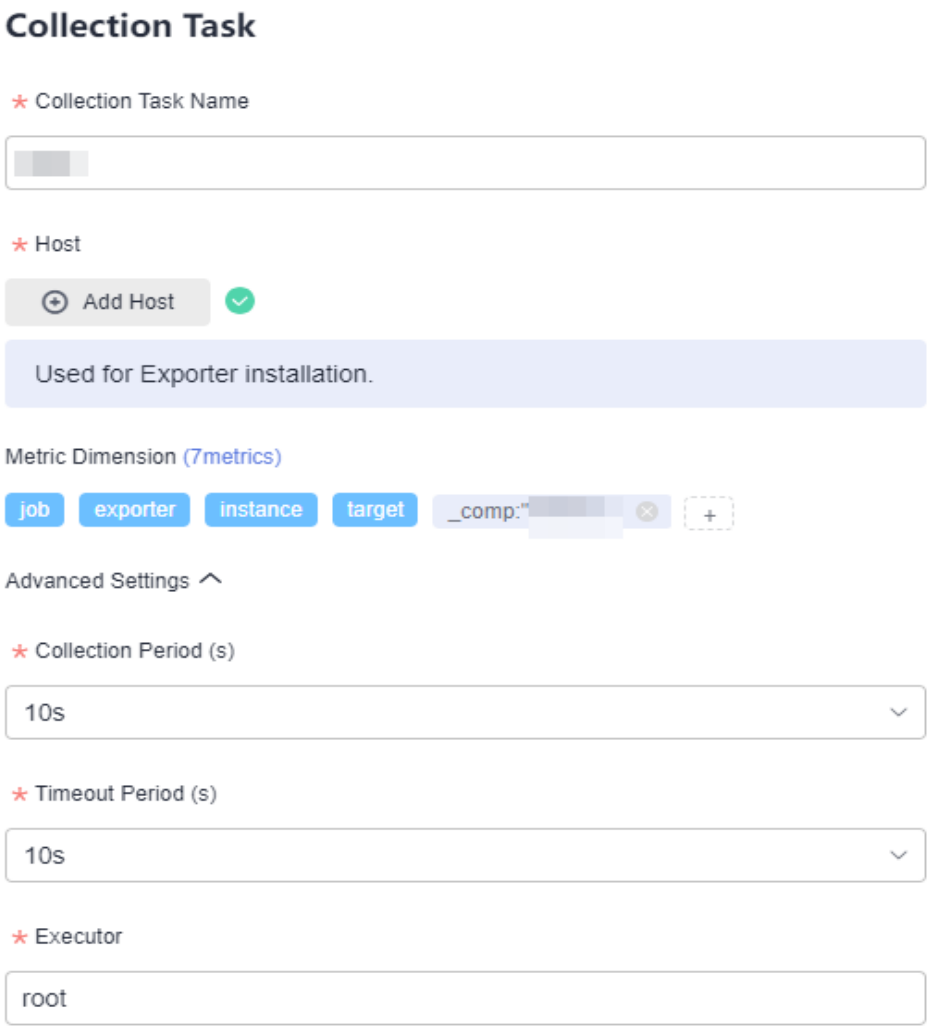


Table 3-29 Parameters for configuring a collection task

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. Only Linux is supported.
	Collection Plug-in	The default value is **CONSUL**.
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. • Search for and select a host by the host name, IP address, or Agent status. • You can click in the upper right corner to deselect the selected host. • Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.

Operation	Parameter	Description
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: ● **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). ● **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

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

Figure 3-25 Installing Exporter

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

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

----End

3.5.8 Ingesting HAProxy Metrics to AOM

Create a collection task and install HAProxy Exporter to monitor HAProxy metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **HAProxy** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **HAProxy** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **HAProxy** card.

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

Figure 3-26 Configuring a collection task

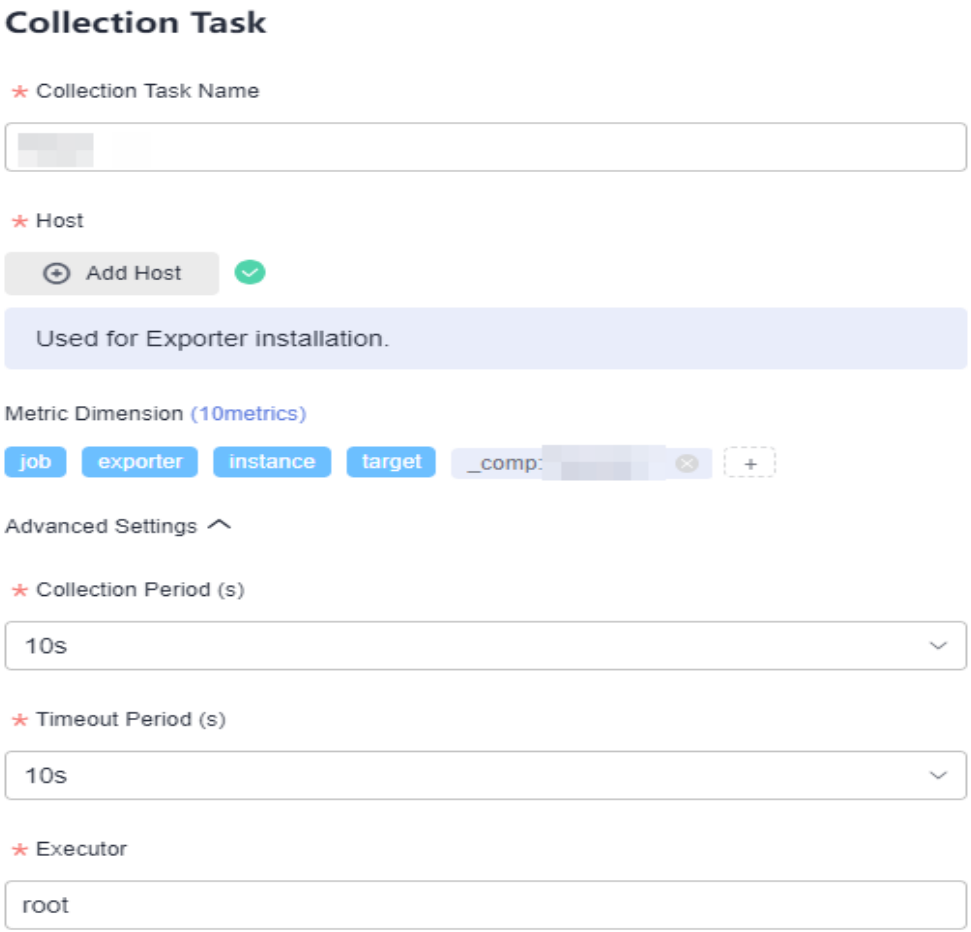


Table 3-30 Parameters for configuring a collection task

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. Only Linux is supported.
	Collection Plug-in	The default value is **HAPROXY**.

Operation	Parameter	Description
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

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

Figure 3-27 Installing Exporter

Parameter	Description
HAProxy URL	HAProxy connection address, which must be in the format of "http://*{username}*:*{password}*@*{IP address}*:*{port}*/haproxy_stats;csv". • *{username}*: username for logging in to HAProxy. • *{password}*: password for logging in to HAProxy. • *{IP}*:*{port}*: HAProxy IP address and port number, for example, **10.0.0.1:3306**. Example: **http://admin:**************@10.0.0.1:3306/haproxy_stats;csv**

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

----End

3.5.9 Ingesting PostgreSQL Metrics to AOM

Create a collection task and install PostgreSQL Exporter to monitor PostgreSQL metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **PostgreSQL** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **PostgreSQL** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **PostgreSQL** card.

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

Figure 3-28 Configuring a collection task

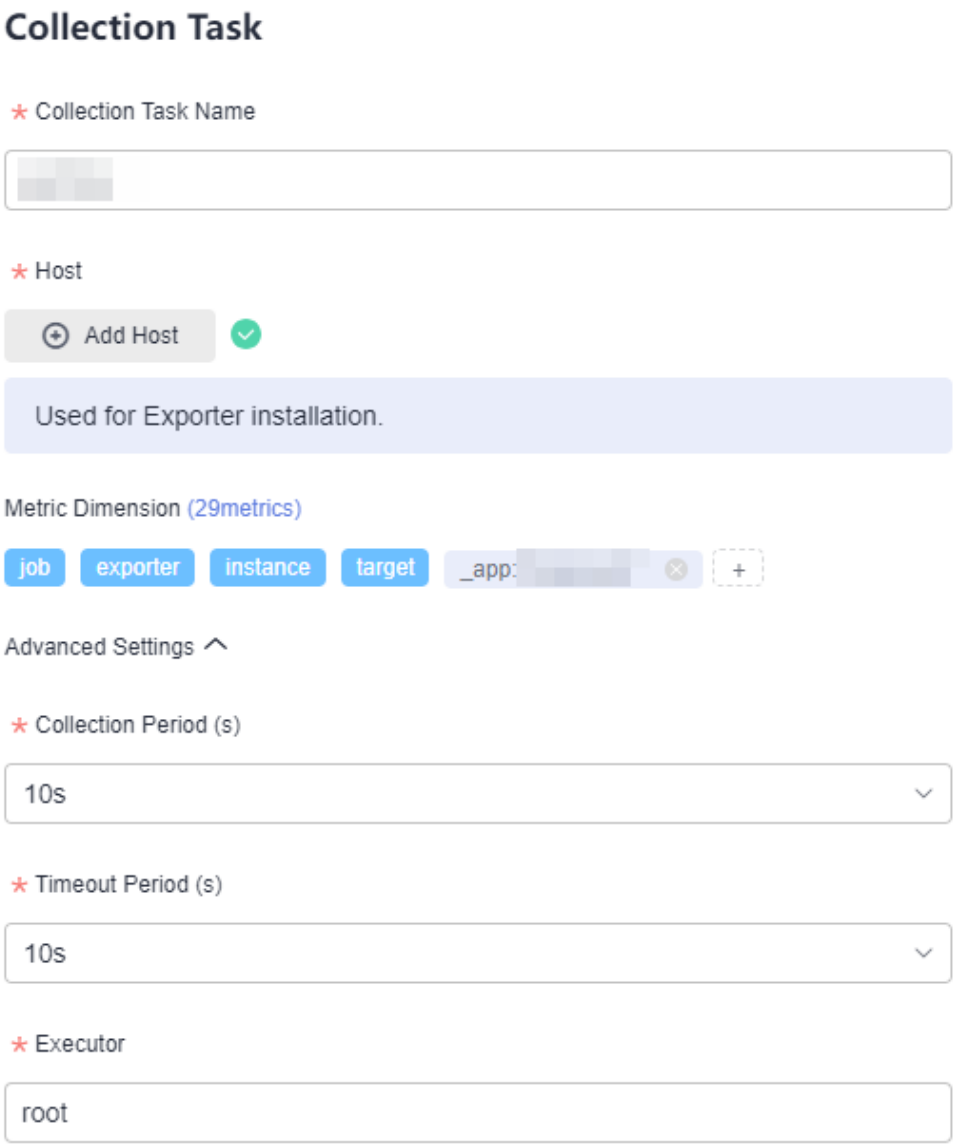


Table 3-31 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, **create one**.
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is **POSTGRESQL**.

Operation	Parameter	Description
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

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

Figure 3-29 Installing Exporter

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

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

----End

3.5.10 Ingesting Elasticsearch Metrics to AOM

Create a collection task and install Elasticsearch Exporter to monitor Elasticsearch metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **Elasticsearch** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **Elasticsearch** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Elasticsearch** card.

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

Figure 3-30 Configuring a collection task

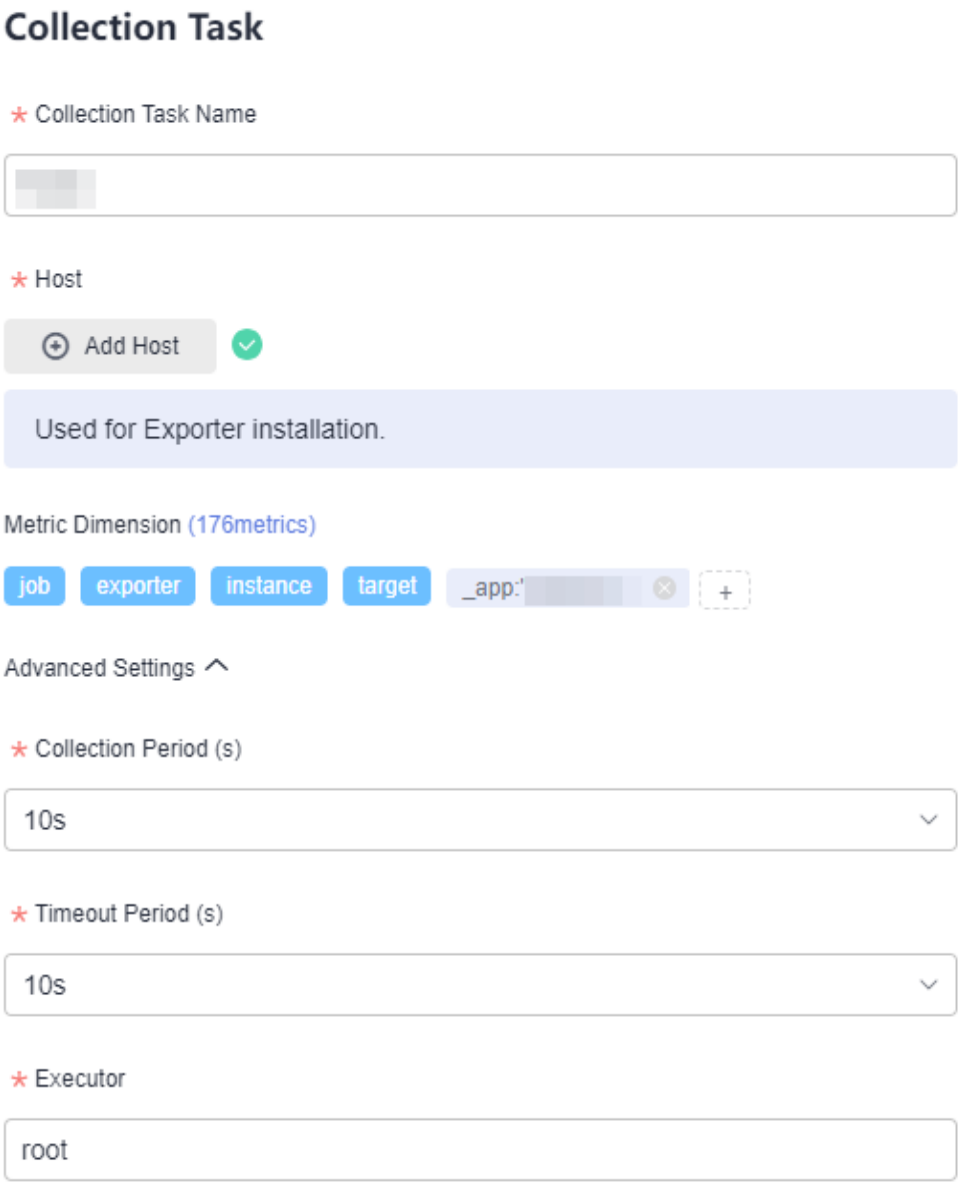


Table 3-32 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, **create one**.
Set Plug-in	OS	Operating system of the host. Only Linux is supported.

Operation	Parameter	Description
	Collection Plug-in	The default value is **ELASTICSEARCH**.
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

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

Figure 3-31 Installing Exporter

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

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

----End

3.5.11 Ingesting RabbitMQ Metrics to AOM

Create a collection task and install RabbitMQ Exporter to monitor RabbitMQ metrics on a host.

Prerequisites

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

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, select either of the following methods to ingest middleware metrics:

- Method 1: Choose **Access** > **Access Center**.

  There are old and new access centers. To switch from the old access center to **the new one**, click **Experience the new version** in the upper right corner of the page.

  - In the old access center, click the **RabbitMQ** card in the **Prometheus Middleware** panel.
  - In the new access center, locate the **RabbitMQ** card under **Self-built middleware** and click **Ingest Metric (AOM)** on the card.
- Method 2: Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **RabbitMQ** card.

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

Figure 3-32 Configuring a collection task

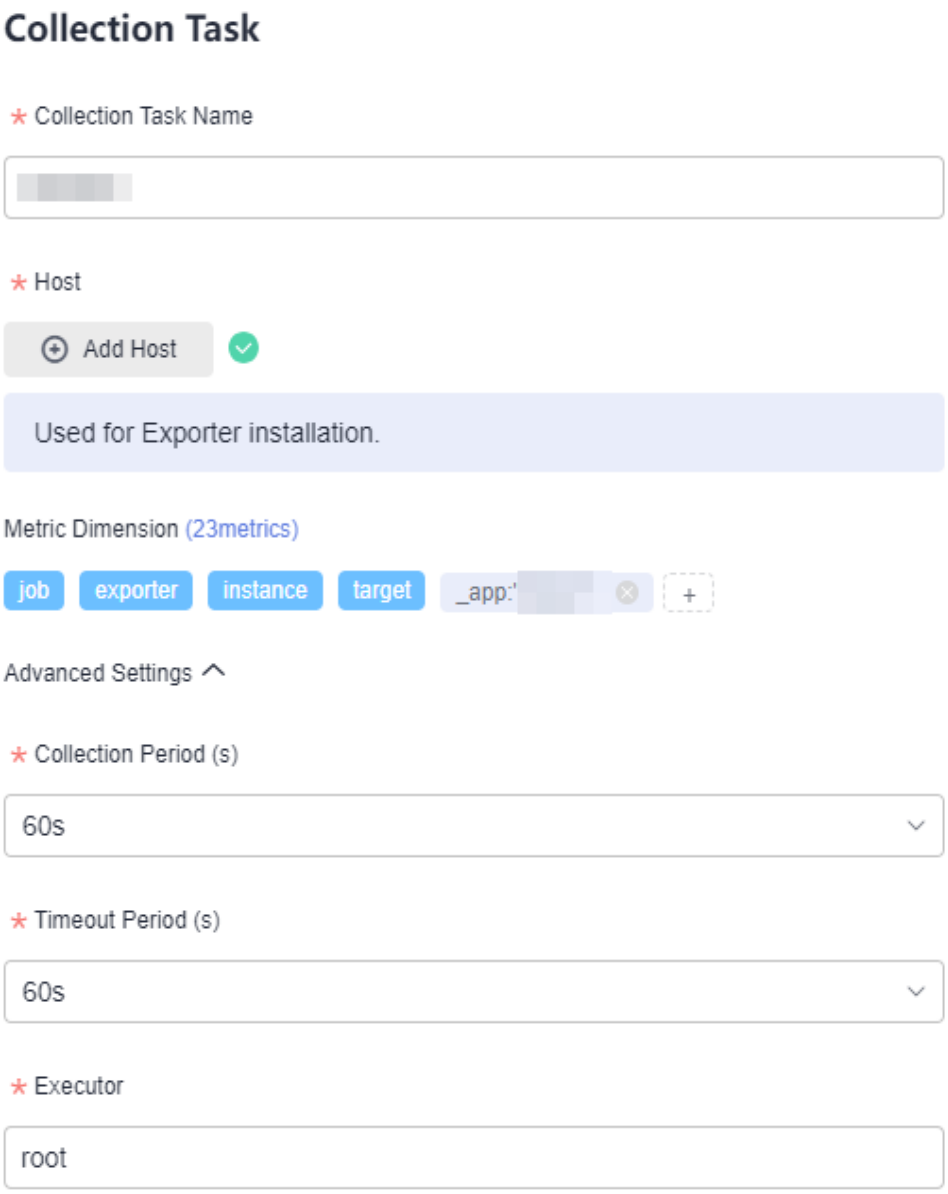


Table 3-33 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, **create one**.
Set Plug-in	OS	Operating system of the host. Only Linux is supported.

Operation	Parameter	Description
	Collection Plug-in	The default value is **RABBITMQ**.
	Plug-in Version	Select a plug-in version. 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 starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click **Add Host**. On the **Add Host** page, select the host for configuring the collection task and installing Exporter. ● Search for and select a host by the host name, IP address, or Agent status. ● You can click in the upper right corner to deselect the selected host. ● Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	Click . In the displayed dialog box, select **Built-in** or **Custom** to add a metric dimension. ● Metric dimension name: – Built-in metric dimensions: **_app**, **_comp**, and **_env** are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. For a host, each metric dimension name must be unique. ● Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: &|><$;'!-() 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	Configure the following parameters: • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time allowed for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). 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 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

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

Figure 3-33 Installing Exporter

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

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

----End

3.5.12 Managing Middleware Collection Tasks

After connecting the middleware to AOM, you can manage the collection tasks created during the connection in the access center.

1. Log in to the **AOM 2.0** console.
2. In the navigation pane on the left, choose **Access** > **Access Center**.

   If the old Access Center is displayed, click **Experience the new version** in the upper right corner.
3. Under **Self-built middleware**, locate the middleware for collection tasks have been configured. Then click **Ingest Metric (AOM)** to go to the details page.
4. On the **Collection Tasks** tab page, manage the collection tasks created for the middleware. Perform the operations listed in the following table if needed.

Table 3-34 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click  in the **Start/Stop** column of a collection task to start or stop it.
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	Click  in the **Operation** column of the target collection task. On the displayed page, change target hosts. You can only change the target hosts for the collection tasks created using custom plug-ins.
Sorting collection tasks	Click in the **Timeout Period** or **Collection Period** column to sort collection tasks. indicates the default order.  indicates the ascending order (that is, the maximum time is displayed at the bottom).  indicates the descending order (that is, the maximum time is displayed at the top).
Copying a collection task	Click  in the **Operation** column of a collection task. On the displayed page, modify parameters as required.

Operation	Description
Modifying a collection task	Choose ••• > **Modify** in the **Operation** column of the target collection task. On the displayed page, modify parameters as required. • Modifying a custom plug-in collection task: The plug-in version and collection task details can be modified. • Modifying a middleware collection task: Only metric dimensions can be modified.
Deleting a collection task	Locate a collection task and choose ••• > **Delete** in the **Operation** column. On the displayed page, confirm the deletion.

3.6 Connecting Running Environments to AOM

AOM provides a unified entry for observability analysis of Huawei Cloud services. Through the access center, you can ingest the metrics of running environments (such as ECS and CCE) to AOM and check documents related to log ingestion.

Procedure

Step 1 Log in to the **AOM 2.0** console.

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

If the old Access Center is displayed, click **Experience the new version** in the upper right corner.

Step 3 Select the check box next to **Running environments** under **Types** to filter out the running environment cards.

Step 4 Click **Ingest Metric (AOM)** to quickly ingest metrics or click **Ingest Log (LTS) Details** to check documents related to log ingestion.

- **Ingest Metric (AOM)**: AOM supports metric ingestion for running environments. By clicking **Ingest Metric (AOM)**, you can quickly ingest metrics of running environments.
- **Ingest Log (LTS) Details**: AOM provides an entry for ingesting logs of running environments to LTS.
  - By clicking **Details** on **Ingest Log (LTS) Details**, you can check the documents related to log ingestion. You can ingest logs according to the documents.
  - By clicking **Ingest Log (LTS)** on **Ingest Log (LTS) Details**, you can quickly ingest logs of running environments.

Table 3-35 Connecting running environments to AOM

Card	Related Operation
Elastic Cloud Server (ECS)	ECS is a cloud server that allows on-demand allocation and elastic computing capability scaling. It helps you build a reliable, secure, flexible, and efficient application environment to ensure that your services can run stably and continuously, improving O&M efficiency. For details, see: • **Ingesting ECS Text Logs to LTS** • **Ingesting ECS Metrics (AOM)**
Bare Metal Server (BMS)	BMS is a high-performance, high-security physical server on the cloud. For details, see **Ingesting BMS Text Logs to LTS**.
Cloud Container Engine (CCE)	CCE is a high-performance, high-reliability service through which enterprises can manage containerized applications. CCE supports native Kubernetes applications and tools, allowing you to easily set up a container runtime environment on the cloud. For details, see: • CCE metric ingestion to AOM: By default, ICAgents are installed on CCE clusters upon your purchase. CCE cluster metrics will be automatically reported to AOM. • **Ingesting CCE Application Logs to LTS**
Cloud Container Instance (CCI)	CCI provides a serverless container engine that eliminates the need to manage clusters or servers. In only three steps, you can create a workload. CCI automatically reports metrics to AOM as ready-to-use data.
Self-Managed Kubernetes Cluster	Kubernetes is an open-source container orchestration system that automates the deployment, scaling, and management of containerized applications, enhancing application reliability and scalability. **Ingesting Self-Built Kubernetes Application Logs to LTS**

----End

Connecting an ECS to AOM

Node Exporter is an open-source metric collection plug-in from Prometheus. It collects different types of data from target jobs and converts them into the time series data supported by Prometheus. Connect an ECS to AOM. Then you can install Node Exporter and configure collection tasks for the host group. The collected metrics will be stored in the Prometheus instance for ECS for easy management.

Constraints

A host supports only one Node Exporter.

Prerequisites

- A Prometheus instance for ECS has been connected for monitoring. For details, see **Creating a Prometheus Instance for ECS**.
- A host group has been created. For details, see **2.2.7 (New) Managing Host Groups**.

Procedure

1. Log in to the **AOM 2.0** console.
2. In the navigation pane, choose **Access** > **Access Center**. Click **Experience the new version** in the upper right corner of the page.
3. Locate the **Elastic Cloud Server (ECS)** card under **Running environments** and click **Ingest Metric (AOM)** on the card.
4. Set parameters for connecting to the ECS.
   a. Select a Prometheus instance.
      i. **Instance Type**: **Prometheus for ECS** is selected by default and cannot be changed.
      ii. **Instance Name**: Select a Prometheus instance from the drop-down list.
      If no Prometheus instance is available, click **Create Instance** to create one.
   b. Select a host group.
      In the host group list, select a target host group.
      - If no host group is available, click **Create Host Group** to create one.
      - You can also perform editing, deletion, and other operations on the host group as needed. For details, see **Other Operations**.

      Collection configurations are delivered by host group. Therefore, it is easy for you to configure data collection for multiple hosts. When there is a new host, simply add it to a host group and the host will automatically inherit the log ingestion configurations associated with the host group.
   c. Configure the collection.
      Under **Configure Collection**, set parameters by referring to the following table.

Table 3-36 Collection configuration

Category	Parameter	Description
Basic Settings	Configuration Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Metric Collection Rule	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: **10**, **30**, and **60** (default).

Category	Parameter	Description
	Metric Collection Timeout (s)	Timeout period for executing a metric collection task, in seconds. Options: **10**, **30**, and **60** (default). **The timeout period cannot exceed the collection interval.**
	Executor	User who executes the metric ingestion rule, that is, the user of the selected host group. Default: **root**.
Other	Custom Dimensions	Dimensions (key-value pairs) added to specify additional metric attributes. You can click **Add Dimension** to add multiple custom dimensions (key-value pairs). • Key: key of the additional attribute of a metric. Enter 1 to 64 characters starting with a letter or underscore (_). Only letters, digits, and underscores are allowed. • Value: corresponds to the key of the additional attribute of a metric. Up to 10 dimensions can be added. Example: Set the key to **app** and value to **abc**.
	Import ECS Tags as Dimensions	Whether to import ECS tags as dimensions. • **Disable**: AOM does not write ECS tags (key-value pairs) into metric dimensions. ECS tag changes (such as addition, deletion, and modification) will not be synchronized to metric dimensions. This function is disabled by default. • **Enable**: AOM writes ECS tags (key-value pairs) into metric dimensions. ECS tag changes (such as addition, deletion, and modification) will be synchronized to metric dimensions.

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

   After connecting to the ECS, perform the following operations if needed:

   - Go to the **Metric Browsing** page to analyze metrics. For details, see **4 Observability Metric Browsing**.
   - Go to the **Access Management** page to view, edit, or delete the configured ingestion rule. For details, see **3.9 Managing Metric and Log Ingestion**.

  - Go to the **Infrastructure Monitoring** > **Host Monitoring** page to view host monitoring information. For details, see **Host Monitoring**.

3.7 Connecting Cloud Services to AOM

AOM provides a unified entry for observability analysis of Huawei Cloud services. Through the access center, you can ingest cloud service metrics into AOM, ingest cloud service logs to LTS, and check documents related to log ingestion.

Prerequisite

A common Prometheus instance has been connected for monitoring. For details, see **Creating a Common Prometheus Instance**.

Constraints

- You can only select common Prometheus instances to collect metrics.
- One common Prometheus instance corresponds to only one metric ingestion rule.
- A common Prometheus instance supports the ingestion of cloud service metrics under different enterprise projects.

Ingesting Cloud Service Metrics and Logs into AOM

Step 1 Log in to the **AOM 2.0** console.

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

If the old Access Center is displayed, click **Experience the new version** in the upper right corner.

Step 3 Select the check box next to **Cloud services** under **Types** to filter out cloud service cards.

Step 4 Click **Ingest Metric (AOM)** to quickly ingest metrics or click **Ingest Log (LTS) Details** to check documents related to log ingestion.

- **Ingest Metric (AOM)**: AOM supports ingestion of cloud service metrics. By clicking **Ingest Metric (AOM)**, you can quickly ingest cloud service metrics.
- **Ingest Log (LTS) Details**: AOM provides an entry for ingesting cloud service logs to LTS. By clicking **Ingest Log (LTS) Details**, you can check the documents related to log ingestion. You can ingest logs according to the documents.
  - By clicking **Details** on **Ingest Log (LTS) Details**, you can check the documents related to log ingestion. You can ingest logs according to the documents.
  - For some cloud services, you can quickly ingest their logs by clicking **Ingest Log (LTS)**.

Table 3-37 Connecting cloud services to AOM

Card	Data Source	Description
Auto Scaling, API Gateway (APIG) (Dedicated), Cloud Bastion Host (CBH), Cloud Backup and Recovery (CBR), CloudTable, Content Delivery Network (CDN), Cloud Search Service (CSS), Direct Connect, Distributed Cache Service (DCS), Document Database Service (DDS), Data Lake Insight (DLI), Distributed Message Service (DMS) for Kafka, Data Replication Service (DRS), Data Warehouse Service (DWS), Elastic Load Balance (ELB), Enterprise Router, Elastic Volume Service (EVS), FunctionGraph, GaussDB(for MySQL), GeminiDB, IoT Device Access (IoTDA), Intelligent EdgeFabric (IEF), ModelArts, MapReduce Service (MRS), NAT Gateway, Object Storage Service (OBS), Relational Database Service (RDS) for MySQL, RDS for PostgreSQL, RDS for SQL Server, LakeFormation, SMN, Scalable File Service (SFS), SFS Turbo, Virtual Private Cloud (VPC), Virtual Private Network (VPN), and Web Application Firewall (WAF)	Metrics	Ingest cloud service metrics, such as the CPU usage, memory usage, and health status. For details, see **Procedure**.

Card	Data Source	Description
AOM, APIG, Astro Zero, Bare Metal Server (BMS), CBH, Cloud Container Engine (CCE), CDN, Cloud Firewall (CFW), Cloud Trace Service (CTS), DCS, DDS, Anti-DDoS Service (AAD), DMS for Kafka, DRS, DWS, Elastic Cloud Server (ECS), ELB, Enterprise Router, FunctionGraph, GaussDB, Graph Engine Service (GES), GaussDB(for MySQL), GeminiDB Redis, GeminiDB Mongo, GeminiDB Cassandra, Huawei HiLens (HiLens), IoTDA, ModelArts, MRS, RDS for MySQL, RDS for PostgreSQL, RDS for SQL Server, ROMA Connect, Live, Simple Message Notification (SMN), SecMaster, ServiceStage-container application logs, ServiceStage-cloud host logs, VPC, and WAF	Logs	LTS collects log data of many cloud services, such as compute, storage, security, and database services. You can use LTS to search for cloud service logs by keyword, analyze operations data, and monitor the running status and alarms. For details, see **Ingesting Cloud Service Logs to LTS**.

----End

Procedure

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the **Filter** area, select **Metrics** and **Cloud services** to filter out the cloud service metrics to be ingested to AOM.

Step 4 Hover the cursor over a cloud service card and click **Ingest Metric (AOM)**.

Step 5 On the **Set Prometheus Instance** area, select a target Prometheus instance from the drop-down list to collect multidimensional metrics.

- **View Instances**: After selecting an instance, you can click **View Instances** to go to the instance details page.
- **Create Instance**: If no Prometheus instance meets your requirements, click **Create Instance** to **create a common Prometheus instance**.

Step 6 Click **Next** to configure an ingestion rule.

Table 3-38 Parameters for configuring an ingestion rule

Parameter	Description
Ingestion Rule Name	Name of a metric ingestion rule. Enter up to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Set Cloud Service Metric	**Ingest Metric**: Select the cloud service metrics to ingest. • Configure metric ingestion for a cloud service: In the cloud service list, toggle the switch in the **Ingest Metric** column. In this way, you can ingest the metrics of a cloud service into AOM or remove them from AOM. • Configure metric ingestion for cloud services in batches: In the cloud service list, select target cloud services, click **Ingest Metric** above the list, and then choose **Enable** or **Disable**. In this way, you can ingest cloud service metrics into AOM or remove metrics from AOM in batches.
	Add Tag to Dimension: Indicates whether to add tags of cloud service resources to metric dimensions. Tag changes are synchronized every hour. **Each tag name must start with a letter or underscore (_). Only letters, digits, and underscores are allowed.** • Configure the function of adding the tags of one cloud service to metric dimensions: In the cloud service list, toggle the switch in the **Add Tag to Dimension** column. In this way, you can add the tags of a cloud service to metric dimensions or remove them. • Configure the function of adding the tags of multiple cloud services to metric dimensions: In the cloud service list, select target cloud services, click **Add Tag to Dimension** above the list, and then choose **Enable** or **Disable**. In this way, you can add the tags of multiple cloud services to metric dimensions or remove them.

Step 7 After the configuration is complete, click **Confirm**.

- Go to the **Metric Browsing** page to analyze metrics. For details, see **4 Observability Metric Browsing**.
- Go to the **Access Management** page to view, edit, or delete the configured ingestion rule. For details, see **3.9 Managing Metric and Log Ingestion**.

----End

3.8 Ingesting Data to AOM Using Open-Source APIs and Protocols

AOM provides a unified entry for observability analysis of Huawei Cloud services. Through the access center, you can ingest metrics into AOM using open-source

APIs and protocols, ingest traces to APM, and check documents related to log ingestion to LTS.

Procedure

Step 1 Log in to the **AOM 2.0** console.

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

If the old Access Center is displayed, click **Experience the new version** in the upper right corner.

Step 3 Select the check box next to **APIs/protocols...** under **Types** to filter out target cards.

Step 4 Click **Ingest Metric (AOM)** or **Ingest Trace (APM)** to quickly ingest metrics or traces, or click **Ingest Log (LTS) Details** to ingest logs or check documents related to log ingestion.

- **Ingest Metric (AOM)**: AOM supports metric ingestion using open-source APIs and protocols. By clicking **Ingest Metric (AOM)**, you can quickly ingest metrics using open-source APIs and protocols.
- **Ingest Trace (APM)**: AOM provides an entry for ingesting traces to APM using open-source APIs and protocols. By clicking **Ingest Trace (AOM)**, you can quickly ingest traces using open-source APIs and protocols.
- **Ingest Log (LTS) Details**: AOM provides an entry for ingesting logs to LTS using open-source APIs and protocols.
  - By clicking **Details** on **Ingest Log (LTS) Details**, you can check documents related to log ingestion. You can ingest logs according to the documents.
  - For some components, you can quickly ingest their logs by clicking **Ingest Log (LTS)**. For example, the **Cross-Account Ingestion - Log Stream Mapping** card.

Table 3-39 Ingesting metrics using open-source APIs and protocols

Card	Related Operation
AOM APIs	Use the open APIs of AOM to report metric data. For details, see **Using APIs to Ingest Metrics to AOM**.
LTS APIs	Use the open APIs of LTS to report log data. For details, see **Using APIs to Ingest Logs to LTS**.
APM APIs	Use the open APIs of APM to report application performance monitoring data. For details, see **Using APIs to Ingest Traces to APM**.
Common Prometheus Instance	Suitable for customers who have self-built Prometheus servers, but need Prometheus storage availability and scalability through remote write. For details, see **Connecting Common Prometheus Instances (AOM)**.

Card	Related Operation
Kafka Protocol	TCP-based binary protocol used by Kafka (a high-throughput, distributed message system). For details, see **Using Kafka to Report Logs to LTS**.
OpenTelemetry	Report application performance monitoring data using the OpenTelemetry protocol. For details, see **Using OpenTelemetry to Ingest Traces to APM**.
SkyWalking	Report application performance monitoring data using the SkyWalking protocol. For details, see **Using SkyWalking to Ingest Traces to APM**.
Syslog Protocol	Exchange logs between devices based on UDP/TCP. For details, see **Using Flume to Report Logs to LTS**.
Flume	Collect logs and upload them to LTS using Flume. For details, see **Using Flume to Report Logs to LTS**.
Beats	Collect logs and upload them to LTS using Beats. For details, see **Using Kafka to Report Logs to LTS**.
Logstash	Collect logs and upload them to LTS using Logstash. For details, see **Using Kafka to Report Logs to LTS**.
SNMP Protocol	Remotely monitor network devices. Three versions available. For details, see **Using Flume to Report Logs to LTS**.
Java SDK (log4j2)	Configure Huawei Cloud Appender in Log4j2 and then report generated logs to LTS.
Logback SDK	Configure Huawei Cloud Appender in logback and then report generated logs to LTS.
Cross-Account Ingestion - Log Stream Mapping	Create an agency to map the delegator account's log stream to the delegated account's log stream. For details, see **Ingesting Logs to LTS Across IAM Accounts**.
Custom Prometheus Metrics	Ingest custom Prometheus metrics. For details, see **Ingesting Custom Prometheus Metrics to AOM**.

----End

Ingesting Custom Prometheus Metrics to AOM

You can ingest custom Prometheus metrics. They can be automatically reported to AOM.

- **Prerequisites**
  - A Prometheus instance for ECS has been connected for monitoring. For details, see **Creating a Prometheus Instance for ECS**.
  - A host group has been created. For details, see **2.2.7 (New) Managing Host Groups**.

- **Procedure**

1. Log in to the **AOM 2.0** console.
2. In the navigation pane, choose **Access** > **Access Center**. Click **Experience the new version** in the upper right corner of the page.
3. Click **Custom Prometheus Metrics** under **APIs/Protocols...**, and then click **Ingest Metric (AOM)** on the card to enter the configuration page.
4. Configure parameters for ingesting custom Prometheus metrics.
   a. Select a Prometheus instance.
      i. **Instance Type**: **Prometheus for ECS** is selected by default and cannot be changed.
      ii. **Instance Name**: Select a Prometheus instance from the drop-down list.
      If no Prometheus instance is available, click **Create Instance** to create one.
   b. Select a host group.
      In the host group list, select a target host group.
      - If no host group is available, click **Create Host Group** to create one.
      - You can also perform editing, deletion, and other operations on the host group as needed. For details, see **Other Operations**.

      Collection configurations are delivered by host group. Therefore, it is easy for you to configure data collection for multiple hosts. When there is a new host, simply add it to a host group and the host will automatically inherit the log ingestion configurations associated with the host group.
   c. Configure the collection.
      Under **Configure Collection**, set parameters by referring to the following table.

Table 3-40 Parameters for configuring a collection task

Operation	Parameter	Description
Basic Settings	Configuration Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Metric Collection Rule	Collection Target	Enter the target IP address and port number for collecting Prometheus metrics, for example, **10.0.0.1:3306**.
	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: **10**, **30**, and **60** (default).

Operation	Parameter	Description
	Metric Collection Timeout (s)	Timeout period for executing a metric collection task, in seconds. Options: **10**, **30**, and **60** (default). The timeout period cannot exceed the collection interval.
	Executor	User who executes the metric ingestion rule, that is, the user of the selected host group. By default, the executor is **root**.
Other	Custom Dimensions	Dimensions (key-value pairs) added to specify additional metric attributes. You can click **Add Dimension** to add multiple custom dimensions (key-value pairs). • Key: key of the additional attribute of a metric. Enter 1 to 64 characters starting with a letter or underscore (_). Only letters, digits, and underscores are allowed. • Value: corresponds to the key of the additional attribute of a metric. A maximum of 10 custom dimensions can be added. Example: Set the key to **app** and value to **abc**.

After the parameters are configured, you can click **YAML** to view the configuration data in YAML format.

5. After the configuration is complete, click **Next**. The custom Prometheus metrics can then be ingested.

   After ingesting custom Prometheus metrics, you can perform the following operations:

   – Go to the **Metric Browsing** page to analyze metrics. For details, see **4 Observability Metric Browsing**.

   – Go to the **Access Management** page to view, edit, or delete the configured ingestion rule. For details, see **3.9 Managing Metric and Log Ingestion**.

3.9 Managing Metric and Log Ingestion

After ingesting metrics to AOM and logs to LTS in the access center, you can manage ingestion rules on the **Access Management** page.

Constraints

- AOM provides both old and new access management functions. To switch from the **old function** to the new function, click **Experience the new version** in the upper right corner of the **Access Center** page and then go to the **Access Management** page.

- To use LTS functions on the AOM console, you need to obtain LTS permissions in advance. For details, see **Permissions**.
- To use the log ingestion rule function on the AOM 2.0 console, **purchase LTS resources** first.

Managing Metric Ingestion Rules

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, choose **Access** > **Access Management**. The **Metric Ingestion Rules** tab page is displayed.

Step 3 Click **Ingest Metric**. In the dialog box, select a target card. For details, see **3.1 AOM Access Overview**.

Step 4 After the ingestion is complete, check the rule on the **Metric Ingestion Rules** tab page under **Access Management**.

Perform the operations listed in **Table 3-41** if needed.

Table 3-41 Related operations

Operation	Description
Searching for a metric ingestion rule	Search for metric ingestion rules by **Ingestion Configuration**, **Ingestion Type**, or **Status** in the search box. Alternatively, enter a keyword to search for a metric ingestion rule.
Refreshing the metric ingestion rules list	Click  in the upper right corner of the list to refresh current metric ingestion rules.
Setting the metric ingestion rule list	Click  in the upper right corner of the list. In the displayed dialog box, customize column display. • Basic settings – **Table Text Wrapping**: If you enable this function, excess text will move down to the next line; otherwise, the text will be truncated. – **Operation Column**: If you enable this function, the **Operation** column is always fixed at the rightmost position of the table. • **Custom Columns**: Select or deselect the columns to display.
Editing a metric ingestion rule	Click **Edit** in the **Operation** column to modify a metric ingestion rule. For details, see **3.1 AOM Access Overview**.
Deleting a metric ingestion rule	• To delete a metric ingestion rule, click **Delete** in the **Operation** column. • To delete one or more metric ingestion rules, select them and click **Delete** above the list.

Operation	Description
Enabling or disabling a metric ingestion rule	• Enable or disable the rule in the **Status** column. • To enable or disable one or more rules, select them and click **Enable** or **Disable** above the list.
Viewing the associated Prometheus instance	Click an instance in the **Instance Name** column to go to the instance details page.

----End

Managing Log Ingestion Rules

AOM is a unified platform for observability analysis. It does not provide log functions by itself. Instead, it uses the log ingestion rule function of **Log Tank Service (LTS)**. You can perform operations on the AOM 2.0 or LTS console.

Table 3-42 Description

Function	Description	AOM 2.0 Console	LTS Console	References
Log ingestion rules	Logs can be ingested through ICAgents, cloud services, APIs, and SDKs. After logs are ingested, they are displayed in a simple and orderly manner on the console and can be queried easily.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane on the left, choose **Access** > **Access Management**. 3. Click the **Log Ingestion Rules** tab.	1. Log in to the LTS console. 2. In the navigation pane on the left, choose **Access** > **Access Management**.	**Log Ingestion**

4 Observability 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.

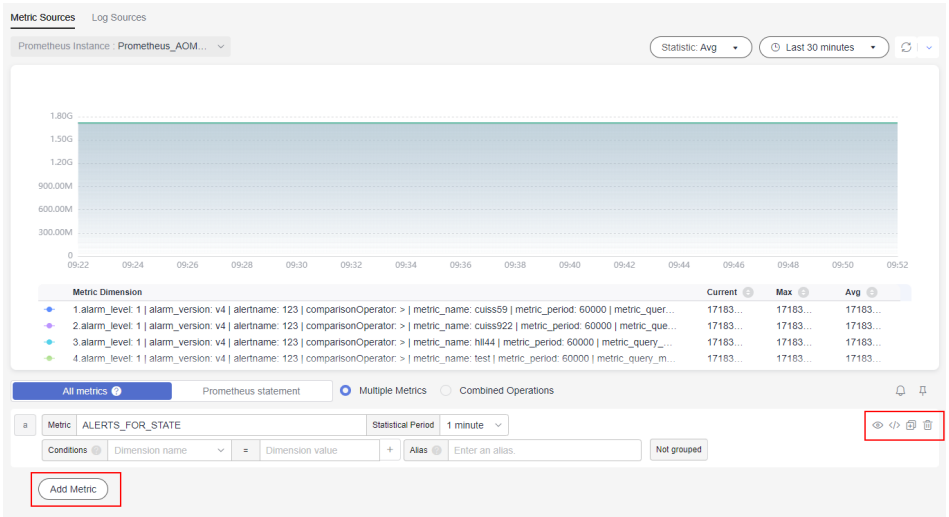
Step 2 In the navigation pane, choose **Metric Browsing**.

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. For details about how to set monitoring conditions, see **Table 5-4**.

- Select metrics from all metrics.

Figure 4-1 Selecting metrics from all metrics



After selecting a target metric, you can set condition attributes to filter information. For example, RDS DB instances have the CPU usage metric. To check the CPU usage of a specified RDS DB instance type, do as follows:

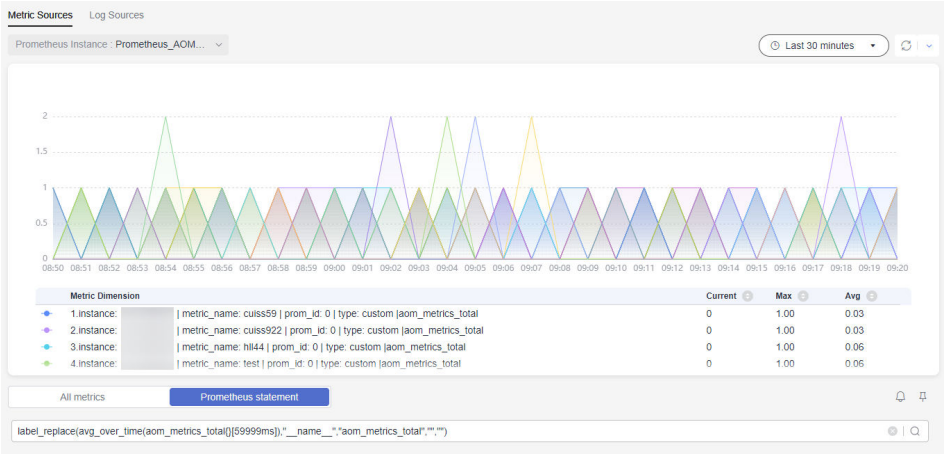
In the **Metric** text box, select the CPU usage metric of the corresponding RDS DB instance. In the **Conditions** area, set the dimension name to **RDS for MySQL** or **RDS for PostgreSQL** and select the corresponding dimension value. The CPU usage metric of the specified RDS DB instance type will 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 **6.3.8 Prometheus Statements**.

Figure 4-2 Selecting metrics by running Prometheus statements



Step 5 Set metric parameters by referring to **Table 4-1**, view the metric graph in the upper part of the page, and analyze metric data from multiple perspectives.

Table 4-1 Metric parameters

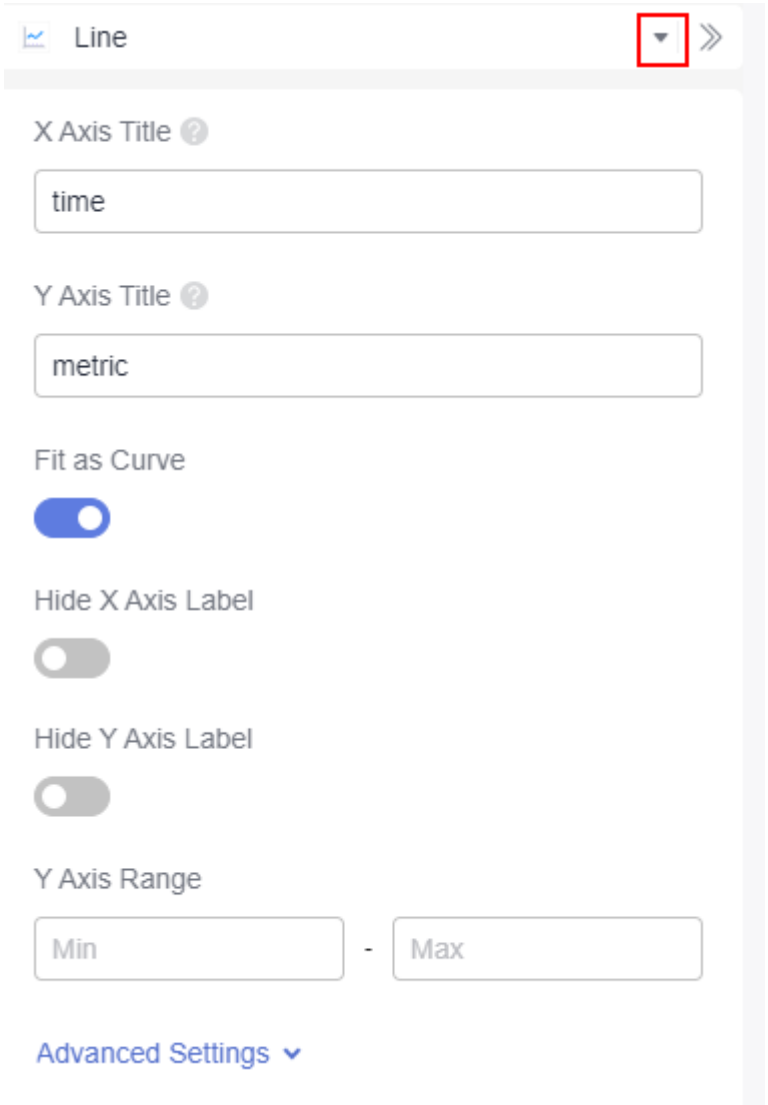
Parameter	Description
Statistic	Method used to measure metrics. Options: **Avg**, **Min**, **Max**, **Sum**, and **Samples**. **Samples**: the number of data points.
Time Range	Time range in which metric data is collected. Options: **Last 30 minutes**, **Last hour**, **Last 6 hours**, **Last day**, **Last week**, and **Custom**.

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

Figure 4-3 Selecting a graph type



----End

Related Operations

You can also perform the operations listed in **Table 4-2**.

Table 4-2 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. **When you are redirected to the Create Alarm Rule page, your settings made on the Metric Browsing page will be automatically applied to Alarm Rule Settings and Alarm Rule Details areas.**
Deleting a metric	Click next to the target metric.
Adding a metric graph to a dashboard	After selecting a metric, click in the upper right corner of the metric list.
Display Background	If this option is enabled, the background will be displayed in the line graph.

Monitoring Logs

AOM can monitor and analyze log data. However, you need to structure logs first. For details, see **Log Structuring**.

Step 1 In the navigation pane, choose **Metric Browsing**.

Step 2 On the displayed page, click the **Log Sources** tab.

Step 3 Select a log group name and a log stream name from the drop-down lists.

Step 4 In the search box, enter an SQL statement, and click **Search** to view the log data analysis of the log stream.

Step 5 Select a graph or table to display the query result. For details about graph types and configurations, see **Log Data 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. **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

5 Dashboard Monitoring

5.1 AOM Dashboard Overview

Dashboards enable you to monitor metrics and logs in real time. You can create dashboards for metrics or logs, so that monitoring data can be displayed in graphs on the monitoring panel. This helps you monitor and analyze metrics or logs.

Function Introduction

Table 5-1 Function introduction

Function	Description
5.2 Creating a Dashboard	With a dashboard, different graphs are displayed on the same screen, so you can view metrics or logs comprehensively.
5.3 (New) Creating a Dashboard	With a dashboard, different graphs are displayed on the same screen, so you can view metrics or logs comprehensively.
5.4 Setting Full-Screen Online Duration for an AOM Dashboard	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.
5.5 Adding AOM Dashboard Filters	You can customize filters by adding variables to filter monitoring data when viewing or adding graphs on the **Dashboard** page.

Constraints

- 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.

- Preset container dashboards can be used only after you install **kube-prometheus-stack** on the **Add-ons** page of CCE.
- Preset native middleware dashboards can be used only after you **create middleware collection tasks** on the UniAgent page.
- Preset cloud service dashboard **dms-rabbitmq** does not support monitoring of certain metrics in the RabbitMQ AMQP-0-9-1 version. For details about the supported RabbitMQ metrics, see **RabbitMQ Metrics**.
- Up to 1,000 dashboard groups can be created in a region.
- Up to 1,000 dashboards can be created in a region.
- A maximum of 50 graphs can be added to a dashboard.
- A maximum of 200 metric data records can be displayed in a line graph.
- Only one resource can be displayed on a digit graph.

5.2 Creating a Dashboard

With a dashboard, different graphs are displayed on the same screen, so you can view metrics or logs comprehensively.

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 5-2 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.

Parameter	Description
Bind to Application	Select an application created in CMDB to bind. This configuration item is available only when the **Application Insights** function is enabled. To enable this function, see **14.4 Configuring AOM Menus**.
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. Enter a maximum of 255 characters. The following special characters are not allowed: "$# %&'+;<=>?\

Step 6 Click **OK**.

----End

Adding a Graph to a Dashboard

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

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

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

Step 3 Go to the dashboard page. Click **Add Graph** or  in the upper right corner to add a graph to the dashboard. For details about the graphs that can be added to the dashboard, see **5.6 Graph Description**. The data can be metric/log data. Select a graph as required.

Table 5-3 Parameters for adding a graph

Data Source	How to Add	Scenario
Metric Sources	See **Add a metric graph**.	Monitors metrics of the business layer, application layer, Prometheus middleware, Prometheus running environments, Prometheus cloud services, open-source monitoring systems, Prometheus APIs/SDKs, and custom Prometheus plug-ins.

Data Source	How to Add	Scenario
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 5-4**. Then click **Save**.

Figure 5-1 Adding a metric graph

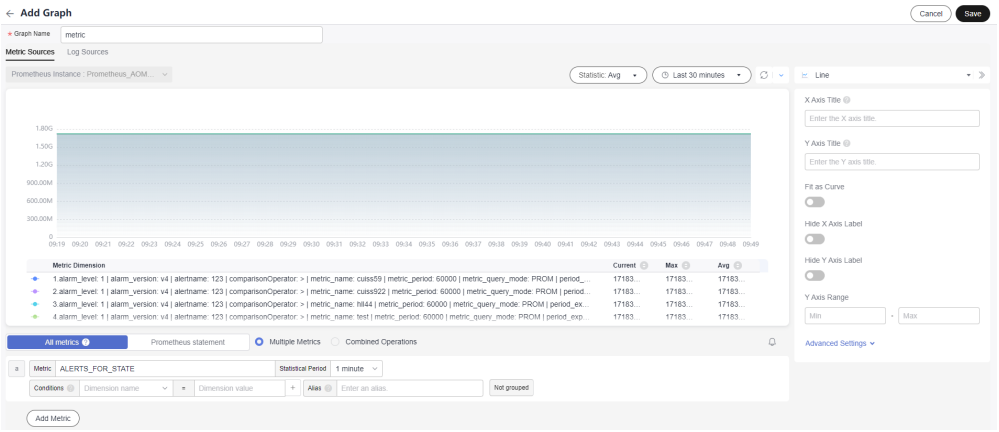


Table 5-4 Adding a metric graph

Parameter	Description
Graph Name	Name of a graph to distinguish it from other graphs. For graph names, **variables can be added** to dynamically filter graph information. Duplicate names are supported. Enter a maximum of 255 characters. The following special characters are not allowed: "$# %&'+;<=>?\
Data Source	The default value is **Metric Sources**.
Graph Type	Options: line, digit, top N, table, bar, and digital line.
How to Add	Add metrics as required. You can select metrics from **All metrics** or using Prometheus statements.

Parameter	Description
All metrics	Select target metrics from the metric drop-down list. – Calculation method: ▪ **Multiple Metrics**: Performs calculation for metrics and their conditions separately, and displays the results on the graph. ▪ **Combined Operations**: Performs calculation on multiple metrics and their conditions based on expressions, and displays the results on the graph. – **Metric**: Select a target metric from the drop-down list. You can also directly enter a metric name in the search box and click **Generate**. If no metric is reported, configure one. – **Statistical Period**: Interval at which metric data is collected. The statistical periods that are available for you to select vary according to the time range. **Relationship Between the Time Range and Statistical Period** – **Condition**: Metric monitoring scope. Each metric condition is in "key:value" format and can be selected from the drop-down list. You can also enter a dimension name and value, and click **Generate** to add a metric condition. You can also click + and select **AND** or **OR** to add more conditions for the metric. – **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. – **Formatted Legend Name**: Use a fixed name or variable as the legend name. Format: *{{dimension name}}*. If the displayed legend name is **{{dimension name}}**, there is no such dimension. For example, enter **{{hostname}}** and a host name will be displayed as the legend name. **Tables and digit/line graphs do not support Formatted Legend Name.** You can click **Add Metric** to add more metrics. A maximum of 100 can be added.

Parameter	Description
Prometheus statement	Add metric data by entering a Prometheus statement related to the metric. – **Prometheus Statement**: See **6.3.8 Prometheus Statements**. – **Formatted Legend Name**: Use a fixed name or variable as the legend name. If the displayed legend name is **{{dimension name}}**, there is no dimension. Format: *{{dimension name}}*. For example, enter **{{hostname}}** and a host name will be displayed as the legend name. To add more metrics, click **Add Prometheus Statement**. You can add 100 metrics in total.
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**.
Statistic	Method used to measure metrics. Options: **Avg**, **Min**, **Max**, **Sum**, and **Samples**.
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 5-5**. Then click **Save**.

Figure 5-2 Adding a log graph

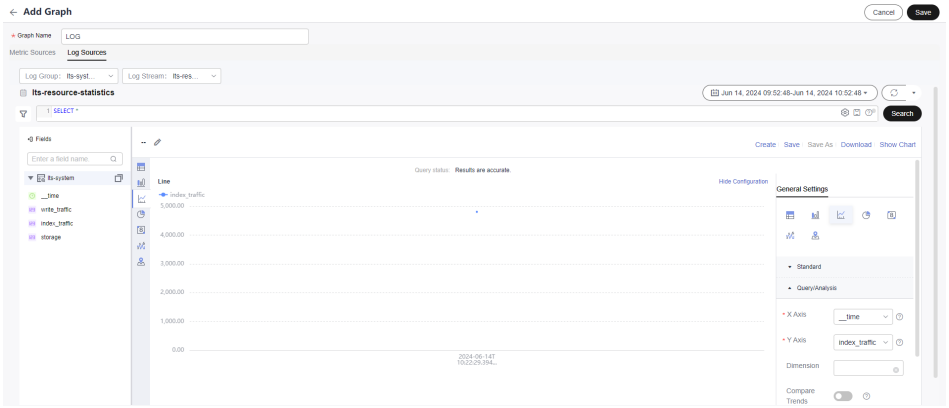


Table 5-5 Log graph parameters

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 5-7**.
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 5-7**.
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 Data 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 5-6**.

Table 5-6 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.

Operation	Description
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.
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. The graph configurations of new dashboards are different from those of old dashboards. • Old dashboards are incompatible with the graph configurations of new dashboards. • However, new dashboards are compatible with the graph configurations of old dashboards.

Operation	Description
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 **6.3.2 Creating an AOM 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 **6.3.2 Creating an AOM Metric Alarm Rule**.
Displaying a graph in full screen	Click the target dashboard, move the cursor to the upper right corner of a graph, and choose > **Full Screen**.
Exiting the full-screen mode	Move the cursor to the upper part of the screen and click  , or choose > **Exit Full Screen**, or press **Esc** on the keyboard to exit the full-screen mode.
Rotating dashboards	Click a target dashboard and click  in the upper right corner of the dashboard details page. Set full-screen display by referring to **5.4 Setting Full-Screen Online Duration for an AOM Dashboard**.
Setting a dashboard	Click a target dashboard and click  in the upper right corner of the dashboard details page. For details, see **5.5 Adding AOM Dashboard Filters**.
Setting the query time	Select the target dashboard. In the upper right corner of the dashboard page, click the time range next to and select **Last 30 minutes**, **Last hour**, **Last 6 hours**, **Last day**, **Last week**, or **Custom** from the drop-down list. If you select **Custom**, select a time range in the calendar that is displayed. The time can be accurate to seconds. Then click **OK**, so that you can query data in the dashboard based on the selected time range.
Exporting a dashboard	Export the metric graph data of a dashboard in JSON format and save it to your local PC for further analysis. You can export a dashboard using either of the following methods: Method 1: In the dashboard list, locate a dashboard, and choose  > **Export Dashboard** in the **Operation** column. Method 2: Click a dashboard to go to its details page and choose  > **Export Dashboard** in the upper right corner.

Operation	Description
Importing a dashboard	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 5-2**. 3. Click **OK**.
Exporting a monitoring report	Select the target dashboard, click in the upper right corner of the **Dashboard** page, and click **Export Line Graph Report** to export the line graph as a CSV file for local storage and further analysis.

Table 5-7 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 1–30 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**.

Relationship Between the Time Range and Statistical Period

In AOM, a maximum of 1,440 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 1,440

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 5-8 Relationship between the time range and statistical period

Time Range	Statistical Period
Last 30 minutes	1 minute, or 5 minutes
Last hour	
Last 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

5.3 (New) Creating a Dashboard

With a dashboard, different graphs are displayed on the same screen, so you can view metrics or logs comprehensively.

Constraints

The graph configurations of new dashboards are different from those of old dashboards.

- Old dashboards are incompatible with the graph configurations of new dashboards.
- However, new dashboards are compatible with the graph configurations of old dashboards.

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, choose **Dashboard**. Click **New Version** in the upper right corner of the page.

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 5-9 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: "$# %&'+;<=>?\
Enterprise Project	Enterprise project. • If you have selected All for **Enterprise Project** on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be dimmed and cannot be changed.
Bind to Application	Select an application created in CMDB to bind. This configuration item is available only when the **Application Insights** function is enabled. To enable this function, see **14.4 Configuring AOM Menus**.
Group Type	Options: **Existing** and **New**. • **Existing**: Select an existing dashboard group from the drop-down list. • **New**: Enter a dashboard group name to create one. Enter a maximum of 255 characters. The following special characters are not allowed: "$# %&'+;<=>?\

Step 6 Click **OK**.

----End

Adding a Graph to a Dashboard

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

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

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

Step 3 Go to the dashboard page. Click **Add Graph** or  in the upper right corner to add a graph to the dashboard. For details about the graphs that can be added to

the dashboard, see **5.7 (New) Graphs**. The data can be metric or log data. Select a graph type as required.

- Adding a metric graph: Set parameters by referring to **Table 5-4** and click **Save**.

  Table 5-10 Adding a metric graph

Parameter	Description
Graph Name	Name of a graph to distinguish it from other graphs. For graph names, **variables can be added** to dynamically filter graph information. Duplicate names are supported. Enter a maximum of 255 characters. The following special characters are not allowed: "$# %&'+;<=>?\
Data Source	The default value is **Metric Sources**.
Graph Type	Options: line, digit, top N, table, bar, and digital line.
How to Add	Add metrics as required. You can select metrics from **All metrics** or using Prometheus statements.

Parameter	Description
All metrics	Select target metrics from the metric drop-down list. – Calculation method: ▪ **Multiple Metrics**: Performs calculation for metrics and their conditions separately, and displays the results on the graph. ▪ **Combined Operations**: Performs calculation on multiple metrics and their conditions based on expressions, and displays the results on the graph. – **Metric**: Select a target metric from the drop-down list. You can also directly enter a metric name in the search box and click **Generate**. If no metric is reported, configure one. – **Statistical Period**: Interval at which metric data is collected. The statistical periods that are available for you to select vary according to the time range. **Relationship Between the Time Range and Statistical Period** – **Condition**: Metric monitoring scope. Each metric condition is in "key:value" format and can be selected from the drop-down list. You can also enter a dimension name and value, and click **Generate** to add a metric condition. You can also click + and select **AND** or **OR** to add more conditions for the metric. – **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. – **Formatted Legend Name**: Use a fixed name or variable as the legend name. Format: *{{dimension name}}*. If the displayed legend name is **{{dimension name}}**, there is no such dimension. For example, enter **{{hostname}}** and a host name will be displayed as the legend name. **Tables and digit/line graphs do not support Formatted Legend Name.** You can click **Add Metric** to add more metrics. A maximum of 100 can be added.

Parameter	Description
Prometheus statement	Add metric data by entering a Prometheus statement related to the metric. – **Prometheus Statement**: See **6.3.8 Prometheus Statements**. – **Formatted Legend Name**: Use a fixed name or variable as the legend name. If the displayed legend name is **{{dimension name}}**, there is no dimension. Format: *{{dimension name}}*. For example, enter **{{hostname}}** and a host name will be displayed as the legend name. To add more metrics, click **Add Prometheus Statement**. You can add 100 metrics in total.
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**.
Statistic	Method used to measure metrics. Options: **Avg**, **Min**, **Max**, **Sum**, and **Samples**.
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**.

- Adding a log graph: Set parameters by referring to **Table 5-11** and click **Save**.

Table 5-11 Adding a log 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 **Log Sources**.
Log Group	Select a desired 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 5-13**.
Log Stream	Select a desired 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 5-13**.

Parameter	Description		
Go to Old Version	Click **Back to Old Version** to add a log graph of the old version. For details, see **Adding a Log Graph**.		
Time Range	Options: **From now**, **From last**, and **Specified**. – **From now**: queries data generated in a time range that ends with the current time, such as the previous 1, 5, or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from now, the graphs on the dashboard display the data that is generated from 18:20:31 to 19:20:31. – **From last**: queries data generated in a time range (on the hour) that ends with the current time, such as the previous 1 or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from last, the graphs on the dashboard display the data that is generated from 18:00:00 to 19:00:00. – **Specified**: queries data that is generated in a specified time range.		
Refresh Frequency	Interval at which the data is refreshed. Options: **Refresh now**, **Refresh every 30 seconds**, **Refresh every 1 minute**, and **Refresh every 5 minutes**.		
Graph Type	Options: line, digit, table, bar, digital line, pie, and map graphs.		
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 **Log Data Graphs**.		
Interactive mode	Metrics	Use a statistics function on a selected field to calculate your desired metric. You can select an option from the drop-down list. Options: **Log count**, **Aggregation statistics**, and **Estimation function**. – **Log count**: **count(*)**, **Logs with non-null field values**, **Logs with non-zero field values**, and **Logs with different field values** – Aggregation statistics: **max()**, **min()**, **avg()**, **sum()**, **earliest()**, and **latest()**. – Estimation function: **Median** and **Percentile**
	Alias	Alias of a metric. After setting an alias, it takes precedence.
	Conditions	Conditions for filtering metric data. A condition comprises a field and a value. The field can be selected directly from the drop-down list. Multiple conditions can be set using **AND** or **OR**.

Parameter	Description	
	Group	Group the values by selected field (**group by**), collect metric statistics by group, and sort the results by order (**order by**).
	Sort	
	Copy to Syntax Mode	After setting parameters such as **Metrics** and **Conditions** in interactive mode, you can preview the search statement. By clicking **Copy to Syntax Mode**, you can switch to the syntax mode.
	Format SQL	Click to set the formatting SQL statement and reverse formatting SQL statement to optimize the search statement and improve the search efficiency.
Syntax Mode	Enter a statement in the search box to query logs. The search analysis syntax consists of the search statement and SQL analysis statement. The two statements are associated by using the pipe character (|).	

Step 4 Click **Save**. 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 5-12**.

Table 5-12 Related operations

Operation	Description
Setting column display	Click in the upper right corner of the dashboard list. In the displayed dialog box, customize column display. • Basic Settings – **Table Text Wrapping**: If you enable this function, excess text will move down to the next line; otherwise, the text will be truncated. – **Operation Column**: If you enable this function, the **Operation** column is always fixed at the rightmost position of the table. • **Custom Columns**: Select or deselect the columns to display.
Adding dashboards to favorites	In the dashboard list, locate a dashboard and click **Add to Favorites** in the **Operation** column.

Operation	Description
Moving dashboards to another group	• Move a dashboard group. – In the dashboard list, locate a dashboard and click **Move** in the **Operation** column. – Click a dashboard in the dashboard list to access the dashboard page. In the upper left corner, locate the target dashboard, and choose ··· > **Move**. • To move multiple dashboards, select them and click **Move** above the list.
Deleting a dashboard	• In the dashboard list, locate a dashboard and click **Delete** in the **Operation** column. • Click a dashboard in the dashboard list to access the dashboard page. In the upper left corner, locate the target dashboard, and choose ··· > **Delete**. • Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click 🗑. In the displayed dialog box, click **OK**.
Changing a dashboard group name	1. Click a dashboard in the dashboard list to access the dashboard page. 2. In the upper left corner, locate the target dashboard. 3. 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. Click a dashboard in the dashboard list to access the dashboard page. 2. In the upper left corner, locate the target dashboard. 3. 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 a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click ✎. 2. Move the pointer to the upper right corner of a graph and choose ⋮ > **Delete**. 3. Click 💾 to delete the graph.

Operation	Description
Relocating a graph on a dashboard	1. Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click . 2. Move the cursor into the target graph and move it to any position in the dashboard. 3. Click to adjust the current graph layout.
Full-screen display	Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click .
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 a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click .
Auto refresh	Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click the arrow next to and select a refresh mode or frequency. Options: **Refresh now**, **Refresh every 5 seconds**, **Refresh every 10 seconds**, **Refresh every 30 seconds**, and **Refresh every 1 minute**.
Manually refreshing a graph	Click the target dashboard, move the cursor to the upper right corner of a graph, and choose > **Refresh**.
Modifying a graph	1. Click the target dashboard, move the cursor to the upper right corner of a graph, and choose > **Edit** to modify the graph. For details, see **Adding a Graph to a Dashboard**. 2. Click **Save**. 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 **6.3.2 Creating an AOM 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 **6.3.2 Creating an AOM Metric Alarm Rule**.

Operation	Description
Rotating dashboards	Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click . Set full-screen display by referring to **5.4 Setting Full-Screen Online Duration for an AOM Dashboard**.
Setting a dashboard	Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click . For details, see **5.5 Adding AOM Dashboard Filters**.
Setting the query time	Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click  to set a time range to query. Options: **From now**, **From last**, and **Specified**. • **From now**: queries data generated in a time range that ends with the current time, such as the previous 1, 5, or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from now, the graphs on the dashboard display the data that is generated from 18:20:31 to 19:20:31. • **From last**: queries data generated in a time range (on the hour) that ends with the current time, such as the previous 1 or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from last, the graphs on the dashboard display the data that is generated from 18:00:00 to 19:00:00. • **Specified**: queries data that is generated in a specified time range.
Exporting a dashboard	Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click and click **Export Dashboard** to export the metric graph data in JSON format and save the data to the local PC for further analysis.
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 a target dashboard group 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 **Step 5**. 3. Click **OK**.

Operation	Description
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.
Copying a dashboard	1. Click a target system built-in dashboard or custom dashboard and then click in the upper right corner of the dashboard details page. 2. In the dialog box that is displayed, set information such as the dashboard name by referring to **Step 5**. 3. After the settings are complete, click **OK**.
Setting a dashboard group	1. Click a target dashboard and click in the upper right corner of the dashboard details page to create a group. 2. Click next to the created group to set a group name. 3. Select a graph and then drag it into the corresponding group. When dragging a graph, left-click the graph and then drag it as required. If only one group is created, all graphs are in that group by default. If there are multiple groups, drag graphs into the desired group as needed. 4. Click in the upper right corner of the dashboard page to save.

Table 5-13 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 1–30 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**.

Relationship between time ranges and statistical periods (for new dashboards)

In AOM, a maximum of 1,440 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 1,440

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 5-14 (New) Relationship between the time range and statistical period

Type	Time Range	Statistical Period
From now	1 minute	1 minute or 5 minutes
	5 minutes	
	15 minutes	
	30 minutes	
	1 hour	
	4 hours	1 minute, 5 minutes, 15 minutes, or 1 hour
	1 day	
	Today	
	1 week	1 hour
	This week	
	30 days	
	This month	
	Specified	1 minute, 5 minutes, 15 minutes, or 1 hour
From last	1 minute	1 minute or 5 minutes
	15 minutes	
	30 minutes	
	1 hour	
	4 hours	1 minute, 5 minutes, 15 minutes, or 1 hour
	1 day	
	1 week	1 hour

Type	Time Range	Statistical Period
	30 days	
	Today	1 minute, 5 minutes, 15 minutes, or 1 hour
	Yesterday	
	Two days ago	
	This week	1 hour
	Last week	
	This month	
	Last month	
	Specified	1 minute, 5 minutes, 15 minutes, or 1 hour
Custom	Custom	1 minute, 5 minutes, 15 minutes, or 1 hour

5.4 Setting Full-Screen Online Duration for an AOM Dashboard

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.

Constraints

- 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**. If you want to use new dashboards, choose **Dashboard** in the navigation pane and then click **New Version** in the upper right corner of the page.

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 5-15**.

Figure 5-3 Setting the online duration

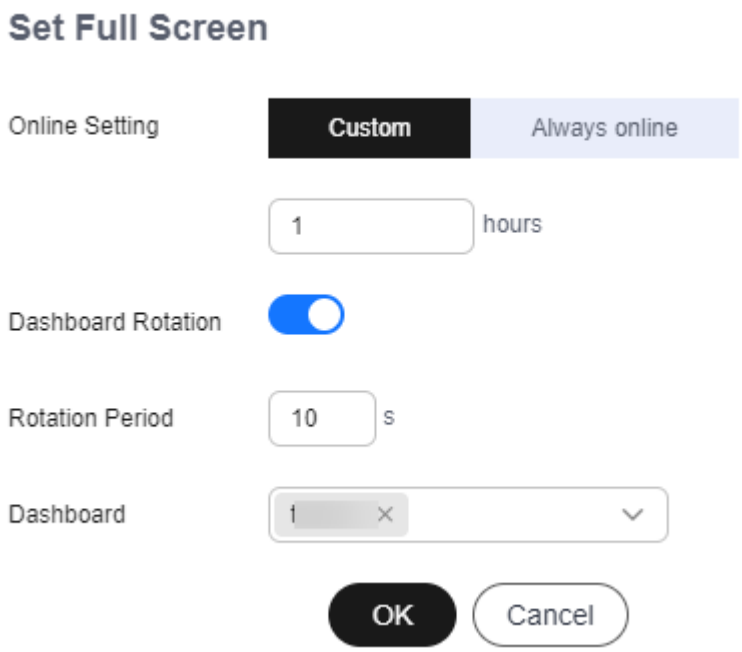


Table 5-15 Online duration parameters

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

5.5 Adding AOM Dashboard Filters

You can customize filters by adding variables to filter monitoring data when viewing or adding graphs on the **Dashboard** page.

Adding Variables

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Dashboard**. If you want to use new dashboards, choose **Dashboard** in the navigation pane and then click **New Version** in the upper right corner of the page.

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 5-16**.

Table 5-16 Parameters for adding variables

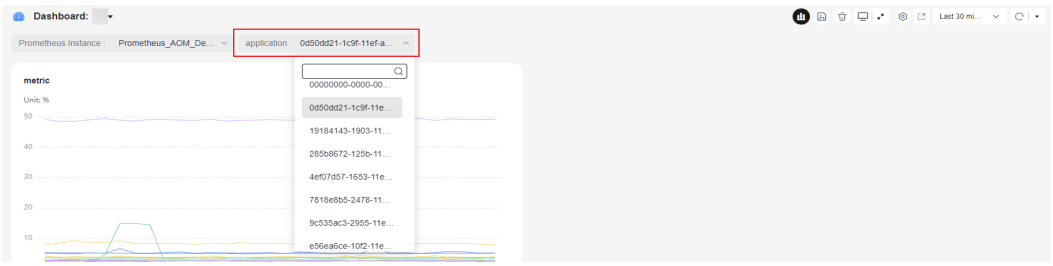
Parameter	Description
Variable Name	Name of a variable. Enter up to 255 characters and do not start or end with an underscore (_). Only digits, letters, and underscores are allowed.
Type	Type of the variable. Only **Query** is supported.

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. Enter up to 1,024 characters.
Data Source	Source of the data. Select a data source on the **Dashboard** page. It is dimmed here and cannot be selected. The default Prometheus instance is selected by default.
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.

Figure 5-4 Checking filters

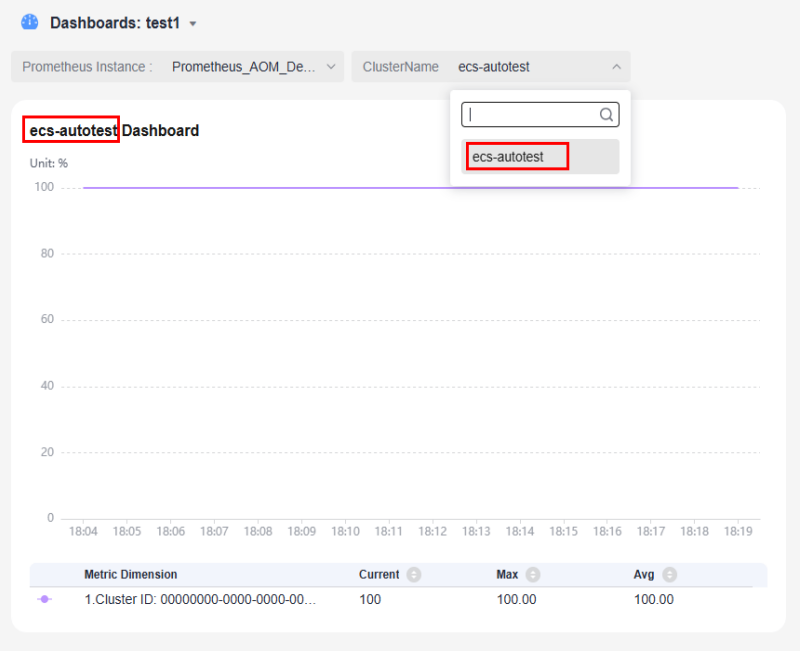


----End

More Operations

After the variable is added, you can perform the operations listed in **Table 5-17** if needed.

Table 5-17 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 5-16**.
Deleting a variable	Click in the **Operation** column of the target variable. In the displayed dialog box, click **Yes**.
Filling a dashboard graph name with variables	Dashboards support the function of filling graph names using variables. After variables are added, dashboard graph names can be filled using *${variable name}* during **graph name configuration**. The graph name is dynamically displayed based on the variable value you select from the drop-down list. For example, if the original graph name is **Dashboard** and the new variable is *ClusterName*, you can set the dashboard graph name to **$***{ClusterName}* **Dashboard**. Then, select values from the drop-down list of **ClusterName**. These values will be dynamically combined with the original dashboard graph name for display. 

5.6 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

Metric data graphs support the following types: **line**, **number**, **top N**, **table**, **bar**, and **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 5-5 Line graph

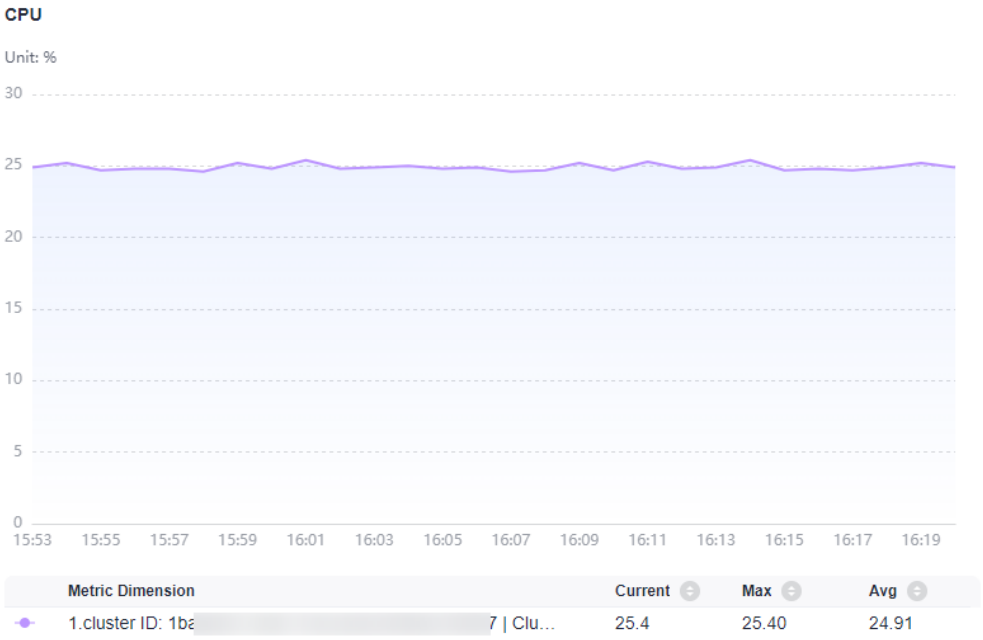


Table 5-18 Line graph parameters

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.

Category	Parameter	Description
	Hide Y Axis Label	Whether to hide the Y axis label.
	Display Background	If this option is enabled, the background will be displayed in the line graph.
	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**: highlights a single value. It can display the latest value and the growth or decrease rate of a resource in a specified period. Use this type of graph to monitor the latest value of a metric in real time.

  As shown in the following figure, you can view the CPU usage of the host in real time. **2.85%** indicates the latest CPU usage, and **-0.08%** indicates the decrease rate in the current monitoring period.

  Figure 5-6 Digit graph

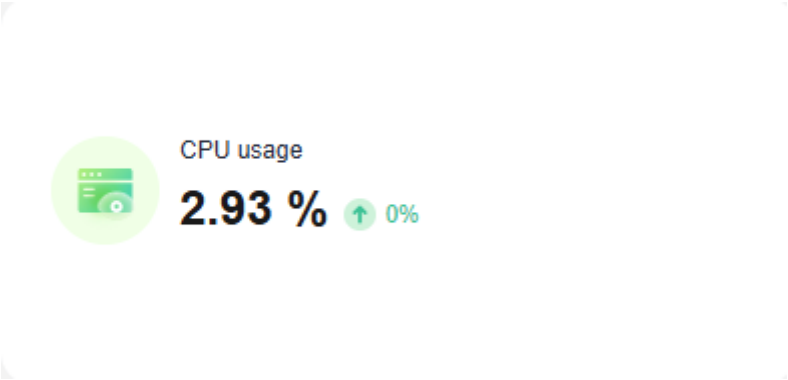
  

  Table 5-19 Digit graph parameters

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 5-7 Top N graph

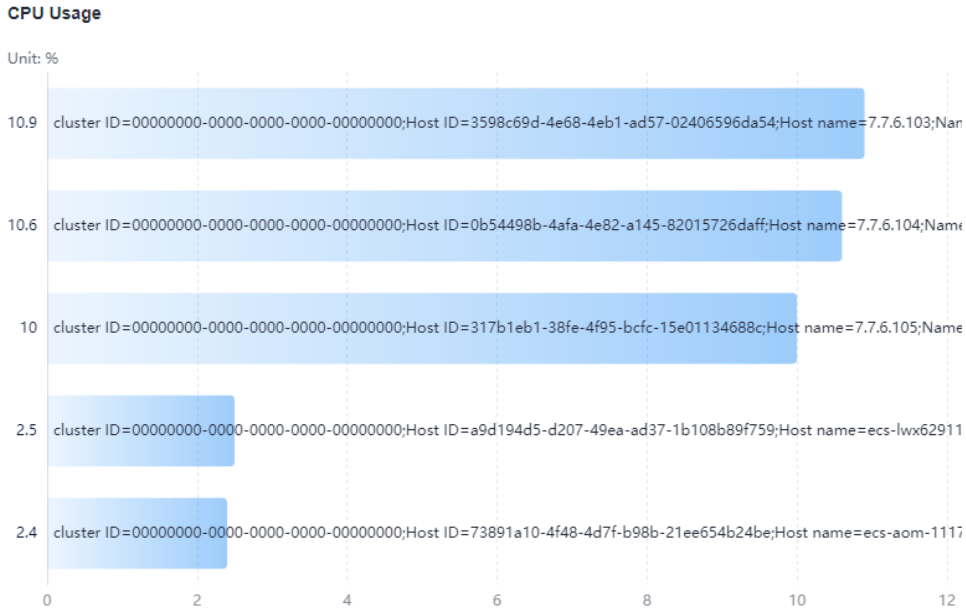


Table 5-20 Top N graph parameters

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

Category	Parameter	Description
	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 5-8 Table

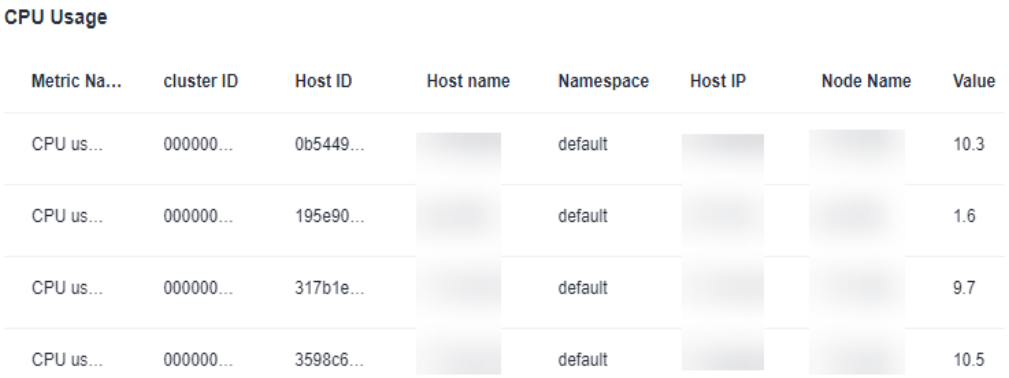
  

  Table 5-21 Table parameters

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

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

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

Figure 5-9 Bar graph

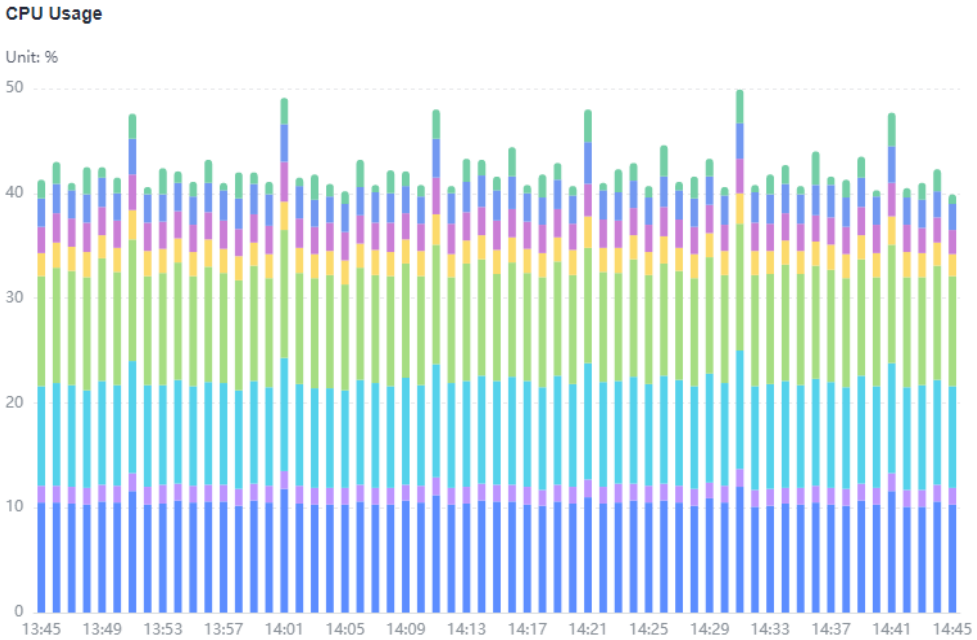


Table 5-22 Bar graph parameters

Category	Parameter	Description
-	X Axis Title	Title of the X axis.
	Y Axis Title	Title 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.
	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.

- **Digital line graph**: a trend analysis graph. It shows the change of a group of ordered data (usually in a continuous time interval) and intuitively displays related data analysis. It can display the latest data and the growth or decrease rate of the resource in a specified monitoring period. Use this type of

graph when you need to monitor the metric data trend of one or more resources within a period.

As shown in the following figure, the CPU usages in different periods are displayed in the same graph. **2.93%** indicates the latest CPU usage, and **0.00%** indicates the growth rate of the CPU usage in the current monitoring period.

Figure 5-10 Digital line graph

Table 5-23 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 Data Graphs

Log data graphs support the following types: **table**, **bar**, **line**, **pie**, **number**, **digital line**, **map**, and **funnel**.

- **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.

Figure 5-11 Table

Table 5-24 Table parameters

Category	Parameter	Description
Standard	Format	Displays the table data in the specified format.
	Unit	Specifies the unit of the data in the custom table.
	Decimal Places	After this function is enabled, decimal places are displayed.
	Decimal Places	Sets the number of decimal places to display.
Query/ Analysis	Hidden Fields	Select a field to hide.
Table	Records per Page	Number of data records displayed on each page.
	Display Total	After this function is enabled, the total number of records in the table is displayed.
Column	Alignment	Alignment mode of table data. Options: **Left**, **Right**, and **Center**.
	Filtering	After this function is enabled, you can search for data in the table column.
	Sorting	After this function is enabled, you can sort data in the table.
	Font Size	Size of the table font. The value ranges from 12 px to 24 px.

- **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 5-12 Bar graph

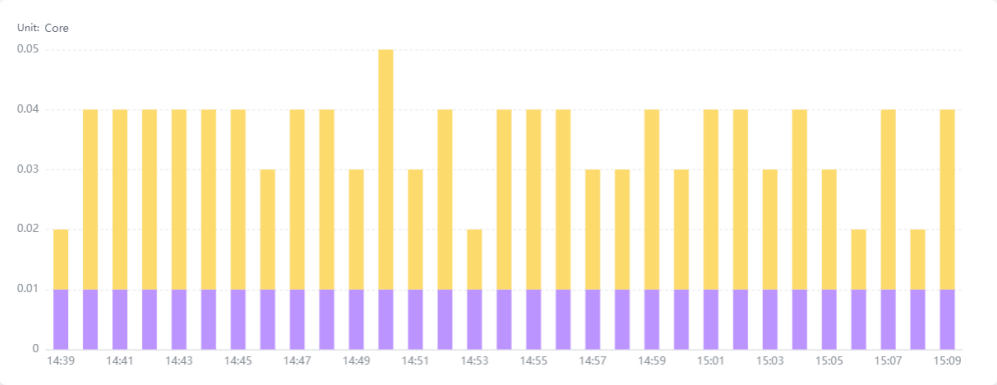


Table 5-25 Bar graph parameters

Category	Parameter	Description
Standard	Format	Displays the Y axis in the specified format.
	Unit	Specifies the unit at the Y axis.
	Decimal Places	After this function is enabled, decimal places are displayed.
	Decimal Places	Sets the number of decimal places to display.
Bar Chart	Direction	Select **Bar chart** or **Horizontal bar chart**.
	Column Width	Sets the column width.
	Display Value	After this function is enabled, the value indicated by each bar is displayed.
	Font Size	Sets the font size of each bar.
	Stacked	After this function is enabled, the Y axis data is displayed in stack mode.
Query/ Analysis	X Axis	Numeric or string data is supported.
	Y Axis	Numeric or string data is supported. You can select multiple data records.
Legend	Hide Legend	After this function is enabled, you can hide the legend and comparison results.

Category	Parameter	Description
	Legend Position	Position of the legend in the chart. Select **Top** or **Right**.
	Comparison Value	Indicates whether to display the maximum value, minimum value, average value, and sum value. You can select multiple options.
Graphics	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.
	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.
Tooltip	Sort By	Dialog box configuration. When multiple Y-axis data records are selected, they can be sorted and displayed based on your configuration. Options: **None**, **Ascending**, and **Descending**.
X Axis	Show	After this function is enabled, data on the X axis is displayed.
	X Axis Title	Title of the X axis.
Y Axis	Show	After this function is enabled, data on the Y axis is displayed.
	Y Axis Title	Title of the Y axis.
	Position	Position of the Y axis. Select **Left** or **Right**.

- **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 5-13 Line graph

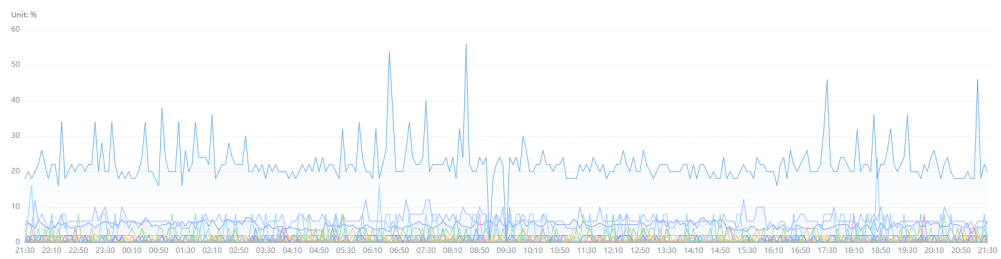
  

Table 5-26 Line graph parameters

Category	Parameter	Description
Standard	Format	Select **K,Mil,Bil**, **1,000,000**, or **Byte,KB,MB** from the drop-down list to specify the format of the Y axis.
	Unit	Specifies the unit at the Y axis.
	Decimal Places	After this function is enabled, decimal places are displayed.
	Decimal Places	Sets the number of decimal places to display.
Query/ Analysis	X Axis	Numeric or string data is supported.
	Y Axis	Numeric or string data is supported. You can select multiple data records.
	Dimension	Select a value from the drop-down list. Generally, it is an ordinal variable.
	Compare Trends	This function can be enabled when the X axis shows time data and **Dimension** is not specified. After this function is enabled, set **Comparison** to a duration less than or equal to 24 hours. After the setting is complete, compare the data of the current time with the object time data.
Legend	Hide Legend	After this function is enabled, you can hide the legend and comparison results.
	Legend Position	Select **Top** or **Right**.
	Comparison Value	Indicates whether to display the maximum value, minimum value, average value, and sum value. You can select multiple options.
Graphics	Line Shape	Line type. Options: **Straight** and **Curved**.
	Line Width	Width of a line.
	Show Data Markers	Whether to display the connection points.
	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.
	Left Margin	Distance between the axis and the left boundary of the graph.

Category	Parameter	Description
	Right Margin	Distance between the axis and the right boundary of the graph.
Tooltip	Sort By	Dialog box configuration. When multiple Y-axis data records are selected, they can be sorted and displayed based on your configuration.
X Axis	Show	After this function is enabled, data on the X axis is displayed.
	X Axis Title	Title of the X axis.
Y Axis	Show	After this function is enabled, data on the Y axis is displayed.
	Y Axis Title	Title of the Y axis.
	Position	Position of the Y axis. Select **Left** or **Right**.

- **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 5-14 Pie graph

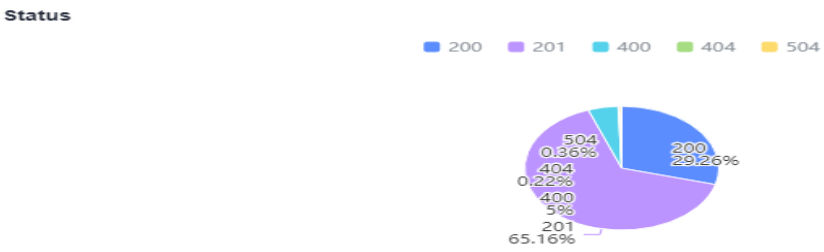


Table 5-27 Pie graph parameters

Category	Parameter	Description
Standard	Format	Select **K,Mil,Bil**, **1,000,000**, or **Byte,KB,MB** from the drop-down list to specify the format of the Y axis.
	Unit	Specifies a unit.
	Decimal Places	After this function is enabled, decimal places are displayed.

Category	Parameter	Description
	Decimal Places	Sets the number of decimal places to display.
Pie Chart	Pie Chart Type	Options: **Pie**, **Cyclic**, and **Coxcomb**. ● Pie A pie chart displays the proportion of each part. It divides a circle into different sectors. The area (or arc length and central angle) of each sector corresponds to the proportion of each part. In this way, the relationship between each part and the whole is intuitively displayed. ● Cyclic Essentially, a cyclic chart hollows out the center of a pie chart. Cyclic charts are better than pie charts in the following aspects: – Cyclic charts display more information such as the total number. – It is not intuitive to compare two pie charts directly. You can compare two cyclic charts by the cyclic bar length. ● Coxcomb A Coxcomb chart is not a cyclic chart in essence. Instead, it is a bar chart drawn in the polar coordinate system. Each category is evenly divided by an arc. The radius of the arc indicates the data size. Coxcomb charts are better than pie charts in the following aspects: – A pie chart can contain a maximum of 10 categorized data records, while a Coxcomb chart can contain 10 to 30 data records. – Because the radius and area are squared, a Coxcomb chart magnifies the difference between the values of each category. It is suitable for comparing the values of similar sizes. – Due to the periodicity of a circle, a Coxcomb chart is also suitable for displaying data by period, such as by week and month.
	Show Scale	After this function is enabled, text labels are displayed on the pie chart to describe data details, such as the value and name.

Category	Parameter	Description
	Scale Text	Options: **Category**, **Percent**, **Category: %**, and **Category: Value (%)**.
	Label Position	After **Show Scale** is enabled, you can set this parameter to adjust the position of the label in the chart.
Query/ Analysis	Value	Specifies the value corresponding to the categorized data.
	Layer 1 Data	
	Category	Specifies the categorized data.
	Display as Sectors	Specifies the number of categorized data records to display.
	Sort By	Options: **Ascending** and **Descending**.
	Display Rest as Others	Specifies whether to display the data of other types as **Others**.
	Add Layer	Click **Add Layer** and set the data of the second layer. The data of each layer includes the category, display sectors, sorting mode, and displaying rest sectors as others.
Legend	Hide Legend	After this function is enabled, you can hide the legend and its content.
	Legend	Select **Value** or **Percent**, or both.
	Legend Position	Position of the legend in the chart. Select **Top** or **Right**.
Graphics	Outer Radius	Outer radius of the pie chart. The value ranges from 40 to 100.
	Inner Radius	Inside radius of the pie chart. The value ranges from 0 to 100.
	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.
	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.

- **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 5-15 Number graph

Table 5-28 Number graph parameters

Category	Parameter	Description
Query/ Analysis	Data Column	Numeric or string data is supported.
	Comparison Data	Select a field to compare. The value of the field is displayed in the chart.
Main Items	Format	Displays data in the specified format.
	Data Text Size	Font size of the displayed value. The value ranges from 12 px to 80 px.
	Data Unit	Unit of the displayed value.
	Unit Text Size	Font size of the displayed value unit. The value ranges from 12 px to 50 px.
	Decimal Places	After this function is enabled, decimal places are displayed.
	Decimal Places	Sets the number of decimal places to display.
	Add Comparison Data	After this function is enabled, the value of the field to compare is displayed.
	Comparison Formatting	Displays the data to compare in the specified format.
	Comparison Data Text Size	Font size of the value to compare. The value ranges from 12 px to 50 px.
	Comparison Data Unit	Unit to compare.
	Comparison Data Unit Text Size	Font size of the value unit to compare. The value ranges from 12 px to 50 px.

Category	Parameter	Description
	Description	Description of the displayed value and comparison trend. The description is displayed below the value.
Background	Background	Background color of a chart, which can be dark or light.

- **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 5-16 Digital line graph

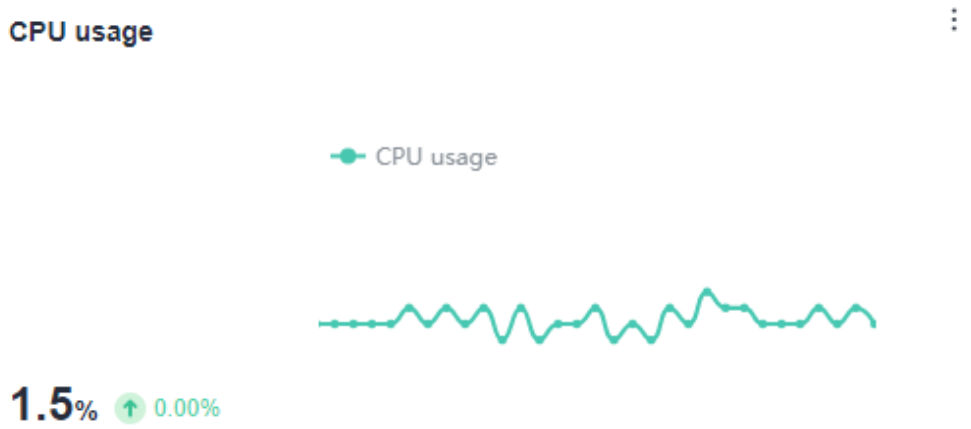


Table 5-29 Digital line graph parameters

Category	Parameter	Description
Query/Analysis	X Axis	Numeric or string data is supported.
	Y Axis	Numeric or string data is supported. You can select multiple data records.
Chart Mode	Line Shape	Line type. Options: **Straight** and **Curved**.
Main Items	Number Format	Displays data in the specified format.
	Data Text Size	Font size of the displayed value. The value ranges from 12 px to 80 px.
	Data Unit	Unit of the displayed value.
	Unit Text Size	Font size of the displayed value unit. The value ranges from 12 px to 50 px.

Category	Parameter	Description
	Decimal Places	After this function is enabled, decimal places are displayed.
	Decimal Places	Sets the number of decimal places to display.
Background	Background	Background color of a chart, which can be dark or light.

- **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 5-17 Map

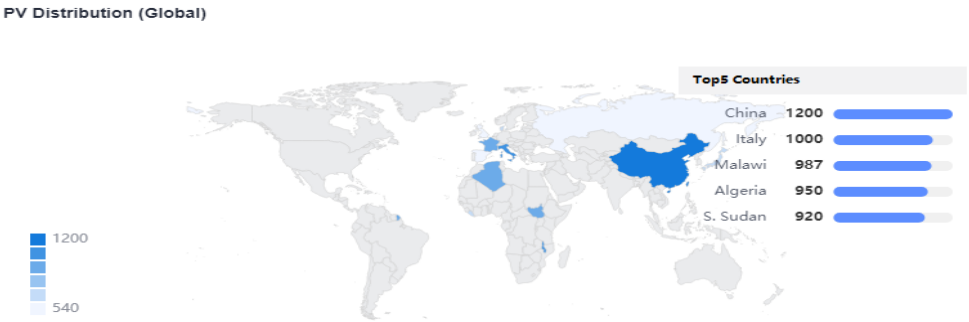


Table 5-30 Map graph parameters

Parameter	Description
Map Type	Select a value from the drop-down list. You can select a provincial 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.
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.

- **Funnel graph**: is applicable to unidirectional analysis of a single process with a standard service procedure, a long period, and many phases. By comparing service data in each phase of the procedure, you can intuitively find and describe the phase where a problem occurs and solve the problem.

Figure 5-18 Funnel graph

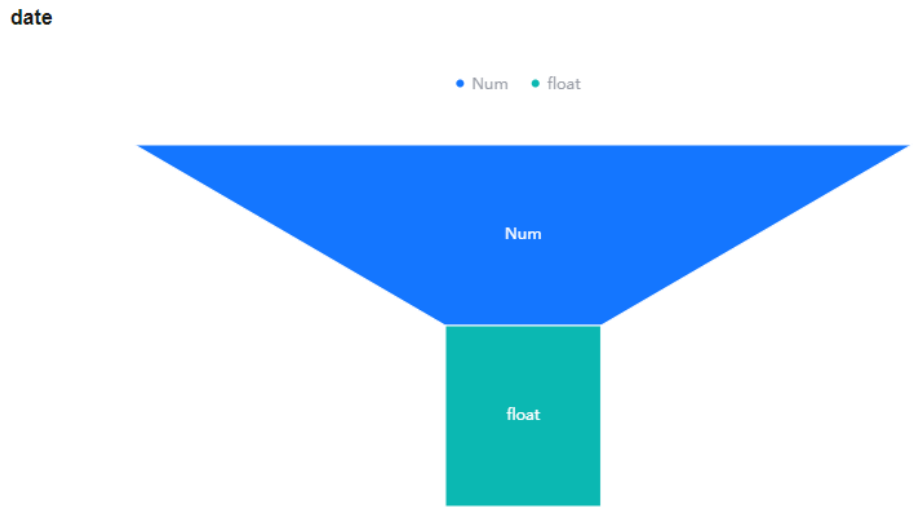


Table 5-31 Funnel graph parameters

Parameter	Description
Series Name	Name of a funnel graph.
Data Column	Select a numeric field. The larger the value of a field, the higher the position of the field.
Hide Legend	After this function is enabled, you can hide the legend names above the funnel graph.

5.7 (New) Graphs

Dashboard graphs show the query and analysis results of metrics and logs.

Metric Data Graphs

The following types of graphs are supported: **line graphs**, **digit graphs**, **top N graphs**, **tables**, **bars**, and **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 5-19 Line graph

Table 5-32 Line graph parameters

Category	Parameter	Description
Graphics	Line Shape	Line type. Options: **Straight** and **Curved**.
	Display Background	If this option is enabled, the background will be displayed in the line 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.
	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.
X Axis	Show	Whether to display the X axis.
	X Axis Title	Title of the X axis.
Y Axis	Show	Whether to display the Y axis.
	Y Axis Title	Title of the Y axis.
	Y Axis Range	Value range of the Y axis.

- **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 5-20 Digit graph

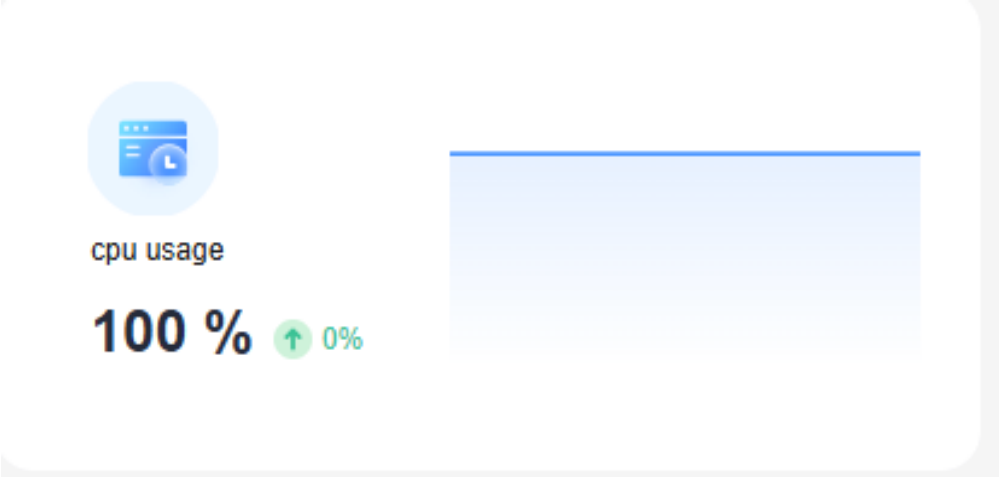


Table 5-33 Digit graph parameters

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 5-21 Top N graph

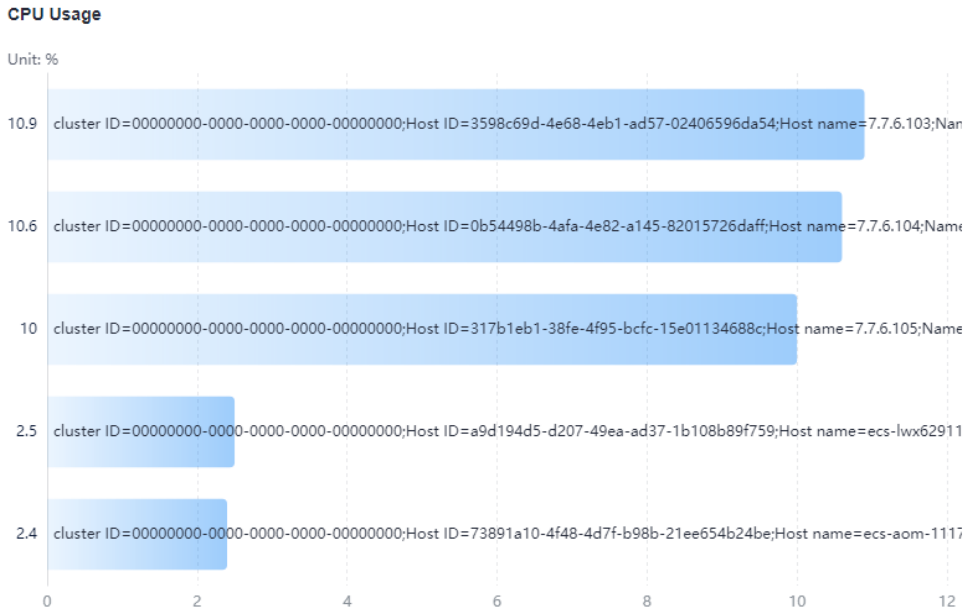


Table 5-34 Top N graph parameters

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

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

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

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

  Figure 5-22 Table

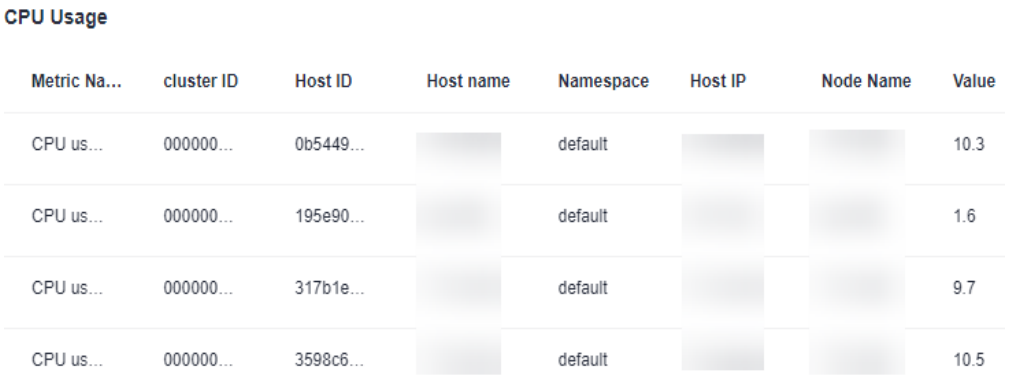
  

  Table 5-35 Table parameters

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

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

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

Figure 5-23 Bar graph

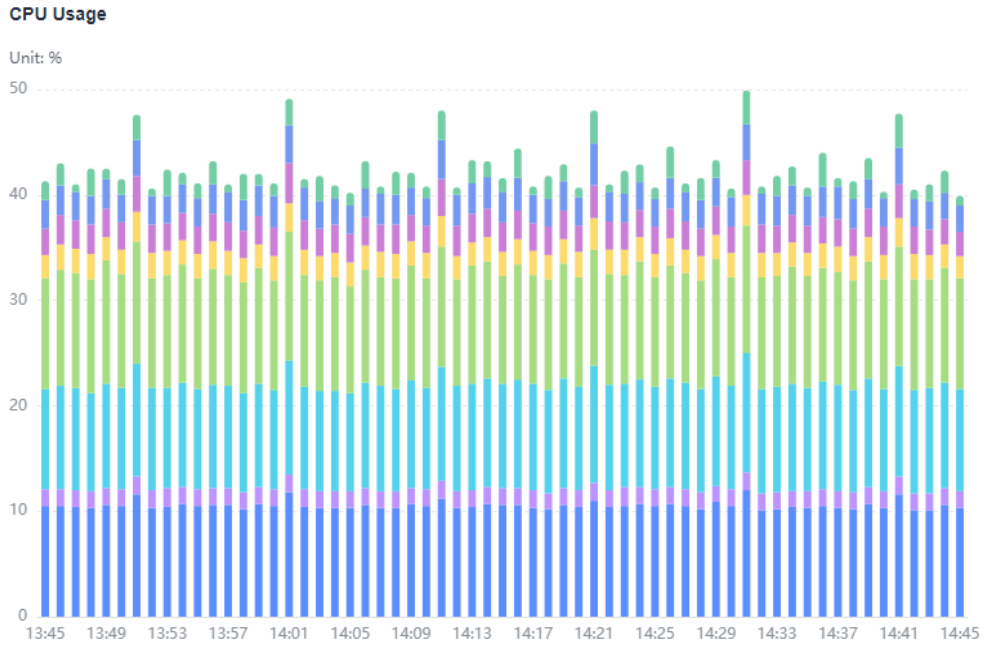


Table 5-36 Bar graph parameters

Category	Parameter	Description
Graphics	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.
	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.
X Axis	Show	Whether to display the X axis.
	X Axis Title	Title of the X axis.
Y Axis	Show	Whether to display the Y axis.
	Y Axis Title	Title of the Y axis.
	Y Axis Range	Value range of the Y axis.

- **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 5-24 Digital line graph

Table 5-37 Digital line graph parameters

Category	Parameter	Description
Chart Mode	Line Shape	Line type. Options: **Straight** and **Curved**.
	Hide Legend	Whether to hide legends.
	Show	Whether to display the X axis.
	Show	Whether to display the Y axis.
	Show Data Markers	Whether to display the connection points.

Log Data Graphs

The following types of graphs are supported: **line graphs**, **digit graphs**, **tables**, **bars**, **digital line graphs**, **pies**, and **maps**.

- **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 5-25 Line graph

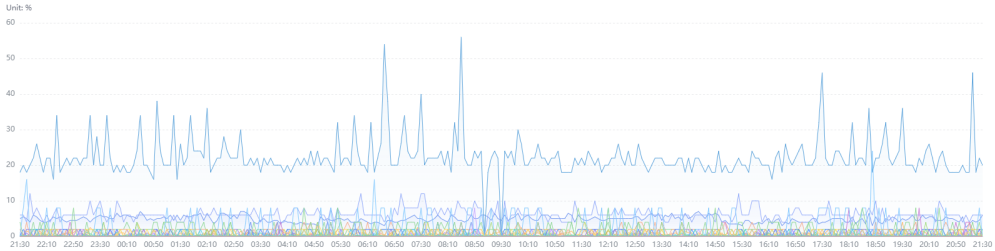


Table 5-38 Line graph parameters

Category	Parameter	Description
Standard	Format	Select **K,Mil,Bil**, **1,000,000**, or **Byte,KB,MB** from the drop-down list to specify the format of the Y axis.

Category	Parameter	Description
	Unit	Specifies the unit at the Y axis.
	Decimal Places	After this function is enabled, decimal places are displayed.
	Decimal Places	Sets the number of decimal places to display.
Query/ Analysis	X Axis	Numeric or string data is supported.
	Y Axis	Numeric or string data is supported. You can select multiple data records.
	Dimension	Select a value from the drop-down list. Generally, it is an ordinal variable.
	Compare Trends	This function can be enabled when the X axis shows time data and **Dimension** is not specified. After this function is enabled, set **Comparison** to a duration less than or equal to 24 hours. After the setting is complete, compare the data of the current time with the object time data.
Legend	Hide Legend	After this function is enabled, you can hide the legend and comparison results.
	Legend Position	Select **Top** or **Right**.
	Comparison Value	Indicates whether to display the maximum value, minimum value, average value, and sum value. You can select multiple options.
Graphics	Line Shape	Line type. Options: **Straight** and **Curved**.
	Line Width	Width of a line.
	Show Data Markers	Whether to display the connection points.
	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.
	Left Margin	Distance between the axis and the left boundary of the graph.
	Right Margin	Distance between the axis and the right boundary of the graph.

Category	Parameter	Description
Tooltip	Sort By	Dialog box configuration. When multiple Y-axis data records are selected, they can be sorted and displayed based on your configuration.
X Axis	Show	After this function is enabled, data on the X axis is displayed.
	X Axis Title	Title of the X axis.
Y Axis	Show	After this function is enabled, data on the Y axis is displayed.
	Y Axis Title	Title of the Y axis.
	Position	Position of the Y axis. Select **Left** or **Right**.

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

Figure 5-26 Digit graph

Table 5-39 Digit graph parameters

Category	Parameter	Description
Query/ Analysis	Data Column	Numeric or string data is supported.
	Comparison Data	Select a field to compare. The value of the field is displayed in the chart.
Main Items	Format	Displays data in the specified format.
	Data Text Size	Font size of the displayed value. The value ranges from 12 px to 80 px.
	Data Unit	Unit of the displayed value.
	Unit Text Size	Font size of the displayed value unit. The value ranges from 12 px to 50 px.
	Decimal Places	After this function is enabled, decimal places are displayed.

Category	Parameter	Description
	Decimal Places	Sets the number of decimal places to display.
	Add Comparison Data	Whether to display the value of the field to compare.
	Comparison Formatting	Displays the data to compare in the specified format.
	Comparison Data Text Size	Font size of the value to compare. The value ranges from 12 px to 50 px.
	Comparison Data Unit	Unit to compare.
	Comparison Unit Text Size	Font size of the value unit to compare. The value ranges from 12 px to 50 px.
	Description	Description of the displayed value and comparison trend. The description is displayed below the value.
Background	Background	Background color of a chart, which can be dark or light.

- **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.

Figure 5-27 Table

Table 5-40 Table parameters

Category	Parameter	Description
Standard	Format	Displays the table data in the specified format.
	Unit	Specifies the unit of the data in the custom table.
	Decimal Places	After this function is enabled, decimal places are displayed.
	Decimal Places	Sets the number of decimal places to display.
Query/ Analysis	Hidden Fields	Select a field to hide.
Table	Records per Page	Number of data records displayed on each page.
	Display Total	After this function is enabled, the total number of records in the table is displayed.
Column	Alignment	Alignment mode of table data. Options: **Left**, **Right**, and **Center**.
	Filtering	After this function is enabled, you can search for data in the table column.
	Sorting	After this function is enabled, you can sort data in the table.
	Font Size	Size of the table font. The value ranges from 12 px to 24 px.

- **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 5-28 Bar graph

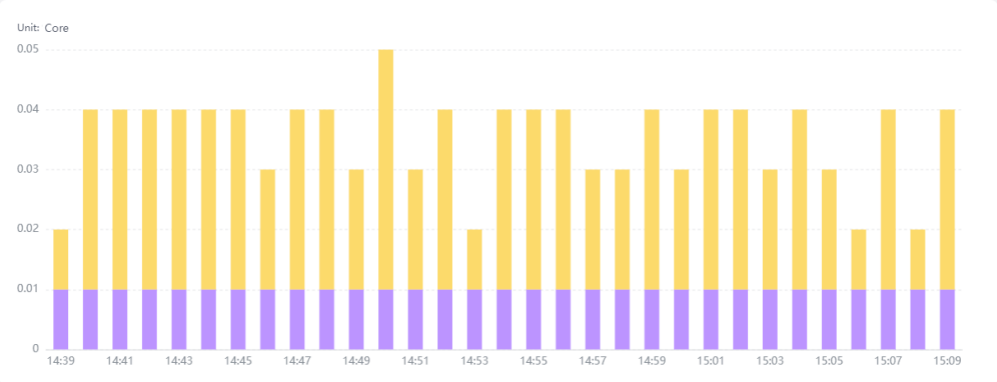


Table 5-41 Bar graph parameters

Category	Parameter	Description
Standard	Format	Displays the Y axis in the specified format.
	Unit	Specifies the unit at the Y axis.
	Decimal Places	After this function is enabled, decimal places are displayed.
	Decimal Places	Sets the number of decimal places to display.
Bar Chart	Direction	Select **Bar chart** or **Horizontal bar chart**.
	Column Width	Sets the column width.
	Display Value	After this function is enabled, the value indicated by each bar is displayed.
	Font Size	Sets the font size of each bar.
	Stacked	After this function is enabled, the Y axis data is displayed in stack mode.
Query/ Analysis	X Axis	Numeric or string data is supported.
	Y Axis	Numeric or string data is supported. You can select multiple data records.
Legend	Hide Legend	After this function is enabled, you can hide the legend and comparison results.
	Legend Position	Position of the legend in the chart. Select **Top** or **Right**.
	Comparison Value	Indicates whether to display the maximum value, minimum value, average value, and sum value. You can select multiple options.
Graphics	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.
	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.
Tooltip	Sort By	Dialog box configuration. When multiple Y-axis data records are selected, they can be sorted and displayed based on your configuration. Options: **None**, **Ascending**, and **Descending**.

Category	Parameter	Description
X Axis	Show	After this function is enabled, data on the X axis is displayed.
	X Axis Title	Title of the X axis.
Y Axis	Show	After this function is enabled, data on the Y axis is displayed.
	Y Axis Title	Title of the Y axis.
	Position	Position of the Y axis. Select **Left** or **Right**.

- **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 5-29 Digital line graph

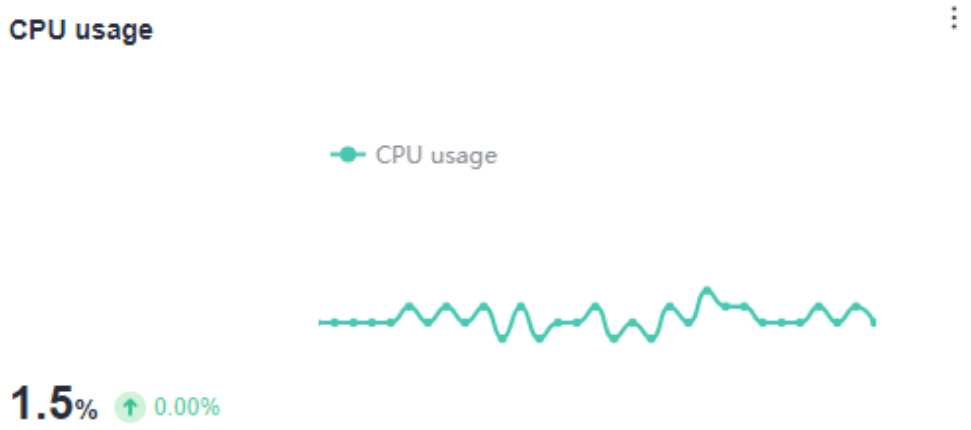


Table 5-42 Digital line graph parameters

Category	Parameter	Description
Query/Analysis	X Axis	Numeric or string data is supported.
	Y Axis	Numeric or string data is supported. You can select multiple data records.
Chart Mode	Line Shape	Line type. Options: **Straight** and **Curved**.
Main Items	Number Format	Displays data in the specified format.
	Data Text Size	Font size of the displayed value. The value ranges from 12 px to 80 px.

Category	Parameter	Description
	Data Unit	Unit of the displayed value.
	Unit Text Size	Font size of the displayed value unit. The value ranges from 12 px to 50 px.
	Decimal Places	After this function is enabled, decimal places are displayed.
	Decimal Places	Sets the number of decimal places to display.
Background	Background	Background color of a chart, which can be dark or light.

- **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 5-30 Pie graph

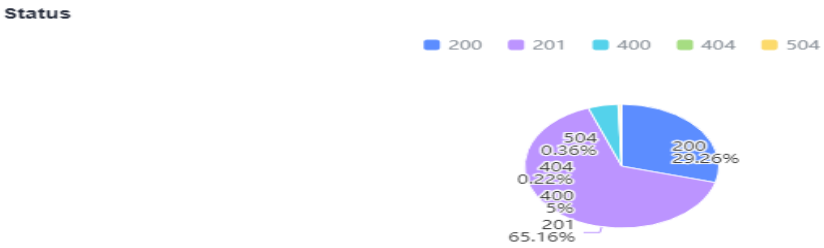


Table 5-43 Pie graph parameters

Category	Parameter	Description
Standard	Format	Select **K,Mil,Bil**, **1,000,000**, or **Byte,KB,MB** from the drop-down list to specify the format of the Y axis.
	Unit	Specifies a unit.
	Decimal Places	After this function is enabled, decimal places are displayed.
	Decimal Places	Sets the number of decimal places to display.

Category	Parameter	Description
Pie Chart	Pie Chart Type	Options: **Pie**, **Cyclic**, and **Coxcomb**. • Pie A pie chart displays the proportion of each part. It divides a circle into different sectors. The area (or arc length and central angle) of each sector corresponds to the proportion of each part. In this way, the relationship between each part and the whole is intuitively displayed. • Cyclic Essentially, a cyclic chart hollows out the center of a pie chart. Cyclic charts are better than pie charts in the following aspects: – Cyclic charts display more information such as the total number. – It is not intuitive to compare two pie charts directly. You can compare two cyclic charts by the cyclic bar length. • Coxcomb A Coxcomb chart is not a cyclic chart in essence. Instead, it is a bar chart drawn in the polar coordinate system. Each category is evenly divided by an arc. The radius of the arc indicates the data size. Coxcomb charts are better than pie charts in the following aspects: – A pie chart can contain a maximum of 10 categorized data records, while a Coxcomb chart can contain 10 to 30 data records. – Because the radius and area are squared, a Coxcomb chart magnifies the difference between the values of each category. It is suitable for comparing the values of similar sizes. – Due to the periodicity of a circle, a Coxcomb chart is also suitable for displaying data by period, such as by week and month.
	Show Scale	After this function is enabled, text labels are displayed on the pie chart to describe data details, such as the value and name.
	Scale Text	Options: **Category**, **Percent**, **Category: %**, and **Category: Value (%)**.

Category	Parameter	Description
	Label Position	After **Show Scale** is enabled, you can set this parameter to adjust the position of the label in the chart.
Query/ Analysis	Value	Specifies the value corresponding to the categorized data.
	Layer 1 Data	
	Category	Specifies the categorized data.
	Display as Sectors	Specifies the number of categorized data records to display.
	Sort By	Options: **Ascending** and **Descending**.
	Display Rest as Others	Specifies whether to display the data of other types as **Others**.
	Add Layer	Click **Add Layer** and set the data of the second layer. The data of each layer includes the category, display sectors, sorting mode, and displaying rest sectors as others.
Legend	Hide Legend	After this function is enabled, you can hide the legend and its content.
	Legend	Select **Value** or **Percent**, or both.
	Legend Position	Position of the legend in the chart. Select **Top** or **Right**.
Graphics	Outer Radius	Outer radius of the pie chart. The value ranges from 40 to 100.
	Inner Radius	Inside radius of the pie chart. The value ranges from 0 to 100.
	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.
	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.

- **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 5-31 Map

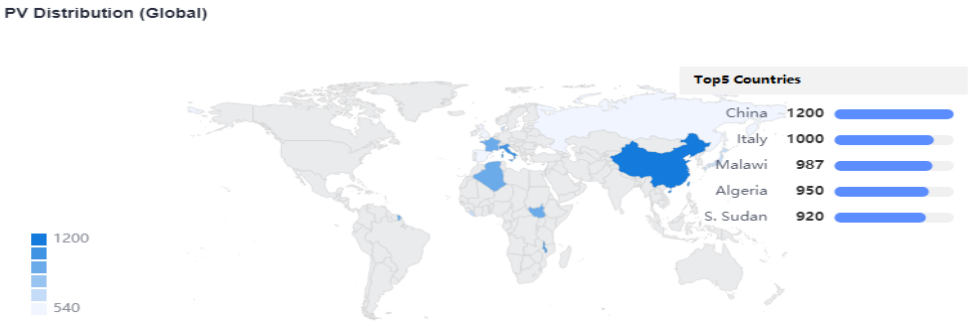


Table 5-44 Map graph parameters

Parameter	Description
Map Type	Select a value from the drop-down list. You can select a provincial 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.
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.

6 Alarm Monitoring

6.1 AOM Alarm Monitoring Overview

AOM provides alarm monitoring capabilities. 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. Events generally carry some important information. They are reported when AOM or an external service has some changes. Such changes do not necessarily cause service exceptions.

Description

- Alarm action rules: 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.
- Alarm noise reduction: The system processes alarms based on noise reduction rules to prevent an alarm storm.
- Alarm rules: Create alarm or event rules to monitor resource usage in real time.
- Viewing alarms or events: Query alarms and events for quick fault detection, locating, and recovery.

6.2 Configuring AOM Alarm Notification

6.2.1 Creating AOM Alarm Message Templates

In AOM, you can create message templates to customize notifications. When a preset notification rule is triggered, notifications can be sent to specified personnel by email, SMS, Lark, WeCom, DingTalk, voice call, WeLink, HTTP, or HTTPS.

Function Introduction

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

- You can customize message templates. For details, see **Step 3.3**.

Constraints

- 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.
- AOM provides preset message templates. They cannot be deleted or edited. If there is no custom message template, notifications are sent based on a preset message template by default.
- If no message template is created, the default message template will be used.
- WeLink message templates are not yet generally available. If you need this function, **submit a service ticket**.

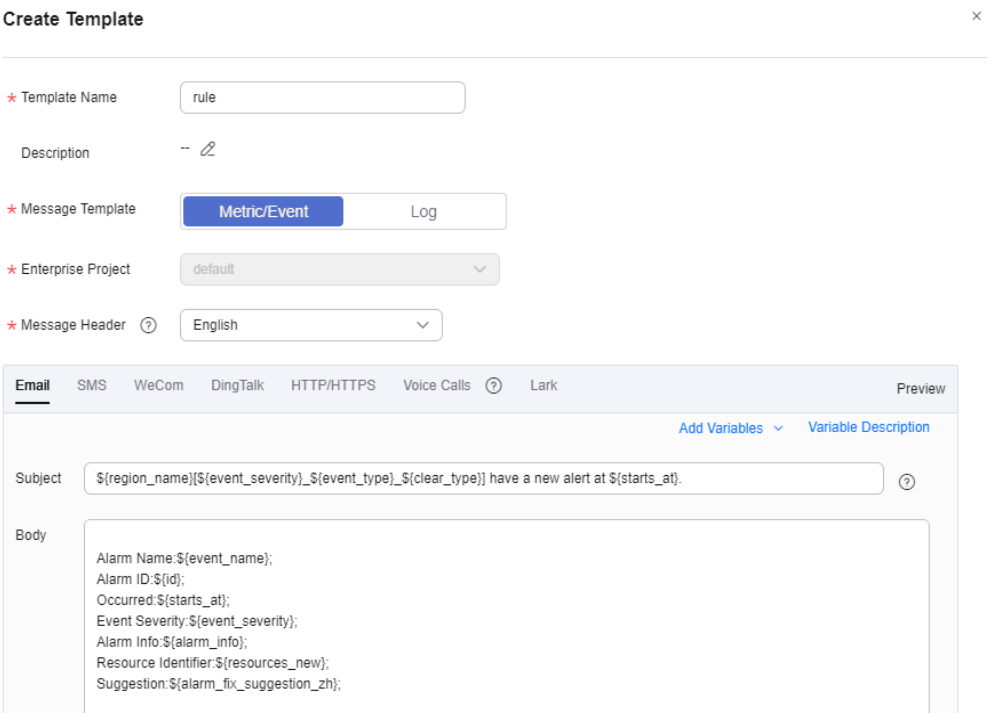
Creating a Message Template

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 6-1 Creating a message template



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

Table 6-1 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 6-2**. For details about log templates, see **Table 6-3**.
   - 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.
   - 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 copy required variables.
   - The **TMS tag: $event.annotations.tms_tags** variable configured in the alarm message template takes effect only after **TMS Tag Display** is enabled.
   - If you select **Emails**, you can click **Preview** to view the final effect. On the **Preview** page, change the message topic if necessary.

Table 6-2 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}

Variable	Description	Definition
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_new}
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 6-3 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: *$event.annotations.results[0].resource_id* **Only the original name of the log group or stream created for the first time can be added.** – SQL variables 1. Log group/stream names of chart 0: *$event.annotations.results[0].resource_id* **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 6-4**.

Table 6-4 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. **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  .

6.2.2 Creating an AOM 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

- You have created a topic. For details, see **Creating a Topic**.
- You have configured a topic policy. For details, see **Configuring Topic Policies**.
- You have added a subscriber, that is, the email or SMS message recipient, for the topic. For details, see **Adding a Subscription to a Topic**

Constraints

- You can create a maximum of 1,000 alarm action rules. If this number has been reached, delete unnecessary rules.

Creating an Alarm Action Rule

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 6-5**.

Figure 6-2 Creating an alarm action rule

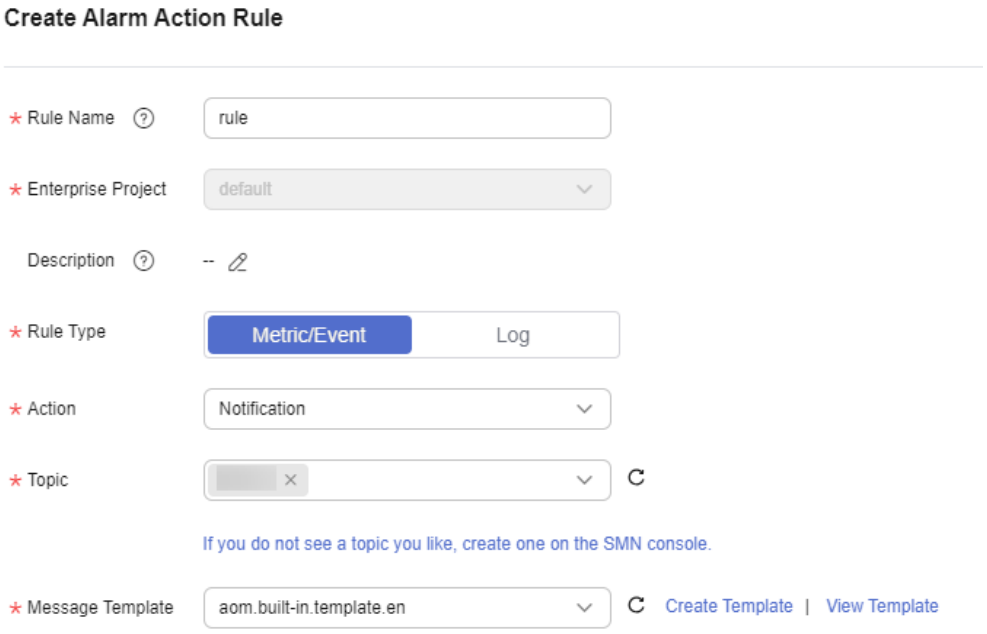


Table 6-5 Parameters of an alarm action rule

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.
Rule Type	Type of an alarm action rule. • 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.

Parameter	Description
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. AOM provides preset message templates. If the preset templates do not meet requirements, click **Create Template** to create a template. For details, see **6.2.1 Creating AOM Alarm Message Templates**.

Step 5 After the settings are complete, click **OK**. The alarm action rule is created. You can then perform the following operations:

- Go to the **Alarm Noise Reduction** page, **create a grouping rule**, and associate it with the action rule.
- Go to the **Alarm Rules** page, **create an alarm rule**, and associate it with the action rule.

----End

More Operations

After an alarm action rule is created, you can perform operations described in **Table 6-6**.

Table 6-6 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. When deleting an alarm action rule, note that: • Before deleting an alarm action rule, you need to delete the alarm rule or grouping rule bound to it. • If an alarm action rule is deleted, alarm notifications cannot be received in a timely manner.

Operation	Description
Searching for an alarm action rule	Enter a rule name in the search box in the upper right corner and click  .

6.3 Configuring AOM Alarm Rules

6.3.1 AOM Alarm Rule Overview

AOM allows you to set alarm and event rules. You can create metric/log alarm rules to monitor the real-time usage of resources such as hosts and components in the environment, helping you quickly detect, locate, and rectify faults. By creating event alarm rules, you can simplify alarm notifications and quickly troubleshoot resource usage problems.

Description

- **6.3.2 Creating an AOM Metric Alarm Rule**

  For metric alarm rules, you can set threshold conditions for resource metrics. If a metric value meets a threshold condition, AOM generates a threshold alarm. If no metric data is reported, AOM generates an insufficient data event.
- **6.3.3 Creating an AOM 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.
- **6.3.4 Creating an AOM Log Alarm Rule**

  You can create alarm rules based on keyword statistics, search analysis, or SQL statistics so that AOM can monitor log data in real time and report alarms if there are any.
- **6.3.5 Creating AOM Alarm Templates in Batches**

  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.

Constraints

A maximum of 3,000 metric/event alarm rules can be created. If the number of alarm rules has reached the upper limit, delete unnecessary rules and create new ones.

6.3.2 Creating an AOM Metric Alarm Rule

For metric alarm rules, you can set threshold conditions for resource metrics. If a metric value meets a threshold condition, AOM generates a threshold alarm. If no metric data is reported, AOM generates an insufficient data event.

Creation Mode

You can create metric alarm rules in the following ways: **Select from all metrics** and **PromQL**.

Constraints

- If you need AOM to send WeCom/DingTalk/Lark/voice call/WeLink/email/SMS notifications when the metric alarm rule status (**Exceeded**, **Normal**, **Effective**, or **Disabled**) changes, set an alarm action rule according to **6.2.2 Creating an AOM Alarm Action Rule**.
- Second-level monitoring is supported when you create metric alarm rules by selecting metrics from all metrics or using PromQL. The timeliness of metric alarms depends on the metric reporting period, rule check interval, and notification send time.
- A maximum of 3,000 metric/event alarm rules can be created.

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 6-7**.

Table 6-7 Basic information

Parameter	Description
Rule Name	Name of the alarm 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 6-8** 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 6-3 Setting alarm rule details

Table 6-8 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.

Parameter	Description
Combined Operations	The system performs calculation based on the expression you set. If the condition is met, an alarm will be triggered. For example, if there is no metric showing the CPU core usage of a host, do as follows: – Set the metric of alarm condition "a" to **aom_node_cpu_used_core** and retain the default values for other parameters. This metric is used to count the number of CPU cores used by a measured object. – Set the metric of alarm condition "b" to **aom_node_cpu_limit_core** and retain the default values for other parameters. This metric is used to count the total number of CPU cores that have been applied for a measured object. – If the expression is set to "a/b", the CPU core usage of the host can be obtained. – Set **Rule** to **Max > 0.2**. – In the trigger condition, set **Consecutive Periods** to **3**. – Set **Alarm Severity** to **Critical**. If the maximum CPU core usage of a host is greater than 0.2 for three consecutive periods, a critical alarm will be generated.
Metric	Metric to be monitored. 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 15 seconds, 30 seconds, 1 minute, 5 minutes, 15 minutes, or 1 hour.

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

Parameter	Description
Trigger Condition	When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated. Range: 1 to 30. **NOTE** The period refers to **Check Interval** set in **Advanced Settings**. For example, if **Statistical Period** is set to **5 minutes**, **Consecutive Periods** is set to **2**, and **Check Interval** is set to **1 minute**, the metric data within 5 minutes is calculated, and a metric alarm is triggered if the detection rule is met for two consecutive periods (a total of 2 minutes).
Alarm Severity	Metric alarm severity. Options: – : critical alarm. – : major alarm. – : minor alarm. – : warning.

Step 6 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see **Table 6-9**.

Table 6-9 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. **You can set Check Interval to 15 seconds or 30 seconds to implement second-level monitoring.** • **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.

Parameter	Description
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 30 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.
Action Taken for Insufficient Data	Action to be taken when no metric data is generated or metric data is insufficient for a specified number of consecutive periods. 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 **No 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**. **If tag policies have been configured in your organization, you need to add alarm tags based on these policies. If your tags do not comply with these policies, the tags may fail to be added. Contact the administrator when necessary.**
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 6-10**.

Figure 6-4 Setting an alarm notification policy

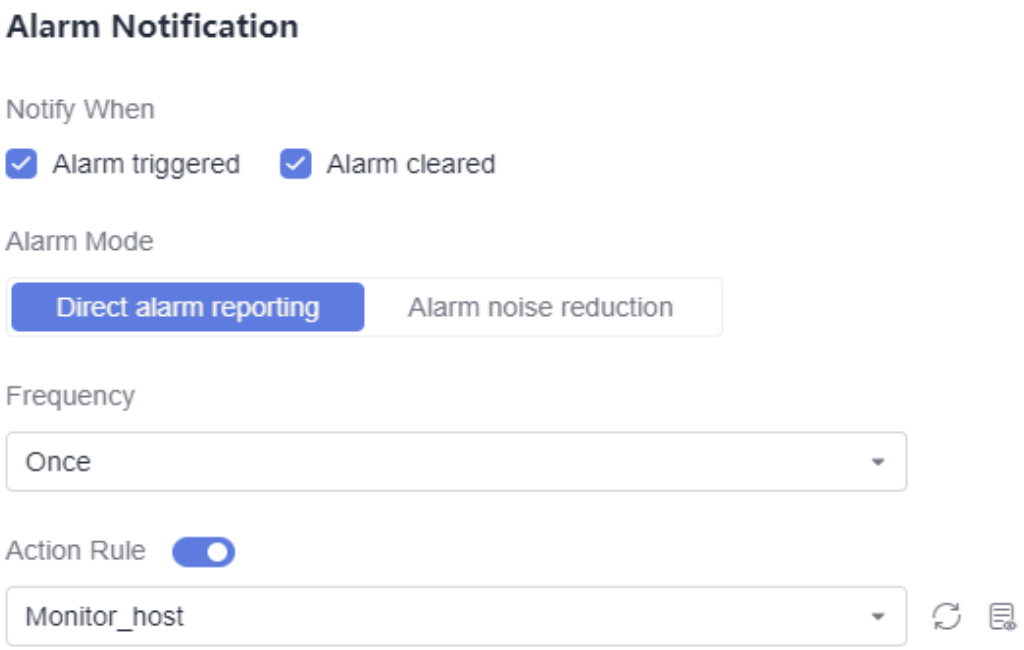


Table 6-10 Parameters for setting an alarm notification policy

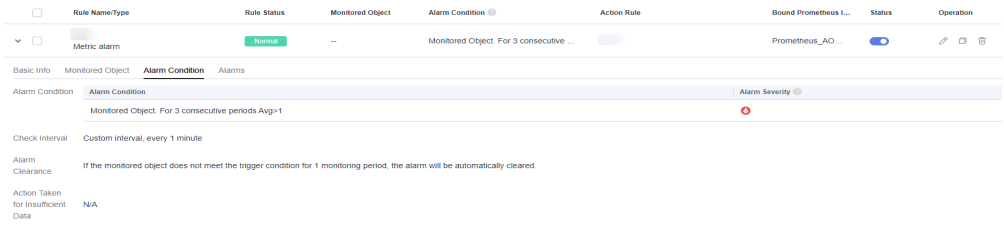
Parameter	Description
Notify When	Set the scenario for sending alarm notifications. • **Alarm triggered**: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. • **Alarm cleared**: If the alarm clearance condition is met, the system 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 **6.5.2 Creating an AOM Alarm Grouping Rule**. **The alarm severity and tag configured in the selected grouping rule must match those configured in the alarm rule. Otherwise, the grouping rule does not take effect.**

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 6-5 Created metric alarm rule



----End

Creating Metric Alarm Rules by Running Prometheus Statements

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 Click **Create**.

Step 4 Set basic information about the alarm rule by referring to **Table 6-11**.

Table 6-11 Basic information

Parameter	Description
Rule Name	Name of the alarm 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 6-12** 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 6-6 Setting alarm rule details

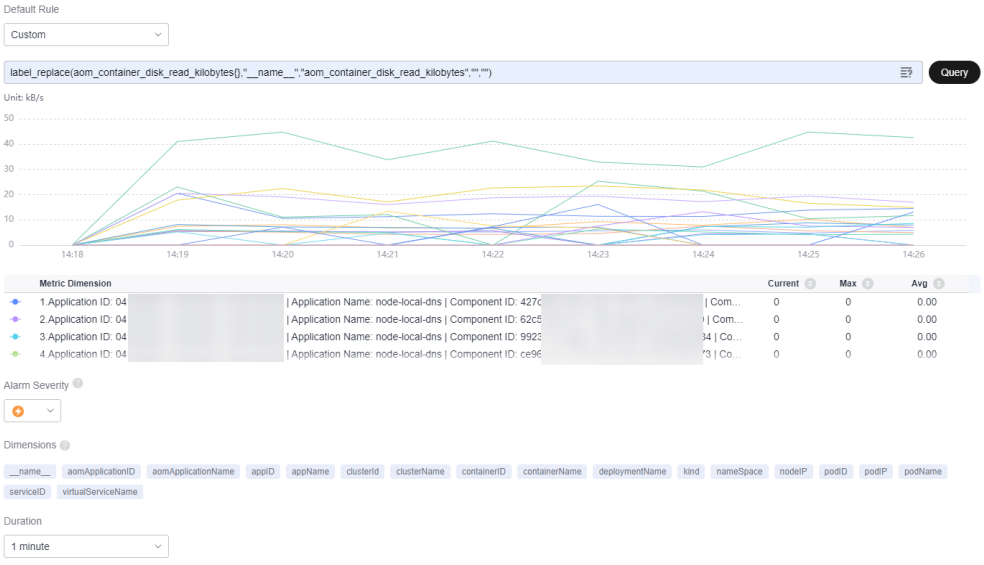


Table 6-12 Alarm rule details

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 **6.3.8 Prometheus Statements**.
Alarm Severity	Metric alarm severity. Options: – : critical alarm. – : major alarm. – : minor alarm. – : 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. Options: Include **Immediate**, **15 seconds**, **30 seconds**, **1 minute**, **2 minutes**, **5 minutes**, and **10 minutes**. For example, if **Duration** is set to **2 minutes**, a metric alarm is triggered when the default rule condition is met for 2 minutes.

Step 6 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see **Table 6-13**.

Table 6-13 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. • *XX* **seconds**: Check the query and analysis results every *XX* seconds. **You can set Check Interval to 15 seconds or 30 seconds to implement second-level monitoring.**
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 **6.3.7 Alarm Tags and Annotations**. **If tag policies have been configured in your organization, you need to add alarm tags based on these policies. If your tags do not comply with these policies, the tags may fail to be added. Contact the administrator when necessary.**
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 **6.3.7 Alarm Tags and Annotations**.

Step 7 Set an alarm notification policy. For details, see **Table 6-14**.

Figure 6-7 Setting an alarm notification policy

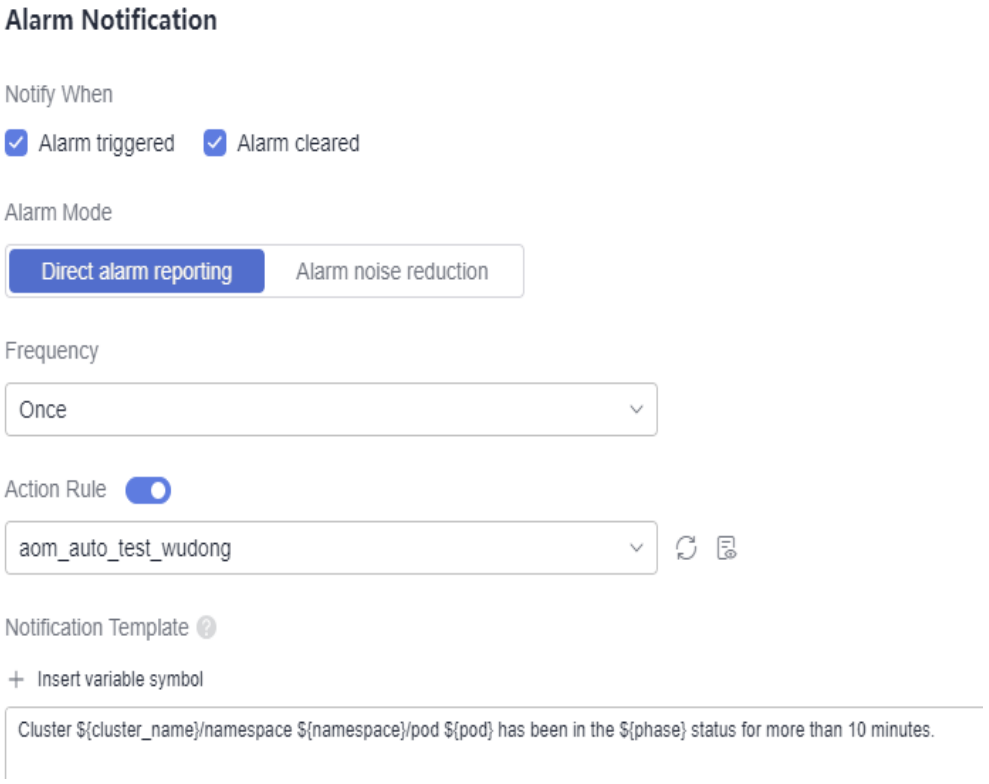


Table 6-14 Parameters for setting an alarm notification policy

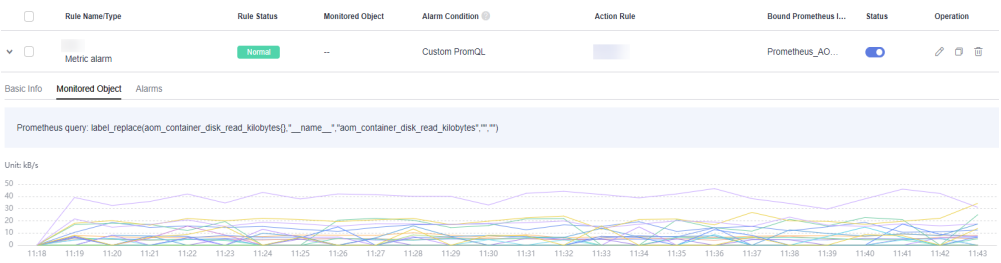
Parameter	Description
Notify When	Set the scenario for sending alarm notifications. • **Alarm triggered**: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. • **Alarm cleared**: If the alarm clearance condition is met, the system 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 **6.5.2 Creating an AOM Alarm Grouping Rule**. **The alarm severity and tag configured in the selected grouping rule must match those configured in the alarm rule. Otherwise, the grouping rule does not take effect.**
Notification Template	Template for sending alarm notifications. Notification content is automatically generated when **Default Rule** is set to **CCEFromProm**. • You can use variables (that is, dimensions) in a notification template. The format is "${Dimension}".

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 6-8 Created metric alarm rule



----End

6.3.3 Creating an AOM 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.

Constraints

- If you want to receive WeCom/DingTalk/Lark/voice call/WeLink/email/SMS notifications when the resource data meets the event condition, set an alarm action rule by referring to **6.2.2 Creating an AOM Alarm Action Rule**.
- A maximum of 3,000 metric/event alarm rules can be created.
- When setting an alarm notification policy, enabling alarm noise reduction and associating the policy with a grouping rule are not recommended. This is because accumulated triggering is similar to alarm noise reduction.

Procedure

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 Click **Create**.

Step 4 Set basic information about the alarm rule by referring to **Table 6-15**.

Table 6-15 Basic information

Parameter	Description
Rule Name	Name of the alarm 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.
   - **System**: events ingested to AOM by default. Options: CCE/IoTDA/ModelArts.
   - **Custom**: third-party service events ingested to AOM. Select an event source from the existing service list.
3. Set alarm rule details.

Figure 6-9 Setting alarm rule details

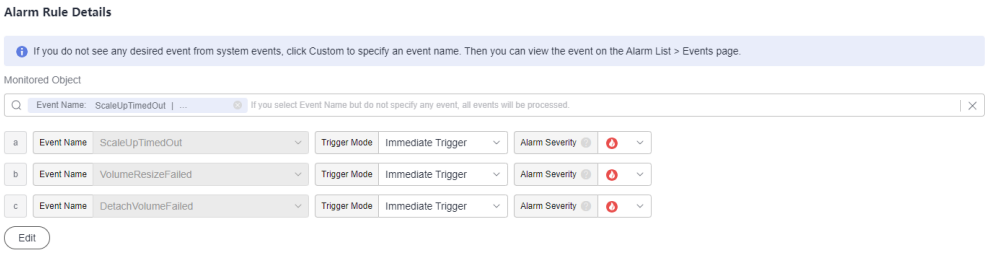


Table 6-16 Alarm rule parameters

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. **Set Event Name as the filter criterion. If no event name is selected, all events are selected by default.**

Parameter	Description
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**: A notification is triggered at a preset frequency after an event or alarm trigger condition is met for a specified number of times. If **Alarm Frequency** is set to **N/A**, there is no limit on the number of notifications. That is, one notification is sent when an event or alarm trigger condition is met for a specified number of times. 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. **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**: A notification is triggered immediately after an event or alarm trigger condition is met. – **Alarm Severity**: Severity of an alarm. ▪ : critical alarm. ▪ : major alarm. ▪ : minor alarm. ▪ : warning. In case of multiple events, click **Batch Set** to set alarm conditions for these events in batches.

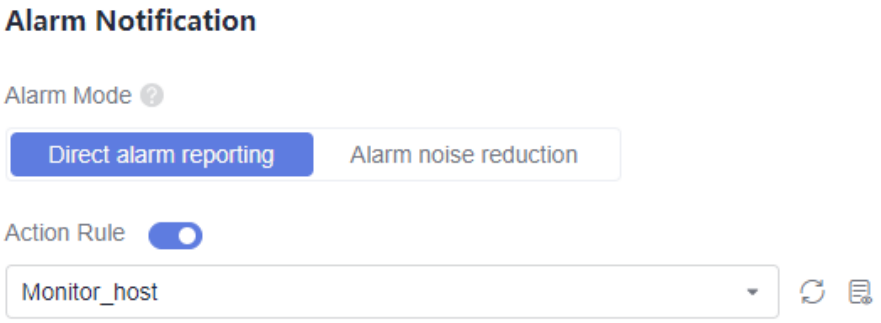
Step 6 Set an alarm notification policy. There are two alarm notification modes. Select one as required.

- **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 **6.2.2 Creating an AOM Alarm Action Rule**.

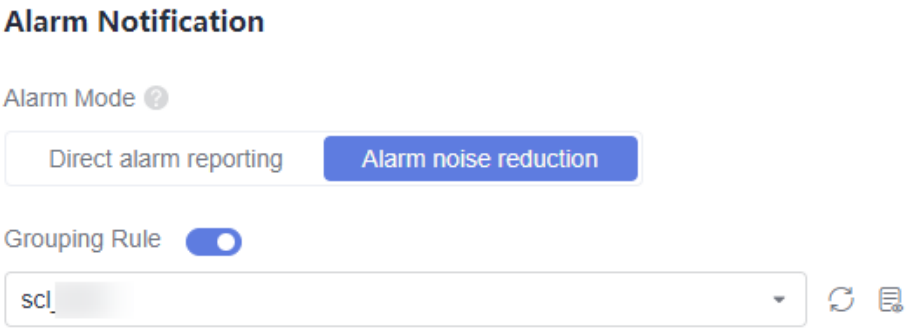
Figure 6-10 Selecting the direct alarm reporting mode



- **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 **6.5.2 Creating an AOM Alarm Grouping Rule**. **The alarm severity and tag configured in the selected grouping rule must match those configured in the alarm rule. Otherwise, the grouping rule does not take effect.**

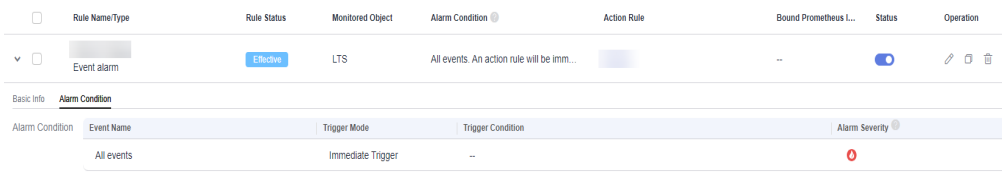
Figure 6-11 Selecting the alarm noise reduction mode



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 6-12 Created event alarm rule



----End

6.3.4 Creating an AOM Log Alarm Rule

You can create alarm rules based on keyword statistics, search analysis, 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**.

Constraints

- 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

Log alarm rules can be created by referring to **Creating Log Alarm Rules by Keyword**, **Creating Log Alarm Rules Based on Search Analysis**, 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 6-17**.

Table 6-17 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. **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	**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. 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. ● The alarm severity can be **Critical** (default), **Major**, **Minor**, or **Info**. ● 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. Number of queries: 1–10 ● Click **+** to add a conditional expression with an OR relationship. A maximum of 20 conditional expressions can be added. ● Click  to delete a conditional expression. 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 (%).

Category	Parameter	Description
		– 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
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. When the query time range is larger than 1 hour, the interval must be at least 5 minutes. 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. ● **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 **6.2.2 Creating an AOM 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 **Create**.

Step 4 On the displayed page, set alarm rule parameters by referring to **Table 6-18**.

Table 6-18 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. **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. 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.
		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 (**<=**). • The alarm severity can be **Critical** (default), **Major**, **Minor**, or **Info**. • 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. Number of queries: 1–10 • Click **+** to add a conditional expression with an OR relationship. A maximum of 20 conditional expressions can be added. • Click  to delete a conditional expression.

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. When the query time range is larger than 1 hour, the interval must be at least 5 minutes. 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. • **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 **6.2.2 Creating an AOM 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 6-19**.

Table 6-19 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. **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. If no structuring rule has been configured, **configure structuring** first. Set parameters as follows: **Log Group Name**: (Required) Select a log group. **Log Stream Name**: (Required) Select a log stream. **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. – 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. **NOTE**

Category	Parameter	Description
	Check Rule	Enter a specific conditional expression. When the expression execution result is **true**, an alarm is generated. ● The alarm severity can be **Critical** (default), **Major**, **Minor**, or **Info**. ● 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. Number of queries: 1–10 ● Click **+** to add a conditional expression with an OR relationship. A maximum of 20 conditional expressions can be added. ● Click  to delete a conditional expression. 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 (%).

Category	Parameter	Description
		– 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
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. When the query time range is larger than 1 hour, the interval must be at least 5 minutes. 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. ● **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 **6.2.2 Creating an AOM Alarm Action Rule**.
	Languages	Specify the language (**English**) in which alarms are sent.

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

----End

6.3.5 Creating AOM Alarm Templates in Batches

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.

Constraints

- 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 6-20** describes the parameters.

Table 6-20 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 6-21**.

Figure 6-13 Adding an alarm rule for the cloud service

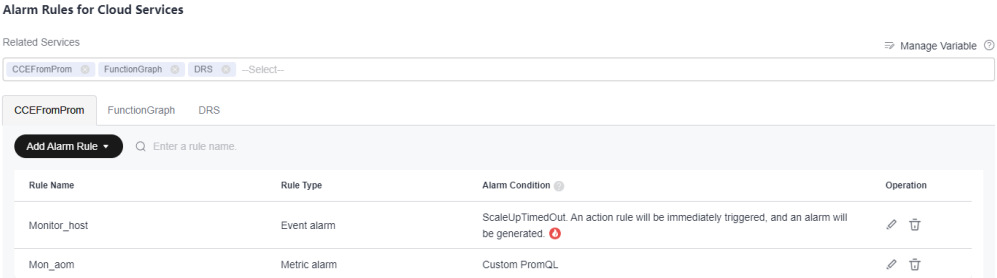


Table 6-21 Parameters for adding an alarm rule for the cloud service

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 **Create Rule** dialog box, set a rule name, metric, and alarm condition. For details, see **Step 5.4** and **Step 6** in **Creating Metric Alarm Rules by Selecting Metrics from All Metrics**. 3. Click **OK**.
CCEFromProm	Event alarm rule	See **Step 6**.
	PromQL alarm rule	See **Step 7**.

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

1. Choose **Add Alarm Rule** > **Add Event Alarm Rule**.
2. In the displayed dialog box, set the rule name and event rule details. For details, see **Table 6-22**.
   - 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 6-14 Adding an event alarm rule

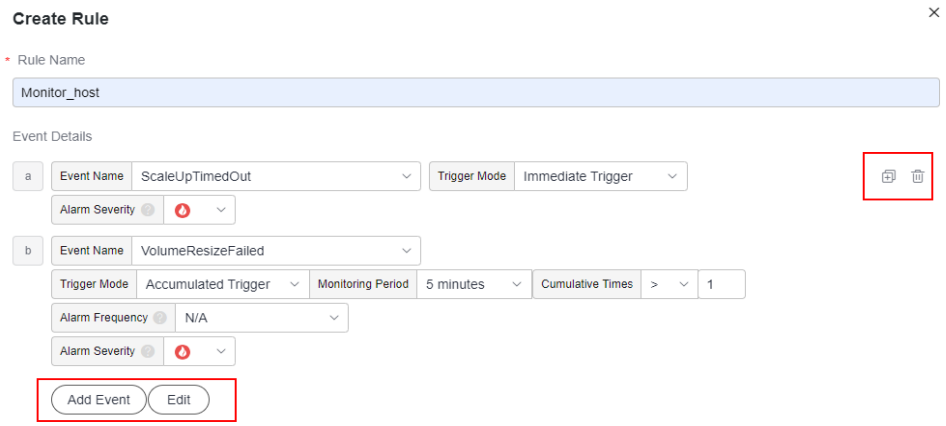


Table 6-22 Event rule parameters

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.
Alarm Severity	Severity of an event alarm. – : critical alarm. – : major alarm. – : minor alarm. – : warning.

3. Click **OK**.

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

1. Choose **Add Alarm Rule** > **Add PromQL Alarm Rule**.
2. In the displayed dialog box, set the rule name, default rule, and alarm severity. For details, see **Table 6-23**.

Figure 6-15 Adding a PromQL alarm rule

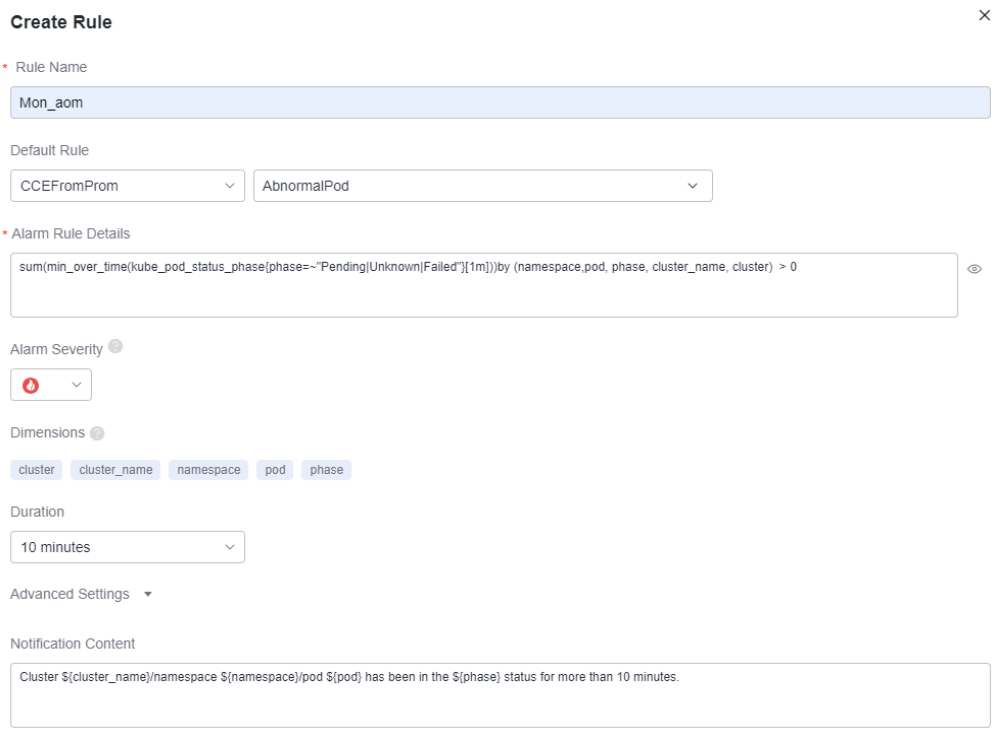


Table 6-23 PromQL alarm rule parameters

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 supports the following two input modes: – **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. Click next to the alarm rule details to lock the content. Then you can perform the following operations: – Click next to the alarm rule details to unlock the content. – Click next to the alarm rule details to copy the Prometheus statement. For details, see **6.3.8 Prometheus Statements**.
Alarm Severity	Severity of a metric alarm. – : critical alarm. – : major alarm. – : minor alarm. – : 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. Options: Include **Immediate**, **15 seconds**, **30 seconds**, **1 minute**, **2 minutes**, **5 minutes**, and **10 minutes**. For example, if **Duration** is set to **2 minutes**, a metric alarm is triggered when the default rule condition is met for 2 minutes.

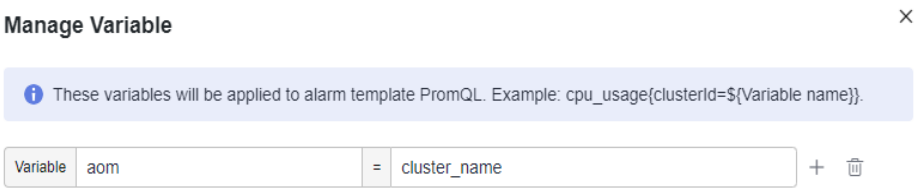
Parameter		Description
Advanced Settings	Check Interval	Interval at which metric query and analysis results are checked. – *XX* **hours**: Check the query and analysis results every *XX* hours. – *XX* **minutes**: Check the query and analysis results every *XX* minutes. – *XX* **seconds**: Check the query and analysis results every *XX* seconds. You can set **Check Interval** to **15 seconds** or **30 seconds** to implement second-level monitoring. The timeliness of metric alarms depends on the metric reporting period, rule check interval, and notification send time. For example, if the metric reporting period is 15 seconds, rule check interval is 15 seconds, and notification send time is 3 seconds, an alarm can be detected and an alarm notification can be sent within 33 seconds.
	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 **6.3.7 Alarm Tags and Annotations**. 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 **6.3.7 Alarm Tags and Annotations**.
Notification Content		Content of an alarm notification to be sent. This content is automatically generated when **Default Rule** is set to **CCEFromProm**.

3. Click **OK**.

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

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

Figure 6-16 Managing variables



3. Click **OK**.

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

Step 10 (Optional) In the displayed **Bind Alarm Template with Prometheus Instance/Cluster** dialog box, set the cluster or Prometheus instance to be bound with the alarm template. For details about the parameters, see **Table 6-24**. After the settings are complete, click **OK**.

Figure 6-17 Binding an alarm template with a Prometheus instance or cluster

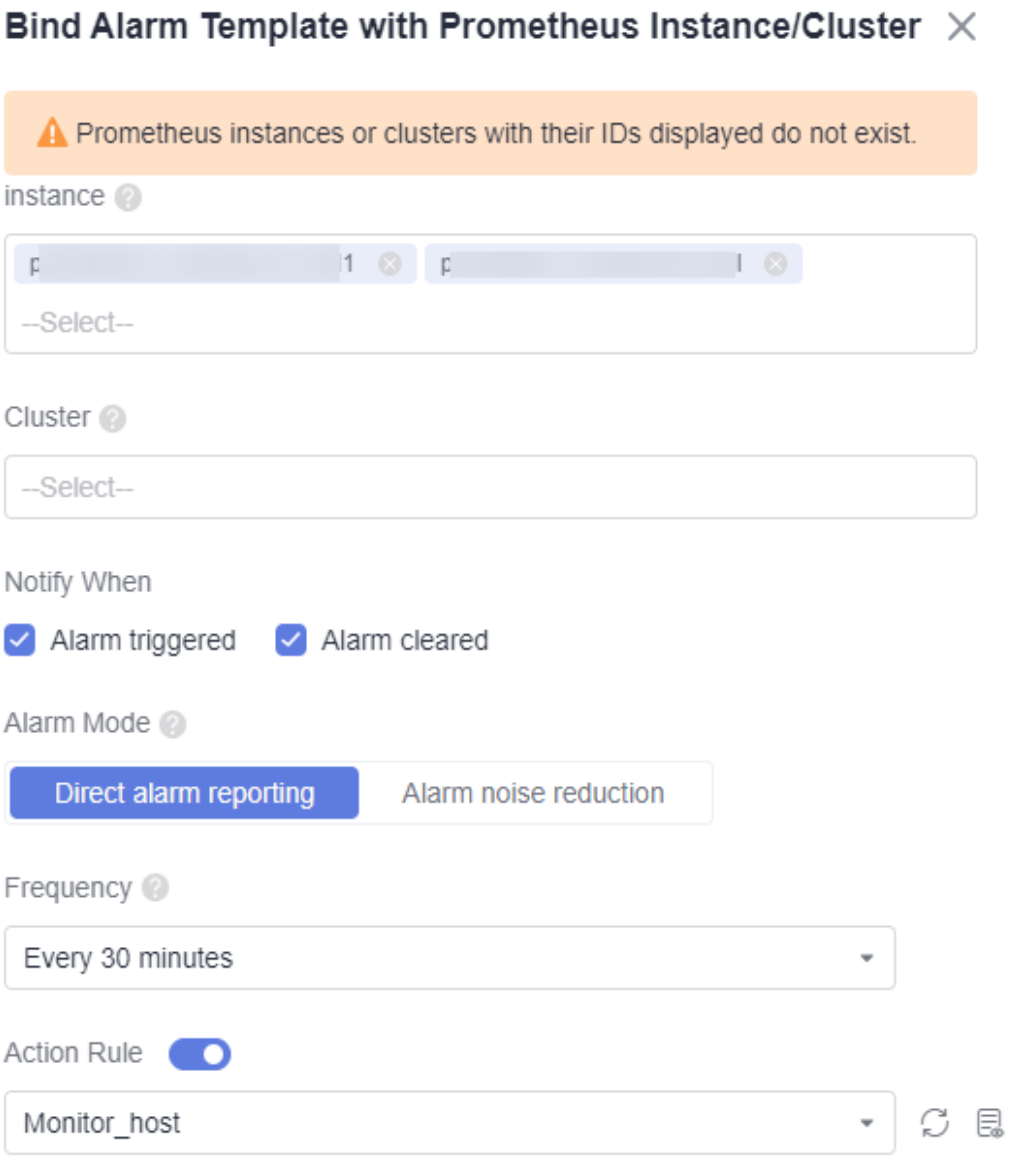


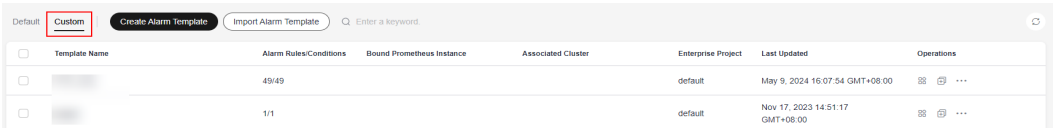
Table 6-24 Parameters for binding an alarm template

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 the current account. To associate an alarm template with a CCE cluster, you need to obtain CCE permissions in advance. For details, see **Permissions**.
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 **6.5.2 Creating an AOM Alarm Grouping Rule**. **The alarm severity and tag configured in the selected grouping rule must match those configured in the alarm rule. Otherwise, the grouping rule does not take effect.**

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

If a resource or metric meets the alarm condition set in the alarm template, an alarm will be triggered. In the navigation pane, choose **Alarm Management** > **Alarm List** to view the alarm. The system also sends alarm notifications to specified personnel by email or SMS.

Figure 6-18 Creating an alarm template



----End

Importing an Alarm Template

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

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 Click **Import Alarm Template**.

Step 4 In the displayed dialog box, set parameters. For details, see **Table 6-25**. Click **OK**.

Figure 6-19 Importing an alarm template

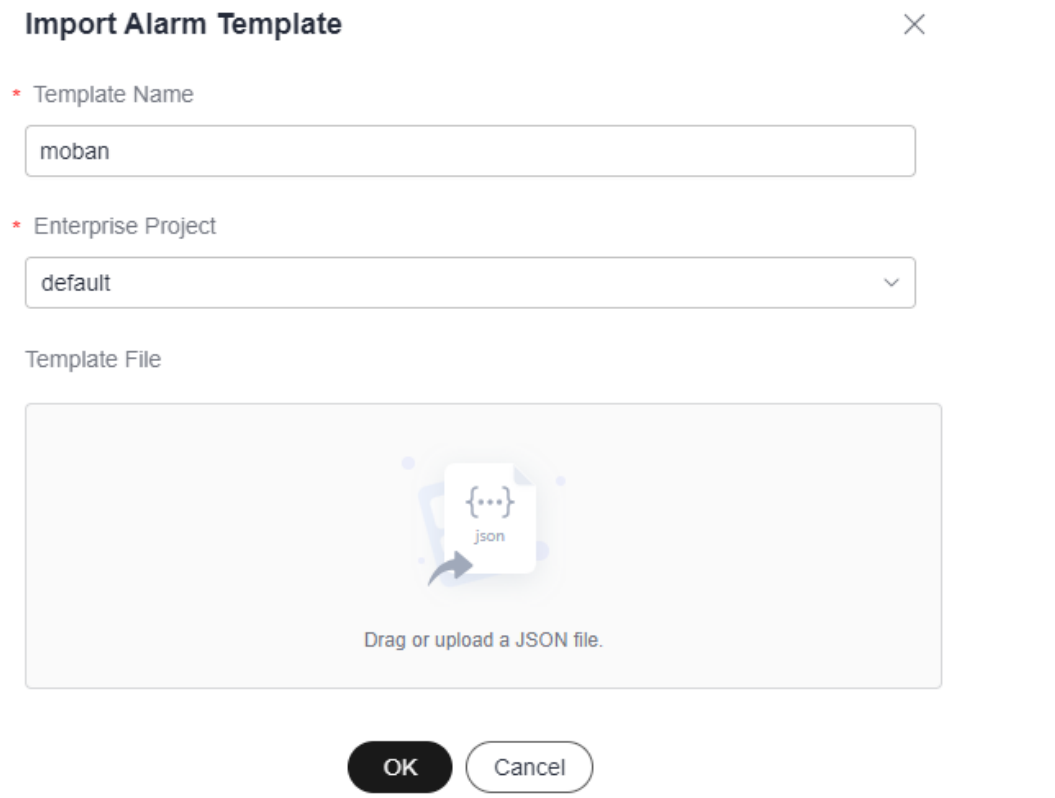


Table 6-25 Parameters for importing an alarm template

Parameter	Description
Template Name	Name of an alarm template. Enter a maximum of 100 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, underscores, and hyphens are allowed.
Enterprise Project	Enterprise project. Select a value from the drop-down list.
Template File	Directly upload or drag a JSON file to the box to upload.

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

----End

More Operations

After the alarm template is created, you can also perform the operations listed in **Table 6-26**.

Table 6-26 Related operations

Operation	Description
Checking an alarm template	In the template list, check the information such as **Template Name**, **Alarm Rules/Conditions**, **Associated Cluster**, and **Enterprise Project**.
Binding alarm templates with Prometheus instances/ clusters	Click in the **Operation** column. For details, see **Bind alarm templates with Prometheus instances/clusters**.
Modifying an alarm template	Choose > **Edit** in the **Operation** column. For details, see **Creating an Alarm Template**.
Exporting a custom alarm template	Choose > **Export** in the **Operation** column.
Copying an alarm template	Click in the **Operation** column.
Deleting an alarm template	• To delete an alarm template, choose > **Delete** in the **Operation** column. • To delete one or more alarm templates, select them and click **Delete** in the displayed dialog box.

Operation	Description
Searching for an alarm template	Enter a template name in the search box in the upper right corner and click .
Viewing alarm rules created using a template	In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**. Enter a template name keyword in the search box above the alarm rule list and click . If an alarm template has been bound with a Prometheus instance or cluster, you can also search for the alarm rule by the bound Prometheus instance or cluster name.
Viewing alarms	When the metric value of a resource meets an alarm condition, an alarm will be generated. In the navigation pane, choose **Alarm Management** > **Alarm List**. On the **Alarms** tab page, view alarms. For details, see **6.4 Checking AOM Alarms or Events**.
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, check events. For details, see **6.4 Checking AOM Alarms or Events**.

6.3.6 Managing AOM 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**
- **Managing Log Alarm Rules**

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 6-27**.

Figure 6-20 Checking alarm rules

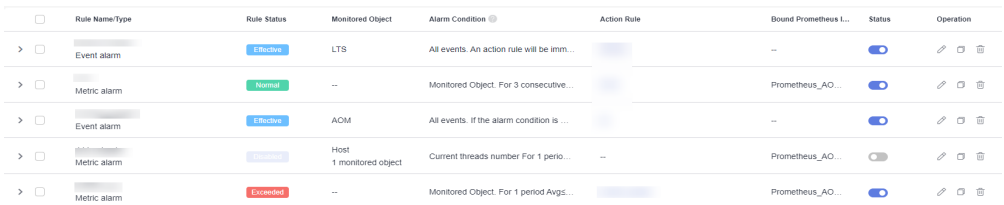


Table 6-27 Operations related to alarm rules

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 **6.3.2 Creating an AOM Metric Alarm Rule** and **6.3.3 Creating an AOM Event Alarm Rule**. **If the alarm rule configuration is modified, the rule may fail to monitor the target resource or to take effect. Exercise caution.**
Copying an alarm rule	Click in the **Operation** column. For details, see **6.3.2 Creating an AOM Metric Alarm Rule** and **6.3.3 Creating an AOM 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)**.
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.

Operation	Description
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 **6.4 Checking AOM Alarms or Events**.
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, check events. For details, see **6.4 Checking AOM Alarms or 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 6-28** if needed.

Figure 6-21 Checking alarm rules

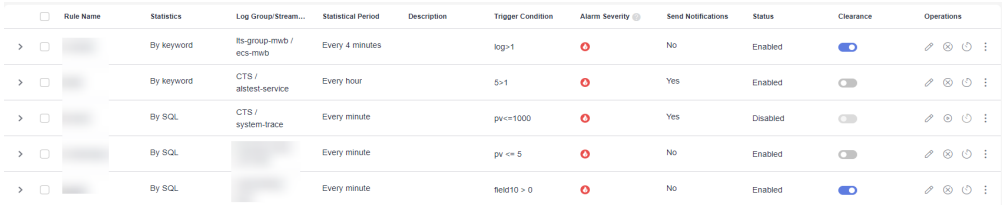


Table 6-28 Operations related to log alarm rules

Operation	Description
Searching for alarm rules	Enter an alarm rule name to search.
Refreshing alarm rules	Click in the upper right corner of the rule list to obtain the latest information about all alarm rules.
Customizing columns to display	Click in the upper right corner of the rule list and select or deselect the columns to display.

Operation	Description
Modifying alarm rules	Click  in the **Operation** column. For details, see **6.3.4 Creating an AOM Log Alarm Rule**. 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 **6.3.4 Creating an AOM 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**.
Viewing detailed alarm information	Click next to a rule name to view details.

Operation	Description
Viewing alarms	During the configured consecutive periods, if a log data record meets the preset condition, an alarm will be generated. In the navigation pane, choose **Alarm Management** > **Alarm List**. On the **Alarms** tab page, view alarms. For details, see **6.4 Checking AOM Alarms or Events**.

----End

6.3.7 Alarm Tags and Annotations

When creating alarm rules, you can set alarm tags and annotations. Tags are attributes that can be used to identify alarms. They are applied to alarm noise reduction scenarios. Annotations are attributes that cannot be used to identify alarms. They are applied to scenarios such as alarm notification and message templates.

Alarm Tag Description

- Alarm tags can apply to grouping rules, suppression rules, and silence rules. The alarm management system manages alarms and notifications based on the tags.
- Each tag is in "key:value" format and can be customized. Each key and value can contain only letters, digits, and underscores (_).
- If you set a tag when creating an alarm rule, the tag is automatically added as an alarm attribute when an alarm is triggered.
- In a message template, the **$event.metadata.key1** variable specifies a tag. For details, see **Table 6-2**.
- 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. Each key and value can contain only letters, digits, and underscores (_).
- In a message template, the **$event.annotations.key2** variable specifies an annotation. For details, see **Table 6-2**.

Managing Alarm Tags and Annotations

You can add, delete, modify, and query alarm tags or annotations on the alarm rule page.

Step 1 Log in to the AOM 2.0 console.

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

Step 3 Click **Create**, or locate a desired alarm rule and click in the **Operation** column.

Step 4 On the displayed page, click **Advanced Settings**.

Step 5 Under **Alarm Tag** or **Alarm Annotation**, click + Tag and enter a key and value.

Step 6 Click **OK** to add an alarm tag or annotation.

- Adding multiple alarm tags or annotations: Click + Tag multiple times to add alarm tags or annotations (max.: 20).
- 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

6.3.8 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 6-29 lists the common Prometheus commands for querying metrics. You can modify parameters such as the IP address and ID based on site requirements.

Table 6-29 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"}
Available cluster virtual memory	{clusterId="",clusterName=""}	aom_cluster_virtual_memory_free_megabytes{clusterId="4ba8008c-b93c-11ec-894a-0255ac101afc",clusterName="servicestage-test"}

Metric	Tag Definition	PromQL
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"}

6.4 Checking AOM Alarms or Events

The **Alarm List** page allows you to query and handle alarms and events, so that you can quickly detect, locate, and rectify faults.

Function Introduction

- The alarm list provides the following key functions:
  - Alarm list: Check alarm information by alarm severity in a graph.
  - Advanced filtering: Filter alarms by alarm severity, source, or keyword in the search box. By default, alarms are filtered by alarm severity.
  - Alarm clearance: Clear alarms one by one or in batches.
  - Alarm details: Check the alarm object and handling suggestions in the alarm details. Handling suggestions are provided for all alarms.
- The event list provides the following key functions:
  - Event list: Check event information by event severity in a graph.
  - Advanced filtering: Filter events by event severity, source, or keyword in the search box. By default, events are filtered by event severity.

Constraints

- The alarms triggered by metric alarm rules last for five days by default. After five days, they will be automatically cleared and become historical 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** or **Events** tab to check alarms or events.

1. Set a time range to check alarms or events. You can use a predefined time label, such as **Last hour** and **Last 6 hours**, or customize a time range. Max.: 31 days.
2. Set the interval for refreshing alarms or events. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.
3. Set filter criteria and click  to check the alarms or events generated in the period. You can filter alarms or events through the search box.

Table 6-30 Search criteria

Search Criteria	Description	Example
Alarm/ Event Severity	Search by alarm/ event severity. Options: – Critical – Major – Minor – Warning	**Major**: Filter the alarms whose severity is **Major** within the specified time range.
Resource Type	Search by resource type.	**Host**: Filter the alarms whose resource type is **Host** within the specified time range.
Alarm/ Event Source	You can select an alarm source to search for alarms or select an event source to search for events.	**AOM**: Filter the alarms whose source is **AOM** within the specified time range.

Search Criteria	Description	Example
Alarm/ Event Keyword	– **Alarm Keyword**: Fuzzy search by alarm name, alarm source, or resource type. Select **Alarm Keyword** in the search box and then enter a keyword. – **Event Keyword**: Fuzzy search by event name, event source, resource type, or other keywords. Select **Event Keyword** in the search box and then enter a keyword.	**AOMRule**: Filter the alarm named **AOMRule** within the specified time range.
Custom Attribute	Exact query by custom attribute. Select **Custom Attribute** in the search box and then enter "custom attribute name=custom attribute value".	– **nodeIP=192.168.0.106**: Filter the alarms whose host IP address is **192.168.0.106** within the specified time range.

Step 4 Perform the operations listed in **Table 6-31** as required:

Table 6-31 Operations

Operation	Description
Checking alarm/ event statistics	Click  , and check alarm/event statistics that meet filter criteria within a specific time range on a bar graph.
Clearing alarms	You can clear alarms after the problems that cause them are resolved. • 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.

Operation	Description
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 check details.
Checking event details	Click an event name to check event details and handling suggestions.
Checking cleared alarms	Click **Active Alarms** in the upper right corner and select **Historical Alarms** from the drop-down list to check alarms that have been cleared.

----End

6.5 Configuring AOM Alarm Noise Reduction

6.5.1 AOM Alarm Noise Reduction Overview

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

Description

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 **6.5.2 Creating an AOM Alarm Grouping Rule**, **6.5.3 Creating an AOM Alarm Suppression Rule**, and **6.5.4 Creating an AOM Alarm Silence Rule**.

Constraints

- This module is used only for message notification. All triggered alarms and events can be viewed on the **alarm list** page.
- 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"
 }
}
```

6.5.2 Creating an AOM Alarm 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.

Constraints

- You can create a maximum of 100 grouping 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 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 6-32**.

Figure 6-22 Creating a grouping rule

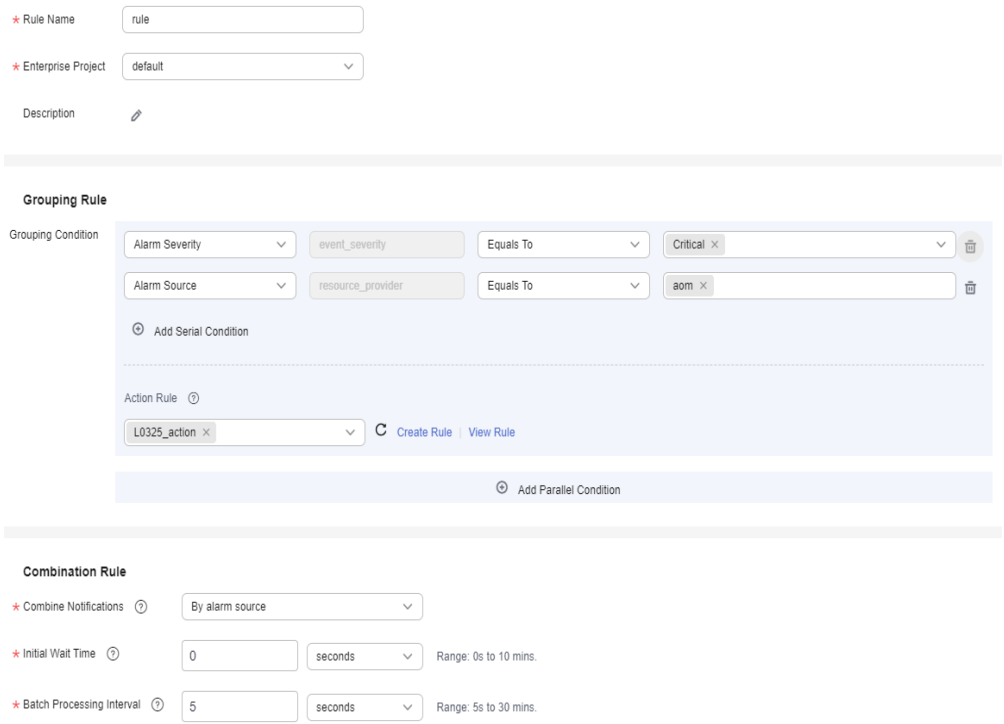


Table 6-32 Grouping rule parameters

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 1,024 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** • **Notify When**: scenario when notifications are triggered. Options: **Alarm triggered** and **Alarm cleared**. For example, select **Notify When** and then select **Alarm triggered**. • *XX* **Exists**: indicates the alarm whose metadata contains parameter *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 6-33** if needed.

Table 6-33 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  .

6.5.3 Creating an AOM Alarm Suppression Rule

By using suppression rules, you can suppress or block notifications related to specific alarms. For example, if a major alarm is generated, the alarms of lower severities can be suppressed. If a node is faulty, all the alarms of the process or container on the node can be suppressed.

Constraints

- 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 a maximum of 100 suppression 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 Noise Reduction**.

Step 3 On the **Suppression Rules** tab page, click **Create** and set parameters such as the rule name and source alarm.

Figure 6-23 Creating a suppression rule

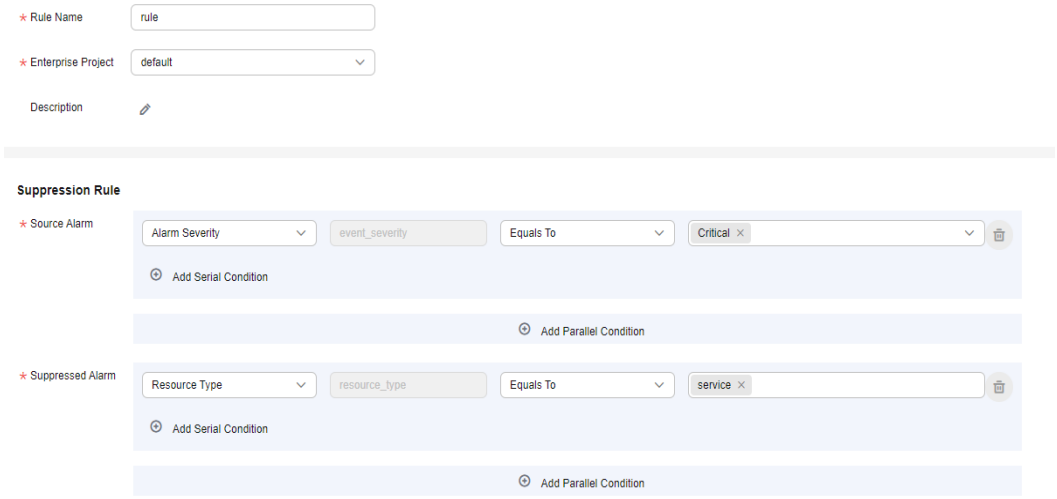


Table 6-34 Setting a suppression rule

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: include **host**, **container**, and **process**. Example: **Resource Type Equals to container** • **Alarm Source**: name of the service that triggers the alarm or event. Options: include **AOM**, **LTS**, and **CCE**. Example: **Alarm Source Equals to AOM** • **Tag**: alarm identification attribute, which consists of the tag name and tag value and can be customized. Example: **Tag aom_monitor_level Equals to infrastructure** • *XX* **Exists**: indicates the alarm whose metadata contains parameter *XX*. Example: For **Alarm Source Exists**, the alarms whose metadata contains the provider will be filtered. • *XX* **Regular Expression**: indicates the alarm whose parameter *XX* matches the regular expression. Example: For **Resource Type Regular Expression host***, the alarms whose resource type contains **host** will be filtered. 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 6-35** if needed.

Table 6-35 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  .

6.5.4 Creating an AOM Alarm Silence Rule

Alarm silence rules can mask alarm notifications in specified periods.

Constraints

- You can create a maximum of 100 silence rules. If this number has been reached, delete unnecessary rules.
- Once a silence rule is created, it takes effect immediately.

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 **Silence Rules** tab page, click **Create** and set parameters such as the rule name and silence condition.

Figure 6-24 Creating a silence rule

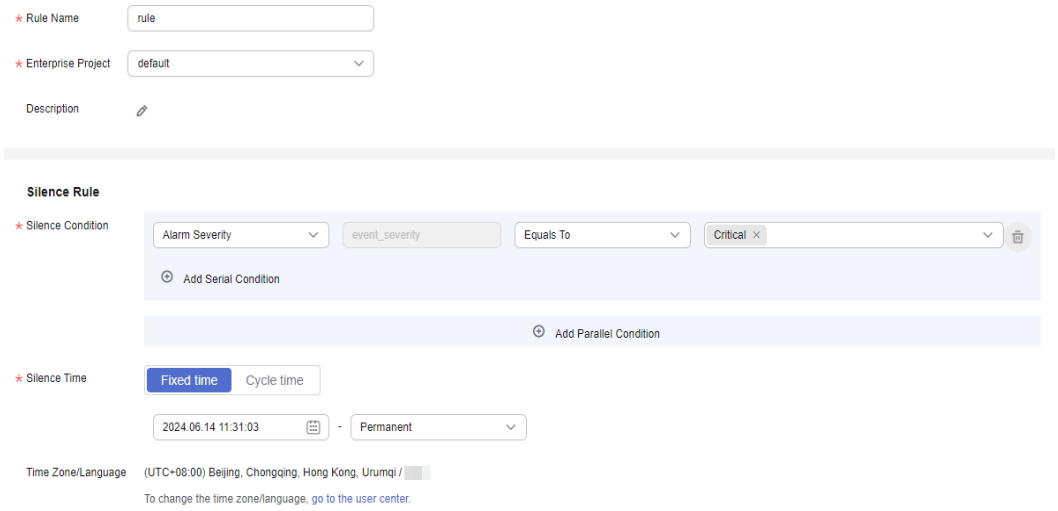


Table 6-36 Setting a silence rule

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: include **host**, **container**, and **process**. Example: **Resource Type Equals to container** • **Alarm Source**: name of the service that triggers the alarm or event. Options: include **AOM**, **LTS**, and **CCE**. Example: **Alarm Source Equals to AOM** • **Tag**: alarm identification attribute, which consists of the tag name and tag value and can be customized. Example: **Tag aom_monitor_level Equals to infrastructure** • *XX* **Exists**: indicates the alarm whose metadata contains parameter *XX*. Example: For **Alarm Source Exists**, the alarms whose metadata contains the provider will be filtered. • *XX* **Regular Expression**: indicates the alarm whose parameter *XX* matches the regular expression. Example: For **Resource Type Regular Expression host***, the alarms whose resource type contains **host** will be filtered. 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 6-37**.

Table 6-37 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  .

7 (New) Log Management

AOM provides a unified entry for observability analysis of Huawei Cloud services. It does not provide log functions by itself. Instead, it integrates the log management, ingestion, job, and transfer functions of **Log Tank Service (LTS)**. You can perform operations on the AOM 2.0 or LTS console.

Constraints

- Before using the log management, ingestion, transfer, and job functions on the AOM 2.0 console, you need to **purchase LTS resources** first.
- **Log Analysis** (new) is available only in the CN North-Beijing1, CN North-Beijing4, AP-Singapore, AF-Johannesburg, LA-Santiago, LA-Sao Paulo1, LA-Mexico City1, LA-Mexico City2, AP-Jakarta, TR-Istanbul, ME-Riyadh, CN East-Qingdao, CN East-Shanghai2, CN South-Guangzhou, CN North-Beijing2, CN-Hong Kong, AP-Bangkok, and CN East2 regions.
- To use LTS functions on the AOM console, you need to obtain LTS permissions in advance. For details, see **Permissions**.

Table 7-1 Function description

Function	Description	AOM 2.0 Console	LTS Console	References
Log management	The overview page provides the following: • Log management Provides **Statistics**, **Log Applications**, **My Favorites**/**My Favorites (Local Cache)**, **Recently Visited**, **Alarms**, **Latest Alarms**, **Notices**, and **FAQs**. • Log search and analysis Enables you to quickly query logs, and locate faults based on log sources and contexts. • Log application LTS supports access to standard logs of multiple cloud services and provides out-of-the-box dashboard templates for the logs. After the logs are ingested, you can quickly analyze them.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane, choose **Log Analysis** > **Log Management**.	1. Log in to the LTS console. 2. In the navigation pane, choose **Log Management**.	• **Log Management** • Log search and analysis – **Log Search and Analysis** • **Log Application**
Log transfer	After the log data of hosts and cloud services is reported to AOM or LTS, you can set the storage period as required. Log data that exceeds the storage period will be automatically deleted. You can transfer logs to other cloud services for long-term storage.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane, choose **Log Analysis** > **Log Transfer**.	1. Log in to the LTS console. 2. In the navigation pane, choose **Log Transfer**.	**Log Transfer**

Function	Description	AOM 2.0 Console	LTS Console	References
Log jobs	Provides SQL scheduled jobs, function processing, and metric generation. • SQL scheduled jobs Used to periodically analyze log content. These jobs use standard SQL syntax. They periodically perform log analysis based on scheduling rules, and store analysis results to a target log stream. Only whitelisted users can use this function by **submitting a service ticket**. • Function processing Normalizes, transfers, anonymizes, and filters logs based on provided function templates or custom functions. This function is available in the CN North-Beijing1, CN North-Beijing4, AP-Singapore, AF-Johannesburg, CN East-Shanghai1, LA-Santiago, LA-Sao Paulo1, LA-Mexico City1, LA-Mexico City2, AP-Jakarta, and TR-Istanbul. • Metric generation You can create log metric rules to extract log data reported to LTS as metrics and monitor them on the metric browsing and dashboard pages. This function is available for whitelisted users only. To use it, **submit a service ticket**.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane, choose **Log Analysis** > **Log Jobs**.	1. Log in to the LTS console. 2. In the navigation pane, choose **Log Jobs**.	**Log Processing**

Log Analysis (Old)

Log analysis (old) provides log search, log files, log paths, log dumps, and LTS access. You can click **Back to Old Version** to use log functions of the old version.

Table 7-2 Function description

Function	Description	AOM 2.0 Console	References
Log search	AOM enables you to quickly query logs, and locate faults based on log sources and contexts.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane, choose **Log Analysis** > **Log Management**. 3. Click **Back to Old Version** in the upper right corner of the page. The **Log Search** tab page is displayed.	**8.3 Searching for Logs**
Log files	You can quickly check log files of component instances or hosts to locate faults.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane, choose **Log Analysis** > **Log Management**. 3. Click **Back to Old Version** in the upper right corner of the page. The **Log Search** tab page is displayed. 4. Click the **Log Files** tab.	**8.4 Checking Log Files**

Function	Description	AOM 2.0 Console	References
Log 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.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane, choose **Log Analysis** > **Log Management**. 3. Click **Back to Old Version** in the upper right corner of the page. The **Log Search** tab page is displayed. 4. Click the **Log Paths** tab.	**8.2 Configuring VM Log Collection Paths**
Log transfer	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.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane, choose **Log Analysis** > **Log Management**. 3. Click **Back to Old Version** in the upper right corner of the page. The **Log Search** tab page is displayed. 4. Click the **Log Transfer** tab.	**8.5 Dumping Logs to OBS**
LTS access	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, 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.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane, choose **Log Analysis** > **LTS Access**.	**8.1 Ingesting Logs to LTS**

8 Log Management (Old)

8.1 Ingesting Logs to LTS

8.1.1 Log Access Overview

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, 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.

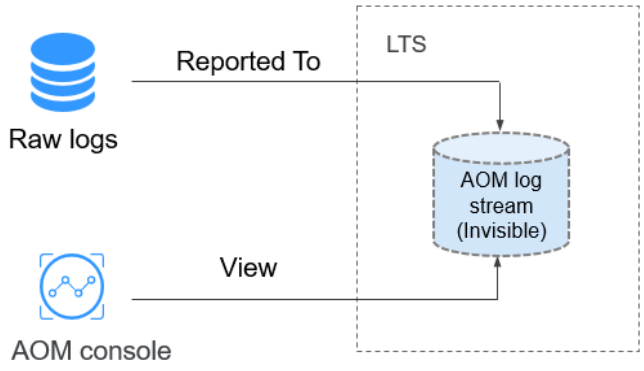
Constraints

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

What Is Mapping?

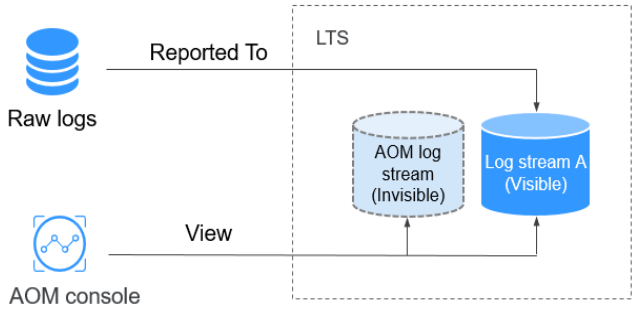
AOM logs exist in LTS in the form of a log stream, as shown in **Figure 8-1**. You can view raw logs in configured log collection paths on AOM, but cannot view the AOM log stream on LTS. You can create a mapping by adding an access rule on AOM. After the mapping is created, you can view and analyze AOM logs on LTS.

Figure 8-1 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 8-2**.

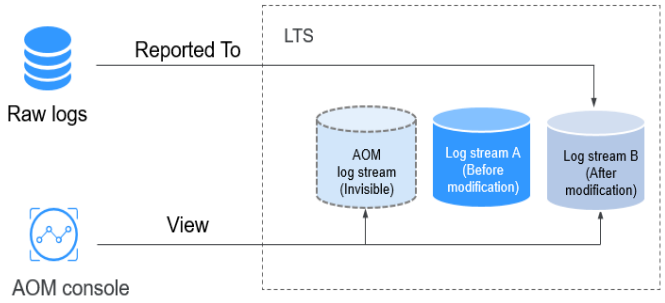
Figure 8-2 After mapping



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 8-3**.

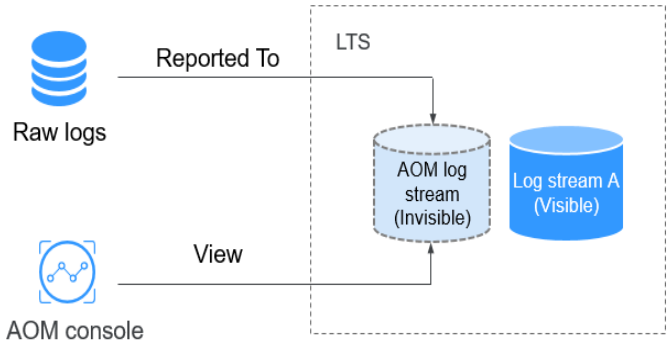
Figure 8-3 Modifying a mapping



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 8-4**. 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. **Deleted access rules or mapped log streams cannot be recovered. Exercise caution when performing this operation.**

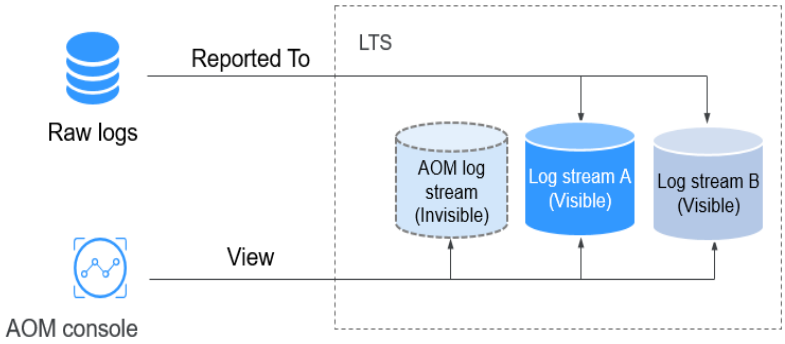
Figure 8-4 Deleting a mapping



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 8-5 Duplicate mapping



8.1.2 Managing Log Access Rules

This section describes how to manage log access rules. You can add, view, and delete these 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 (CCE) User Guide***.

Constraints

Configured log access rules into LTS might impact log data in LTS and result in additional fees. Exercise caution.

Configuring Access Rules

To map the logs of CCE, CCI, 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. 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 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.
- **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. 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 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.
- **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

Other Operations

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

Table 8-1 Related operations

Operation	Description
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.
View	• In the rule list, view the cluster name and namespace of the created rule. • Click a log group name in the **Log Group** column to go to the log group details page on the LTS console.
Customize columns	Click  in the upper right corner of the search box to select columns to display.
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. **Deleted access rules or mapped log streams cannot be recovered. Exercise caution. For the impact, see Deleting a Mapping.**

8.2 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.

Constraints

- 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**.

In regions where new log analysis functions are supported, you can access the **Log Paths** page through the entry described in **Table 7-2**.

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

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

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

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

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

- **Manual configuration**

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

Step 4 Click **Confirm**.

----End

Viewing VM Logs

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

- **Viewing VM Log Files**

  In the navigation pane, choose **Log Analysis** > **Log Files**. Click the **Host** tab to view the collected log files. For details, see **8.4 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 **8.3 Searching for Logs**.

8.3 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**.

In regions where new log analysis functions are supported, you can access the **Log Paths** page through the entry described in **Table 7-2**.

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

- 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**.
- Enter a keyword in the search box. Rules are as follows:
  - Enter keywords for exact search. A keyword is the word between two adjacent delimiters.
  - Use an asterisk (*) or question mark (?) for fuzzy search, for example, **ER?OR**, **ROR***, or **ER*R**.

- Enter a phrase for exact search. For example, enter **Start to refresh** or **Start-to-refresh**. Note that hyphens (-) are delimiters.
- Enter a keyword containing AND (&&) or OR (||) for search. For example, enter **query logs&&error*** or **query logs||error**.
- If no log is returned, narrow down the search range, or add an asterisk (*) to the end of a keyword for fuzzy match.

Step 4 View the search result of logs.

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

1. AOM allows you to view context. Click **Context** in the **Operation** column to view the previous or next logs of a log for fault locating.

   To ensure normal host and component running, some components (for example, kube-dns) provided by the system will run on the hosts. The logs of these components will also be queried during tenant log query.

   - In the **Display Rows** drop-down list, set the number of rows that display raw context data of the log.

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

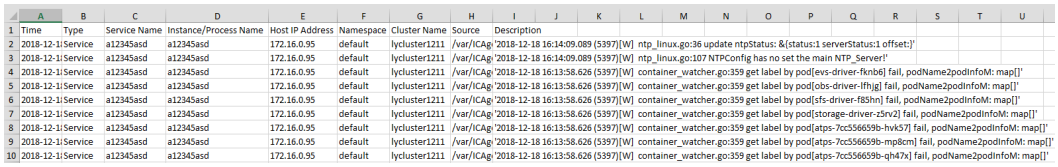
     - If there are 100 logs or more printed before a log and 99 or more logs printed following the log, the preceding 100 logs and following 99 logs are displayed as the context.
     - If there are fewer than 100 logs (for example, 90) printed before a log and fewer than 99 logs (for example, 80) printed 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.
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 8-6**. Only log content will be exported when you select the TXT format (as shown in **Figure 8-7**). Each line indicates a log.

Figure 8-6 Exporting logs in CSV format



	A	B	C	D	E	F	G	H	I
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 8-7 Exporting logs in TXT format

2023-01-19T16:30:38.783448+08:00 host-71-24-40-204 dockerd[1522]: time="2023-01-19T16:30:38.783401876+08:00" level=info msg="handled exit event processID=a9b55efe7ee83e4663a66c59795cafc65b0d3eafc593688199dbf4c3eed38aa6 containerID=32dcbfcf3b782a32f55768dfbc77773eacb862b0b86587103dd334bdab904157 pid=74026" module=libcontainerd namespace=moby

2023-01-19T16:30:38.750722+08:00 host-71-24-40-204 dockerd[1930]: time="2023-01-19T16:30:38+08:00" level=info msg="try publish event(1) /tasks/exit &TaskExit {ContainerID:32dcbfcf3b782a32f55768dfbc77773eacb862b0b86587103dd334bdab904157,ID:a9b55efe7ee83e4663a66c59795cafc65b0d3eafc593688199dbf4c3eed38aa6,Pid:74026,ExitStatus:0,ExitedAt:2023-01-19 16:30:38.731935965 +0800 CST m=+794826.727765440,} <nil>"

2023-01-19T16:30:38.749258+08:00 host-71-24-40-204 dockerd[1522]: time="2023-01-19T16:30:38.749183798+08:00" level=info msg=event ExitStatus=0 ExitedAt="2023-01-19 08:30:38.731935965 +0000 UTC" Pid=74026 ProcessID=a9b55efe7ee83e4663a66c59795cafc65b0d3eafc593688199dbf4c3eed38aa6 containerID=32dcbfcf3b782a32f55768dfbc77773eacb862b0b86587103dd334bdab904157 module=libcontainerd namespace=moby topic=/tasks/exit

2023-01-19T16:30:38.749095+08:00 host-71-24-40-204 dockerd[1930]: time="2023-01-19T16:30:38.749010188+08:00" level=info msg="exit-del moby/32dcbfcf3b782a32f55768dfbc77773eacb862b0b86587103dd334bdab904157.74026.0 error=<nil>"

2023-01-19T16:30:38.727852+08:00 host-71-24-40-204 dockerd[1522]: time="2023-01-19T16:30:38.727801764+08:00" level=info msg="handled exit event processID=dff8c094ea7e209119dfcac8c20ae56befd0e78ee1153bf23ce3cba3c5c1abb9 containerID=38b7025401d815a0e299a9dfce0e9e665ad34e25257fa64677e376f629971c35 pid=73999" module=libcontainerd namespace=moby

2023-01-19T16:30:38.692915+08:00 host-71-24-40-204 dockerd[1930]: time="2023-01-19T16:30:38+08:00" level=info msg="try publish event(1) /tasks/exit &TaskExit {ContainerID:38b7025401d815a0e299a9dfce0e9e665ad34e25257fa64677e376f629971c35,ID:dff8c094ea7e209119dfcac8c20ae56befd0e78ee1153bf23ce3cba3c5c1abb9,Pid:73999,ExitStatus:0,ExitedAt:2023-01-19 16:30:38.674153885 +0800 CST m=+197458.957089482,} <nil>"

2023-01-19T16:30:38.691108+08:00 host-71-24-40-204 dockerd[1522]: time="2023-01-19T16:30:38.690862578+08:00" level=info msg=event ExitStatus=0 ExitedAt="2023-01-19 08:30:38.674153885 +0000 UTC" Pid=73999 ProcessID=dff8c094ea7e209119dfcac8c20ae56befd0e78ee1153bf23ce3cba3c5c1abb9 containerID=38b7025401d815a0e299a9dfce0e9e665ad34e25257fa64677e376f629971c35 module=libcontainerd namespace=moby topic=/tasks/exit

2023-01-19T16:30:38.690739+08:00 host-71-24-40-204 dockerd[1930]: time="2023-01-19T16:30:38.690699053+08:00" level=info msg="exit-del moby/38b7025401d815a0e299a9dfce0e9e665ad34e25257fa64677e376f629971c35.73999.0 error=<nil>"

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

----End

8.4 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.

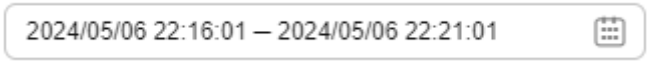
Step 2 In the navigation pane, choose **Log Analysis** > **Log Files**.

In regions where new log analysis functions are supported, you can access the **Log Paths** page through the entry described in **Table 7-2**.

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.

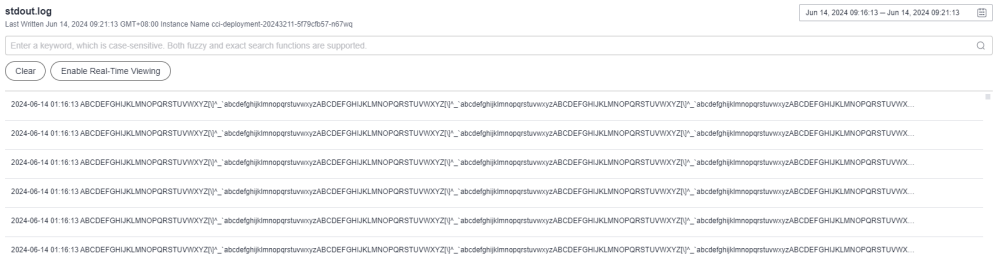
Step 4 Click **View** in the **Operation** column of the desired instance. **Table 8-2** shows how to view log file details. **Figure 8-8** shows log file details.

Table 8-2 Operations

Operation	Settings	Description
Setting a time range	Date	Click  to select a date.

Operation	Settings	Description
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.
	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.

Figure 8-8 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

8.5 Dumping Logs to OBS

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**.

Constraints

- To add a log dump task, 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.
- 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.

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**.

In regions where new log analysis functions are supported, you can access the **Log Paths** page through the entry described in **Table 7-2**.

Step 3 Click **Add Log Dump** in the upper right corner of the page. Then, set parameters according to **Table 8-3** and click **OK**.

Table 8-3 Periodical dump parameters

Parameter	Description	Example
Dump Mode	Select **Periodic dump**.	Periodic dump
Filter Criteria	Logs can be filtered by multiple criteria such as log type, cluster, or namespace, so that you can dump the logs that meet specific criteria.	Select the **Component** log type and select the **als0320a** component.
Log Group	Logs can be categorized into logical groups, so that you can dump them based on groups.	log-group1

Parameter	Description	Example
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. To create an OBS bucket, click **View OBS** to go to 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.

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 8-4 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**.

In regions where new log analysis functions are supported, you can access the **Log Paths** page through the entry described in **Table 7-2**.

Step 3 Click **Add Log Dump** in the upper right corner of the page. Then, set parameters according to **Table 8-5** and click **OK**.

Table 8-5 One-off dump parameters

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

Parameter	Description	Example
Filter Criteria	Logs can be filtered by multiple criteria such as log collection time, cluster, or namespace, so that you can dump the logs that meet specific criteria.	Set the log collection time to **Last 30 minutes**, select the **als0320a** component, and set the keyword to **warn**.
Log Group	Logs can be categorized into logical groups, so that you can dump them based on groups. **After a dump task is deleted, log groups will also be deleted.**	log-group2
Target OBS Bucket	OBS bucket for storing logs. • If no OBS bucket is available, click **View OBS** to create a bucket on the OBS console. • If you select an unauthorized OBS bucket, AOM will take 15 minutes to authorize the ACL for the bucket. If your configuration fails, try again 15 minutes later. • Data cannot be dumped to an OBS bucket whose storage class is **Archive** or for which cross-region replication has been configured.	obs-store-test
OBS Bucket Directory	OBS bucket directory for storing logs. **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 8-6 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

Other Operations

Table 8-7 Log dump operations

Operation	Description
Modifying a log dump task	1. Locate the target dump task and click **Modify** in the **Operation** column. In the displayed dialog box, modify the log dump information. 2. After modification, click **OK**. **Only periodical dump tasks can be modified.**
Deleting a log dump task	1. Locate the target dump task and click **Delete** in the **Operation** column. 2. Click **OK**. **Once a dump task is deleted, logs will no longer be dumped, affecting the query of historical logs. Exercise caution.**
Starting/ Stopping a log dump task	Locate the target dump task and click **Start** or **Stop** in the **Operation** column. **Only periodical dump tasks can be started and stopped.**

9 Prometheus Monitoring

9.1 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.

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 instances are logical units used to manage Prometheus data collection, storage, and analysis. **Table 9-1** lists different types of instances classified based on monitored objects and application scenarios.

Table 9-1 Prometheus instance description

Prometheus Instance Type	Monitored Object	Monitoring Capability	Application Scenario
Default Prometheus instance	• 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.	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 ingested.
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
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 Prometheus middleware and custom plug-ins to monitor through the access center.
Prometheus instance for cloud services	Multiple cloud services	Monitors multiple cloud services. 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.
Common Prometheus instance	Self-built Prometheus	• Provides remote storage for Prometheus time series databases. • Provides a self-developed monitoring dashboard to display data. You maintain self-built Prometheus servers. You need to configure metric management 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
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. The following metrics can be ingested through this Prometheus instance: • 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.
Prometheus for APM	APM traces	Integrates APM's application monitoring capabilities to monitor traces for Java, Go, Python, Node.js, PHP, .NET, and C++ applications.	Applicable when you have enabled APM and need to monitor application traces.

Functions

AOM Prometheus monitoring supports monitoring data collection, storage, computing, display, and alarm reporting. It monitors metrics of containers, cloud services, middleware, databases, applications, and services. The following lists the functions supported by AOM Prometheus monitoring.

Table 9-2 Monitored object access

Function	Description
Managing Prometheus Instances	AOM supports multiple types of Prometheus instances. You can create Prometheus instances as required.
Connecting a CCE Cluster	AOM supports the Prometheus cloud-native monitoring plug-in. You can install the plug-in for CCE clusters through **Integration Center** to report metrics to the Prometheus instance for CCE. **Only Prometheus instances for CCE support this function.**

Function	Description
2.5.2 Connecting Middleware to AOM	AOM supports the Prometheus middleware plug-in. You can install the middleware Exporter for VMs through **Access Center** to report metrics to the Prometheus instance for ECS. **Only Prometheus instances for ECS support this function.**
Connecting Cloud Services to AOM	You can connect cloud services to AOM through **Cloud Service Connection** to report metrics to the Prometheus instance for cloud services. **Only Prometheus instances for cloud services support this function.**
9.5 Configuring Multi-Account Aggregation for Unified Monitoring	You can connect multiple member accounts within the same organization through **Account Access** to monitor metrics. Through data multi-write, cross-VPC access can be achieved without exposing the network information about servers.

Table 9-3 Monitoring metric collection

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

Table 9-4 Data processing

Function	Description
9.11 Configuring the Remote Read Address to Enable Self-built Prometheus to Read Data from AOM	With the remote read and write addresses, you can store the monitoring data of self-built Prometheus to AOM Prometheus instances for remote storage.

Function	Description
9.7 Configuring Recording Rules to Improve Metric Query Efficiency	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.
9.8 Configuring Data Multi-Write to Dump Metrics to Self-Built Prometheus Instances	Cross-VPC access is enabled through data multi-write.

Advantages

Table 9-5 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

Basic Concepts

The following lists the basic concepts about Prometheus monitoring.

Table 9-6 Basic concepts

Item	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**.

Item	Description
Target	Target to be captured by a Prometheus probe. A target either exposes its own operation and service metrics or serves as a proxy to expose the operation and service metrics of a monitored object.
Job	Configuration set for a group of targets. Jobs specify the capture interval, access limit, and other behavior for a group of targets.
Prometheus monitoring	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.
9.2 Managing Prometheus Instances	Logical units used to collect, store, and analyze Prometheus data.
Prometheus probes	Deployed in the Kubernetes clusters on the user or cloud product side. Prometheus probes automatically discover targets, collect metrics, and remotely write data to databases.
PromQL	Prometheus query language. Supports both query based on specified time spans and instantaneous query, and provides multiple built-in functions and operators. Raw data can be aggregated, sliced, predicted, and combined.
Sample	Value corresponding to a time point in a timeline. For Prometheus monitoring, each sample consists of a value of the float64 data type and a timestamp with millisecond precision.
Alarm rules	Alarm configuration for Prometheus monitoring. An alarm rule can be specified using PromQL.
Tags	A key-value pair that describes a metric.
Metric management	Automatically discovers collection targets without static configuration. Supports multiple metric management modes (such as Kubernetes SD, Consul, and Eureka) and exposes collection targets through ServiceMonitor or PodMonitor.
Recording rules	Prometheus monitoring's recording rule capability. You can use PromQL to process raw data into new metrics 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.

Item	Description
Cloud product monitoring	Seamlessly integrates monitoring data of multiple cloud products. To monitor cloud products, connect them first.
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.

9.2 Managing Prometheus Instances

AOM allows you to create multiple types of 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.

Creating a Prometheus Instance

Step 1 Log in to the **AOM 2.0** console.

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

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

Table 9-7 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.

Parameter	Description
Instance Type	Type of the Prometheus instance. Options: • Prometheus for CCE • Prometheus for ECS • Prometheus for Cloud Services • Common Prometheus Instance • Prometheus for Multi-Account Aggregation Select a Prometheus instance type by referring to **Table 9-1**. The following instances cannot be directly created: • **default**: **Prometheus_AOM_Default** is preset. • **Prometheus for APM**: When an application is connected to the APM console, the system automatically creates a Prometheus instance for APM and displays it on the **Prometheus Monitoring** > **Instances** page of the AOM console.

Step 4 Click **OK**. The Prometheus instance is created.

Then you can perform the operations listed in the following table as required.

Table 9-8 Related operations

Sub-Menu	Description
Connecting a CCE Cluster	AOM supports the Prometheus cloud-native monitoring plug-in. You can install the plug-in for CCE clusters through **Integration Center** to report metrics to the Prometheus instance for CCE. **Only Prometheus instances for CCE support this function.**
2.5.2 Connecting Middleware to AOM	AOM supports the Prometheus middleware plug-in. You can install the middleware Exporter for VMs through **Access Center** to report metrics to the Prometheus instance for ECS. **Only Prometheus instances for ECS support this function.**
Connecting Cloud Services to AOM	You can connect cloud services to AOM through **Cloud Service Connection** to report metrics to the Prometheus instance for cloud services. **Only Prometheus instances for cloud services support this function.**
Connecting Accounts	You can connect multiple member accounts within the same organization through **Account Access** to monitor metrics. Through data multi-write, cross-VPC access can be achieved without exposing the network information about servers. **Only Prometheus instances for multi-account aggregation support this function.**

Sub-Menu	Description
9.3 Managing Prometheus Instance Metrics	AOM allows you to view Prometheus instance metrics, including new and discarded ones on the **Metric Management** page. **Only the default/common Prometheus instances, and the Prometheus instances for cloud services/ECS/CCE/APM support this function.**
9.10 Monitoring Prometheus Instance Metrics Through Dashboards	AOM allows you to use preset templates to quickly monitor metrics of Prometheus instance for cloud services and the default Prometheus instance on the **Dashboards** page. In this way, you can locate problems in a timely manner, improving O&M efficiency. **Only the Prometheus instance for cloud services and the default Prometheus instance support this function.**
9.8 Configuring Data Multi-Write to Dump Metrics to Self-Built Prometheus Instances	AOM supports cross-VPC access through the data multi-write function. Only the default or common Prometheus instance and the Prometheus instances for CCE, cloud service, and ECS are supported.
9.9 Setting Metric Storage Duration	AOM allows you to configure the metric storage duration of Prometheus instances. **Only the default/common Prometheus instances, and the Prometheus instances for cloud services/ECS/CCE/multi-account aggregation/APM support this function.**
9.11 Configuring the Remote Read Address to Enable Self-built Prometheus to Read Data from AOM	AOM allows you to check the basic information, call credentials, and service address of a Prometheus instance on the **Settings** page. **Only the default/common Prometheus instances, and the Prometheus instances for cloud services/ECS/CCE/multi-account aggregation/APM support this function.**

----End

Managing Prometheus Instances

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 9-9** if needed.

Figure 9-1 Managing Prometheus instances

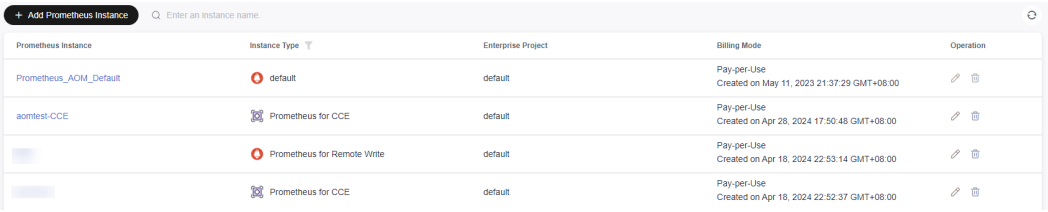


Table 9-9 Related operations

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

Operation	Description
Checking a Prometheus instance	The Prometheus instance list displays information such as the instance name, instance type, billing mode, and enterprise project 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 remote read and write 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 **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 **Other 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. (The **default** and **Prometheus for APM** instance names cannot be changed.) • Modify Prometheus instance configurations: In the Prometheus instance list, click the name of a Prometheus instance for cloud services/CCE/multi-account aggregation and modify the **cloud services**/**CCE clusters**/**accounts** if needed.

Operation	Description
Deleting a Prometheus instance	Click in the **Operation** column that contains the target Prometheus instance. • The **default** and **Prometheus for APM** instances cannot be deleted. • If you delete a Prometheus instance connected to a CCE cluster, cluster metrics cannot be hosted to this instance after it is deleted.
Checking the billing information of a Prometheus instance	In the Prometheus instance list, the **Billing Mode** column displays the billing mode and creation time of the Prometheus instance. Currently, only pay-per-use billing is supported. • If your account is frozen or restricted, you cannot add, delete, or modify Prometheus instances. • To continue using your cloud services, top up your account in time. For details, see **Arrears**.

----End

9.3 Managing Prometheus Instance Metrics

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

Prerequisites

Your service has been connected for Prometheus monitoring. For details, see **9.2 Managing Prometheus Instances**.

Constraints

- Only the default/common Prometheus instance, and Prometheus instance for CCE/ECS/cloud services/APM support the functions of checking/adding/discarding metrics.
- On the **Metric Management** page, you can query only the metrics reported in the last three hours.
- Default Prometheus instance: Metrics whose names start with **aom_** or **apm_** and resource type is **ICAgent** cannot be discarded.
- Prometheus instances for ECS: Only metrics collected by UniAgent can be displayed and configured.
- Prometheus instances for CCE:

  Only the metrics reported by kube-prometheus-stack 3.9.0 or later installed on CCE **Add-ons** or AOM **Integration Center** can be discarded. Ensure that this add-on is running when discarding metrics.

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 Prometheus Instance Metrics

Only the default/common Prometheus instance, and Prometheus instance for CCE/ECS/APM/cloud services support the functions of checking metrics.

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 desired Prometheus instance. The instance details page is displayed.

Step 4 In the navigation pane on the left, choose **Metric Management**. On the **Metrics** tab page, check the metric names and types of the current Prometheus instance.

- Prometheus instance for CCE: You can filter metrics by cluster name, job name, or metric type, or enter a metric name keyword for fuzzy search.
- Prometheus instance for cloud services: You can filter metrics by metric or resource type, or enter a metric name keyword for fuzzy search.
- Prometheus instance for ECS: You can filter metrics by metric type, plug-in type, or collection task, or enter a metric name keyword for fuzzy search.
- Default Prometheus instance: You can filter metrics by metric or resource type, or enter a metric name keyword for fuzzy search.
- Common Prometheus instance: You can filter metrics by metric or resource type, or enter a metric name keyword for fuzzy search.
- Prometheus instance for APM: You can filter metrics by environment, metric type, or resource type, or enter a metric name keyword for fuzzy search.

Table 9-10 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 the resource that reports the metric. This parameter is unavailable for metrics of Prometheus instances for ECS.
Metrics in Last 10 Min	Number of metrics that are stored in the last 10 minutes. This parameter is not supported for Prometheus instances for cloud services.
Proportion	Number of a certain type of metrics/Total number of metrics This parameter is not supported for Prometheus instances for cloud services.

----End

Discarding Prometheus Instance Metrics

If Prometheus instance metrics do not need to be reported, discard them.

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 desired Prometheus instance. The instance details page is displayed.

Step 4 In the navigation pane, choose **Metric Management**.

Step 5 Perform the following operations to discard metrics:

- To discard a metric, locate it and click  in the **Operation** column.
- To discard one or more metrics, select them and click **Delete** in the displayed dialog box.

----End

Adding Prometheus Instance Metrics

After metrics in a Prometheus instance are discarded, you can add they again.

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 desired Prometheus instance. The instance details page is displayed.

Step 4 In the navigation pane, choose **Metric Management**.

Step 5 Click **Add Metric**. In the displayed dialog box, select one or more metrics to restore and click **OK**.

----End

9.4 Using Prometheus Monitoring to Monitor CCE Cluster Metrics

Based on the Prometheus monitoring ecosystem, AOM provides hosted Prometheus instances for CCE, which are suitable for monitoring CCE clusters and applications running on them. By default, Prometheus instances for CCE support integration with the Cloud Native Cluster Monitoring add-on. After installing the add-on, metrics will be automatically reported to a specified Prometheus instance for CCE.

Constraints

- Only when the Cloud Native Cluster Monitoring add-on (kube-prometheus-stack) exists on the **Add-ons** page of CCE, can you install the add-on for clusters.
- 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 an instance name, enterprise project, and instance type.

Table 9-11 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.
Instance Type	Type of the Prometheus instance. Select **Prometheus for CCE**.

Step 4 Click **OK**.

To use more functions on the details page of a Prometheus instance for CCE, you need to obtain CCE permissions in advance. For details, see **Permissions**.

----End

Connecting a CCE Cluster

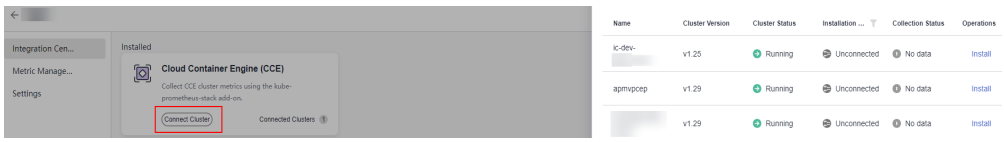
Step 1 Log in to the **AOM 2.0** console.

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

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

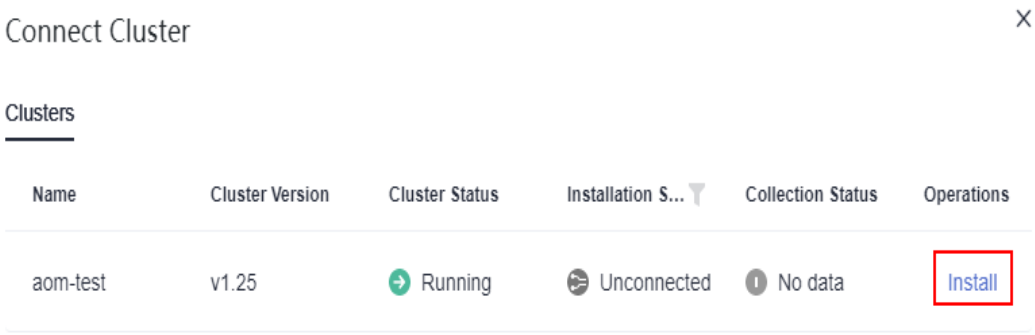
Step 4 On the **Integration Center** page, click **Connect Cluster**. In the cluster list, you can view the cluster information, installation status, and collection status.

Figure 9-2 Viewing cluster connection information



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

Figure 9-3 Connecting a CCE cluster



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

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

----End

9.5 Configuring Multi-Account Aggregation for Unified Monitoring

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.

Constraints

- Only the organization administrator or delegated administrator can create Prometheus instances for multi-account aggregation and connect accounts. For details about how to set a delegated administrator, see **Specifying, Viewing, or Removing a Delegated Administrator**.
- 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.

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.

Table 9-12 Parameters for creating a Prometheus instance

Parameter	Description
Instance Name	Prometheus instance name. Enter a maximum of 100 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, underscores, and hyphens are allowed.
Enterprise Project	Enterprise project. • 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 Multi-Account Aggregation**.

Step 4 Click **OK**.

----End

Connecting Accounts

Step 1 Log in to the **AOM 2.0** console.

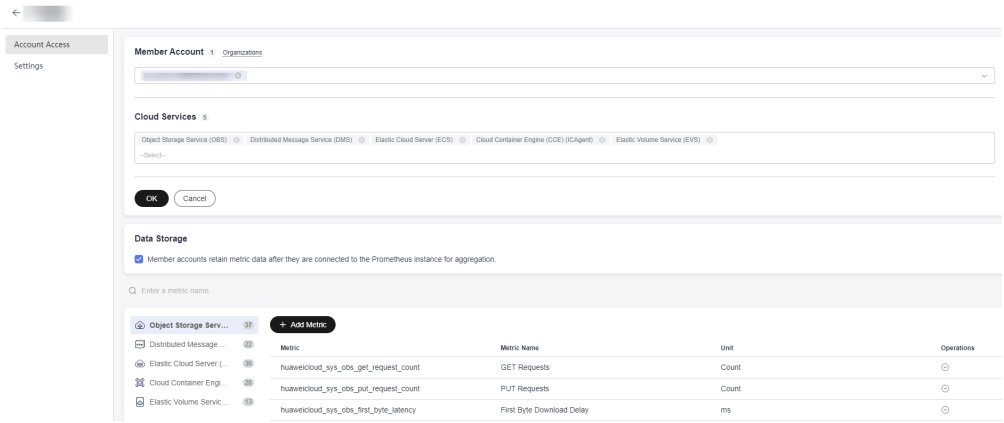
Step 2 On the Prometheus instance list page, click a Prometheus instance for multi-account aggregation.

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 9-4 Account access page



----End

9.6 Configuring Metric Collection Rules 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 **9.4 Using Prometheus Monitoring to Monitor CCE Cluster Metrics**.

Constraints

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

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

Adding ServiceMonitor

Step 1 Log in to the **AOM 2.0** console.

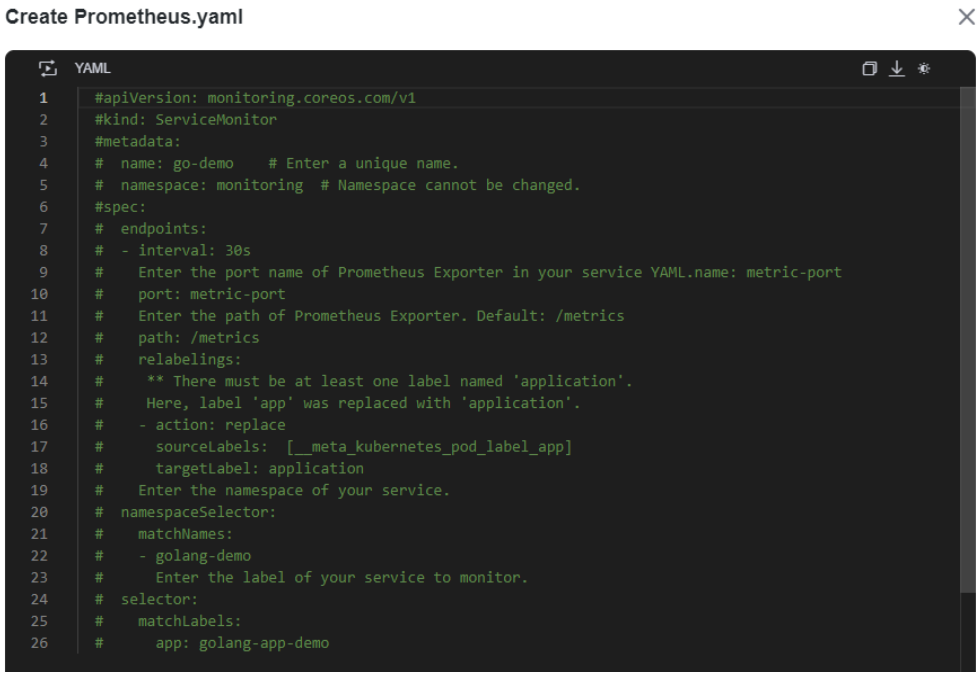
Step 2 In the navigation pane on the left, choose **Prometheus Monitoring** > **Instances**.

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

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

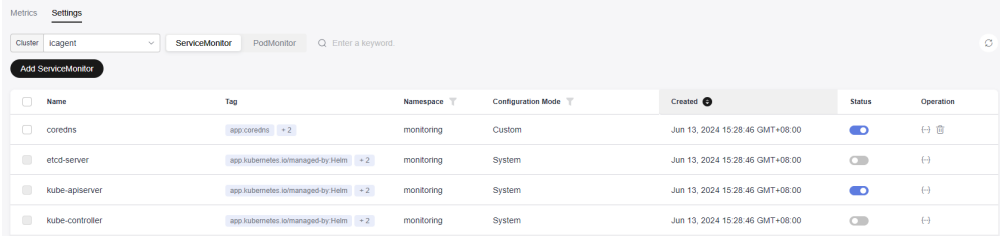
Step 5 Click **Add ServiceMonitor**. In the displayed dialog box, set related parameters and click **OK**.

Figure 9-5 Adding ServiceMonitor



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

Figure 9-6 Configuring a collection rule



----End

Adding PodMonitor

Step 1 Log in to the **AOM 2.0** console.

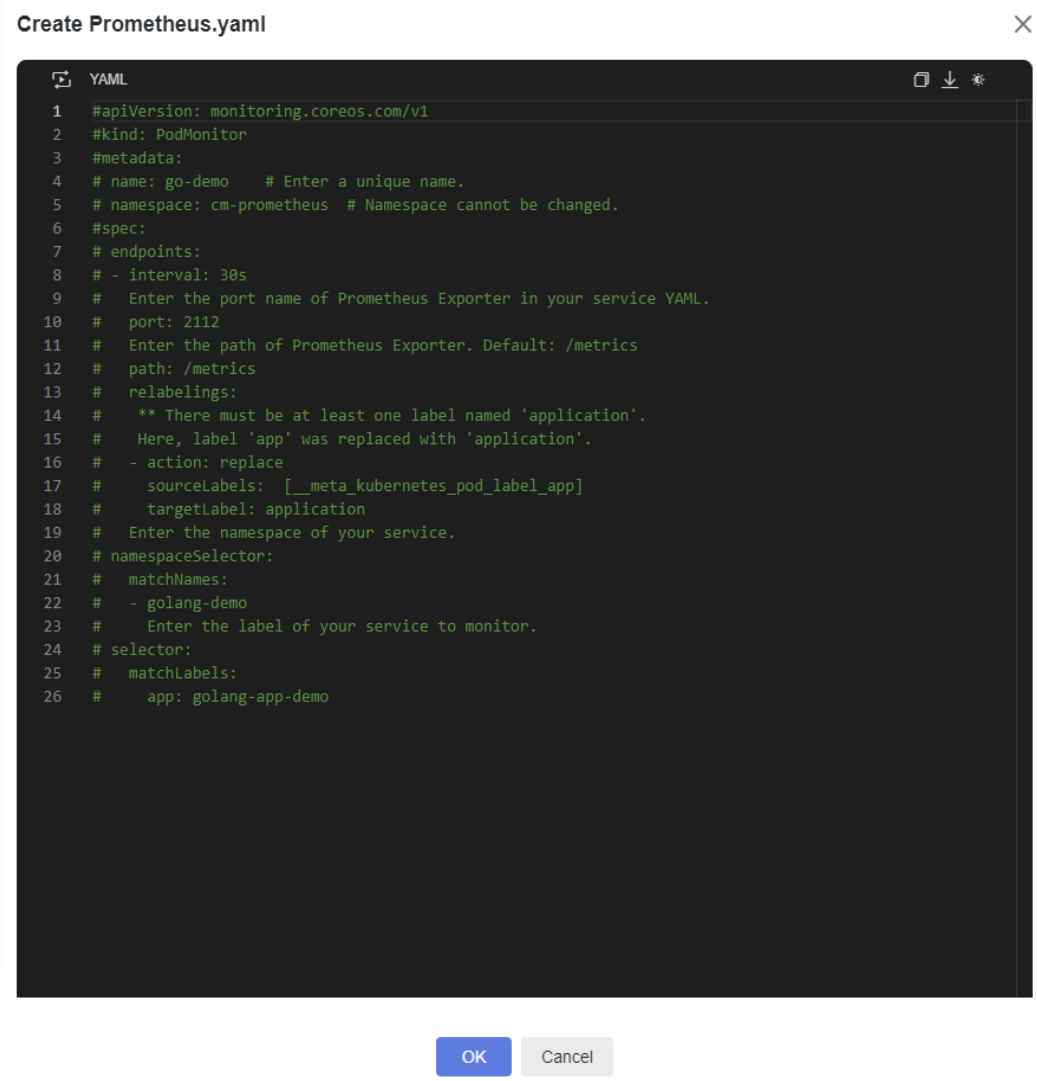
Step 2 In the navigation pane on the left, choose **Prometheus Monitoring** > **Instances**.

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

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

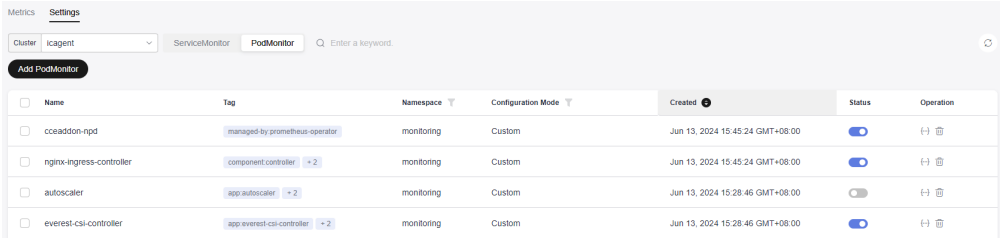
Step 5 Click **Add PodMonitor**. In the displayed dialog box, set related parameters and click **OK**.

Figure 9-7 Adding PodMonitor



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

Figure 9-8 Configuring a collection rule



----End

Other Operations

Perform the operations listed in **Table 9-13** if needed.

Table 9-13 Related operations

Operation	Description
Checking metric management configuration	• In the list, check information such as the name, tag, namespace, and configuration mode. You can filter information by cluster name, namespace, or configuration mode. • Click {...} in the **Operation** column. In the displayed dialog box, view details about the ServiceMonitor or PodMonitor collection rule.
Enabling or disabling collection rules	On the **Settings** tab page of the **Metric Management** page, click in the **Status** column to enable or disable collection rules. indicates that collection rules are disabled. indicates that collection rules are enabled.
Deleting metric management configuration	Click in the **Operation** column to delete the metric.

9.7 Configuring Recording Rules to Improve Metric Query Efficiency

Recording rules can be used for secondary development of metric data. By setting recording rules, you can move the computing process to the write end, reducing resource usage on the query end.

Scenario

Some metrics may require much calculation on the query end, affecting query performance. You can configure recording rules to calculate common or complex metrics in advance. Especially in large-scale clusters and complex service scenarios, recording rules can reduce PromQL complexity, improve metric query performance, and prevent slow configuration and query.

Prerequisite

- Both your service and CCE cluster have been connected to a Prometheus instance for CCE. For details, see **9.4 Using Prometheus Monitoring to Monitor CCE Cluster Metrics**.

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.

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

Figure 9-9 Configuring a recording rule

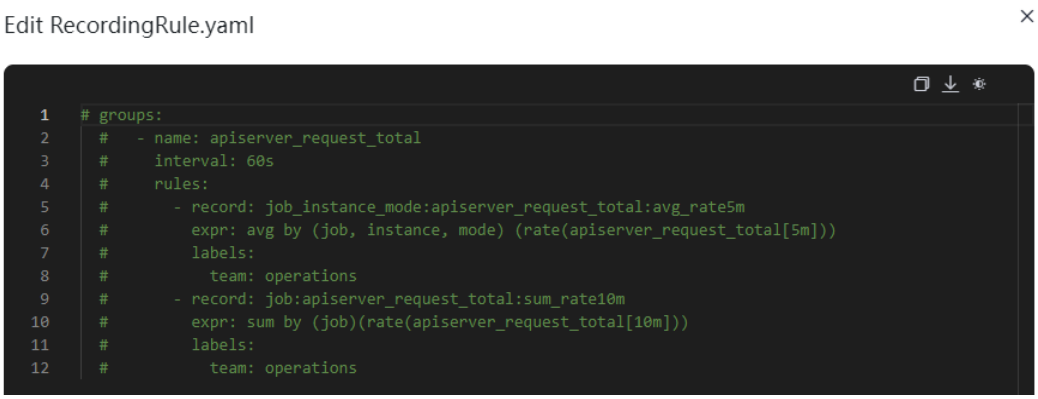


Table 9-14 Recording rule parameters

Parameter	Description
groups	Rule group. You can set multiple rule groups in one **RecordingRule.yaml** file.
name	Rule group name. Each rule group name must be unique.
interval	Execution interval of a rule group. The default value is **60s**. (Optional)
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	Metric label. Labels must comply with **Prometheus metric label specifications**. (Optional)

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**.

After the recording rule is configured, you can view metrics through:

- **Metric Browsing** page
- **Grafana**

----End

9.8 Configuring Data Multi-Write to Dump Metrics to Self-Built Prometheus Instances

This function enables cross-VPC access without exposing server network information. Monitoring data can be reported to self-built Prometheus instances more securely.

Prerequisites

Your service has been connected for Prometheus monitoring. For details, see **9.2 Managing Prometheus Instances**.

Constraints

- Only the default or common Prometheus instance, and the Prometheus instances for CCE, cloud services, and ECS support data multi-write.
- For Prometheus instances for CCE, the metrics processed using recording rules do not support data multi-write.
- Some default metrics generated by AOM (such as **aom_metrics_total**, **aom_metrics_total_per_hour**, **ALERTS**, and **ALERTS_FOR_STATE**) do not support data multi-write.
- When the metrics of the default Prometheus instance are dumped using the data multi-write function, the names of some dumped metrics may be inconsistent with those displayed on the AOM page. For example, the names of metrics reported by ICAgent are in lower camel case. These names are converted to the snake case when being displayed on the AOM page. (Example: **memUsage** is displayed as **aom_container_memory_usage**.)

Procedure

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 Prometheus instance list, click a Prometheus instance that supports data multi-write. The instance details page is displayed.

Step 4 In the navigation pane on the left, choose **Data Write**.

Step 5 Configure the intranet.

1. Select a VPC endpoint service. Select a VPC endpoint service from the drop-down list.

   The selected VPC endpoint service must be in the same VPC as the self-built Prometheus instance. Only VPC endpoint services whose **Backend Resource Type** is **Cloud Server** or **Elastic Load Balance** can be selected.
2. Add whitelist permissions.

   Click **Add Now** to add the provided account ID to the VPC endpoint service whitelist.
3. Create a VPC endpoint.

   Click **Create VPC Endpoint**.

Step 6 On the VPC endpoint service details page, go to the **Connection Management** tab page and ensure that the status is **Accepted**.

Step 7 Set a data write address. **Table 9-15** describes the parameters.

Table 9-15 Data write address parameters

Parameter	Description
Self-built Prometheus Instance's Remote Write Address	Remote write address of the self-built Prometheus instance. Set this parameter based on site requirements. The format is "{IP address:port number}/{path}". Example: **192.168.0.1:9090/api/v1/write**
Authentication Mode	Authentication mode for accessing a self-built Prometheus instance. • **Basic**: Enter the username and password of the self-built Prometheus instance. • **Token**: A token is required for authentication. • **None**: No authentication is required.

Step 8 Click **Save**.

Wait for about 5 minutes. You can check the reported metric data in the self-built Prometheus instance.

----End

9.9 Setting Metric Storage Duration

This section describes how to set metric storage duration for default/common Prometheus instances and Prometheus instances for cloud services/ECS/CCE/multi-account aggregation/APM.

Prerequisite

Your service has been connected for Prometheus monitoring. For details, see **9.2 Managing Prometheus Instances**.

Constraints

The function of setting metric storage duration is available only to whitelisted users. If you need this function, **submit a service ticket**.

Procedure

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 desired Prometheus instance. The instance details page is displayed.

Step 4 In the navigation tree on the left, choose **Settings**. Then click the **Storage Duration** tab.

Step 5 On the displayed page, select a storage duration. Options: **30 days**/**60 days**/**90 days**.

Step 6 In the displayed dialog box, click **OK** to change the storage duration.

This storage can only be changed once within 24 hours.

----End

9.10 Monitoring Prometheus Instance Metrics Through Dashboards

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

Prerequisite

Both your service and cloud services have been connected to a Prometheus instance for cloud services. For details, see **2.7 Connecting Cloud Services to AOM**.

Constraints

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

Monitoring the Metrics of a Default Prometheus Instance

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the instance list, click a default Prometheus instance.

Step 4 In the navigation pane, choose **Dashboards** to check all preset dashboard templates.

Step 5 Click a desired dashboard template to monitor the metrics of the current Prometheus instance.

For example, to monitor the disk partition information of a host, click **disk-partition-template** and select the target host IP address and disk partition. You can also perform the operations listed in **Table 9-16**.

----End

Monitoring the Metrics of a Prometheus Instance for Cloud Services

Step 1 Log in to the **AOM 2.0** console.

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

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

Step 4 In the navigation pane, choose **Dashboards** to check all preset dashboard templates.

Step 5 Click a desired dashboard template to monitor the metrics of the current Prometheus instance.

For example, to monitor the CCE workload information, click **cce-workload-template** and select the target service ID. You can also perform the operations listed in **Table 9-16**.

----End

More Operations

Table 9-16 Operations related to dashboards

Operation	Description
Full-screen display	Click the target dashboard and click in the upper right corner of the dashboard page to view the dashboard in full screen.

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

9.11 Configuring the Remote Read Address to Enable Self-built Prometheus to Read Data from AOM

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 use self-built Prometheus.

Constraints

When configuring Prometheus for remote read, ensure that **global:external_labels**:** is correct since **external_labels** will be added to the search criteria. If a label is incorrect, required data may fail to be queried.

You can set **filter_external_labels: false** (Prometheus: v2.34 or later) to prevent **external_labels** from being added to the search criteria.

Prerequisite

Your service has been connected for Prometheus monitoring. For details, see **9.2 Managing Prometheus Instances**.

Configuring the Remote Read Address

You are advised to configure the **prometheus.yml** file of self-built Prometheus. 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 to go to the details page.

Step 3 In the navigation pane on the left, choose **Settings**. On the **Intranet** or **Public Network** tab page in the **Service Addresses** area, click on the right to copy the configuration code for Prometheus remote read.

```
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
```

Step 4 Add the copied configuration code to the **prometheus.yml** file of self-built Prometheus.

Step 5 Restart the self-built Prometheus service.

Then you can view AOM Prometheus data.

----End

Complete Configuration Items of Remote Read

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 ]
```

9.12 Configuring the Remote Write Address to Report Self-Built Prometheus Data to AOM

AOM can obtain the remote write address of a 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.

Prerequisites

- You have **purchased** an ECS.
- Your service has been connected for Prometheus monitoring. For details, see **9.2 Managing Prometheus Instances**.

Reporting Self-Built Prometheus Instance Data to AOM

Step 1 Install and start open-source Prometheus. For details, see **Prometheus official documents**. (Skip this step if open-source Prometheus has been deployed.)

Step 2 Add an access code.

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

   An access code is an identity credential for calling APIs. A maximum of two access codes can be created for each project. Keep them 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 click on the right to copy the configuration code for Prometheus remote write from the **Service Addresses** area.

Figure 9-10 Configuration code for Prometheus remote write

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

1. Run the following command to find and start the **prometheus.yml** file:
   ```
   ./prometheus --config.file=prometheus.yml
   ```
2. 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

9.13 Checking 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.
- You have **purchased** an EIP and bound it to the purchased ECS. For details, see ***Elastic Cloud Server (ECS) Getting Started***.
- Your service has been connected for Prometheus monitoring. For details, see **9.2 Managing Prometheus Instances**.

Procedure

Step 1 Install and start Grafana. For details, see the **Grafana official documentation**.

Step 2 Add an access code.

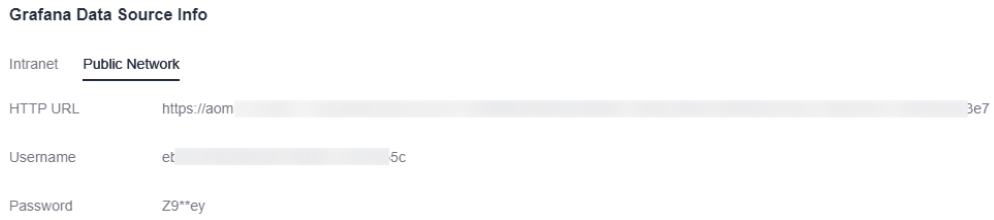
1. Log in to the **AOM 2.0** console.
2. In the navigation pane, choose **Settings**.
3. On the displayed page, choose **Authentication** in the navigation pane. Click **Add Access Code**.
4. In the dialog box that is displayed, click **OK**. The system then automatically generates an access code.

   An access code is an identity credential for calling APIs. A maximum of two access codes can be created for each project. Keep them 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.

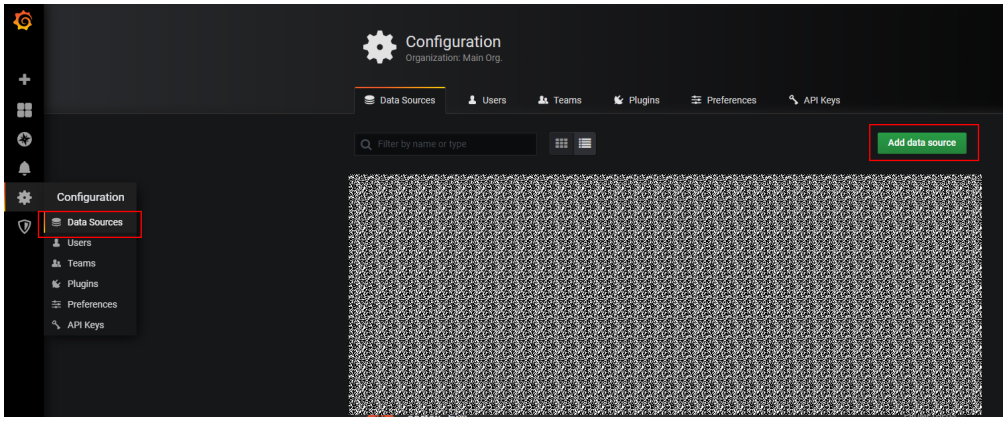
Figure 9-11 Grafana data source information



Step 4 Configure Grafana.

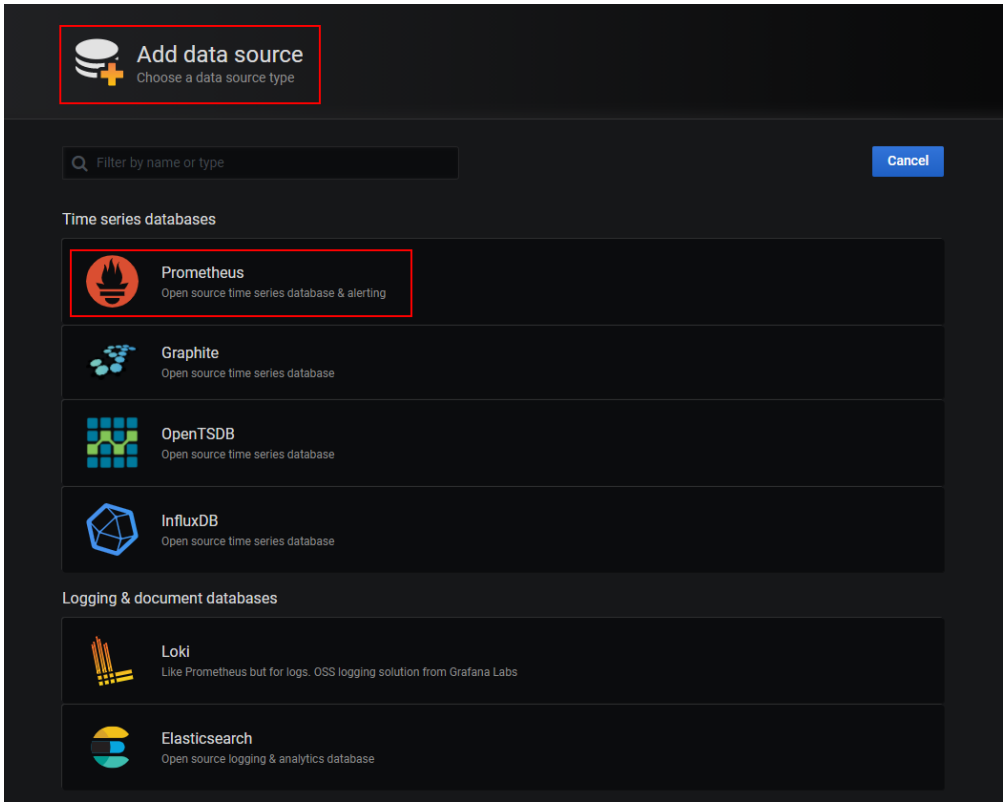
1. Log in to Grafana.
2. In the navigation pane, choose **Configuration** > **Data Sources**. Then click **Add data source**.

Figure 9-12 Configuring Grafana



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

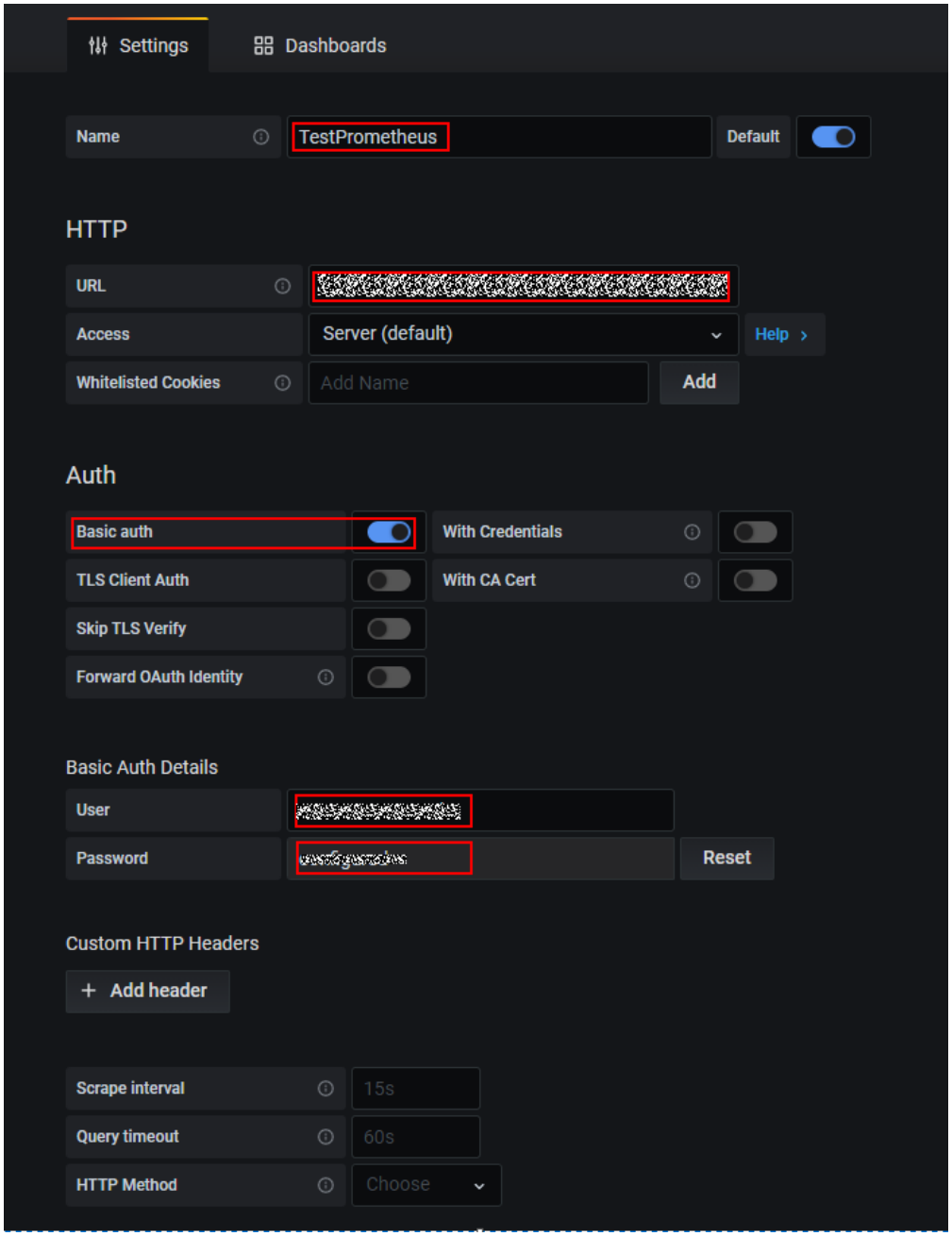
Figure 9-13 Prometheus configuration page



4. Set Grafana data source parameters.
   - **URL**: HTTP URL obtained in **Step 3.3**.
   - **User**: username obtained in **Step 3.3**.
   - **Password**: password obtained in **Step 3.3**.

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

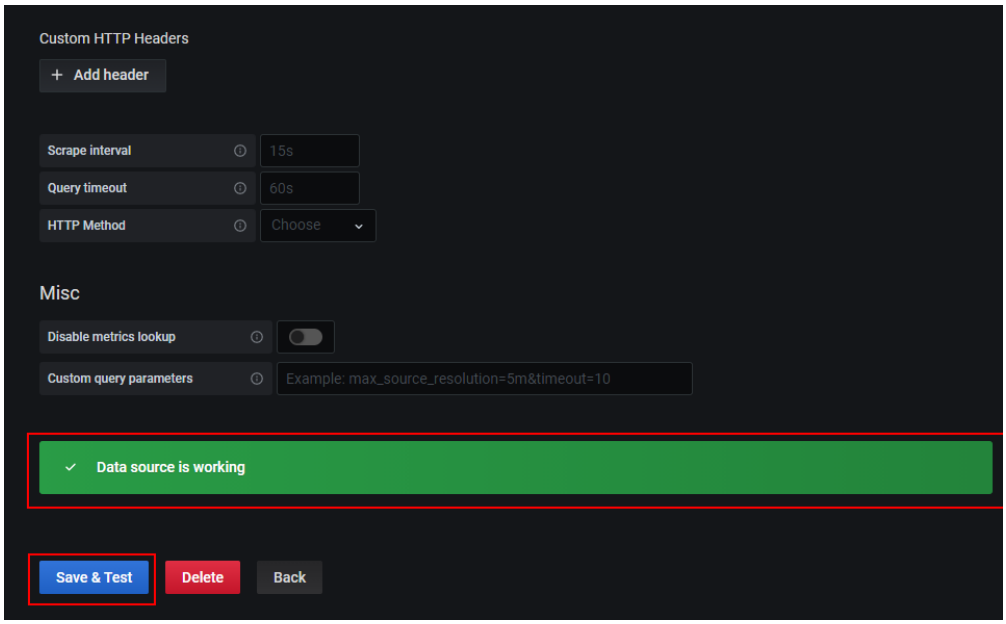
Figure 9-14 Setting parameters



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 9-15 Checking whether the configuration is successful



----End

9.14 Checking the Number of Metric Samples Reported by Prometheus Instances

After metric data is reported to AOM through Prometheus monitoring, you can view the number of basic and custom metric samples reported by Prometheus instances.

Prerequisites

- Your service has been connected for Prometheus monitoring. For details, see **9.2 Managing Prometheus Instances**.

Constraints

- 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. You can use a predefined time label, such as **Last hour** and **Last 6 hours**, or customize a time range. Max.: 30 days.

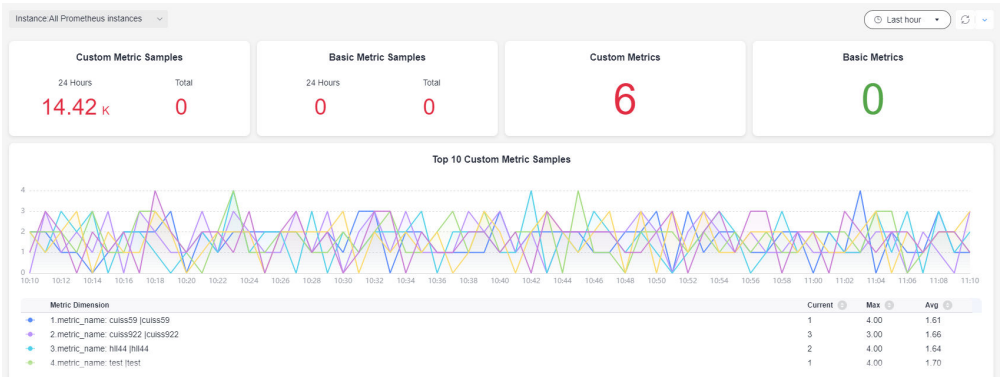
   You are advised to select a time range longer than 1 hour.

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 9-16 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

10 Infrastructure Monitoring

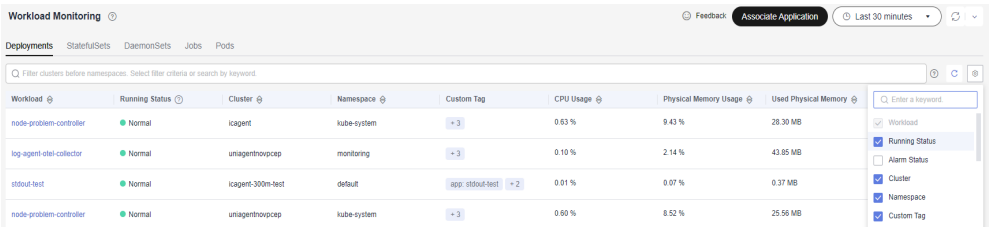
10.1 Using AOM to Monitor Workloads

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

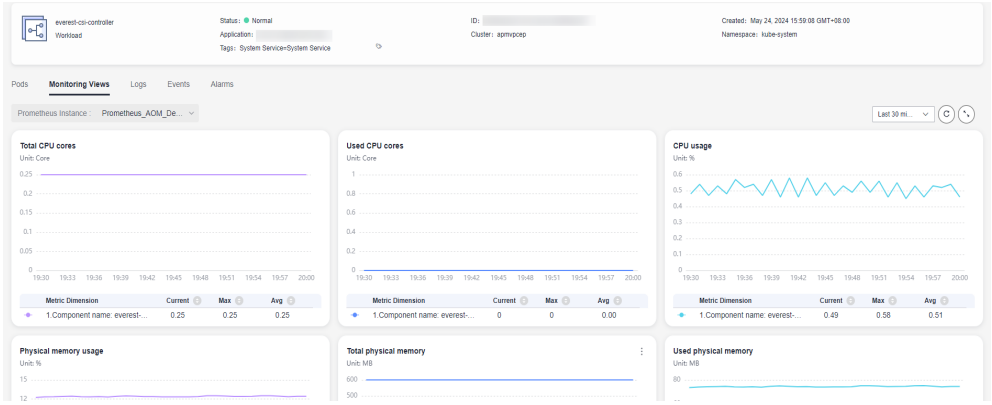
- The workload monitoring solution is ready-to-use. After AOM is enabled, the workload status, CPU usage, and physical memory usage of CCE and CCI are displayed on the workload monitoring page by default.

  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 **4 Observability 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. To use the function of associating applications, enable **Application Insights** in **Menu Settings**. For details, see **14.4 Configuring AOM Menus**.

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 check the workloads reported. You can use a predefined time label, such as **Last hour** and **Last 6 hours**, or customize a time range. 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 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/namespace.

  To query namespaces, IAM users with the **AOM FullAccess** or **AOM ReadOnlyAccess** permission need to log in to the CCE console, choose **Permissions** in the navigation pane, and click **Add Permission** in the upper right corner of the page to add required permissions.

- Click  in the upper right corner to obtain the latest workload information within the time range specified in **Step 3.1**.
- Click  in the upper right corner and select or deselect columns to display.
- Click the name of a workload to view its details.

- On the **Pods** tab page, view the all pod conditions of the workload. Click a pod name to view the resource usage and health status of the pod's containers.
- On the **Monitoring Views** tab page, view the resource usage of the workload.
- On the **Alarms** tab page, view the alarm details of the workload. For details, see **6.4 Checking AOM Alarms or Events**.
- On the **Events** tab page, view the event details of the workload. For details, see **6.4 Checking AOM Alarms or Events**.

----End

10.2 Using AOM to Monitor Clusters

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.

Constraints

- 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.
- To use CCE functions on the AOM console, you need to obtain CCE permissions in advance. For details, see **Permissions**.

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 check the CCE clusters reported. You can use a predefined time label, such as **Last hour** and **Last 6 hours**, or customize a time range. 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 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.

- Choose **Monitoring Center**, **Logging**, or **Alarm Center** in the navigation pane on the left to implement cloud native observability for clusters. (This function is not available in **AF-Johannesburg** only.)

  - Health Center

    Health diagnosis monitors cluster health by leveraging container O&M experts' experience to quickly detect cluster faults and identify risks. It also provides rectification suggestions. For details, see **Health Center**.
  - Monitoring Center

    Monitoring Center provides the container insights, health diagnosis, and dashboard. The container insights function provides monitoring views from dimensions such as cluster, node, workload, and pod. It supports multi-level drill-down and association analysis. The dashboard gives you monitoring graphs for items such as kube-apiserver, CoreDNS, and PVC. For details, see **Monitoring Center**.
  - Logging

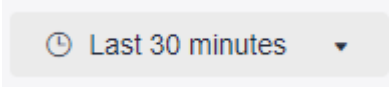
    CCE works with Log Tank Service (LTS) to collect logs of control plane components (kube-apiserver, kube-controller-manager, and kube-scheduler), Kubernetes audit logs, Kubernetes events, and container logs (standard output logs, text logs, and node logs). For details, see **Logging**.
  - Alarm Center

    Alarm Center works with AOM 2.0 to allow you to create alarm rules and check alarms of clusters and containers. For details, see **Alarm Center**.
- In the navigation pane on the left, monitor cluster running conditions by cluster, on dashboards, or through **Alarm Management**. For details, see **Step 6**. (This function is available in **AF-Johannesburg** only.)

Step 6 Click a cluster to go to its details page. In the navigation pane on the left, monitor cluster running conditions by cluster, on dashboards, or through **Alarm Management**.

- View information about nodes, workloads, pods (container groups), and containers by cluster.
  - In the navigation pane on the left, choose **Insights** > **Node** to view information about all nodes in the cluster in real time, including the status, IP address, pod status, CPU usage, and memory usage.
    - In the upper part of the node list, filter nodes by node name.
    - Click  in the upper right corner and select or deselect options as required.
    - Click a node to view its related resources, alarms, and events, and common system devices such as GPUs and NICs.
      - On the **Overview** tab page, **Cloud-Native Monitoring (New)** is selected by default. You can view metrics such as CPU, memory, and network. Click **Using ICAgent (Old)** and select a target Prometheus instance from the drop-down list. You can view metrics such as CPU, physical memory, and host status.

        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 **9.4 Using Prometheus Monitoring to Monitor CCE Cluster Metrics**. 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. Check nodes, workloads, and container groups by name.
- Check the cluster running status through **Alarm Management**.
  - In the navigation pane on the left, choose **Alarm Management** > **Alarm List** to view alarm details of the cluster. For details, see **6.4 Checking AOM Alarms or Events**.
  - In the navigation pane on the left, choose **Alarm Management** > **Event List** to view event details of the cluster. For details, see **6.4 Checking AOM Alarms or 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 **6.3.6 Managing AOM 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 **9.4 Using Prometheus Monitoring to Monitor CCE Cluster Metrics** 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 Using AOM to Monitor Hosts

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.

Constraints

- 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 check the hosts reported. You can use a predefined time label, such as **Last hour** and **Last 6 hours**, or customize a time range. Max.: 30 days.
  - Set the interval for refreshing information. Click  and select a value from the drop-down list as required, such as **Refresh manually**, **30 seconds auto refresh**, **1 minute auto refresh**, or **5 minutes auto refresh**.
  - Click  in the upper right corner and select or deselect **Tags**.

Step 3 Perform the following operations if needed:

- **Adding an alias**

  If a host name is too complex to identify, you can add an alias, which makes it easy to identify a host as required.

  In the host list, click  in the **Operation** column of the target host, enter an alias, and click **OK**. The added alias can be modified but cannot be deleted.

- **Adding a tag**

  Tags are identifiers of hosts. You can manage hosts using tags. After a tag is added, you can quickly identify and select a host.

  In the host list, click  in the **Operation** column of the target host. In the displayed dialog box, enter a tag key and value, and click  and **OK**.

- **Synchronizing host data**

  In the host list, locate the target host and click  in the **Operation** column to synchronize host information.

Step 4 Set filter criteria to search for the desired host. **Hosts cannot be searched by alias.**

Step 5 Click a host name. On the displayed host details page, you can view the running status and ID of the host.

Step 6 Click any tab. In the list, you can monitor the instance resource usage and health status, and information about common resources such as GPUs and NICs.

- On the **Process List** tab page of the ECS host, you can view the process status and IP address of the host.
  - In the search box in the upper right corner of the process list, you can set search criteria such as the process name to filter processes.
  - Click  in the upper right corner to obtain the latest process information within the specified time range.
- On the **Pods** tab page of the CCE host, you can view the pod status and node IP address.
  - Click a pod name to view details about the container and process of the pod.
  - In the search box in the upper right corner of the pod list, you can set search criteria such as pod names to filter pods.
  - Click  in the upper right corner to obtain the latest pod information within the specified time range.
- On the **Monitoring Views** tab page, view key metric graphs of the host.
- On the **File Systems** tab page, view the basic information about the file system of the host. Click a disk file partition to monitor its metrics on the **Monitoring Views** page.
- On the **Disks** tab page, view the basic information about the disks of the host. Click a disk to monitor its metrics on the **Monitoring Views** page.
- On the **Disk Partitions** tab page, view the disk partition information about the host. Click a disk partition to monitor its metrics on the **Monitoring Views** page.
- Click the **NICs** tab to view the basic information about the NICs of the host. Click a NIC to monitor its metrics on the **Monitoring Views** page.
- Click the **GPUs** tab to view the basic information about the GPUs of the host. Click a GPU to monitor its metrics on the **Monitoring Views** page.
- On the **Events** tab page, view the event details of the host. For details, see **6.4 Checking AOM Alarms or Events**.
- On the **Alarms** tab page, view the alarm details of the host. For details, see **6.4 Checking AOM Alarms or Events**.
- 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. **Disk partitions are supported by CentOS 7.x and EulerOS 2.5.**

----End

10.4 Using AOM to Monitor Processes

10.4.1 Configuring AOM Application Discovery Rules

AOM can discover applications and components 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 or components on the host based on **Built-in Discovery Rules** and displays them on the application or component 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 Rule Description

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**.

Filtering Rule	Example
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.

Customizing a 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**. Enter 4 to 63 characters starting with a lowercase letter and ending with a lowercase letter or digit. Only lowercase letters, digits, and hyphens (-) are allowed.
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. Enter 1 to 255 characters.

   For example, AOM can detect the processes whose command parameters contain **ovs-vswitchd unix:** and environment variables contain **SUDO_USER=paas**.

   - 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. Enter 1 to 255 characters.

   - 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. Enter 1 to 255 characters. For example, add the text **app-test** as a component name.

   - Application types indicate 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 then collects metric data based on the discovery rule. After about two minutes, you can perform the following operations:

- On the application monitoring page, find the applications that have been monitored. For details, see **10.4.2 Using AOM to Monitor Application Processes**.
- On the component monitoring page, find the components that have been monitored. For details, see **10.4.3 Using AOM to Monitor Component Processes**.

----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. **Built-in discovery rules cannot be deleted.**
Modifying rules	Click **Modify** in the **Operation** column. **Built-in discovery rules cannot be modified.**

10.4.2 Using AOM to Monitor Application Processes

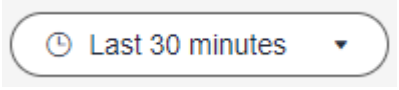
An application groups identical or similar components based on service requirements. Applications are classified into system applications and custom applications. System applications are discovered based on built-in discovery rules, and custom applications are discovered based on custom rules. The application list displays the name, running status, and deployment mode of each application. AOM supports drill-down from applications to components, instances, and processes. By viewing the status of each layer, you can implement dimensional monitoring for applications. After application discovery rules are set, AOM automatically discovers applications that meet the rules and monitors related metrics. For details, see **10.4.1 Configuring AOM Application Discovery Rules**.

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. Click a component name to view the instances of the component. Click an instance name to view the monitoring view and alarm information.
- 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 **6.4 Checking AOM Alarms or Events**.

----End

10.4.3 Using AOM to Monitor Component Processes

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.

Constraints

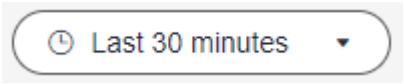
- A maximum of five tags can be created for each component.
  - Tag key: max. 36 characters; tag value: max. 43 characters
  - A tag value can contain only letters, digits, hyphens (-), and underscores (_).
- Components cannot be filtered by alias.

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Infrastructure Monitoring** > **Process Monitoring**. Next, click the **Component Monitoring** tab. Then you can view the component list.

- The component list displays information such as **Component Name**, **Application**, **Deployment Mode**, and **Application Discovery Rules**.
- To view target components, you can set filter criteria (such as the running status, application, cluster name, deployment mode, and component name) above the component list.
- Enable or disable **Hide System Components** as required. By default, system components are hidden.
- Click  in the upper right corner of the page and select or deselect the columns to display.

Step 3 Click 

in the upper right corner of the page and select a desired value from the drop-down list.

1. Set a time range to view components. There are two methods to set a time range:

   Method 1: Use a predefined time label, such as **Last 30 minutes** or **Last hour** in the upper right corner of the page. You can select a time range as required.

   Method 2: Specify the start time and end time to customize a time range. You can specify 30 days at most.

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

Step 4 Perform the following operations if needed:

- **Adding an alias**

  If a component name is complex to identify, you can add an alias for the component.

  In the component list, click  in the **Operation** column of the target component, enter an alias, and click **OK**. The added alias can be modified but cannot be deleted. Enter 1 to 64 characters. The following characters are not allowed: $#%&'+;<=>?/,

- **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**.

Step 5 Set filter criteria to search for the desired component.

Step 6 Click the component name. The component details page is displayed.

- On the **Instance List** tab page, view the instance details. 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 **6.4 Checking AOM Alarms or Events**.
- On the **Events** tab page, view the event details of the component. For details, see **6.4 Checking AOM Alarms or Events**.

----End

10.5 Using AOM to Monitor Cloud Services

Cloud service monitoring displays service instance statuses and metric usage in graphs such as line graphs and digit graphs. You can view the following services on the **Cloud Service Monitoring** page: FunctionGraph, Object Storage Service (OBS), Elastic IP (EIP), Elastic Load Balance (ELB), NAT Gateway, and Relational Database Service (RDS).

Constraints

To use cloud service monitoring, enable this function in **Menu Settings**. For details, see **14.4 Configuring AOM Menus**.

Viewing Cloud Service Monitoring Information

Step 1 Log in to the **AOM 2.0** console.

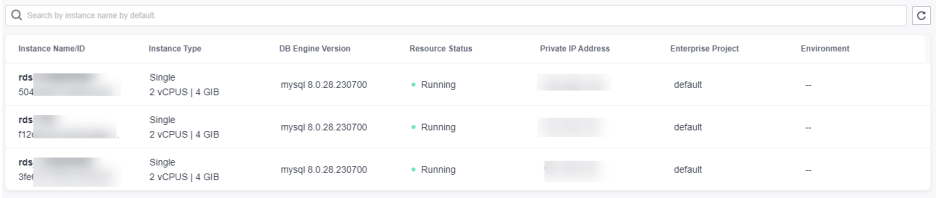
Step 2 In the navigation pane, choose **Infrastructure Monitoring** > **Cloud Service Monitoring**.

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.

- 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 Intelligent Insights (Beta)

11.1 Enabling Intelligent Insights

With intelligent insights, AOM continuously monitors your applications and resources, detects problems based on historical data and problem characteristics, and provides root cause analysis and suggestions.

Function Introduction

- **11.2 Checking Event Inspection Data on AOM**: Provides application monitoring based on APM and monitors service quality based on key metrics such as the average RT and error rate of application services and top N APIs (ranked by traffic) for automatic exception detection.
- **11.3 Checking Root Cause Analysis Results on AOM**: Uses APM tracing to locate root causes. You can analyze problems globally and diagnose and locate root causes of faults based on the traces and metrics of application services and top N APIs (ranked by traffic).
- **11.4 Checking the Fault Propagation Chain on AOM**: Identifies the propagation chain of abnormal calls based on key metrics (such as the trace, average RT, and error rate) provided by APM, and displays key metric data of services and their associated services, helping you locate root causes more effectively.

Advantages

- Extracts data characteristics in terms of periodicity, stability, and auto-correlation for automatic exception detection.
- Monitors service quality based on key metrics such as the average RT and error rate of application services and top N APIs (ranked by traffic), and enables global analysis of problems.
- Drills down traces to locate root causes.

Constraints

- For intelligent insights, analysis is made based on the application data collected by APM. To use this function, **enable APM** and connect target applications to APM first.

- This function is available only in AP-Singapore.

Enabling Intelligent Insights

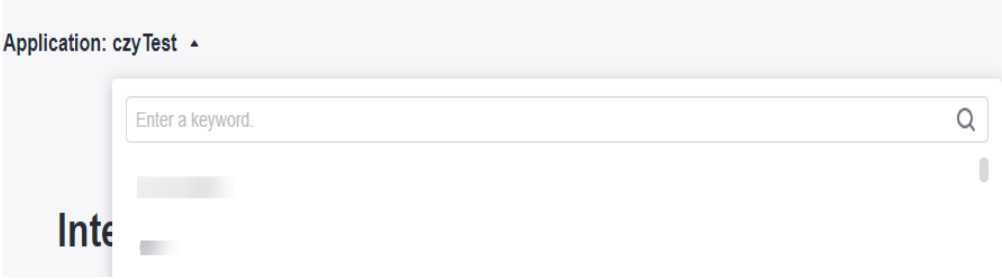
Enable intelligent insights when you use it the first time. To enable it, perform the following steps:

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Intelligent Insights (Beta)**.

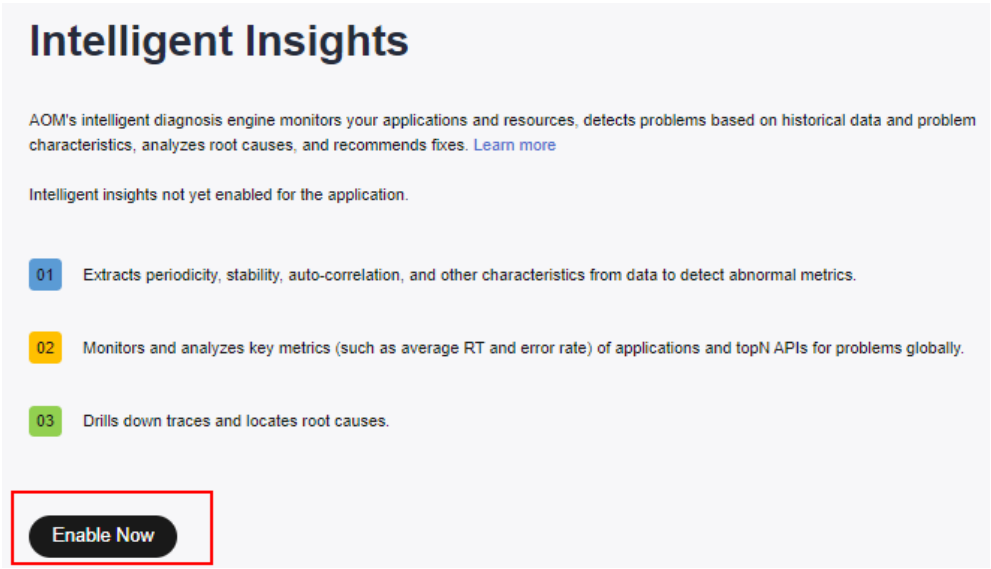
Step 3 On the top of the page, select an application for which you want to enable intelligent insights from the drop-down list.

Figure 11-1 Selecting an application



Step 4 Click **Enable Now** to enable intelligent insights.

Figure 11-2 Enabling intelligent insights



----End

11.2 Checking Event Inspection Data on AOM

AOM periodically inspects application services for which the intelligent insights function has been enabled, monitors service quality based on key metrics (such as the average RT and error rate) of historical data, and enables global analysis of problems.

Description

AOM dynamically determines upper limits based on the historical data of applications and checks whether the recent data is abnormal.

Time range for obtaining basic data:

- Dynamically determines upper limits based on the historical 3-hour data of applications and checks whether the data in the last 10 minutes is abnormal. The following event types are supported:
  - **Service Avg. RT Sharply Increases**
  - **Top N API Avg. RT Sharply Increases**
  - **Service Error Rate Sharply Increases**
  - **Top N API Error Rate Sharply Increases**
- Dynamically determines upper limits based on the historical 1-hour data of applications and checks whether the data in the last 15 minutes is abnormal. The following event type is supported: **Service Traffic Unbalanced**.

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Intelligent Insights (Beta)**.

Step 3 Set a time range in the upper right corner of the page. You can use a predefined time label, such as **Last hour** and **Last 6 hours**, or customize a time range.

Step 4 Select a target application from the drop-down list above the filter.

Step 5 Filter event inspection data. The **Filters** area displays the types and statuses of events captured in a specific time range. You can select different filters to view events.

AOM supports filtering by:

- **Event Type**: types of abnormal events detected during inspection. Options:
  - **Service Avg. RT Sharply Increases**: Based on the historical 3-hour data of applications, AOM determines whether the average RT of the entire service sharply increases in the last 10 minutes.
  - **Top N API Avg. RT Sharply Increases**: By default, the top 5 APIs ranked by traffic are detected. Based on the historical 3-hour data of APIs, AOM determines whether the average RT of the top 5 APIs sharply increases in the last 10 minutes.
  - **Service Error Rate Sharply Increases**: Based on the historical 3-hour data of applications, AOM determines whether the error rate of the entire service sharply increases in the last 10 minutes.
  - **Top N API Error Rate Sharply Increases**: By default, top 5 APIs ranked by traffic are detected. Based on the historical 3-hour data of APIs, AOM determines whether the error rate of the top 5 APIs sharply increases in the last 10 minutes.
  - **Service Traffic Unbalanced**: Based on the historical 1-hour data of applications, AOM checks whether the traffic of all instances in the last 15 minutes is unbalanced.

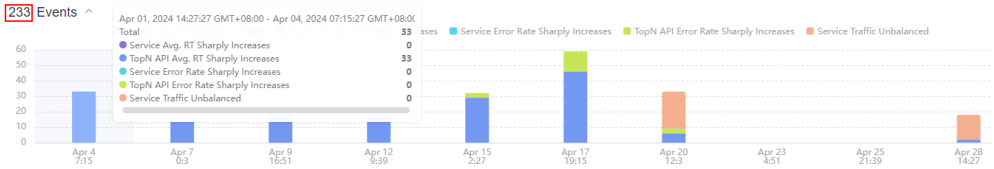
- **Status**: status of events detected during inspection.
  - **In progress**: indicates that an abnormal event is happening.
  - **Completed**: indicates that an abnormal event has completed.

Step 6 Check the event overview, card (list), and details.

- Checking the event overview

  On the **Intelligent Insights (Beta)** page, events in the last 30 minutes are displayed in a bar graph by default. You can adjust the time range as required to view events in the last hour, last 6 hours, last day, last week, or a custom time range.

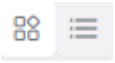
  Figure 11-3 Event statistics view

  In the graph area, perform the following operations if needed:

  - In the upper left corner of the graph, view the total number of abnormal events detected during inspection in the specified period.
  - Move the pointer to the bar graph to view the number of events of each type at a specific time point.
  - Click a legend above the bar graph to hide or display a certain type of events.
  - In the search box, enter a keyword to filter events.

- Checking the event card (list)

  The event card (list) displays the abnormal events detected during inspection in a specified time range. You can click  in the upper right corner of the page to switch the event display mode (card or list). Each event contains the following information:

  - **Event Type**: type of an event.
  - **Description**: describes the component and interface where the event occurs.
  - **Triggered**: time when an exception first occurs.
  - **Duration**: the period for which the exception lasts.

Figure 11-4 Event cards

Figure 11-5 Event list

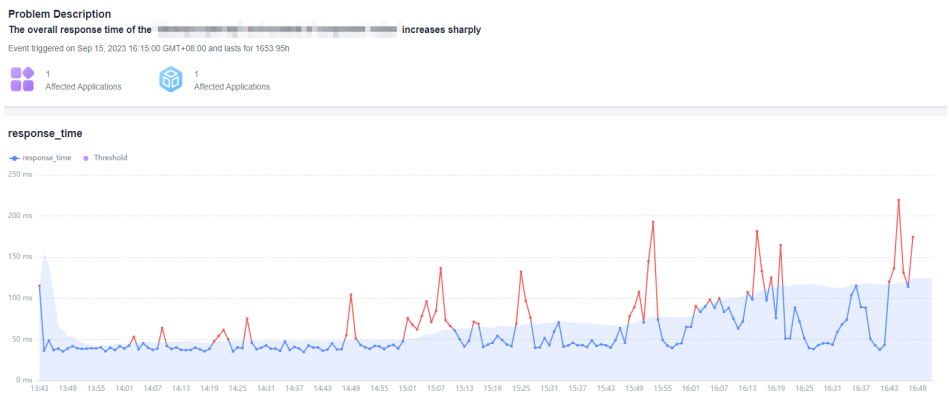
Event Type	Description	Triggered	Duration
TopN API Avg. RT Sharply Increases	The response time of the 'ams-access-go' API increases sharply in the 'cn-north-7' environment of the '/v1/:project_id/:prometheus_instance/push^POST' component	Oct 27, 2023 15:36:00 GMT+08:00	0.17 h
TopN API Avg. RT Sharply Increases	The response time of the 'ams-access-go' API increases sharply in the 'cn-north-7' environment of the '/v1/:project_id/report/metricdata^POST' component	Oct 27, 2023 15:35:00 GMT+08:00	0.17 h
TopN API Error Rate Sharply Increases	The error rate of the 'ams-access-go' API increases sharply in the 'cn-north-7' environment of the '/rest/amsaccess/v1/projectid/:project_id/metricdata^POST' component	Oct 27, 2023 15:19:00 GMT+08:00	1.13 h

- Checking event details

  You can click different event cards or lists to go to the event details page. On the event details page, graphs about key metrics such as RT and error rate are displayed, showing the duration for which an exception lasts, time when the exception first occurs, and upper limit.

  – Details displayed when the service avg. RT sharply increases:

  Figure 11-6 Service avg. RT sharply increases

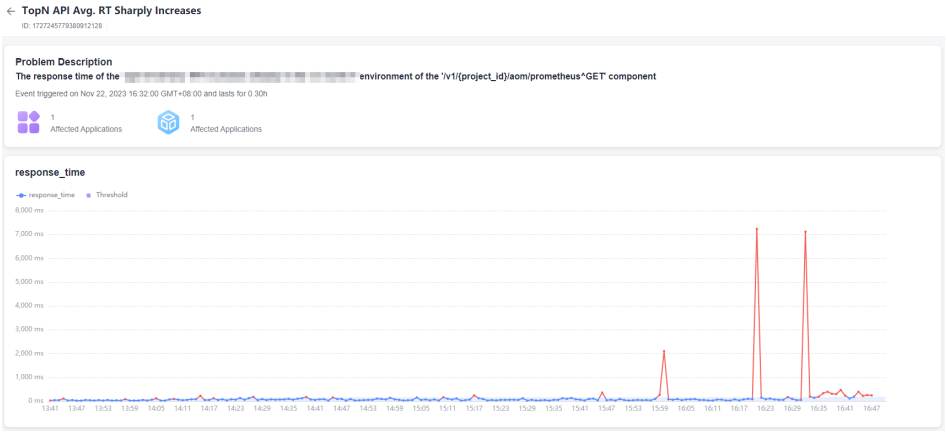


  – Details displayed when the service error rate sharply increases:

Figure 11-7 Service error rate sharply increases

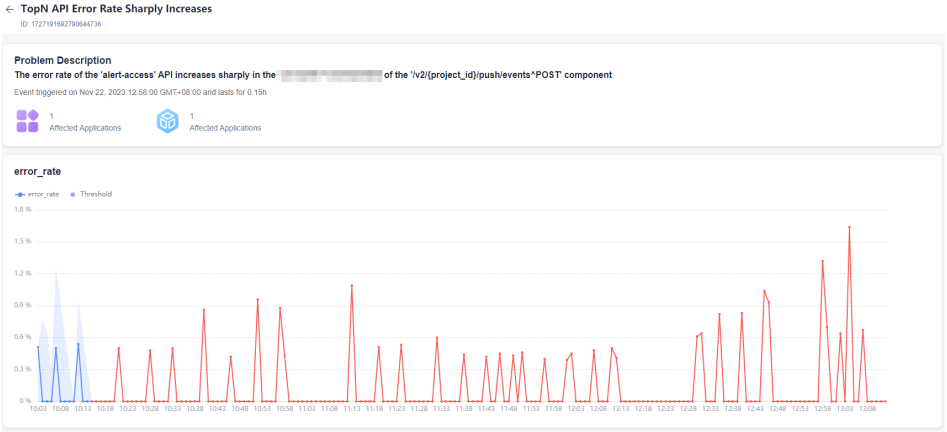
- Details displayed when the top N API avg. RT sharply increases:

Figure 11-8 Top N API avg. RT sharply increases



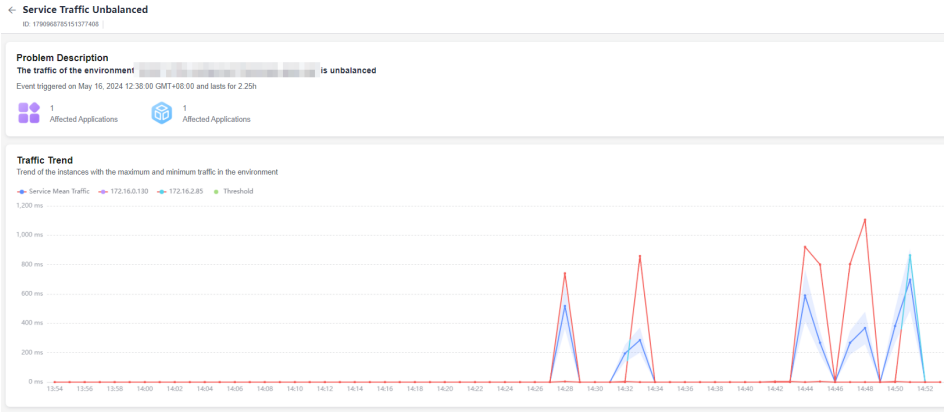
- Details displayed when the top N API error rate sharply increases:

Figure 11-9 Top N API error rate sharply increases



- Details displayed when the service traffic unbalanced:

Figure 11-10 Service traffic unbalanced



----End

11.3 Checking Root Cause Analysis Results on AOM

Intelligent Insights allow you to quickly locate and analyze the root causes of abnormal events. Based on historical service data of event inspection, drill-down analysis is performed based on service metrics and trace data for root cause locating.

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Intelligent Insights (Beta)**.

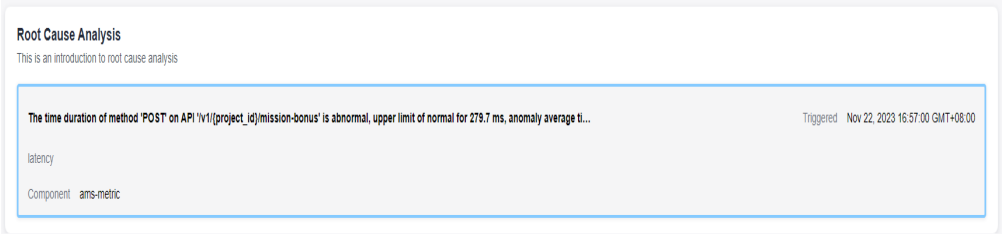
Step 3 Set a time range in the upper right corner of the page. You can use a predefined time label, such as **Last hour** and **Last 6 hours**, or customize a time range.

Step 4 Select a target application from the drop-down list above the filter.

Step 5 Click an event card or list to go to the event details page and view the root cause analysis result.

- **Service Avg. RT Sharply Increases**: Based on application trace data, AOM provides drill-down analysis by application, analyzes the average latency of each component, and locates the component that causes the RT to sharply increase.

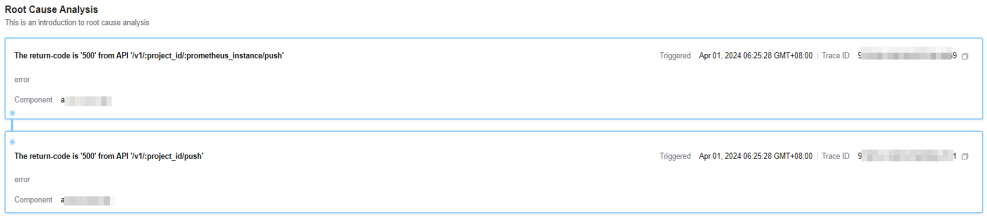
  Figure 11-11 Service avg. RT sharply increases

- **Service Error Rate Sharply Increases**: Based on application trace data, AOM provides drill-down analysis by application, analyzes the error rate of each component, and locates the component that causes the error rate to sharply

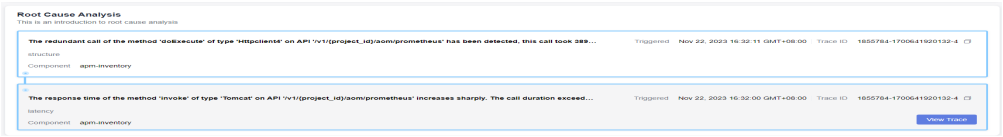
increase. Click **View Trace** to trace the cause of the sharp increase in the error rate.

Figure 11-12 Service error rate sharply increases



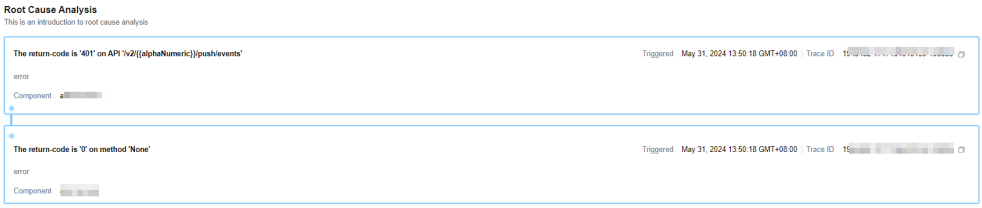
- **Top N API Avg. RT Sharply Increases**: Based on application trace data, AOM provides RT analysis for APIs to quickly locate root causes.

Figure 11-13 Top N API avg. RT sharply increases



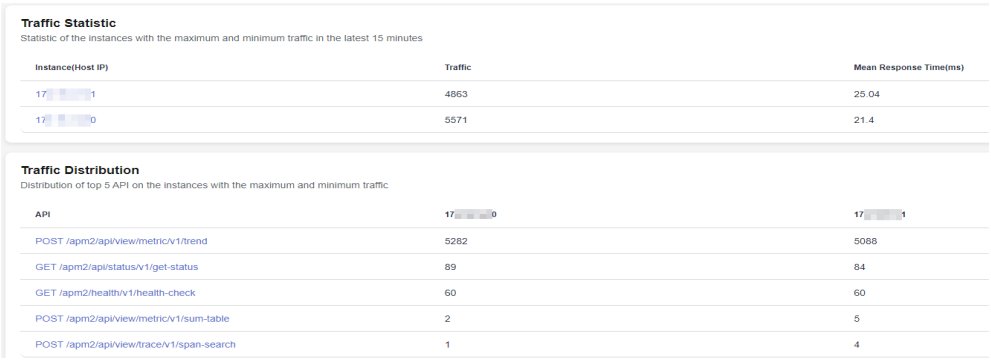
- **Top N API Error Rate Sharply Increases**: Based on application trace data, AOM provides error rate analysis for APIs to quickly locate root causes. Click **View Trace** to trace the cause of the sharp increase in the error rate.

Figure 11-14 Top N API error rate sharply increases



- **Service Traffic Unbalanced**: Based on the traffic data of all instances of an application, AOM displays the instances with the maximum and minimum traffic and their latency. It also shows the distribution of the top 5 APIs with the highest traffic on the instances with the maximum and minimum traffic, helping you quickly locate affected APIs. You can click an API to trace its recent calls.

Figure 11-15 Service traffic unbalanced



----End

Event Root Cause Analysis Methods

The intelligent insights function locates root causes based on trace drill-down. It consists of offline training and online inference.

1. Offline training: After you enable the intelligent insights function, the offline training task of the root cause analysis model will be automatically enabled in the backend. The system then obtains the trace data generated during application API calling and trains the trace model based on the trace data of the last seven days. By default, the model is automatically updated in the backend every 14 days and saved in the backend database.
2. Online inference: After you click an event card to go to the root cause analysis page, the online inference task of the root cause analysis model will be triggered. The system then compares the trace model previously trained offline with the calls of the abnormal event, and analyzes root causes for fast fault locating.

11.4 Checking the Fault Propagation Chain on AOM

AOM provides the propagation chain of abnormal calls based on key metrics (such as the trace, average RT, and error rate), and displays key metric data of services and their associated services, helping you locate root causes more effectively.

Procedure

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane, choose **Intelligent Insights (Beta)**.

Step 3 Set a time range in the upper right corner of the page. You can use a predefined time label, such as **Last hour** and **Last 6 hours**, or customize a time range.

Step 4 Select a target application from the drop-down list above the filter.

Step 5 Click an event card or list to go to the event details page and check the fault propagation chain.

The fault propagation chain displays the faults in traces. You can locate root causes based on this chain. The fault propagation chain function is supported for the following types of abnormal events:

- **Service Avg. RT Sharply Increases**
- **Top N API Avg. RT Sharply Increases**
- **Service Error Rate Sharply Increases**
- **Top N API Error Rate Sharply Increases**

Figure 11-16 Fault propagation graph

----End

12 Application Insights

12.1 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.

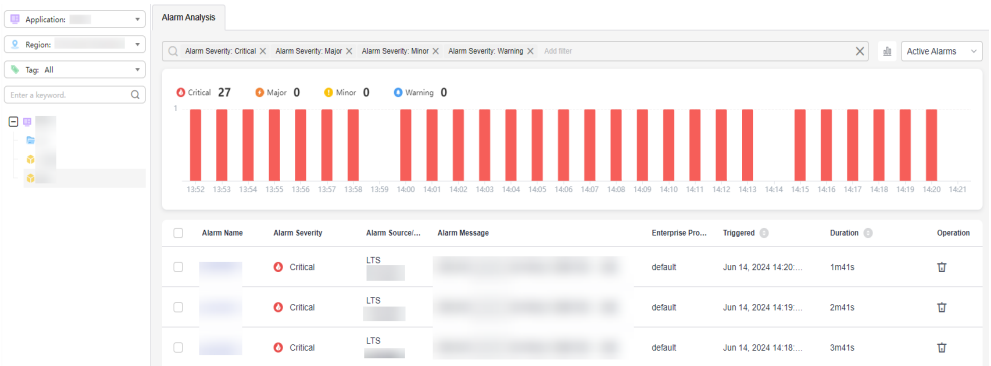
- Application monitoring

  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 12-1 Component monitoring

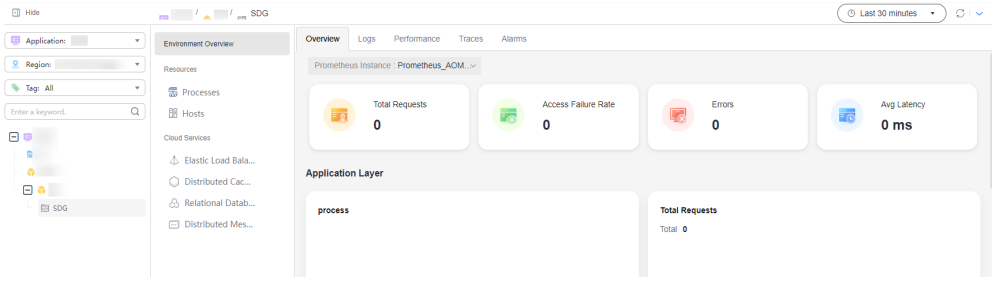
  

- Environment monitoring

  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 12-2 Environment monitoring



Constraints

- To use application monitoring, enable **Application Insights** in **Menu Settings**. For details, see **14.4 Configuring AOM Menus**.
- 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 12-3 Editing the YAML file

  e. Set parameters by referring to **Table 12-1**. **Figure 12-4** shows the details.

Table 12-1 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 12-4 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.

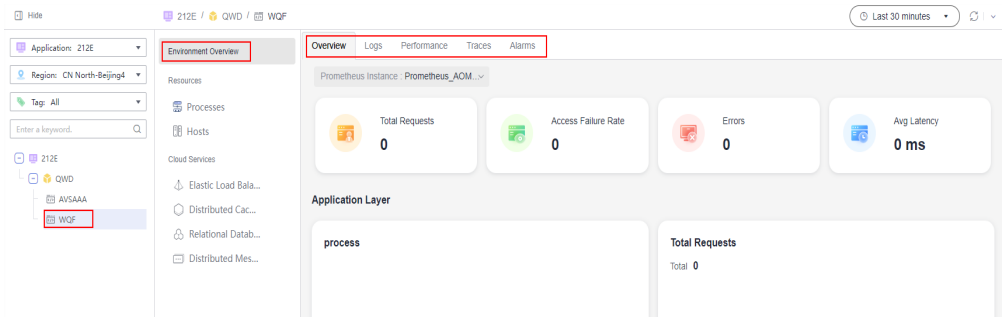
- For details about operations related to dashboards, see **5 Dashboard Monitoring**.

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 **6.4 Checking AOM Alarms or Events**.
- 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 check the environment, process, performance, log analysis, trace, and alarm information in the right pane.

Figure 12-5 Checking the environment



- 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 **Performance** tab page, view the performance about the environment. To use this function, you need to obtain APM permissions. For details, see **Permissions Management**.
- On the **Traces** tab page, view request success/failure, response time, and generation time about URLs and call methods. To use this function, you need to obtain APM permissions. For details, see **Permissions Management**.
- On the **Alarms** tab page, view the alarms and events in the current environment. For details, see **6.4 Checking AOM Alarms or Events**.

----End

12.2 CMDB

12.2.1 CMDB 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.

Constraints

To use CMDB, enable **Application Insights** in **Menu Settings**. For details, see **14.4 Configuring AOM Menus**.

Function Description

Table 12-2 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.

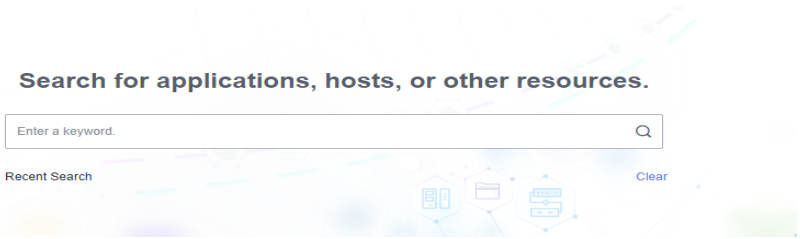
- **Environment**: Components or programs with different configurations form different environments. Each environment has its own region attribute. You can filter environments by region. You can also add one or more tags when creating an environment, and filter environments by tag. For example, environments 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.

12.2.2 Homepage

Resource Retrieval

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

Figure 12-6 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

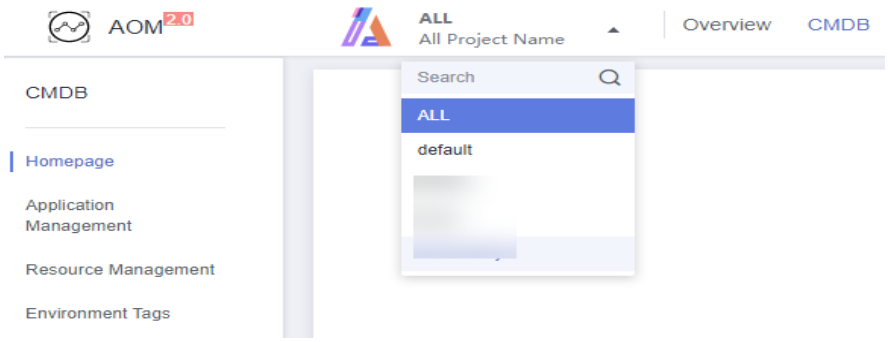
An enterprise project can contain one or more applications.

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 12-7 Enterprise project



----End

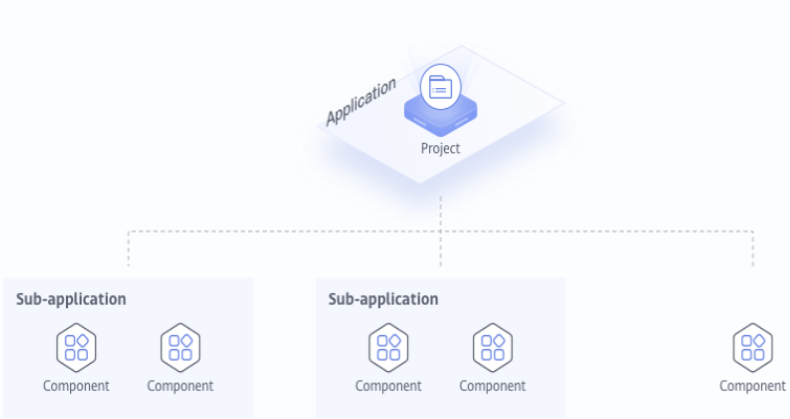
12.2.3 Application Management

12.2.3.1 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".

- **12.2.3.2 Creating an Application**
- **12.2.3.3 Adding a Node**
- **12.2.3.4 Adding an Environment**
- **12.2.3.5 Binding Resources**

Figure 12-8 Application management model



12.2.3.2 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 12-3 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 12-4.

Table 12-4 Related operations

Operation	Description
Adding a node	Locate the target application, click  , and add a node by referring to 12.2.3.3 Adding a Node.
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.

12.2.3.3 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.

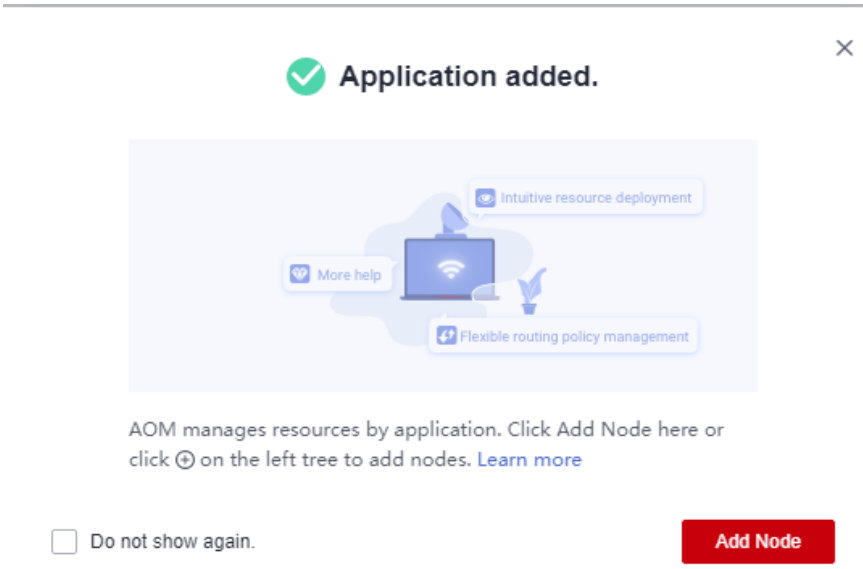
Step 2 In the navigation pane, choose **Application Insights (Retiring)** > **CMDB**.

Step 3 Select **an enterprise project**.

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

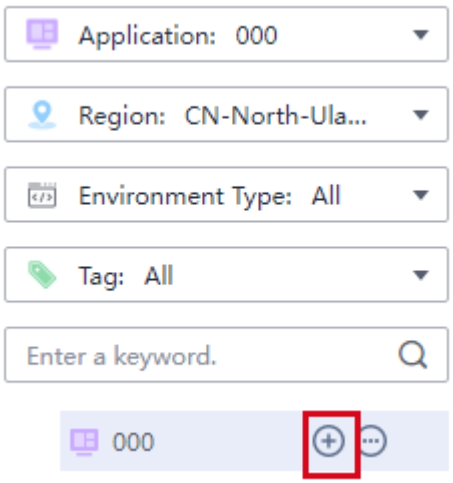
- After an application is created, click **Add Node**.

Figure 12-9 Creating a sub-application



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

Figure 12-10 Application tree



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

Figure 12-11 Adding a node

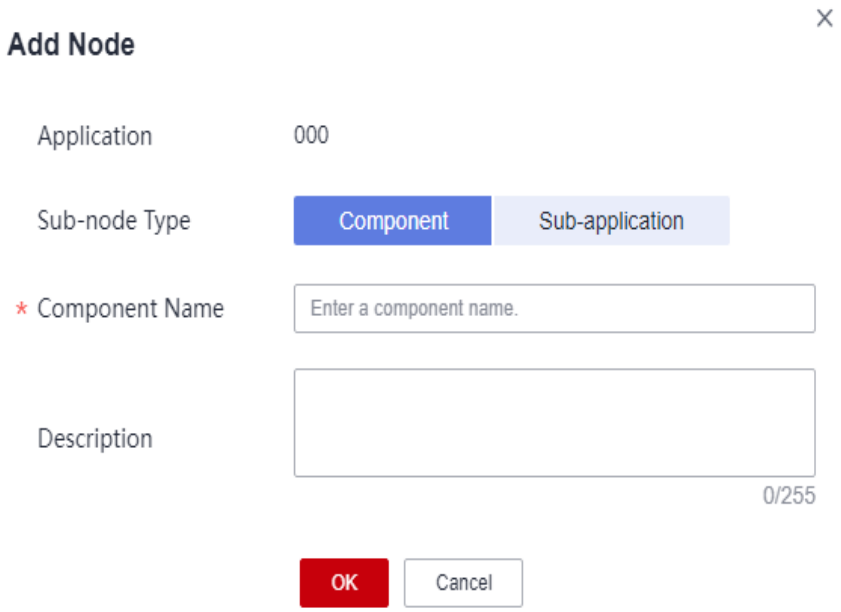


Table 12-5 Parameters for adding a node

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 12-6**.

Table 12-6 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**.
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 **12.2.3.4 Adding an Environment**.
Viewing node information	Locate a sub-application or component and click **Sub-application Info** or **Component Info** in the right pane.

12.2.3.4 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

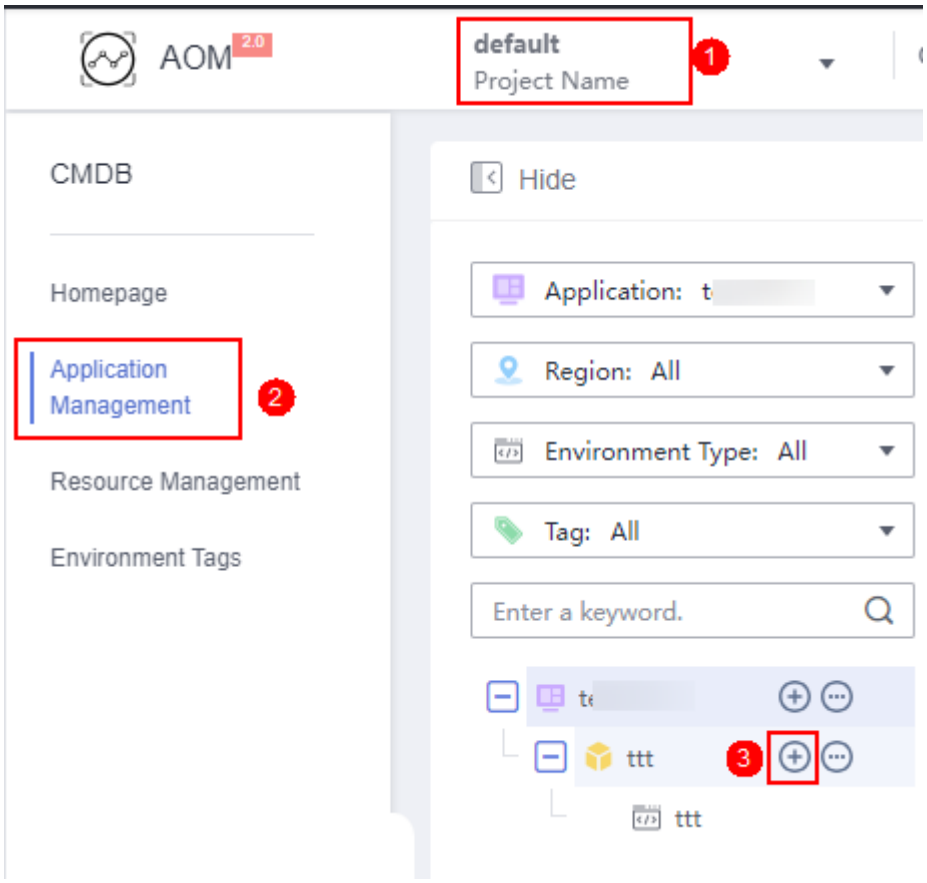
Step 1 Log in to the AOM 2.0 console.

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

Step 3 Select **an enterprise project**. In the navigation pane, choose **Application Management**.

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

Figure 12-12 Adding an environment



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

Table 12-7 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 12-8**.

Table 12-8 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 **12.2.3.5 Binding Resources**.
Viewing environment information	Locate an environment in the tree on the left and click **Environment Info** in the right pane.

12.2.3.5 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.

Checking the Resource List

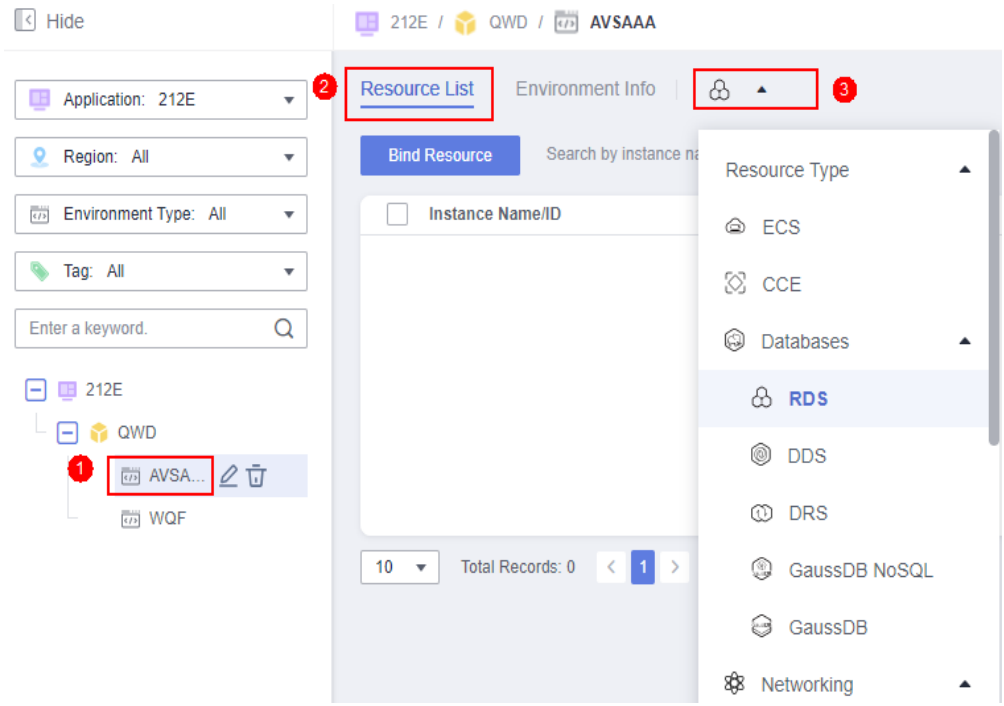
Step 1 Log in to the AOM 2.0 console.

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

Step 3 Select **an enterprise project**. In the navigation pane, choose **Application Management**.

Step 4 In the tree on the left, locate the target environment. In the right pane, click the **Resource List** tab and select a resource type. Then check the information about each resource type. For details, see **Table 12-9**.

Figure 12-13 Checking the resource list



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 12-9 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.

Resource Type		Sub-type	Information
	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.
	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.

Resource Type		Sub-type	Information
	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**. In the navigation pane, choose **Application Management**.

Step 4 In the tree on the left, locate the target environment. In the right pane, click the **Resource List** tab and select a resource type. 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 **2.2.1 Installing UniAgents**.

----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**. In the navigation pane, choose **Application Management**.

Step 3 In the tree on the left, locate the target environment. In the right pane, click the **Resource List** tab and select a resource type.

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 12-10**.

Table 12-10 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.

Parameter	Description
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**. In the navigation pane, choose **Application Management**.

Step 3 In the tree on the left, locate the target environment. In the right pane, click the **Resource List** tab and select a resource type.

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**. In the navigation pane, choose **Application Management**.

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.

12.2.4 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), databases (Relational Database Service (RDS), Data Replication Service (DRS), GaussDB NoSQL, and GaussDB), networking (Virtual Private Cloud (VPC), Elastic Load Balance (ELB), Elastic IP (EIP)), application middleware (Distributed Cache Service (DCS) and Distributed Message Service (DMS) (Kafka and RabbitMQ)), storage (Object Storage Service (OBS), Elastic Volume Service (EVS), and Cloud Backup and Recovery (CBR)), FunctionGraph)

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 12-11**.

Table 12-11 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.
Database	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.
Database	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		

Resource Type		Sub-type	Information	Operation
		Data subscription task		
		Backup migration task		
Database	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.
Database	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.

Resource Type		Sub-type	Information	Operation
	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.
	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.

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.
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.

----End

12.2.5 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 12-14 Adding a tag

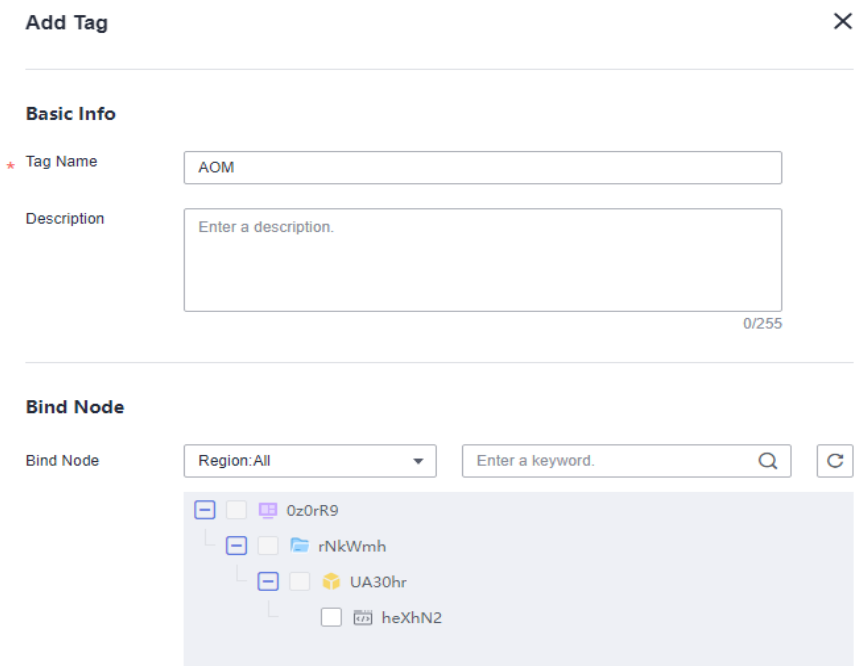


Table 12-12 Parameters for adding a tag

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.

Parameter	Description
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 12-13**.

Table 12-13 Related operations

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

12.3 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 **12.2.3.3 Adding a Node** and **12.2.3.4 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**.

Constraints

- To use log ingestion, enable **Application Insights** in **Menu Settings**. For details, see **14.4 Configuring AOM Menus**.
- 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.

13 O&M Management

13.1 O&M Management 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.

Constraints

To use Automation, enable this function in **Menu Settings**. For details, see **14.4 Configuring AOM Menus**.

Function description

Table 13-1 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.

13.2 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 **16.1 Accessing 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

13.3 Automation Permissions Management

13.3.1 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.

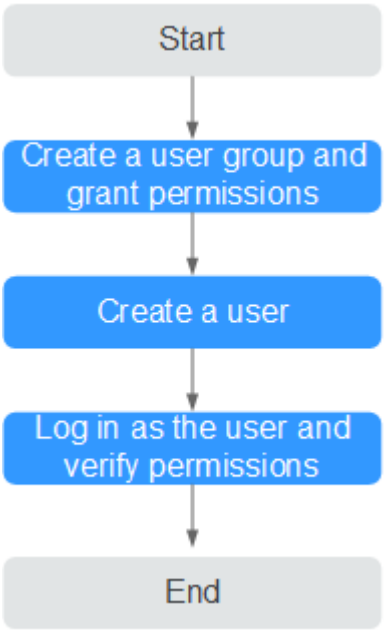
This section describes the procedure for granting permissions (see **Figure 13-1**).

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 13-1 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.

13.3.2 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"
         ],
      }
   ]
}
```

13.4 Scenarios

13.4.1 Scenario Overview

Released tool cards are displayed based on scenarios described in **13.11.3 Checking 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 **13.3.2 Custom Policies for Automation**. For details, see **Table 13-2**.

Table 13-2 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 **13.9 Managing Scripts** and **13.10 Managing Files**.

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 **13.4.2 Starting an ECS**, **13.4.3 Stopping an ECS**, **13.4.4 Restarting an RDS DB Instance**, **13.4.5 Changing an ECS Non-Administrator Password**, and **13.4.6 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 **13.4.7 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.

13.4.2 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 13-3**.

Figure 13-2 Starting an ECS

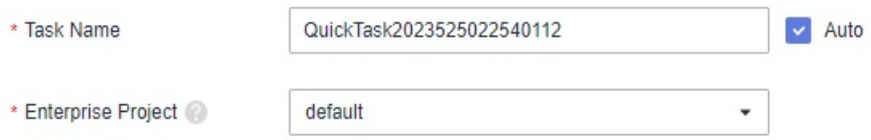


Table 13-3 Parameters for starting an ECS

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 13-4**.

Figure 13-3 Selecting an instance

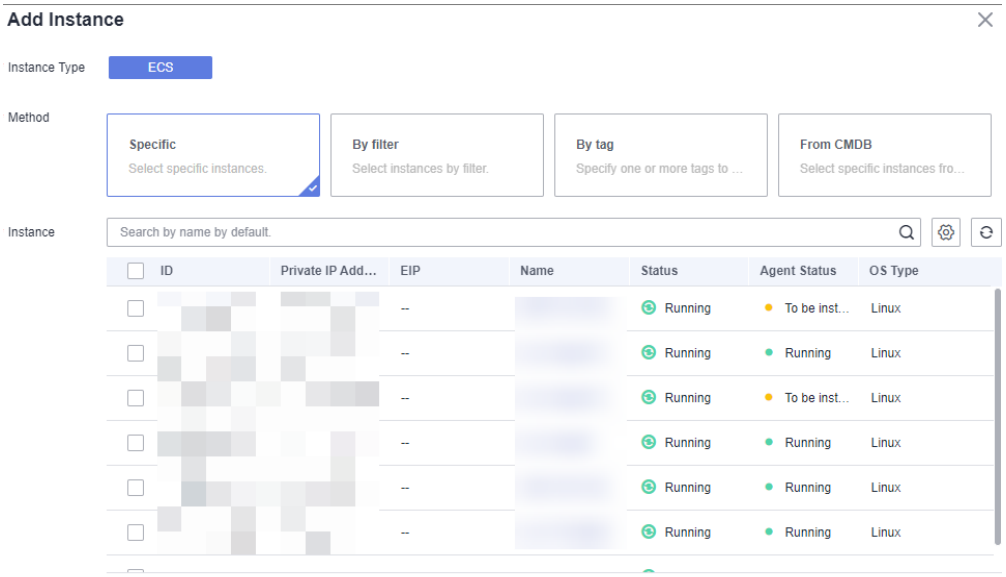


Table 13-4 Selection method description

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 13-5**.

Table 13-5 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

13.4.3 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 13-6**.

Figure 13-4 Stopping an ECS

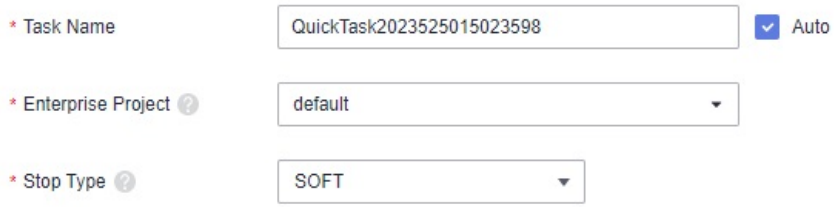


Table 13-6 Parameters for stopping an ECS

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 13-7**.

Figure 13-5 Selecting an instance

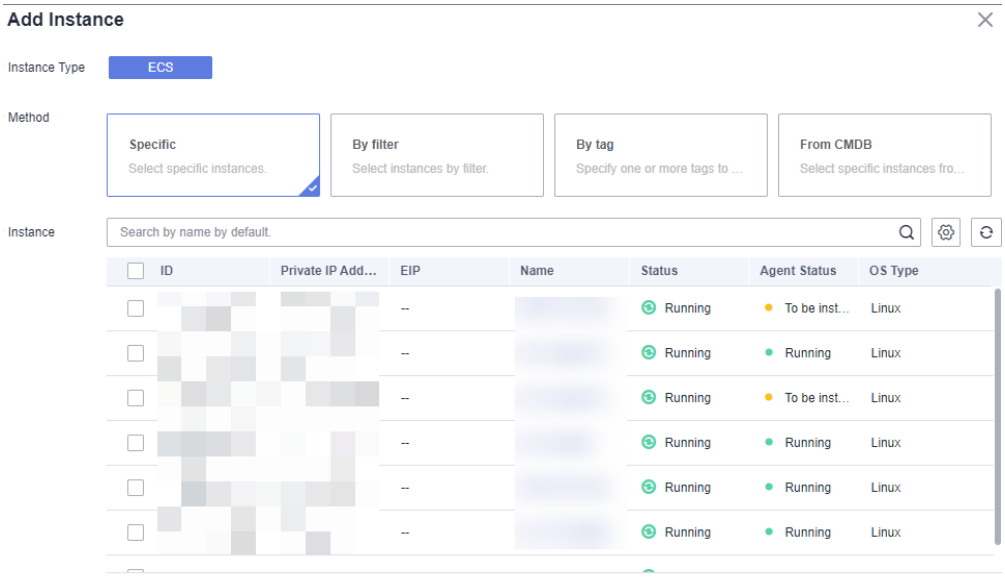


Table 13-7 Selection method description

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 13-8**.

Table 13-8 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

13.4.4 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 13-9**.

Figure 13-6 Restarting an RDS DB instance

Table 13-9 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 13-10**.

Figure 13-7 Selecting an instance

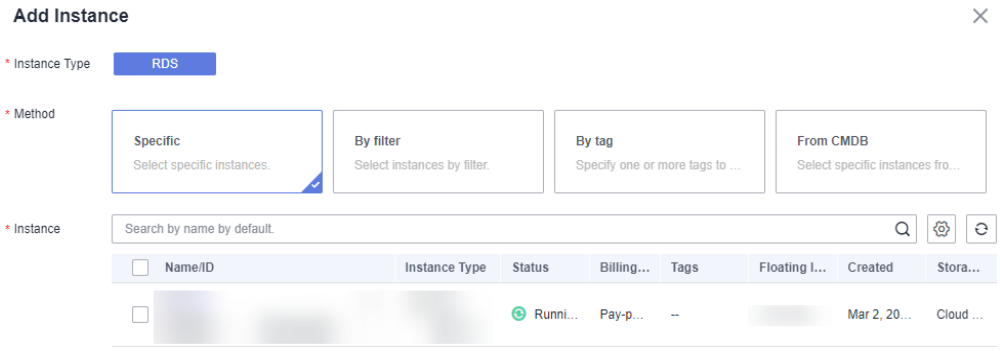


Table 13-10 Selection method description

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 13-11**.

Table 13-11 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

13.4.5 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 13-12**.

Figure 13-8 Changing the ECS non-administrator password

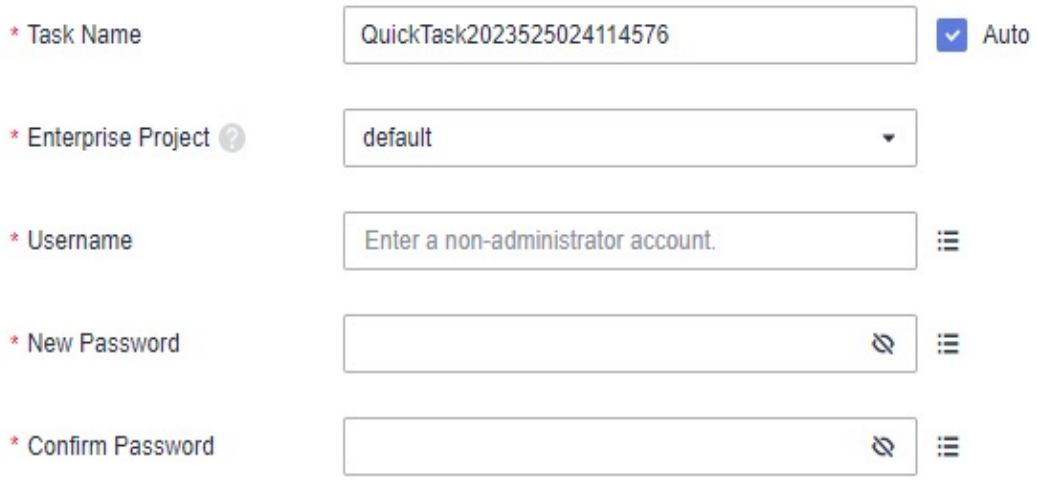


Table 13-12 Parameters for changing the ECS non-administrator password

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 13-13**.

Figure 13-9 Selecting an instance

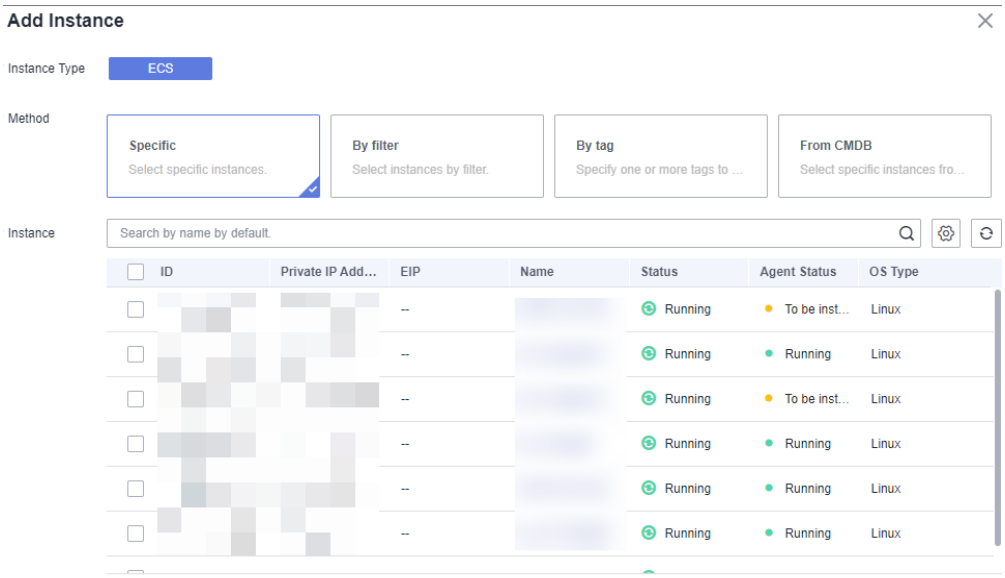


Table 13-13 Selection method description

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 13-14**.

Table 13-14 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

13.4.6 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 13-15**.

Figure 13-10 Restarting a CCE workload

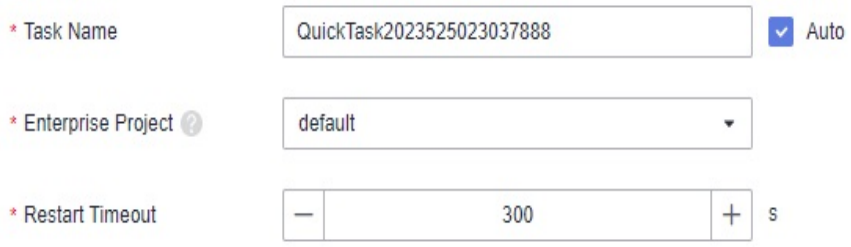


Table 13-15 Parameters for restarting a CCE workload

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 13-16**.

Figure 13-11 Creating a task for restarting a CCE workload

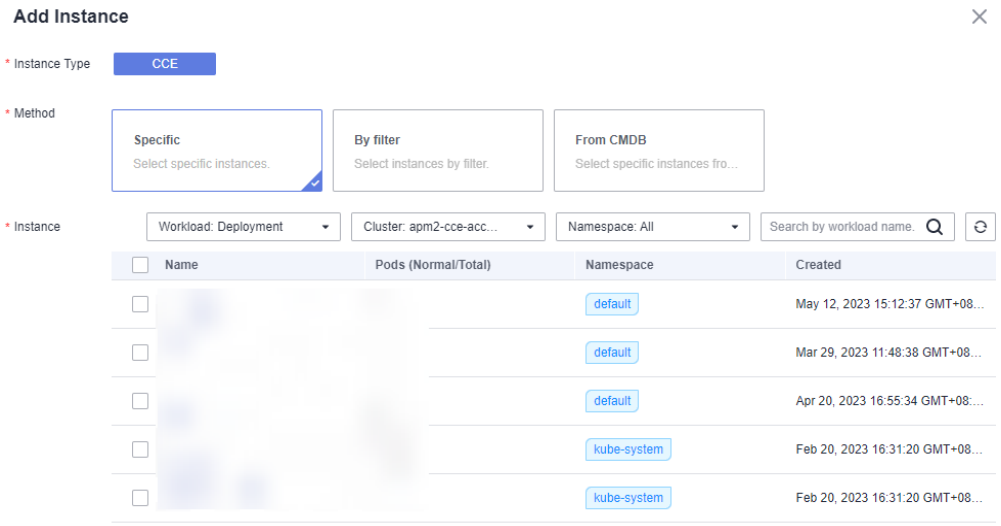


Table 13-16 Selection method description

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 13-17**.

Table 13-17 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

13.4.7 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 13-18**.

Figure 13-12 Clearing disk space

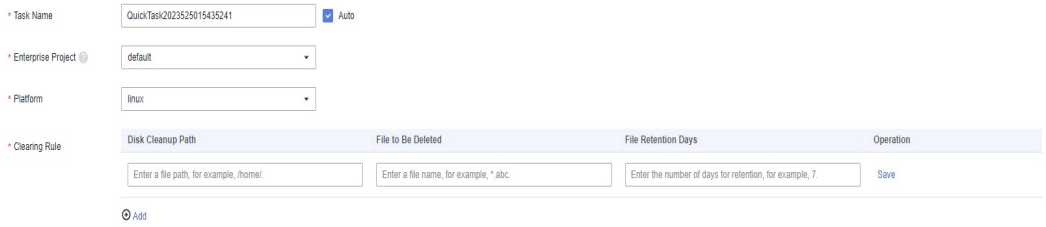


Table 13-18 Parameters for clearing disk space

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 13-19**.

Figure 13-13 Selecting an instance

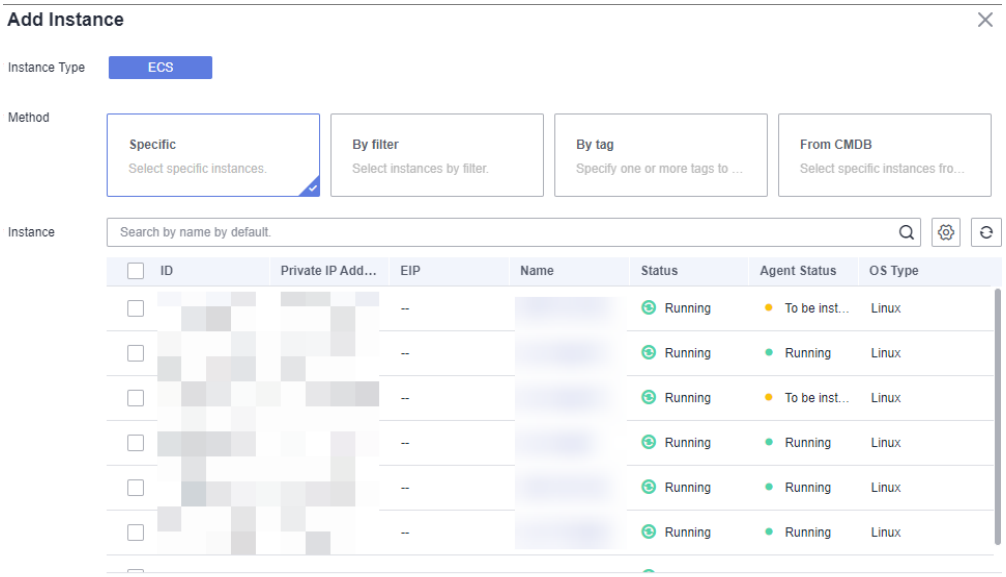


Table 13-19 Selection method description

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 13-20**.

Table 13-20 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

13.5 Managing 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 13-21**.

Figure 13-14 Basic information for creating a scheduled task

Table 13-21 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 13-22**.

Figure 13-15 Creating a scheduled task

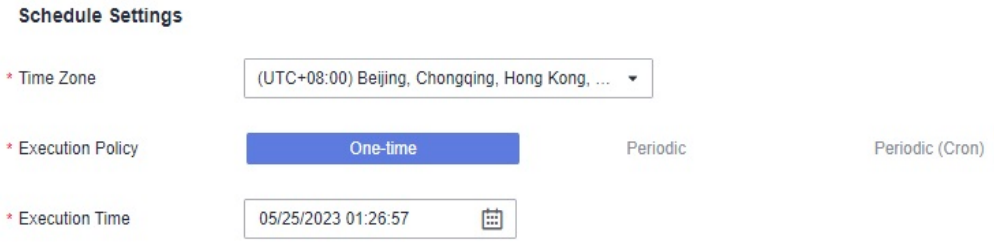


Table 13-22 Parameters for creating a scheduled task

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 13-23**.

Figure 13-16 Notification settings

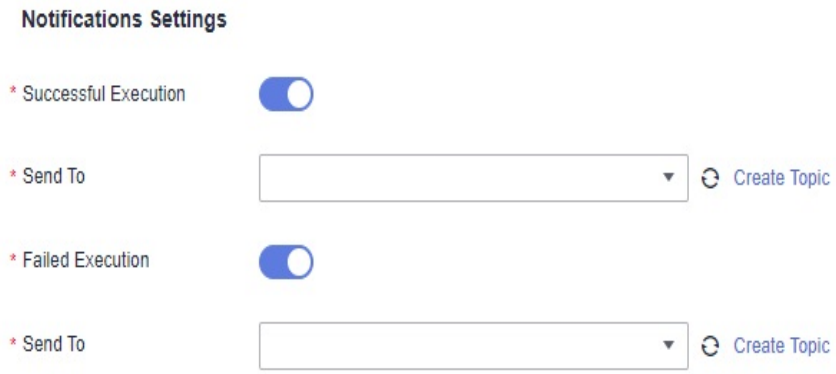


Table 13-23 Notification parameters

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

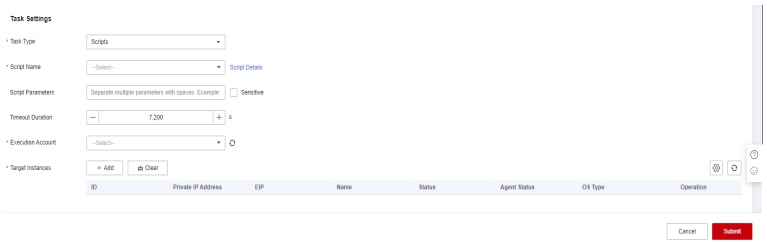
Notifications can be sent by email or SMS.

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 13-17 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 13-24**.

     Table 13-24 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 13-18 Setting a package management task

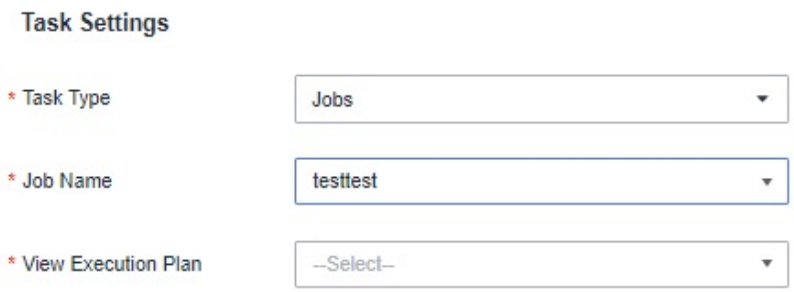
  c. Select target instances. Specifically, click **Add**. The instance selection page is displayed. For **Instance Type**, the default value is **ECS**. For **Method**, the default value is **Specific**. For details about the methods, see **Table 13-24**.
- Set a scenario task.
  a. Set **Task Type** to **Scenarios**.
  b. Select a scenario from the drop-down list. For details about operations in different scenarios, see **13.4 Scenarios**.

  Figure 13-19 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 13-20 Setting a job management task



Step 8 If needed, expand **More** to set the review configuration and execution policy by referring to **Table 13-25**.

Table 13-25 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 13-26**.

Table 13-26 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.

13.6 Managing 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 13-27**.

Table 13-27 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

13.7 Configuring 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 13-28**.

Figure 13-21 Setting parameters

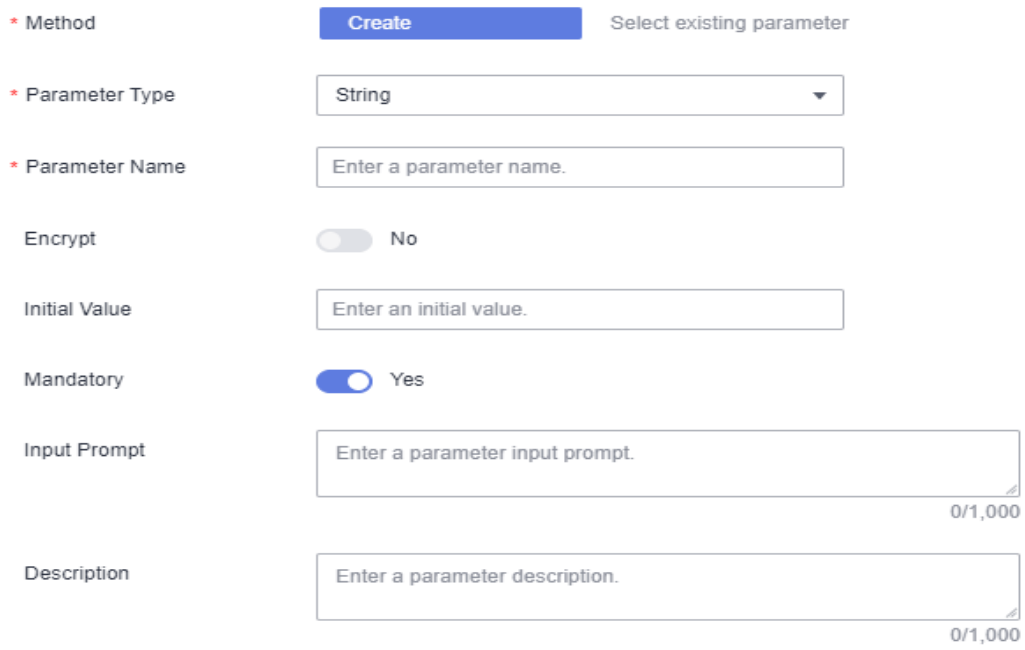


Table 13-28 Parameters

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 13-29**.

Table 13-29 Related operations

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

13.8 Managing 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 **13.4 Scenarios**.

Constraints

- 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 13-30**.

Figure 13-22 Creating a job

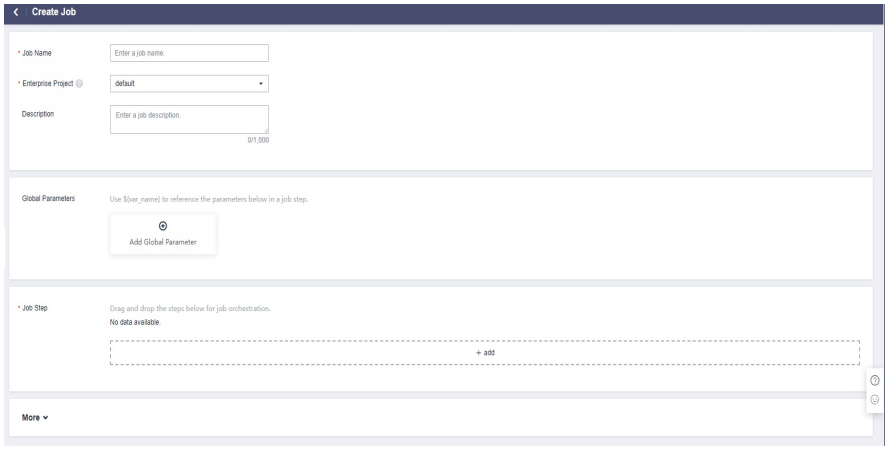


Table 13-30 Parameters for creating a job

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 13-31**.

Figure 13-23 Adding global parameters

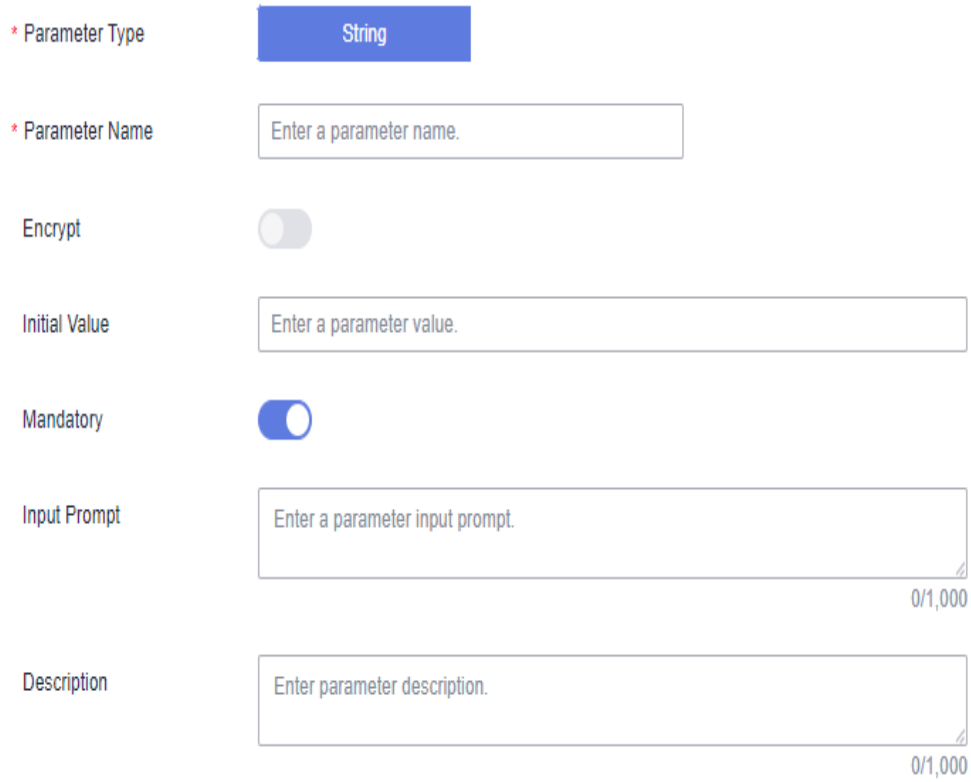


Table 13-31 Global parameters

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 13-32**.

Figure 13-24 Adding a job step (script)

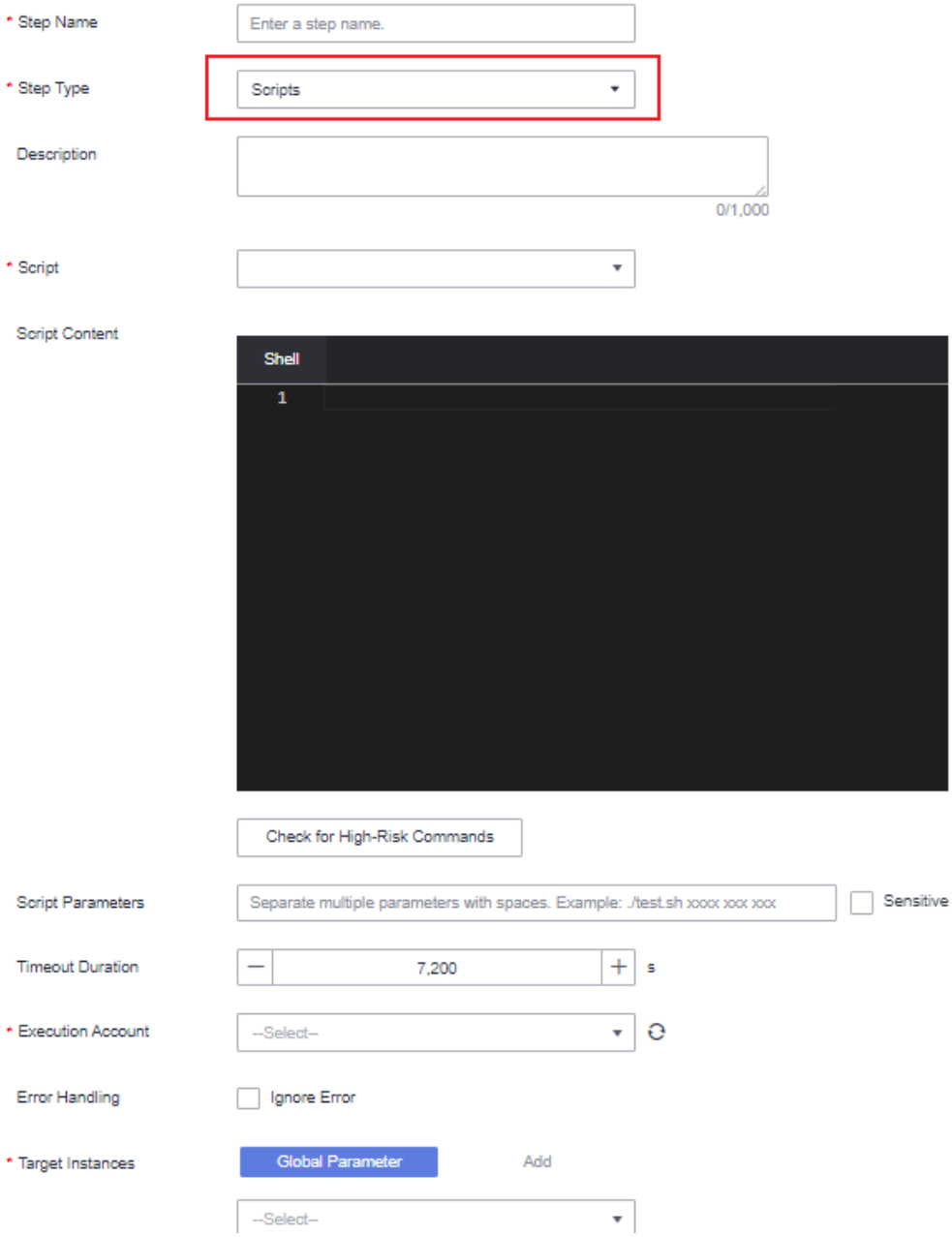


Figure 13-25 Adding a job step (package)

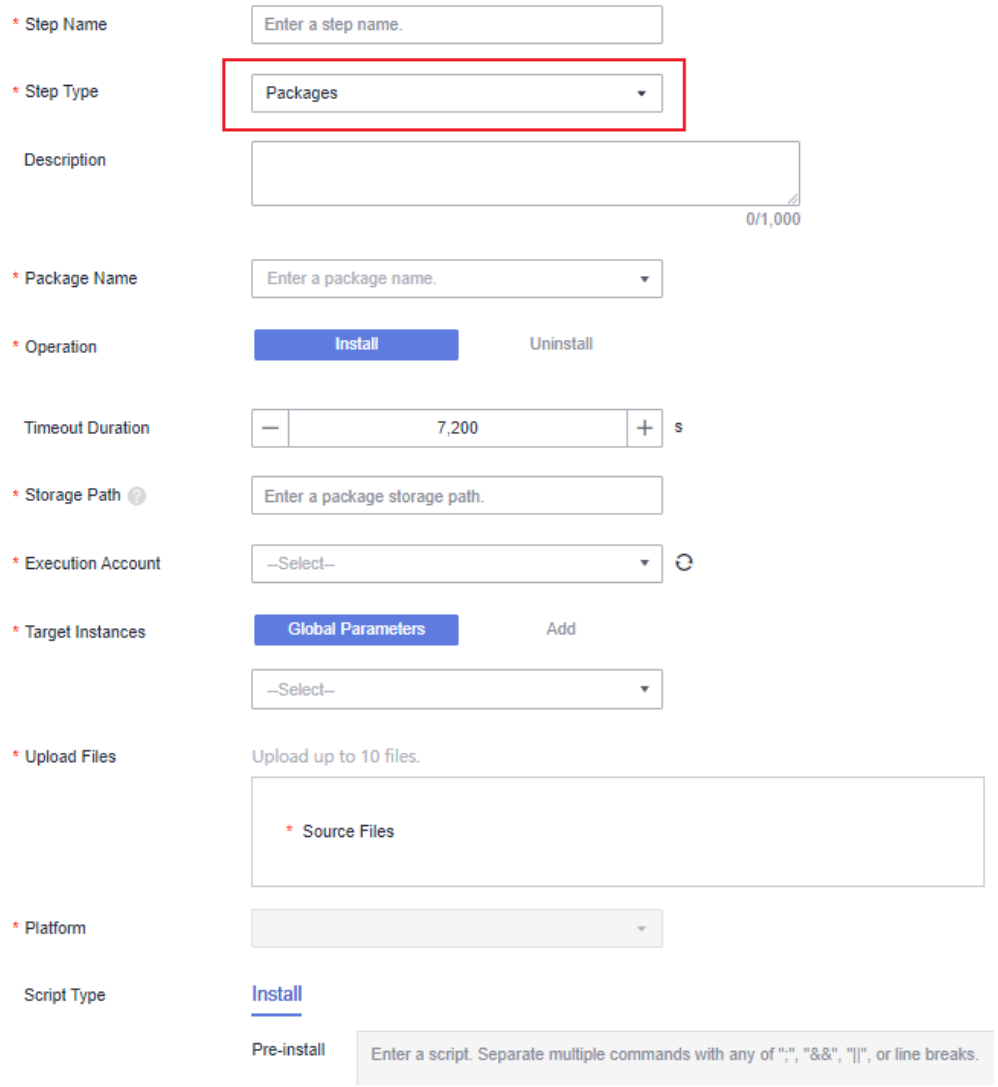


Table 13-32 Parameters for adding a step

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 13-48**.
	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 13-40**.

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 13-33** if needed.

Table 13-33 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

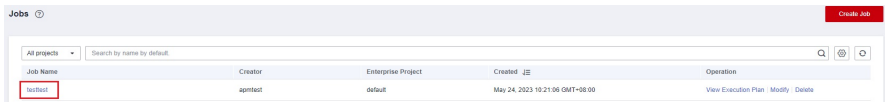
- If the information for adding a job step is incomplete, "Insufficient information" will be displayed after you save the settings.
- To adjust step sequence, drag  at the beginning of the row where the job step is located.
- To delete a step, click  in the row that contains the target step.

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 13-26 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 13-34**.

Figure 13-27 Creating an execution plan

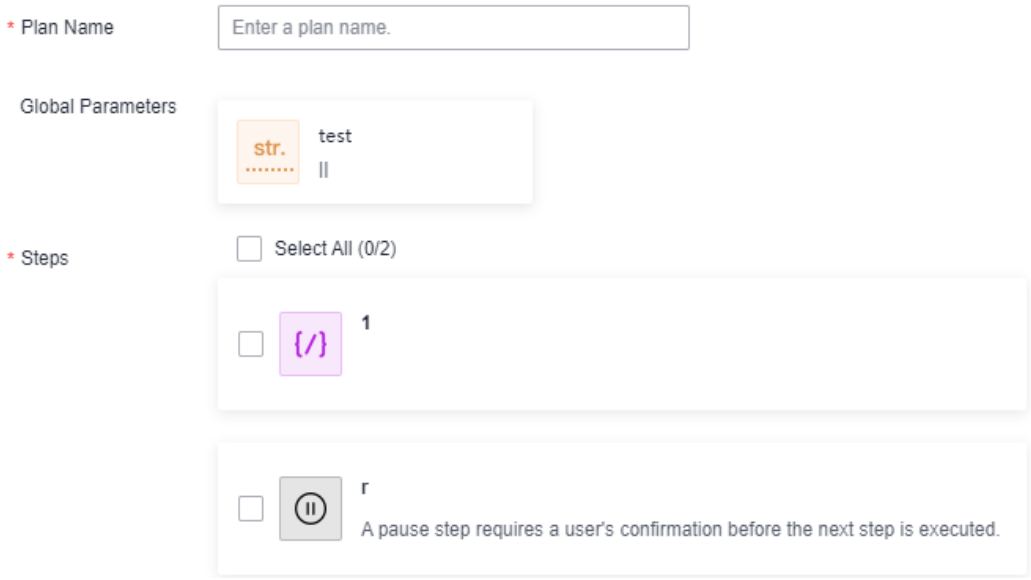


Table 13-34 Parameters for creating an execution plan

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**.

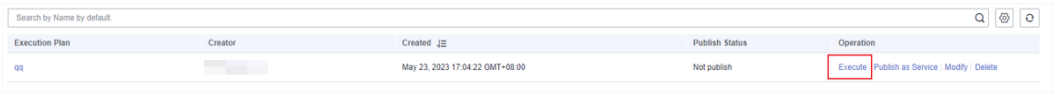
----End

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 13-28 Executing a plan



Step 2 On the task creation page, click **Execute**.

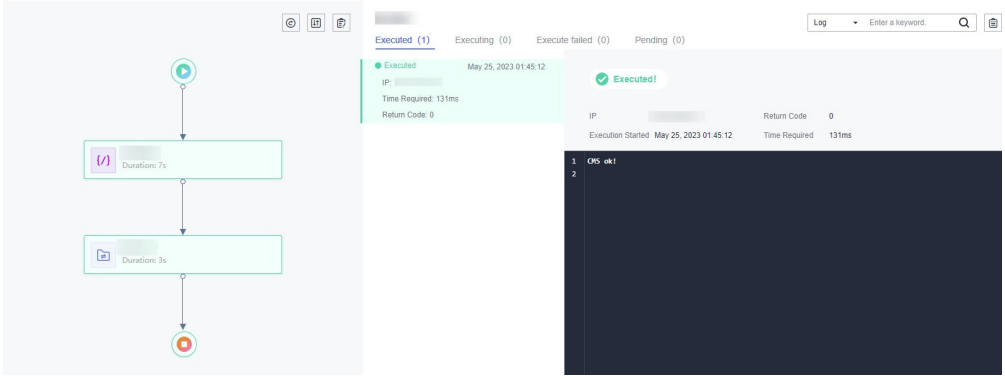
NOTE

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 13-29 Plan execution details



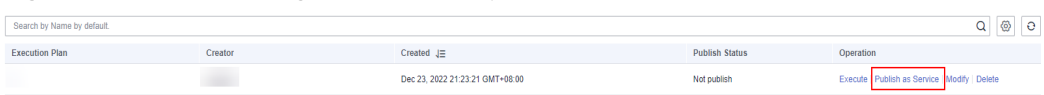
----End

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 **13.4 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 13-30 Publishing an execution plan as a service



Step 2 Enter basic information and click **OK**. For details, see **Table 13-35**.

Figure 13-31 Publishing a plan as a service

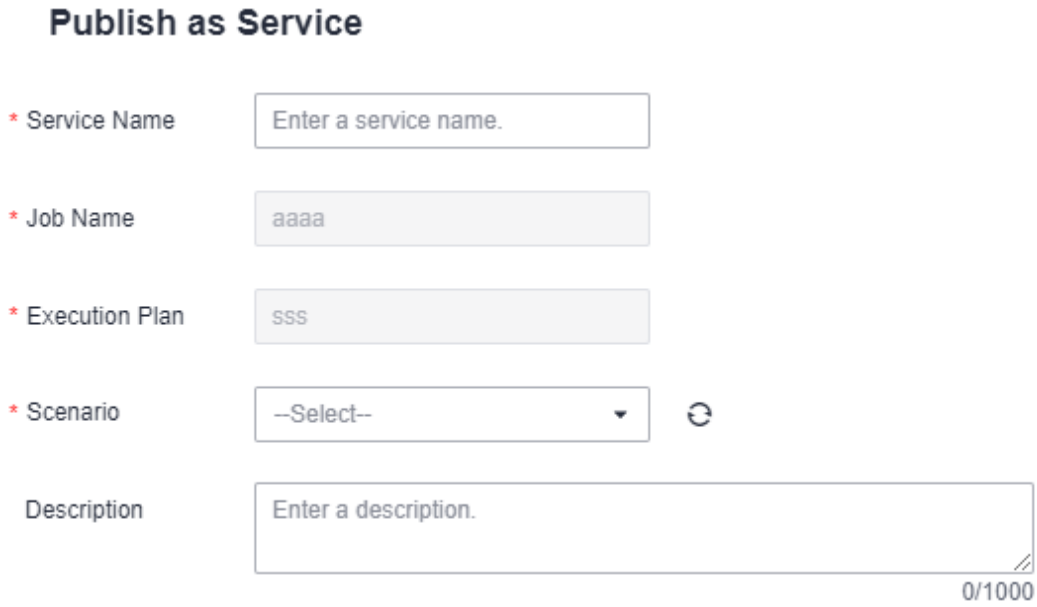


Table 13-35 Parameters for publishing a plan as a service

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.

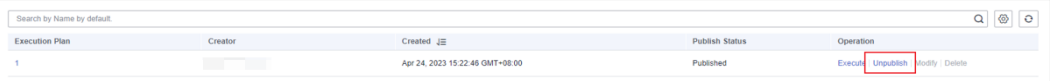
----End

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 13-32 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 13-36**.

Table 13-36 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.

13.9 Managing 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 13-37**.

Figure 13-33 Creating a script

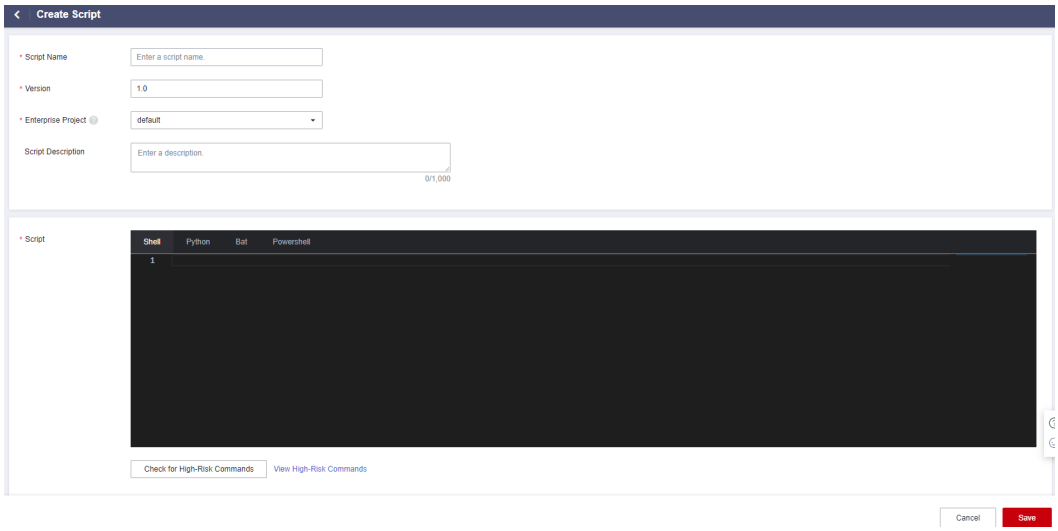


Table 13-37 Script information description

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 13-48**.
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**.

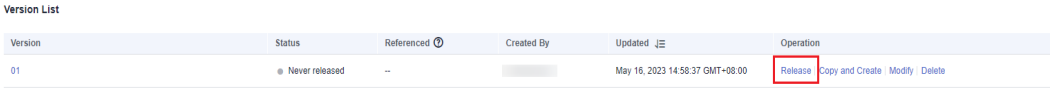
----End

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 13-34 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 13-35 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 13-38**.

Figure 13-36 Adding instances

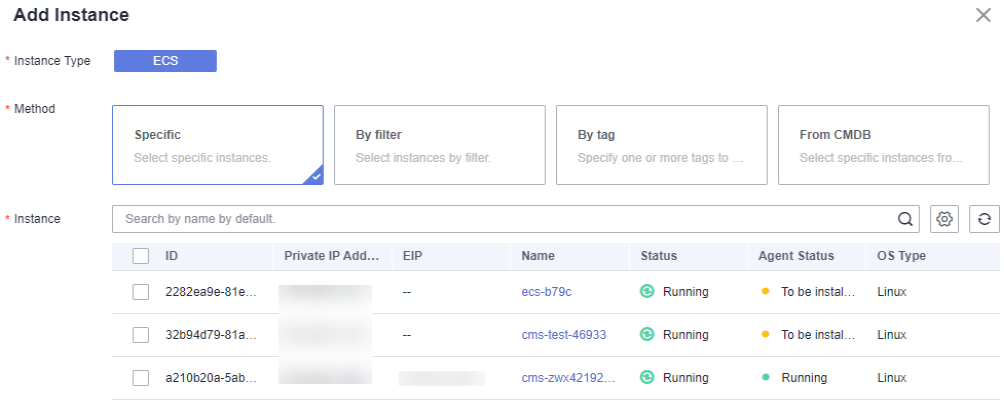


Table 13-38 Selection method description

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 13-39**.

Table 13-39 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.

13.10 Managing Files

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 **13.6 Managing 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 13-40**.

Figure 13-37 Creating a package

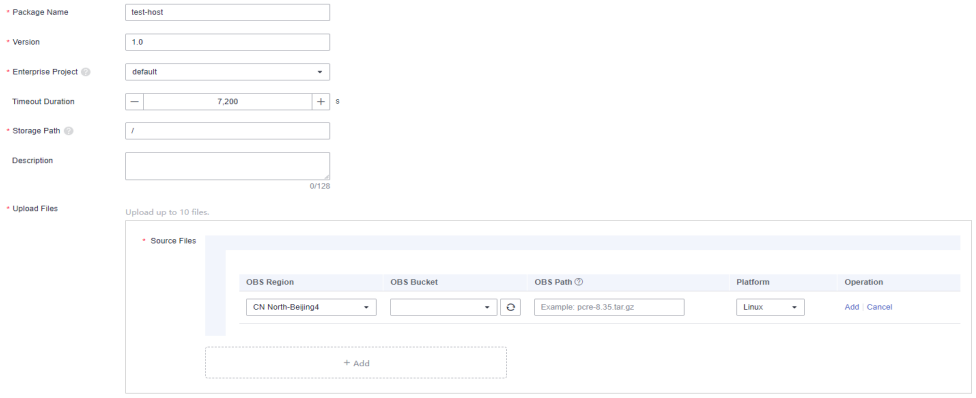


Table 13-40 Parameters for creating a package

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 13-48**.
	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 13-48**.
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 13-41**.

Figure 13-38 Adding instances

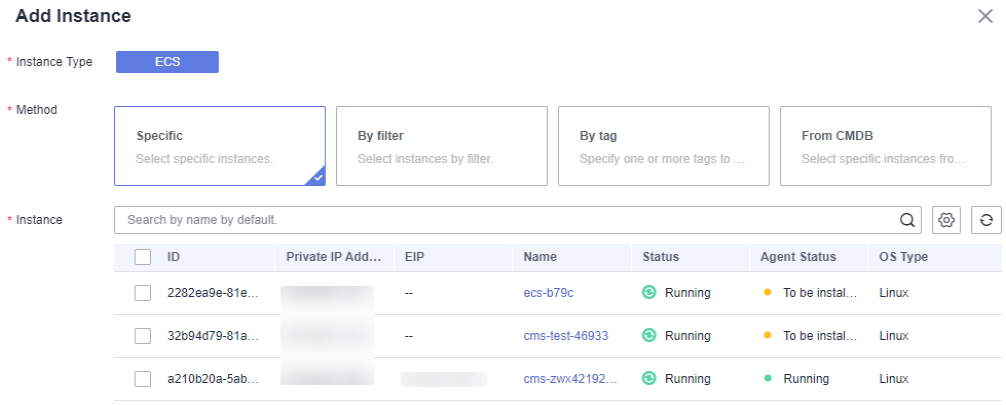


Table 13-41 Selection method description

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 13-42**.

Table 13-42 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.

13.11 O&M Configuration

13.11.1 Managing 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 13-43**.

Figure 13-39 Creating an account

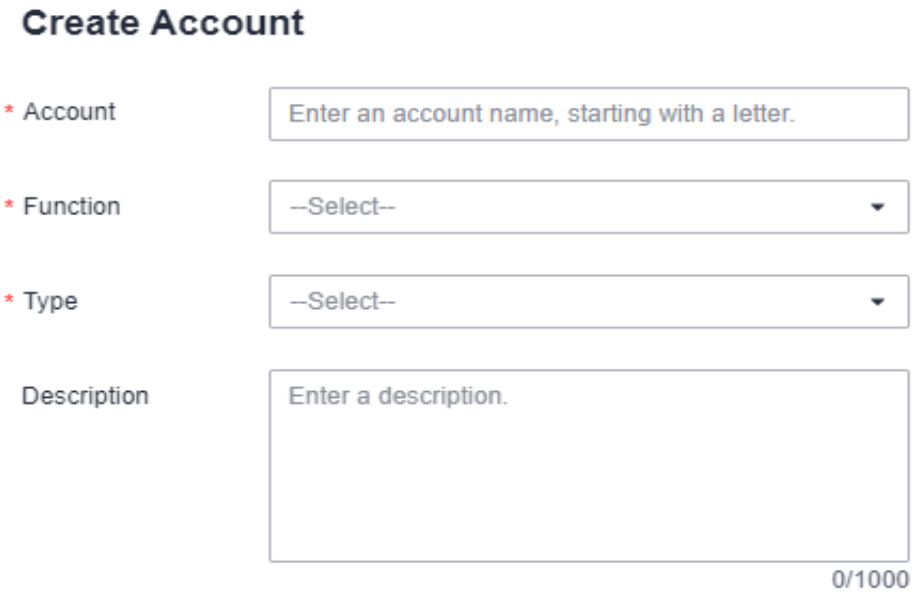


Table 13-43 Parameters for creating an account

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 13-44**.

Table 13-44 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.

13.11.2 Managing Access Credentials

For Automation, to obtain packages from OBS, obtain an access credential first. Each user can create only one credential.

Creating a Credential

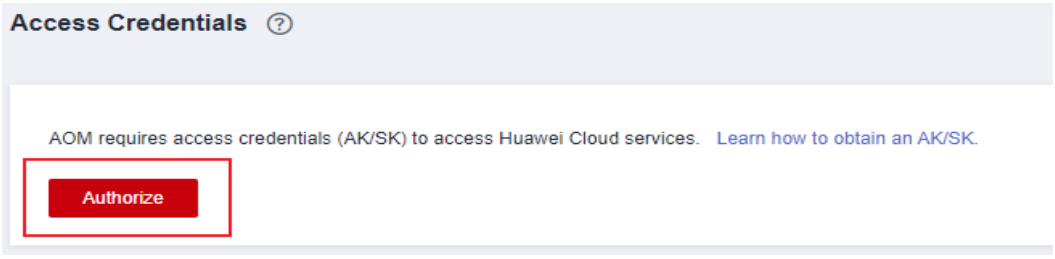
Step 1 Log in to the AOM 2.0 console.

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 13-40 Access credential



Step 5 On the **Create Credential** page that is displayed, set the parameters listed in the following table.

Table 13-45 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 13-46**.

Table 13-46 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**.

13.11.3 Checking Scenarios

Automation can be used in the following scenarios:

- Troubleshooting
- Routine Inspection
- Software Deployment
- Cloud Services
- Common

13.12 Managing the Tool Market

The tool market classifies tool cards based on **13.11.3 Checking Scenarios**. Currently, the following tool cards are supported:

- Common: **13.9 Managing Scripts** and **13.10 Managing Files**
- Cloud services: **13.4.2 Starting an ECS**, **13.4.3 Stopping an ECS**, **13.4.4 Restarting an RDS DB Instance**, **13.4.5 Changing an ECS Non-Administrator Password**, and **13.4.6 Restarting a CCE Workload**
- Software deployment: None
- Routine inspection: None
- Troubleshooting: **13.4.7 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 13-47**.

NOTE

If you do not need to remove, publish, or set a card, prohibit card modifications by referring to **13.3.2 Custom Policies for Automation**.

Table 13-47 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.

13.13 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 13-48**.

Table 13-48 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.

14 Global Settings

14.1 Authorizing AOM to Access Other Cloud Services

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**.

Authorizing AOM to Access Other Cloud Services

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 already have the permissions to access the preceding cloud services.
- To cancel authorization, click **Cancel Authorization**.

----End

14.2 Managing Access Codes

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.

Constraints

- You can create up to two access codes.
- Deleted access codes cannot be recovered.

Creating an Access Code

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 On the displayed page, choose **Authentication** in the navigation pane. Click **Add Access Code**.

Step 4 In the dialog box that is displayed, click **OK**. The system then automatically generates an access code.

----End

Other Operations

After an access code is created, you can perform the operations listed in **Table 14-1**.

Table 14-1 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 to delete an access code. **Deleting an access code may affect API calling. Exercise cautions.**
Refreshing an access code	Click to obtain the latest information of the access code.

14.3 Configuring AOM Global Configuration

AOM supports the following global configuration:

- **Metric Collection**: whether to collect metrics (excluding SLA and custom metrics).
- **TMS Tag Display**: whether to display cloud resource tags in alarm notifications.

Constraints

- The global configuration takes effect for the entire AOM 2.0.
- The **TMS tag: $event.annotations.tms_tags** variable configured in the **alarm message template** takes effect only after **TMS Tag Display** is enabled.
- After metric collection is disabled, ICAgents will stop collecting **VM metrics** and related metric data will not be updated. However, custom metrics can still be reported.

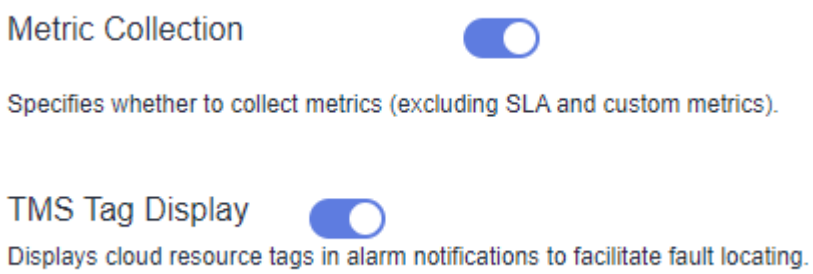
Configuring Metric Collection

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 **Global Configuration**. Then enable or disable **Metric Collection** as required.

Figure 14-1 Global configuration



----End

Configuring TMS Tag Display

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 **Global Configuration**. Then enable or disable **TMS Tag Display** as required.

----End

14.4 Configuring AOM Menus

You can choose to show or hide **Overview**, **Application Insights**, **Automation**, **Cloud Service Monitoring**, and **Business Monitoring** in the navigation pane of the console.

Procedure

Step 1 Log in to the **AOM 2.0** console.

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

Step 3 In the navigation pane, choose **Menu Settings**. All functions are disabled by default. Enable them as required.

For example, if the **Overview** option is enabled, it will be displayed in the navigation tree on the left of the console.

----End

14.5 Subscribing to AOM Metrics or Alarms

AOM allows you to subscribe to metrics or alarms. After subscription, data can be forwarded to DMS or webhook topics for retrieval.

Constraints

- A maximum of 10 data subscription rules can be created.
- Webhook subscription is not yet generally available. If you need 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 **Distributed Message Service (DMS)**:
  a. Set parameters by referring to **Table 14-2** and click **OK**.

Table 14-2 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**.

Parameter	Description
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. For details about how to create the **apm_admin_trust** agency, see **Creating the apm_admin_trust Agency**.

c. Enter the DMS username and password. Only when the access mode of the DMS instance is set to ciphertext access will you need to 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 14-3** and click **OK**.

Table 14-3 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**.
Self-built Prometheus Instance's Remote Write 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 common Prometheus instances under your account are displayed in the drop-down list.
Authentication Mode	Authentication mode for accessing a self-built Prometheus instance. – **Basic**: Enter the username and password of the Prometheus instance. – **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 (JSON)

```
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": "312313123112222222222232131312131",
      "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": "31231312311222222222222322131312131"
}
```


Parameter description:

Table 14-4 Alarm parameters

Parameter	Type	Description
events	Array of objects. For details, see **Table 14-5**.	Event or alarm details.
project_id	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 14-5 Event model

Parameter	Type	Description
id	String	Event or alarm ID, which is automatically generated by the system.
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.

Parameter	Type	Description
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.

Creating the apm_admin_trust Agency

Step 1 Log in to the IAM console.

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

Step 3 On the page that is displayed, click **Create Agency** in the upper right corner. The **Create Agency** page is displayed.

Step 4 Set parameters by referring to **Table 14-6**.

Table 14-6 Parameters for creating an agency

Parameter	Description	Example
Agency Name	Set an agency name. The agency name must be **apm_admin_trust**.	-
Agency Type	Select **Cloud service**.	Cloud service
Cloud Service	Select **Application Operations Management (AOM)**.	-
Validity Period	Select **Unlimited**.	Unlimited
Description	(Optional) Provide details about the agency.	-

Step 5 Click **Next**. The **Authorize Agency** page is displayed.

Step 6 On the **Select Policy/Role** tab page, select **DMS UserAccess** and click **Next**.

DMS UserAccess: Common user permissions for DMS, excluding permissions for creating, modifying, deleting, scaling up instances and dumping.

Step 7 On the **Select Scope** tab page, set **Scope** to **Region-specific Projects** and select target projects under **Project [Region]**.

Step 8 Click **OK**.

----End

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.

14.6 Log Settings

AOM is a unified platform for observability analysis. It does not provide log functions by itself. Instead, it integrates the log functions of **Log Tank Service (LTS)**. You can perform operations on the AOM 2.0 or LTS console.

Constraints

- To use log functions on the AOM 2.0 console, **purchase LTS resources** first.
- To use LTS functions on the AOM console, you need to obtain LTS permissions in advance. For details, see **Permissions**.

Table 14-7 Function description

Function	Description	AOM 2.0 Console	LTS Console	References
Quota configuration	When the monthly free quota (500 MB) is used up, you will be billed for any excess usage on a pay-per-use basis. To avoid extra expenses, you can stop log collection when the quota runs out.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane, choose **Settings**. The **Global Configuration** page is displayed. 3. In the navigation pane on the left, choose **Log Settings**. Click the **Quota Configuration** tab.	1. Log in to the LTS console. 2. In the navigation pane, choose **Configuration Center**.	**Quota Configuration**
Delimiters	You can configure delimiters to split log content into words, so you can search for logs by these words.	1. Log in to the **AOM 2.0** console. 2. In the navigation pane, choose **Settings**. 3. On the displayed page, choose **Log Settings** in the navigation pane. Click the **Delimiters** tab.	1. Log in to the LTS console. 2. In the navigation pane, choose **Configuration Center**. 3. Click the **Delimiters** tab.	**Delimiter Configuration**

Function	Description	AOM 2.0 Console	LTS Console	References
ICAgent collection	Configure ICAgent collection as required to reduce memory, database, and disk space usage.	1. Log in to the AOM 2.0 console. 2. In the navigation pane, choose **Settings**. 3. On the displayed page, choose **Log Settings** in the navigation pane. Click the **ICAgent Collection** tab.	1. Log in to the LTS console. 2. In the navigation pane, choose **Configuration Center**. 3. Click the **ICAgent Collection** tab.	**Log Collection**

15 Querying AOM Traces

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.

Enabling CTS

To enable CTS, see **Enabling CTS**.

After CTS is enabled, if you want to view AOM traces, see **Querying Real-Time Traces**.

AOM Operations That Can Be Recorded by CTS

pe traces actually record AOM operations, but these operations are performed through CCE or ServiceStage.

Table 15-1 Operations logged by CTS

Function	Operation	Resource Type	Trace
Global Configuration	Adding an access code	icmgr	icmgrAddAccessCode
	Deleting an access code	icmgr	icmgrDelAccessCode

Function	Operation	Resource Type	Trace
CMDB	Creating an application	application	createApp
	Updating an application	application	updateApp
	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

Function	Operation	Resource Type	Trace
	Creating an environment	environment	createEnvironment
	Modifying an environment	environment	updateEnvironment
	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

Function	Operation	Resource Type	Trace
	Creating a dashboard group	dashboard_folder	addDashboardFolder
	Updating a dashboard group	dashboard_folder	updateDashboardFolder
	Deleting a dashboard group	dashboard_folder	deleteDashboardFolder
	Creating or updating an alarm rule	audit_v4_alarm_rule	addOrUpdateAlarm
	Deleting an alarm rule	audit_v4_alarm_rule	delAlarmRule
	Creating a process discovery rule	appDiscoveryRule	addAppDiscoveryRule
	Updating a process discovery rule	appDiscoveryRule	updateAppDiscoveryRule
	Deleting a process discovery rule	appDiscoveryRule	delAppDiscoveryRule
	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

Function	Operation	Resource Type	Trace
	Modifying a suppression rule	inhibitRule	updateInhibitRule
	Deleting a suppression rule	inhibitRule	delInhibitRule
	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

Function	Operation	Resource Type	Trace
	Release a job execution plan	template	publishTemplate
	Deleting a job execution plan	template	deleteTemplate
	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

Function	Operation	Resource Type	Trace
	Adding a service to favorites	serviceScenario	serviceScenarioFavorites
	Updating a script	script	updateScript
	Executing a script	ecs	runScript

16 Migrating Data from AOM 1.0 to AOM 2.0

16.1 Accessing AOM 2.0

AOM resources are region-specific and cannot be used across regions. Select a region (such as CN-Hong Kong and AP-Bangkok) before accessing AOM. You can subscribe to AOM using method 1 or 2.

Constraints

- Before subscribing to AOM, register a HUAWEI ID.
- AOM 2.0 is available in ME-Riyadh, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN East-Qingdao, CN East2, 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.
- To return to the AOM 1.0 console, choose **Back to 1.0** in the navigation pane of the AOM 2.0 console. To go to the AOM 2.0 console, choose **AOM 2.0** in the navigation pane of the AOM 1.0 console.

Method 1

Step 1 Go to the **AOM official website**.

Step 2 Click **AOM 2.0 Console** under the AOM introduction.

Figure 16-1 Going to the AOM official website

Step 3 On the notice dialog box that is displayed, read the billing changes for switching AOM 1.0 to AOM 2.0.

Step 4 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 5 Click **Subscribe and Authorize for Free** for AOM 2.0.

Step 6 In the navigation tree on the left, click a function, for example, **Dashboard**.

----End

Method 2

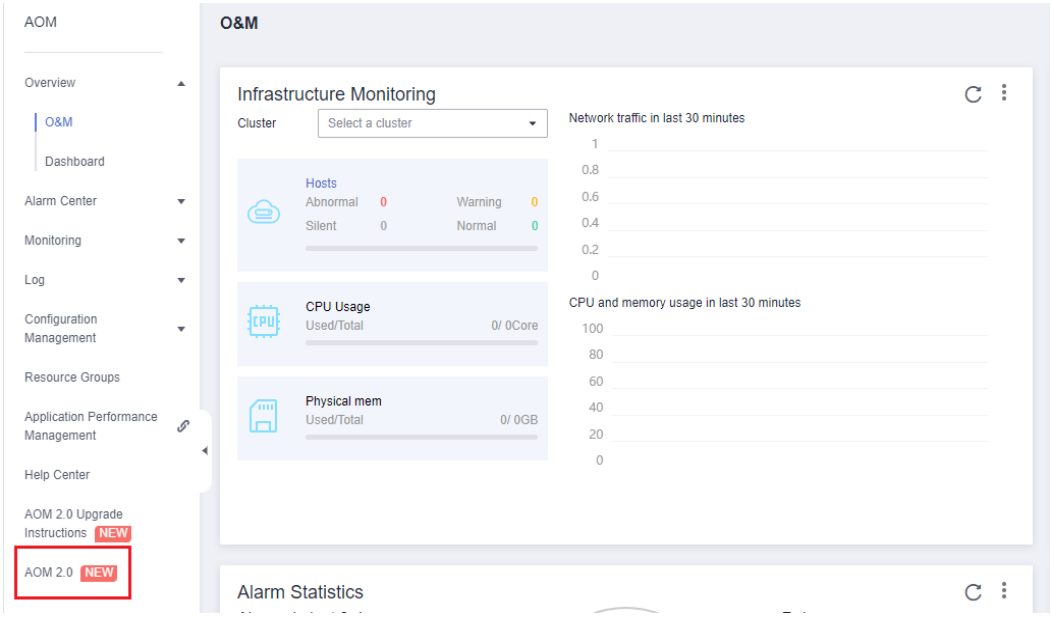
Step 1 Log in to the Huawei Cloud management console.

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

Step 3 Click on the left and choose **Management & Governance** > **Application Operations Management**. The AOM 2.0 console is displayed.

If AOM 1.0 is displayed, choose **AOM 2.0** in the navigation pane to switch to AOM 2.0.

Figure 16-2 Going to the AOM 2.0 console



Step 4 On the notice dialog box that is displayed, read the billing changes for switching AOM 1.0 to AOM 2.0.

Step 5 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 6 Click **Subscribe and Authorize for Free** for AOM 2.0.

Step 7 In the navigation tree on the left, click a function, for example, **Dashboard**.

----End

16.2 Manually Migrating Data from AOM 1.0 to AOM 2.0

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.

Constraints

Migrating alarm rules to AOM 2.0 cannot be undone.

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 **Configuring 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.

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.

Step 4 In the displayed dialog box, click **Confirm**. The selected alarm rules will be migrated to AOM 2.0 in batches.

If the alarm rules to be migrated depend on alarm templates, these alarm templates will also be migrated.

----End

16.3 Migrating Data from AOM 1.0 to AOM 2.0 in One Click

Quickly migrate dashboard and alarm rule data from AOM 1.0 to AOM 2.0.

Precautions

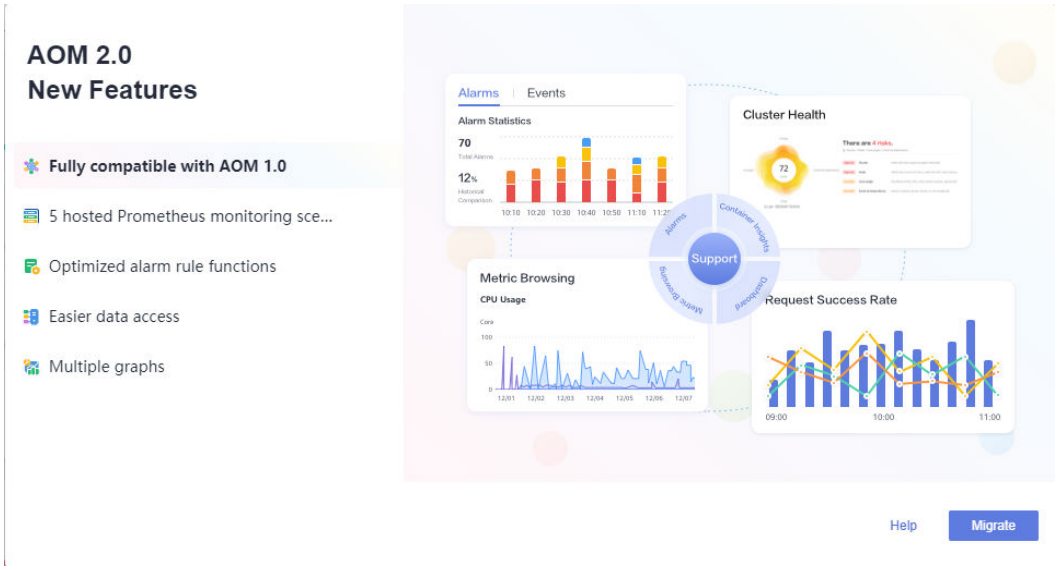
- AOM allows you to migrate all alarm rules in one click and query migration results.
- The backend checks data migration status:
  - Migrated: A dialog box is displayed, indicating that the migration is complete.
  - Not migrated: The one-click migration dialog box is displayed.
  - Migrating: A dialog 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.

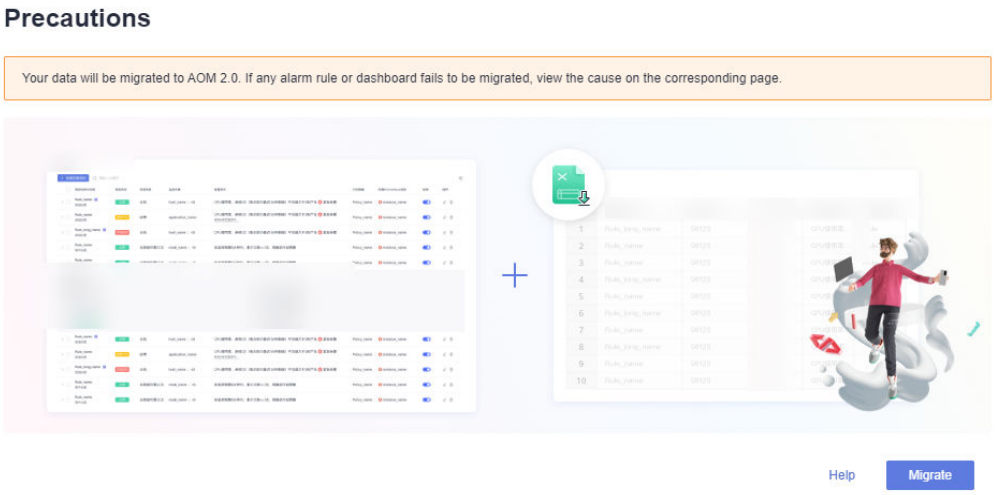
Step 2 In the **AOM 2.0 New Features** dialog box, click **Migrate**.

Figure 16-3 New features dialog box



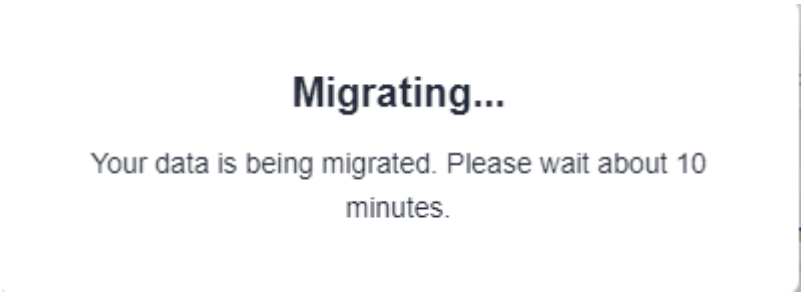
Step 3 In the **Precautions** dialog box, click **Migrate**.

Figure 16-4 Precautions dialog box



Step 4 The migration starts. A dialog box is displayed, showing "Migrating".

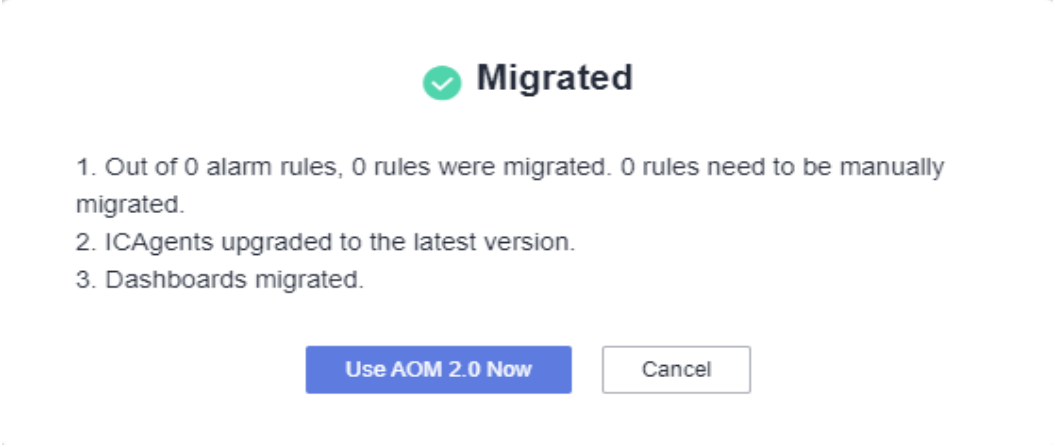
Figure 16-5 Migration in progress



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.

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.

Figure 16-6 Migration completed



----End

