AOM

User Guide

Issue 01

Date 2022-04-25

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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.

Contents

1 Overview

Application Operations Management (AOM) is a one-stop, multi-dimensional O&M management platform for cloud applications. It monitors applications and related cloud resources in real time, collects and associates resource metrics, logs, and events to analyze application health status, and supports alarm reporting and data visualization, helping you detect faults in a timely manner and monitor the running status of applications, resources, and services in real time.

Specifically, AOM monitors and uniformly manages servers, storage devices, networks, web containers, and applications hosted in Docker and Kubernetes, effectively preventing problems, facilitating fault locating, and reducing O&M costs. Unlike traditional monitoring systems, AOM monitors services by applications. 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.

Console Description

Table 1-1 AOM console description

Item	Description
Overview	Both the O&M overview and dashboard are provided. • O&M The **O&M** page supports full-link, multi-layer, and one-stop O&M for resources, applications, and user experience. • Dashboard With a dashboard, different graphs such as line graphs and digit graphs are displayed on the same screen, which lets you view comprehensive monitoring data.

Item	Description
Alarm center	The alarm center displays the alarm list, event list, alarm rules, and notification rules. ● Alarm list Alarms are the information which is reported when AOM or an external service is abnormal or may cause exceptions. You need to take measures accordingly. Otherwise, service exceptions may occur. The alarm list displays the alarms generated within a specified time range. ● Event list Events generally carry some important information, informing you of the changes of AOM or an external service. Such changes do not necessarily cause exceptions. The event list displays the events generated within a specified time range. ● Alarm rules By setting alarms rules, you can define event conditions for services or threshold conditions for resource metrics. If the resource data of a service meets the event condition, an event alarm will be generated. If the metric data of a resource meets the threshold condition, a threshold alarm will be generated. If no metric data is reported, an insufficient data event will be generated. In this way, you can discover and handle exceptions at the earliest time. ● Alarm notification AOM supports alarm notification. You can create notification rules and alarm action policies, and configure alarm noise reduction. When alarms are reported due to an exception in AOM or an external service, alarm information is sent to specified personnel by email or Short Message Service (SMS) message, so that they can rectify faults in time to avoid service loss.

Item	Description
Monitoring	Functions such as application monitoring, component monitoring, host monitoring, container monitoring, and metric monitoring are provided. • Application monitoring An application is a group of identical or similar components divided based on service requirements. AOM supports monitoring by application. • Component monitoring Components refer to the services that you deploy, including containers and common processes. The **Component Monitoring** page displays information such as type, CPU usage, memory usage, and status of each component. AOM supports drill-down from components to instances, and then to containers, enabling multi-dimensional monitoring. • Host monitoring The **Host Monitoring** page enables you to monitor common system devices such as disks and file systems, and resource usage and health status of hosts and service processes or instances running on them. • Container monitoring For container monitoring, only workloads deployed using Cloud Container Engine (CCE) and applications created using ServiceStage are monitored. • Metric monitoring The **Metric Monitoring** page displays metric data of each resource. You can monitor metric values and trends in real time, add desired metrics to dashboards, create threshold rules, and export monitoring reports. In this way, you can monitor services and analyze data in real time. • Cloud service monitoring

Item	Description
	The **Cloud Service Monitoring** page displays historical performance curves of each cloud service instance. You can view cloud service data of the last six months.

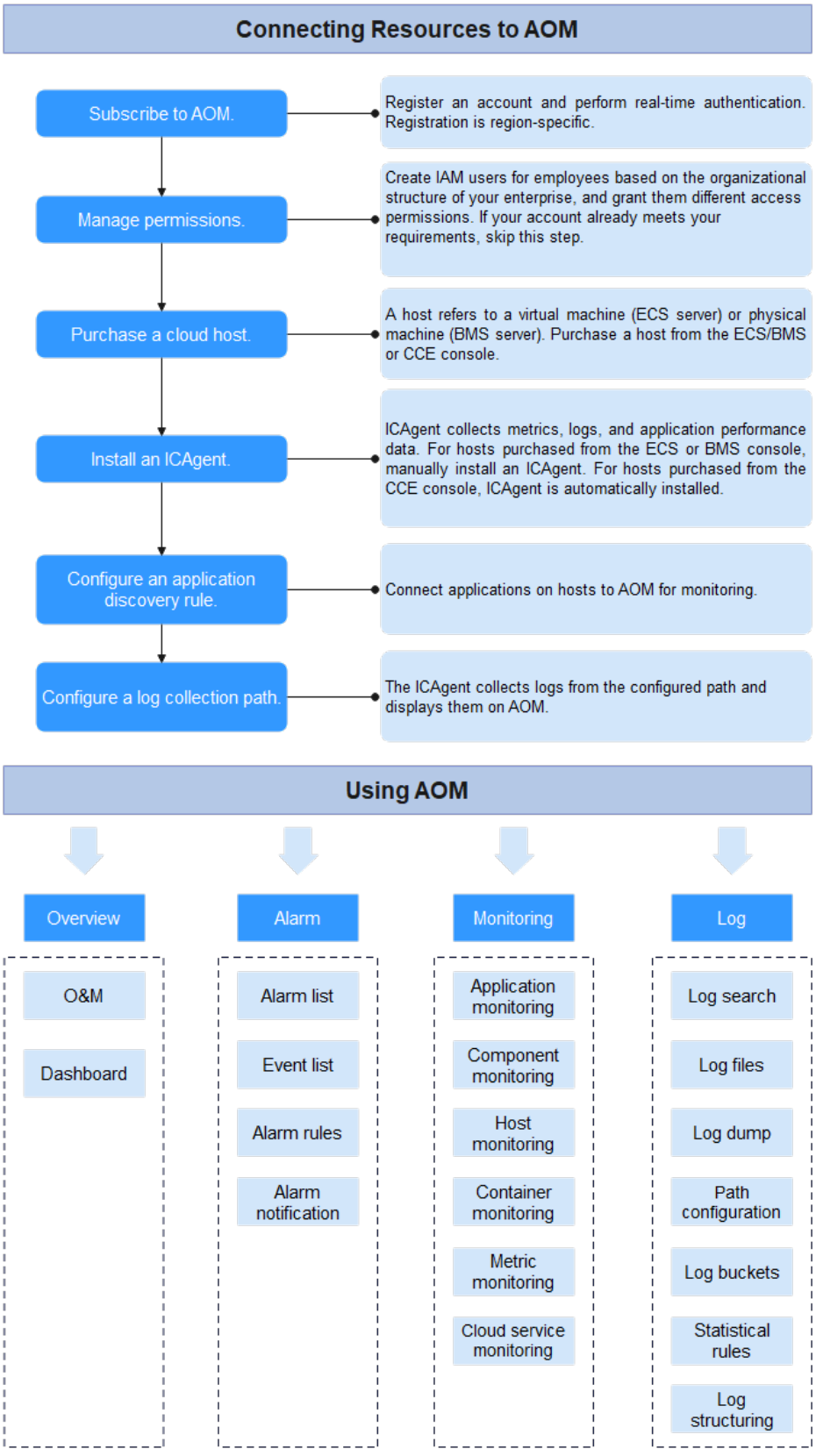
Item	Description
Log	Functions such as log search, log file, log dump, and path configuration are provided. ● Log search AOM enables you to quickly query logs, and locate faults based on log sources and contexts. ● Log files You can quickly view log files of component instances to locate faults. ● Log dumps AOM enables you to dump logs to Object Storage Service (OBS) buckets for long-term storage. ● Path configuration AOM can collect and display container and VM logs. VM refers to an Elastic Cloud Server (ECS) or a Bare Metal Server (BMS) running Linux. Before collecting logs, ensure that you have configured a log collection path. ● Log buckets A log bucket is a logical group of log files. You can dump log files, create statistical rules, and view logs by log bucket. ● Statistical rules A statistical rule takes effect by log bucket. You can configure keywords in statistical rules. Then, AOM periodically counts the number of such keywords in log buckets and generates log metrics. ● Log structuring In log structuring, original logs can be separated by regular expressions or special characters so that structured logs can be queried and analyzed based on the SQL syntax. ● Accessing LTS By adding access rules, you can map logs of CCE, Cloud Container Instance (CCI), or custom clusters in AOM to Log Tank Service (LTS). Then you can view and analyze logs on LTS. Mapping does not generate

Item	Description
	extra fees, but duplicate mapping will.
Configuration management	Functions such as ICAgent management, application discovery, and log configuration are provided. • ICAgent management ICAgent collects metrics, logs, and application performance data in real time. For hosts purchased from the Elastic Cloud Server (ECS) or Bare Metal Server (BMS) console, you need to manually install the ICAgent. For hosts purchased from the CCE console, the ICAgent is automatically installed. • Application discovery AOM can discover applications and collect their metrics based on configured rules. • Log configuration Log quotas and delimiters can be configured. • Quota configuration Earlier metrics will be deleted when the metric quota is exceeded. You can change the metric quota by switching between the basic edition and pay-per-use edition. In the basic edition, limited functions are provided for free. • Metric configuration You can enable the metric collection function to collect metrics (excluding SLA and custom metrics).

Process for Using AOM

The following figure shows the process of using AOM.

Figure 1-1 Process of using AOM



1. (Mandatory) **Subscribe to AOM**.
2. (Optional) Create a sub-account and set permissions.
3. (Mandatory) Purchase a cloud host.
4. (Mandatory) **Install the ICAgent**.

   ICAgent is a collector used to collect metric, log, and application performance data in real time.

   If a cloud host is purchased through CCE, ICAgent is automatically installed on it.
5. (Optional) **Configure an application discovery rule**.

   For the applications that meet **built-in application discovery rules**, they will be automatically discovered after the ICAgent is installed. For the applications that cannot be discovered using built-in application discovery rules, customize an application discovery rule.
6. (Optional) **Configure a log collection path**.

   To use AOM to monitor host logs, configure a log collection path first.
7. (Optional) Implement O&M.

   Use AOM functions such as **Overview**, **Alarm Management**, **Resource Monitoring**, and **Log Management** to perform routine O&M.

2 Subscribing to AOM

Before subscribing to AOM, register **a HUAWEI CLOUD account** and complete **real-name authentication**.

Subscribing to AOM

AOM resources are region-specific and cannot be used across regions. Select a region (such as CN North-Beijing 1 and CN South-Guangzhou) before subscribing to AOM.

The procedure is as follows:

1. Log in to the HUAWEI CLOUD management console.
2. Click in the upper left corner and select your desired region from the drop-down list.
3. Click on the left and choose **Management & Governance** > **Application Operations Management**.
4. In the dialog box that is displayed, click **Subscribe for Free**.

Switching Edition

AOM provides both basic and pay-per-use editions. The basic edition is used by default. You can click **Switch Edition** as required.

Step 1 Log in to the AOM console, choose **Overview** > **O&M** in the navigation pane, and click **Switch Edition** in the upper right corner of the page.

Step 2 Select an edition, select the check box at the bottom, and click **Switch Now**.

----End

3 Permissions Management

3.1 Creating a User and Granting Permissions

This section describes the fine-grained permissions management provided by Identity and Access Management (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, providing access to AOM resources.
- Grant only the permissions required for users to perform a 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 chapter.

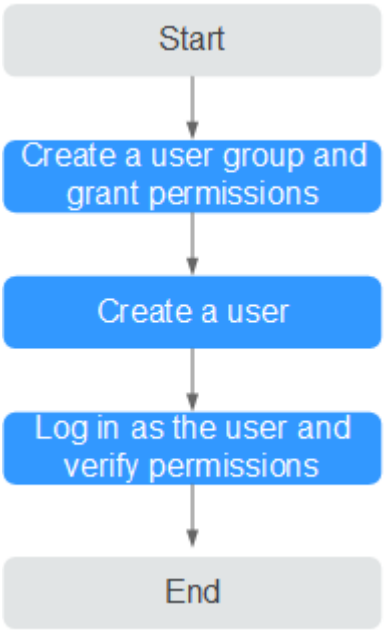
This section describes the procedure for granting permissions (see **Figure 3-1**).

Prerequisites

Before assigning permissions to user groups, you should learn about the AOM permissions listed in **Permissions Management**. For the system permissions of other services, see **System Permissions**.

Process

Figure 3-1 Process for granting AOM permissions



1. **Creating a User Group and Assigning Permissions**

   Create a user group on the IAM console, and assign the **AOM ReadOnlyAccess** policy to the group.
2. **Creating an IAM User**

   Create a user on the IAM console and add the user to the group created in **1**.
3. **Logging In Using an IAM User** and Verifying Permissions

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

3.2 Creating a Custom Policy

Custom policies can be created as a supplement to the system policies of AOM. For the actions supported for custom policies, see **Permissions Policies and Supported Actions**.

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. This section provides examples of common custom AOM policies.

Example Custom Policies

- Example 1: Allowing a user to create threshold rules

```
{
    "Version": "1.1",
```



```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aom:alarmRule:create"
      ]
    }
  ]
}
```

- Example 2: Forbidding a user to delete application discovery rules

  A deny policy 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"
            ]
        }
    ]
}
```


4 Connecting Resources to AOM

4.1 Installing the ICAgent (HUAWEI CLOUD Host)

ICAgent is used to collect metrics, logs, and application performance data. For servers that are directly purchased on the Elastic Cloud Server (ECS) or Bare Metal Server (BMS) console, manually install the ICAgent. For hosts purchased through Cloud Container Engine (CCE), the ICAgent is automatically installed.

Prerequisites

- Before installing the ICAgent, ensure that the time and time zone of the local browser are consistent with those of the server. If multiple servers are deployed, ensure that the local browser and multiple servers use the same time zone and time. Otherwise, metric data of applications and servers displayed on the UI may be incorrect.
- The ICAgent process needs to be installed and run by the **root** user.

Installation Methods

There are two methods to install the ICAgent. Note that the two methods are not applicable to container nodes created using ServiceStage or CCE. For container nodes, you do not need to manually install the ICAgent. Instead, you only need to perform certain operations when creating clusters or deploying applications.

For details, see **Table 4-1**.

Table 4-1 Installation methods

Method	Scenario
Initial installation	This method is used when the following conditions are met: 1. An Elastic IP Address (EIP) has been bound to the server. 2. The ICAgent has never been installed on the server.

Method	Scenario
Inherited installation	This method is used when the following conditions are met: You have multiple servers with ICAgent installed. One server is bound to an EIP, but others are not. The ICAgent has been installed on the server bound to an EIP by using the initial installation method. You can use the inherited method to install the ICAgent on the remaining servers. See **Inherited Installation**.

Initial Installation

After you apply for a server and install the ICAgent for the first time, perform the following operations:

Step 1 Obtain an Access Key ID/Secret Access Key (AK/SK).

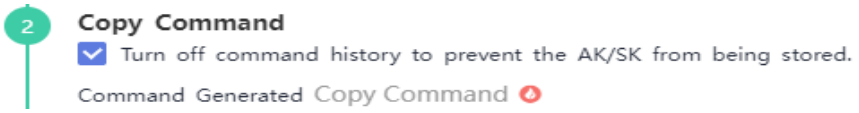
- If you have obtained the AK/SK, skip this step.
- If no AK/SK are available, obtain them first.

Step 2 In the navigation pane, choose **Configuration Management** > **Agent Management**.

Step 3 Click **Install ICAgent**.

Step 4 (Optional) To prevent your AK/SK from being disclosed, select the check box shown in the following figure to disable historical record collection.

Figure 4-1 Copying the ICAgent installation command



Step 5 Generate the ICAgent installation command, and copy and run it to install the ICAgent.

Step 6 After the ICAgent is installed, run the following command to enable historical record collection:

set -o history

NOTE

- If the message **ICAgent install success** is displayed, the ICAgent has been installed in the **/opt/oss/servicemgr/** directory. After the ICAgent has been installed, choose **Configuration Management** > **Agent Management** to view the ICAgent status.
- If the ICAgent fails to be installed, uninstall the ICAgent according to **Uninstalling the ICAgent by Logging In to the Server** and then install it again. If the problem persists, contact technical support.

----End

Follow-up Operations

For more information about how to install, upgrade, and uninstall the ICAgent, see **ICAgent Management (HUAWEI CLOUD Host)**.

4.2 ICAgent Version Description

Table 4-2 ICAgent version description

Version	Description
5.12.100	• Added support for two metrics: used memory working set and memory working set usage. • Supported container log tagging with **stderr.log** or **stdout.log** during collection. • Added the **Pod_ip** tag for container log reporting. • Supported double asterisks (**) for matching files in the current directory.
5.12.98	Supported configuration of LTS log collection blacklists and changed the source of container metrics to **working_set**.
5.12.96	Supported discovery of more types of cloud resources.
5.12.90	Updated the GPU metric source.
5.12.87	Supported more types of disks.
5.12.75	Adapted to secure containers.

4.3 Configuring Application Discovery Rules

AOM can discover applications and collect their metrics based on configured rules. There are two modes to configure application discovery: auto mode and manual mode. This section mainly describes the manual mode.

- **Auto mode**

  After you install the ICAgent on a host according to **Installing the ICAgent**, the ICAgent automatically discovers applications on the host based on **Built-in Discovery Rules** and displays them on the **Application Monitoring** page.

- **Manual mode**

  If you customize an application discovery rule and apply it to the host where the ICAgent is installed (for details, see **Installing the ICAgent**), the ICAgent

discovers applications on the host based on the custom rule and displays them on the **Application Monitoring** page.

Filtering Rules

The ICAgent will periodically implement detection on the target host to find out all its processes. The effect is similar to that of running the **ps -e -o pid,comm,lstart,cmd | grep -v defunct** command on the target host. Then, the ICAgent checks whether processes match the filtering rules in **Table 4-3**. 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 out 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 4-3 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 the container, the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose **PID** is **1154** is not discovered by AOM because its **COMMAND** value is **docker-containe**.
If the **CMD** value of a process starts with **[** and ends with **]**, the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose **PID** is **2** is not discovered by AOM because its **CMD** value is **[kthreadd]**.
If the **CMD** value of a process starts with **(** and ends with **)**, the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose **PID** is **3** is not discovered by AOM because its **CMD** value is **(ksoftirqd/0)**.
If the **CMD** value of a process starts with **/sbin/**, the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose **PID** is **1148** is not discovered by AOM because its **CMD** value starts with **/sbin/**.

Built-in Discovery Rules

AOM provides two built-in discovery rules: **Sys_Rule** and **Default_Rule**. These rules are executed on all hosts, including hosts added later. The priority of

Sys_Rule is higher than that of **Default_Rule**. That is, **Sys_Rule** is executed on the host first. If **Sys_Rule** is met, **Default_Rule** is not executed. Otherwise, **Default_Rule** is executed. Rule details are as follows:

Sys_Rule (cannot be disabled)

When **Sys_Rule** is used, the component name and application name must be used together. The names are determined according to the following priorities:

- Priorities for determining the application name:
  a. Use the value of the **Damp_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.

Custom Discovery Rules

Step 1 In the navigation pane, choose **Configuration Management** > **Application Discovery**.

Step 2 Click **Add Custom Application Discovery Rule** and configure an application discovery rule.

Step 3 Select a host for pre-detection.

1. Customize a rule name, for example, **ruletest**.
2. Select a typical host, for example, **hhhhhh-27465**, to check whether the application discovery rule is valid. The hosts that execute the rule will be configured in **Step 6**. Then, click **Next**.

Step 4 Set an application discovery rule.

1. Click **Add Check Items**. AOM can discover processes that meet the conditions of check items.

   For example, AOM can detect the processes whose command parameters contain **ovs-vswitchd unix:** and environment variables contain **SUDO_USER=paas**.

   NOTE

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

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

Step 5 Set an application name and component name.

Set an application name.

1. Set an application name.

   In the **Application Name Settings** area, click **Add Naming Rule** to set an application name for the detected process.

   NOTE

   - If you do not set an application name, the default name **unknownapplicationname** is used.
   - When you add multiple naming rules, all the naming rules are combined as the application name of the process. Metrics of the same application are aggregated.
2. Set a component name.

   In the **Component Name Settings** area, specify an application type and click **Add Naming Rule** to set a component name for the discovered process. For example, add the fixed text **app-test** as a component name.

   NOTE

   - Application types are specified to identify application categories. They are used only for better rule classification and console display. You can enter any field. For example, you can enter **Java** or **Python** to categorize applications by technology stack or enter **collector** or **database** to categorize applications 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 6 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 7 Click **Add** to complete the configuration. AOM collects metrics of the process.

Step 8 After about two minutes, choose **Monitoring** > **Component Monitoring** in the navigation pane, select the target host from the cluster drop-down list, and find out the monitored component.

----End

More Operations

After creating an application discovery rule, perform the operations listed in **Table 4-4** if needed.

Table 4-4 Related operations

Operation	Description
Viewing rule details	In the **Name** column, click the name of an application discovery rule.
Enabling or disabling a rule	• Click **Enable** in the **Operation** column. • Click **Disable** in the **Operation** column. After a rule is disabled, AOM does not collect corresponding process metrics.
Deleting a rule	• To delete a discovery rule, click **Delete** in the **Operation** column. • To delete one or more application discovery rules, select them and click **Delete** above the rule list. **NOTE** Built-in application discovery rules cannot be deleted.
Modifying a rule	Click **Modify** in the **Operation** column. **NOTE** Built-in application discovery rules cannot be modified.

4.4 Configuring Log Collection Paths

4.4.1 Configuring Container Log Collection Paths

AOM can collect and display container logs. To use this function, first configure a log collection path according to the following procedure.

Precautions

- The ICAgent only collects ***.log**, ***.trace**, and ***.out** text log files.
- AOM collects standard container output logs by default.

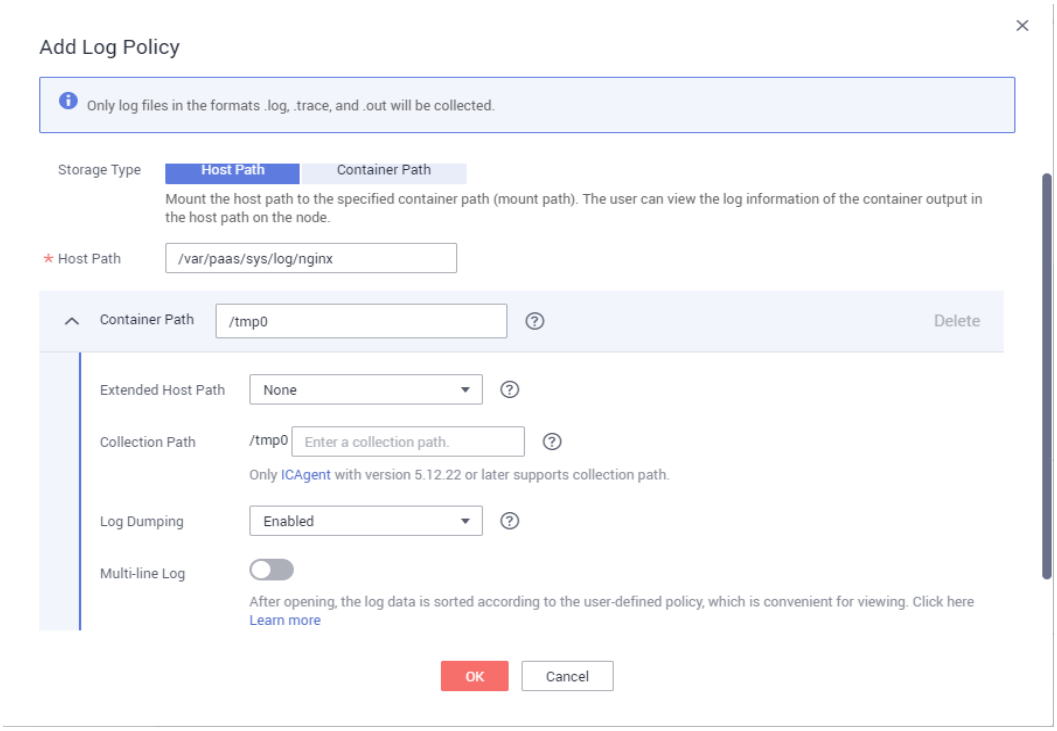
Procedure

Adding a Log Policy on CCE

Step 1 When creating a **workload** on Cloud Container Engine (CCE), click **Log Policies** after adding a container.

Step 2 Click **Add Log Policy**. On the displayed page, configure parameters as required. The following uses Nginx as an example.

Figure 4-2 Adding a log policy



Step 3 Set **Storage Type** to **Host Path** or **Container Path**.

- **Host Path**: You can mount a host path to a specified container path. Set parameters according to the following table.

Table 4-5 Parameters for adding log policies (host path)

Parameter	Description
Storage Type	Set this parameter to **Host Path**. You can mount a host path to a specified container path.
Add Container Path	
*Host Path	Host path to which a container log file is mounted. Example: **/var/paas/sys/log/nginx**
Container Path	Container path to which a logical data volume is mounted. Example: **/tmp** **NOTICE** – Do not mount a data volume to a system directory such as **/** or **/var/run**. Otherwise, the container becomes abnormal. You are advised to mount log files to an empty directory. If the directory is not empty, ensure that there are no files that affect container startup. Otherwise, files will be replaced, causing container startup failures or workload creation failures. – If the volume is mounted to a high-risk directory, you are advised to use an account with minimum permissions to start the container; otherwise, high-risk files on the host may be damaged. – AOM collects only the first 20 log files that have been modified recently. It collects files from two levels of subdirectories by default. – AOM only collects **.log**, **.trace**, and **.out** text log files in mounting paths.
Extended Host Path	Level-3 directory added to the original volume directory or subdirectory. This path enables you to obtain output files of a single pod more easily. – None: No extended paths are configured. – PodUID: Pod ID. – PodName: Pod name. – PodUID/ContainerName: Pod ID/container name. – PodName/ContainerName: Pod name/container name.

Parameter	Description
Collection Path	Path for collecting logs precisely. Details are as follows: – If no collection path is specified, log files in **.log**, **.trace**, and **.out** formats will be collected from the current path by default. – If a collection path contains double asterisks (**), log files in **.log**, **.trace**, and **.out** formats will be collected from 5 levels of subdirectories. – If a collection path contains an asterisk (*), a fuzzy match is performed. Example: If the collection path is **/tmp/**/test*.log**, all **.log** files prefixed with **test** will be collected from **/tmp** and its 5 levels of subdirectories. **CAUTION** To use the collection path function, ensure that the ICAgent version is 5.12.22 or later.
Log Dumping	Log dumping here refers to rolling local log files. – **Enabled**: AOM scans log files every minute. When a log file exceeds 50 MB, it is dumped immediately. A new **.zip** file is generated in the directory where the log file is located. For a log file, AOM stores only the latest 20 **.zip** files. When the number of **.zip** files exceeds 20, earlier **.zip** files will be deleted. After the dump is complete, the log file in AOM will be cleared. – **Disabled**: If you select **Disabled**, AOM does not dump log files. **NOTE** – AOM log file rolling is implemented in the copytruncate mode. During configuration, ensure that log files are written in the append mode. Otherwise, file holes may occur. – Currently, mainstream log components such as Log4j and Logback support log file rolling. If your log files already support rolling, skip the configuration. Otherwise, conflicts may occur. – You are advised to configure log file rolling for your own services to flexibly control the size and number of rolled files.

- **Container Path**: Logs will be stored in a container path. No host path needs to be mounted into the container. Set parameters according to the following table.

  NOTE

  Ensure that the ICAgent version is 5.10.79 or later.

Table 4-6 Parameters for adding log policies (container path)

Parameter	Description
Storage Type	Set this parameter to **Container Path**. Logs will be stored in a container path. No host path needs to be mounted into the container. Ensure that the ICAgent version is 5.10.79 or later.
Add Container Path	
Container Path	Container path to which a logical data volume is mounted. Example: **/tmp** **NOTICE** – Do not mount a data volume to a system directory such as **/** or **/var/run**. Otherwise, the container becomes abnormal. You are advised to mount the volume to an empty directory. If the directory is not empty, ensure that there are no files that affect container startup. Otherwise, files will be replaced, causing container startup failures or workload creation failures. – If the volume is mounted to a high-risk directory, you are advised to use an account with minimum permissions to start the container; otherwise, high-risk files on the host may be damaged. – AOM collects only the first 20 log files that have been modified recently. It collects files from two levels of subdirectories by default. – AOM only collects **.log**, **.trace**, and **.out** text log files in mounting paths.
Collection Path	Path for collecting logs precisely. Details are as follows: – If no collection path is specified, log files in **.log**, **.trace**, and **.out** formats will be collected from the current path by default. – If a collection path contains double asterisks (**), log files in **.log**, **.trace**, and **.out** formats will be collected from 5 levels of subdirectories. – If a collection path contains an asterisk (*), a fuzzy match is performed. Example: If the collection path is **/tmp/**/test*.log**, all **.log** files prefixed with **test** will be collected from **/tmp** and its 5 levels of subdirectories. **CAUTION** To use the collection path function, ensure that the ICAgent version is 5.12.22 or later.

Parameter	Description
Log Dumping	Log dumping here refers to rolling local log files. – **Enabled**: AOM scans log files every minute. When a log file exceeds 50 MB, it is dumped immediately. A new **.zip** file is generated in the directory where the log file is located. For a log file, AOM stores only the latest 20 **.zip** files. When the number of **.zip** files exceeds 20, earlier **.zip** files will be deleted. After the dump is complete, the log file in AOM will be cleared. – **Disabled**: If you select **Disabled**, AOM does not dump log files. **NOTE** – AOM log file rolling is implemented in the copytruncate mode. During configuration, ensure that log files are written in the append mode. Otherwise, file holes may occur. – Currently, mainstream log components such as Log4j and Logback support log file rolling. If your log files already support rolling, skip the configuration. Otherwise, conflicts may occur. – You are advised to configure log file rolling for your own services to flexibly control the size and number of rolled files.

----End

Adding a Log Policy on ServiceStage

Step 1 When **deploying a component** on ServiceStage, add an image, click **Advanced Settings**, and then click the **Container Log** tab.

Step 2 Add a log policy.

The procedure for adding log policies on ServiceStage is the same as that on CCE. For details, see **Step 3**.

----End

Adding a Log Policy on CCI

Step 1 When **creating a deployment** on Cloud Container Instance (CCI), select an image, and then click **Advanced Settings** and the **Log Collection** tab.

Step 2 Add a log policy.

Click **Add Log Storage** and configure a log policy according to **Table 4-7**.

Figure 4-3 Adding a log policy on CCI

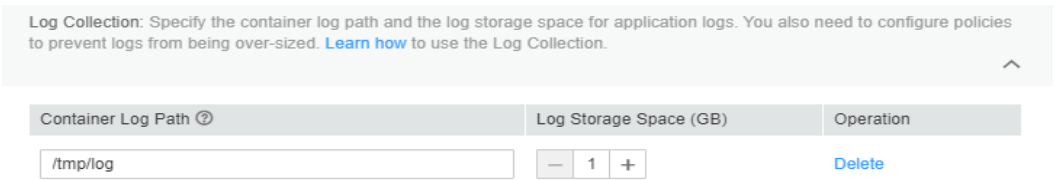


Table 4-7 Parameter description

Parameter	Description
Container Log Path	Ensure that the log output path is consistent with the container log path, so that logs can be written to the log storage volume. **NOTICE** • After the log storage volume is mounted, the existing content under the log path will be overwritten. Ensure that the log path is independent. Otherwise, the original content cannot be seen. • AOM collects only the first 20 log files that have been modified recently. It does not collect files from subdirectories. • AOM only collects **.log**, **.trace**, and **.out** text log files in log paths.
Log Storage Space	Space of log storage. AOM processes logs in the unit of 50 MB to prevent them from being oversized. AOM stores only the latest 20 **.zip** files. When the number of **.zip** files exceeds 20, earlier **.zip** files will be deleted.

----End

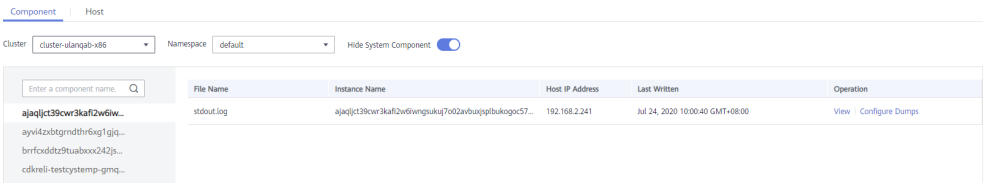
Viewing Container Logs

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 Container Log Files**

  In the navigation pane, choose **Log** > **Log Files**. On the **Component** tab, select the corresponding cluster, namespace, and component to view log files, as shown in the following figure. For details, see **Viewing Log Files**.

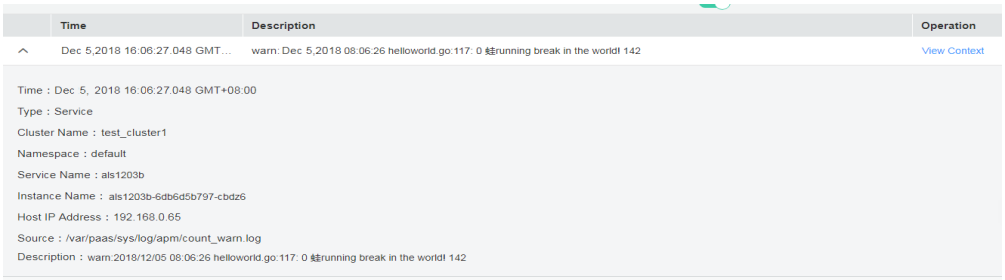
  Figure 4-4 Viewing container log files

- **Viewing and Analyzing Container Logs**

  In the navigation pane, choose **Log** > **Log Search**. On the **Component** tab, select the corresponding cluster, namespace, component, and file to view and analyze the collected logs. For details, see **Searching for Logs**.

Figure 4-5 Viewing and analyzing container logs



4.4.2 Configuring VM Log Collection Paths

AOM can collect and display VM logs. VM refers to an Elastic Cloud Server (ECS) or a Bare Metal Server (BMS) running Linux. To use this function, first configure a log collection path according to the following procedure.

Prerequisites

You have installed the ICAgent on a VM according to **Installing the ICAgent**. Wait for about 5 minutes after the installation is complete. Then you can view the VM in the VM list on the **Path Configuration** page.

Precautions

- If you specify a directory, all **.log**, **.trace**, and **.out** text log files in this directory are collected by default. If you specify a log file, only this file is collected. The specified file must be a text file. Other types of log files, such as binary log files, cannot be collected.
- 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.
- If the difference between the last modification time of a log file and the current time exceeds 12 hours, the log file will not be collected.

Configuring Log Collection Paths for a Single VM Through the Console

Step 1 Log in to the AOM console. In the navigation pane, choose **Log** > **Path Configuration**. The **Host Log** tab page is displayed.

Step 2 In the VM list, click **Configure** in the **Operation** column to configure one or more log collection paths for a VM.

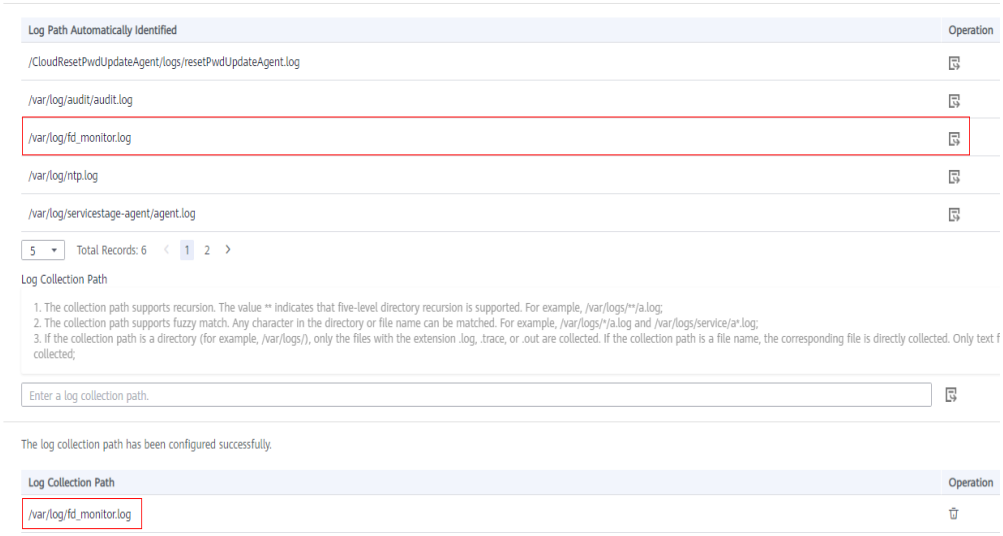
You can use the paths automatically identified by the ICAgent or manually configure paths.

- **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 log collection path list. To configure multiple paths, repeat this operation.

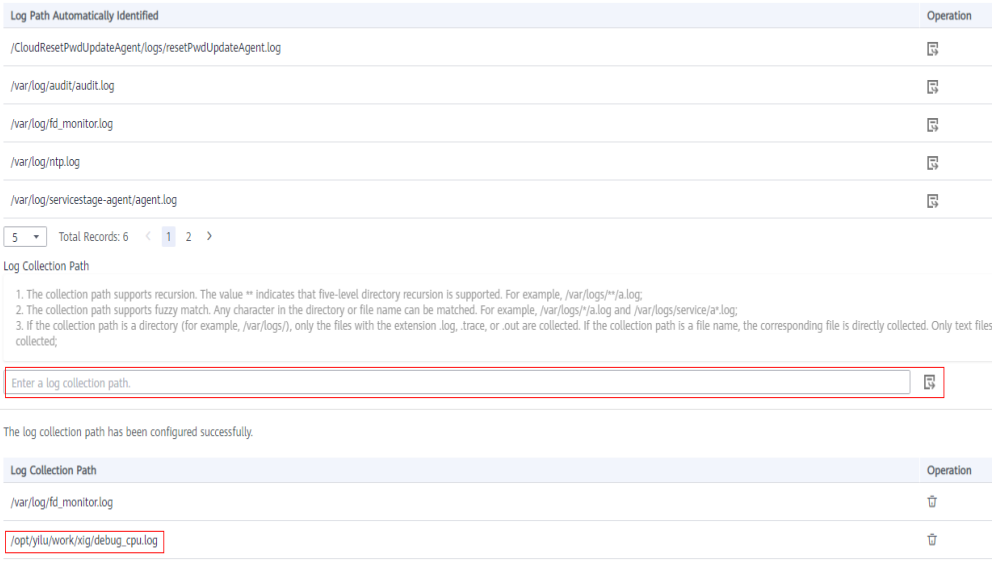
Figure 4-6 Using the paths automatically identified by the ICAgent



- **Manually Configuring Log Collection Paths**

  If the paths automatically identified by the ICAgent cannot meet your requirements, enter a log directory or file (such as **/opt/yilu/work/xig/debug_cpu.log** or **/opt/yilu/work/xig/*.log**) in the **Log Collection Path** text box, and then click  to add the path to the log collection path list. To configure multiple paths, repeat this operation.

Figure 4-7 Manually configuring log collection paths



Step 3 Click **OK**.

----End

Configuring Log Collection Paths for Multiple VMs in Batches Through the Console

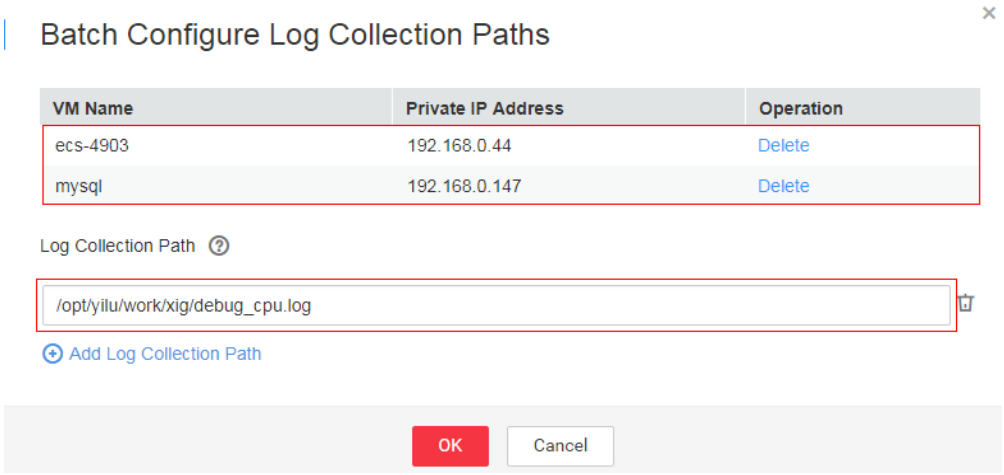
You can configure log collection paths for multiple VMs in batches. When your service is deployed on multiple VMs, you can configure log collection paths in batches to reduce workload.

Step 1 Log in to the AOM console. In the navigation pane, choose **Log** > **Path Configuration**. The **Host Log** tab page is displayed.

Step 2 Configure one or more log collection paths for multiple VMs in batches.

Select one or more VMs in the list, click **Batch Configure**, and enter a log directory or file (for example, **/opt/yilu/work/xig/debug_cpu.log**) in the **Log Collection Path** text box. To configure multiple paths, click **Add Log Collection Path**.

Figure 4-8 Configuring log collection paths in batches



NOTE

If you configure log collection paths for your VM and then configure log collection paths in batches, new paths will be added to the existing path list.

Step 3 Click **OK**.

In the VM list, click in the **Log Collection Path** column to view the configured log collection paths of the VM.

----End

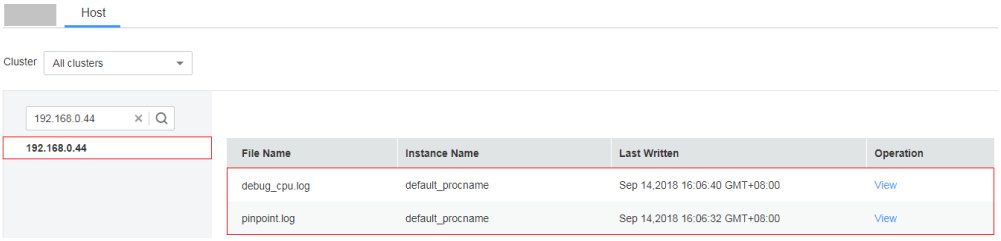
Viewing VM Logs

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** > **Log Files**. Click the **Host** tab to view the collected log files, as shown in the following figure. For details, see **Viewing Log Files**.

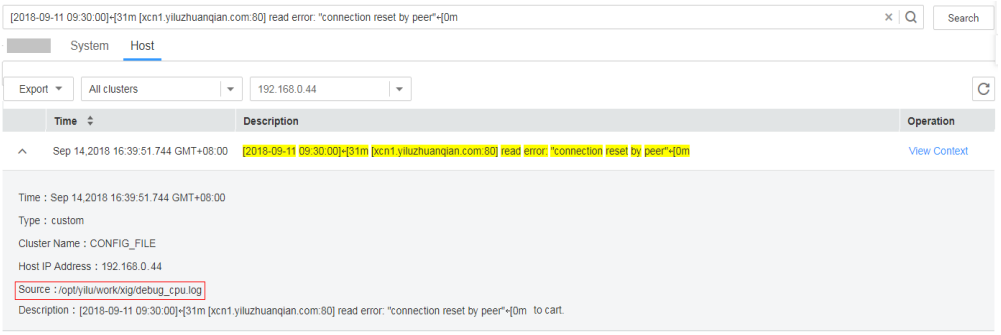
Figure 4-9 Viewing VM log files



- **Viewing and Analyzing VM logs**

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

Figure 4-10 Viewing and analyzing VM logs



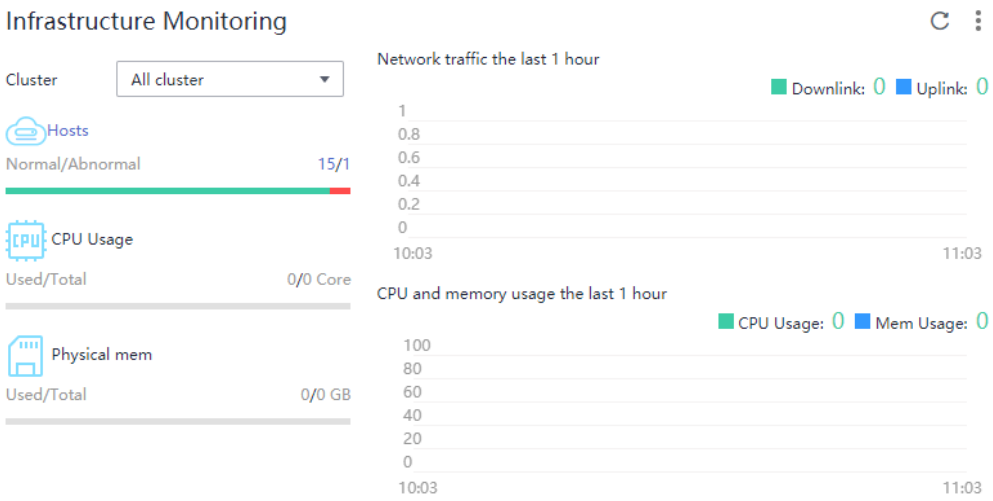
5 Overview

5.1 O&M

The **O&M** page supports full-link, multi-layer, and one-stop O&M for resources, applications, and user experience. Specifically, this page displays the following types of cards: infrastructure monitoring, application monitoring, alarm statistics, host monitoring (CPU and memory), component monitoring (CPU and memory), container instance monitoring (CPU and memory), host monitoring (disk), host monitoring (network), cluster monitoring (CPU and memory), and cluster monitoring (disk) cards.

Infrastructure Monitoring Card

Figure 5-1 Infrastructure monitoring

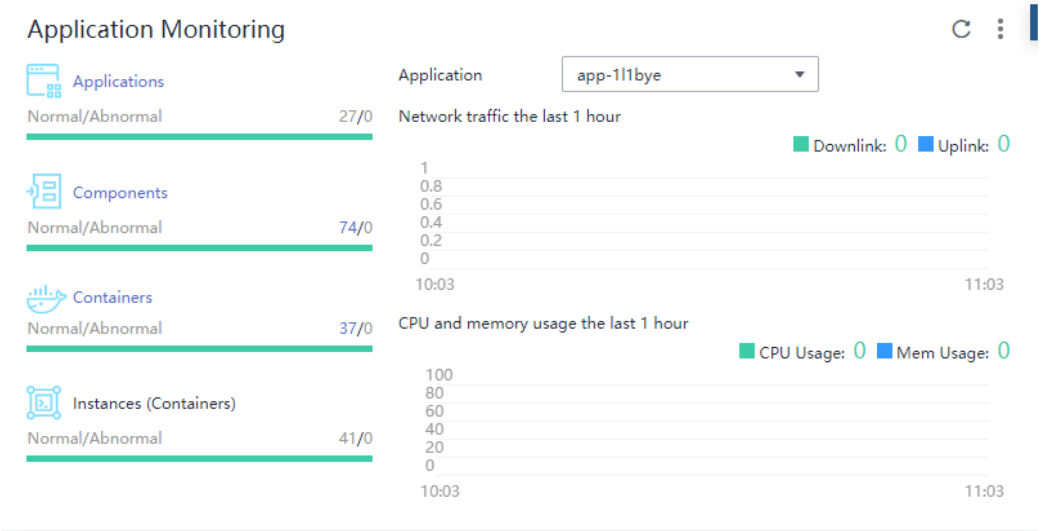


This card mainly displays infrastructure metrics. You can select one or all clusters to view information. When you select all clusters, the following information is displayed:

- Host running status, CPU usage, and physical memory usage.
- Trend graph of network traffic data in the last hour. The values of each point in the graph respectively indicate the total receive rate (BPS) and send rate (BPS) of all clusters in one minute. The values above the graph respectively indicate the total receive rate (BPS) and send rate (BPS) of all clusters at the latest time point.
- Trend graph of CPU and memory usage in the last hour. The values of each point in the graph respectively indicate the average CPU and memory usage of all clusters in one minute. The values above the graph respectively indicate the average CPU and memory usage of all clusters at the latest time point.

Application Monitoring Card

Figure 5-2 Application monitoring

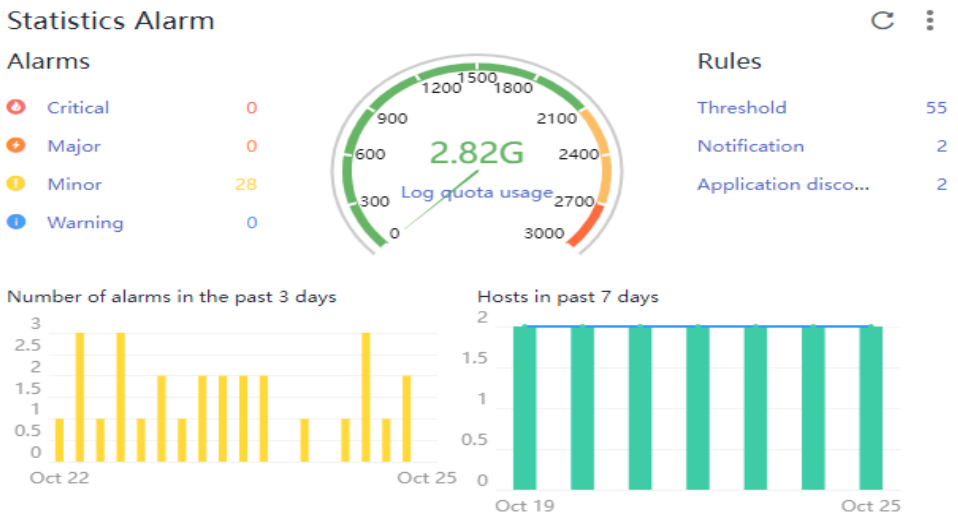


This card mainly displays application metrics:

1. Running status of applications, components, containers, and instances.
2. When you select an application, the following information is displayed:
   - Trend graph of network traffic data in the last hour. The values of each point in the graph respectively indicate the receive rate (BPS) and send rate (BPS) of the selected application in one minute. The values above the graph respectively indicate the receive rate (BPS) and send rate (BPS) of the selected application at the latest time point.
   - Trend graph of CPU and memory usage in the last hour. The values of each point in the graph respectively indicate the CPU and memory usage of the selected application in one minute. The values above the graph respectively indicate the CPU and memory usage of the selected application at the latest time point.

Alarm Statistics Card

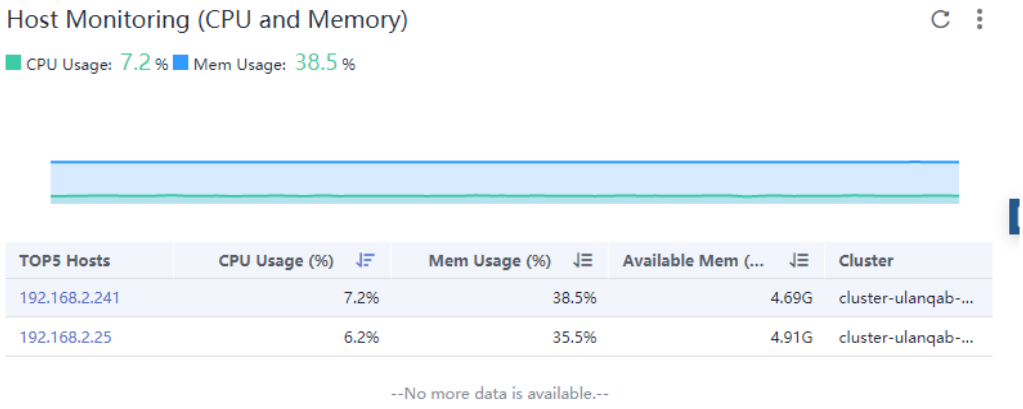
Figure 5-3 Alarm statistics



This card mainly displays alarms, log usage, threshold rules, and trends of alarms and hosts.

Host Monitoring (CPU and Memory) Card

Figure 5-4 Host monitoring (CPU and memory)

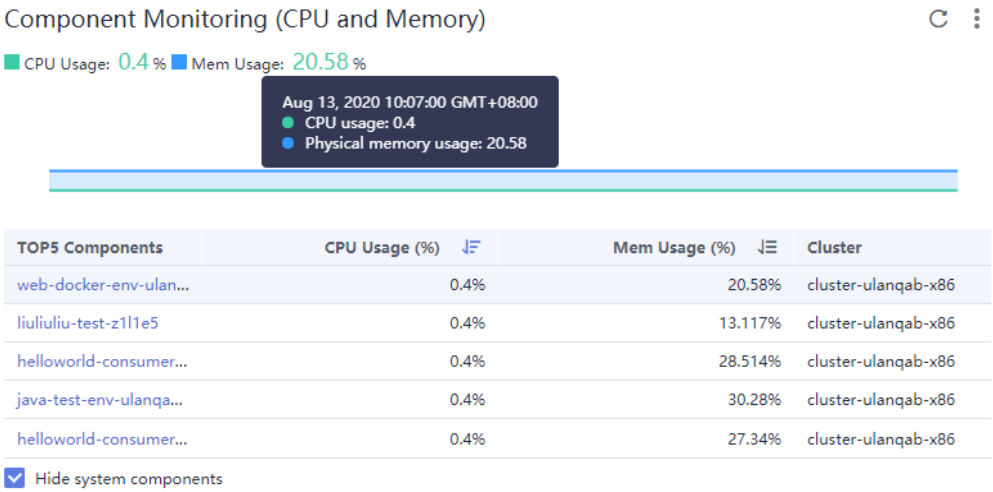


This card mainly displays:

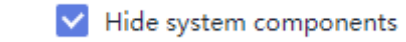
- The top 5 hosts with high CPU and memory usage in the last minute.
- Trend graph of the CPU and memory usage of the selected host in the last hour. The values of each point in the graph respectively indicate the CPU and memory usage of the host in one minute.
- CPU and memory usage of the selected host at the latest time point, which is displayed above the trend graph.

Component Monitoring (CPU and Memory) Card

Figure 5-5 Component monitoring (CPU and memory)



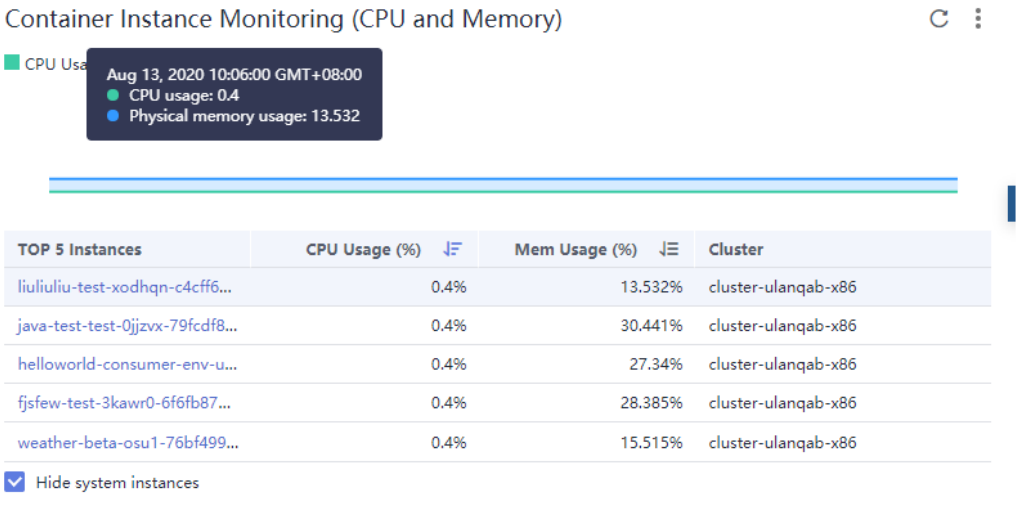
This card mainly displays:

- The top 5 components with high CPU and memory usage in the last minute.
- Trend graph of the CPU and memory usage of the selected component in the last hour. The values of each point in the graph respectively indicate the CPU and memory usage of the component in one minute.
- CPU and memory usage of the selected component at the latest time point, which is displayed above the trend graph.
- 

option, which can be selected to hide system components.

Container Instance Monitoring (CPU and Memory) Card

Figure 5-6 Container instance monitoring (CPU and memory)

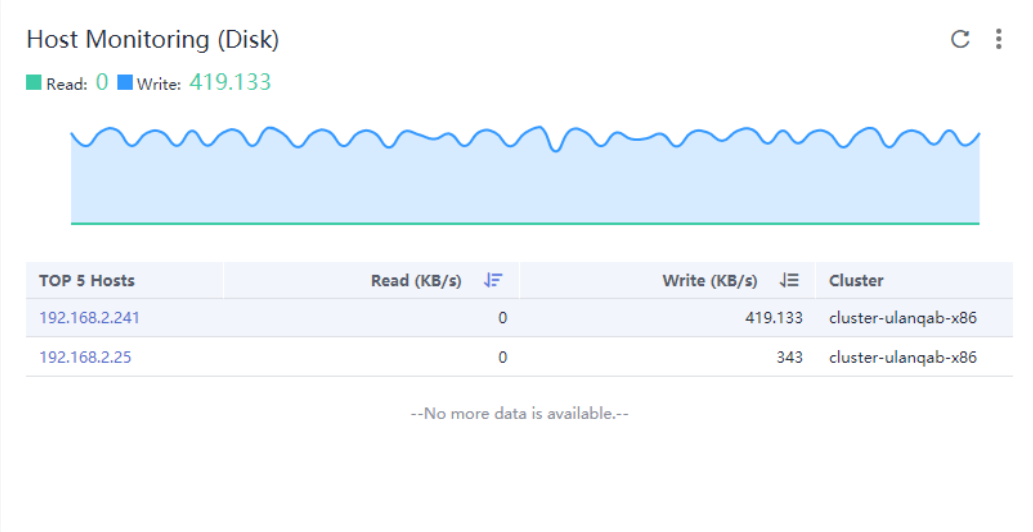


This card mainly displays:

- The top 5 container instances with high CPU and memory usage in the last minute.
- Trend graph of the CPU and memory usage of the selected container instance in the last hour. The values of each point in the graph respectively indicate the CPU and memory usage of the container instance in one minute.
- CPU and memory usage of the selected container instance at the latest time point, which is displayed above the trend graph.
- Hide system instances option, which can be selected to hide system instances.

Host Monitoring (Disk) Card

Figure 5-7 Host monitoring (disk)

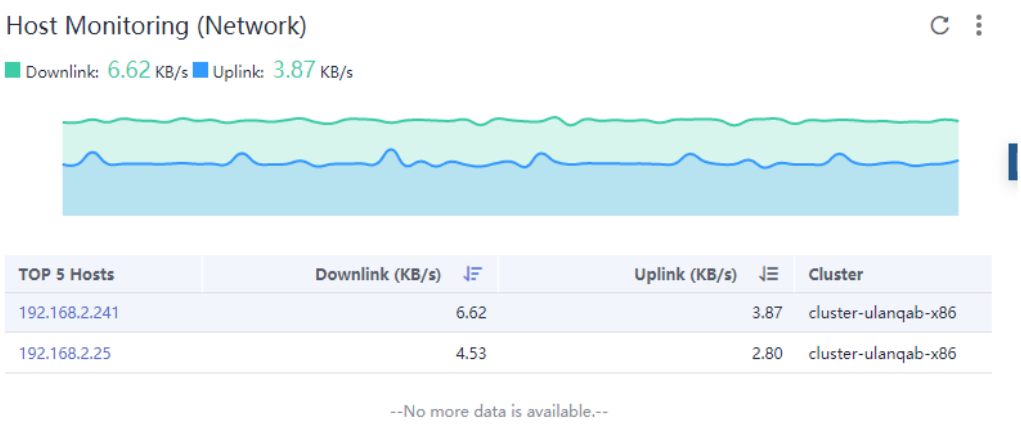


This card mainly displays:

- The top 5 hosts with high disk read/write rate in the last minute.
- Trend graph of the disk read/write rate of the selected host in the last hour. The values of each point in the graph respectively indicate the disk read/write rate of the selected host in one minute.
- Disk read/write rate of the selected host at the latest time point, which is displayed above the trend graph.

Host Monitoring (Network) Card

Figure 5-8 Host monitoring (network)

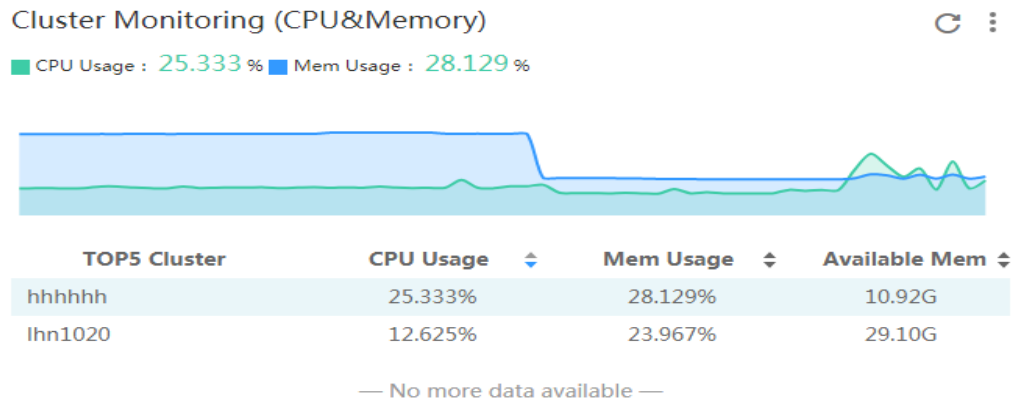


This card mainly displays:

- The top 5 hosts with high send/receive rate in the last minute.
- Trend graph of the send/receive rate of the selected host in the last hour. The values of each point in the graph respectively indicate the send/receive rate of the selected host in one minute.
- Send/receive rate of the selected host at the latest time point, which is displayed above the trend graph.

Cluster Monitoring (CPU and Memory) Card

Figure 5-9 Cluster monitoring (CPU and memory)



This card mainly displays:

- The top 5 clusters with high CPU and memory usage in the last minute.

- Trend graph of the CPU and memory usage of the selected cluster in the last hour. The values of each point in the graph respectively indicate the CPU and memory usage of the cluster in one minute.
- CPU and memory usage of the selected cluster at the latest time point, which is displayed above the trend graph.

More Operations

Perform the operations listed in **Table 5-1** if needed.

Table 5-1 Related operations

Operation	Description
Adding a card to favorites	To hide a card, click in the upper right corner of the card and choose **Add to Favorites**. After a card is added to favorites, it is hidden from the **O&M** page. To view the card later, obtain it from favorites.
Adding a card to dashboard	Click in the upper right corner of the card and choose **Add to Dashboard**.
Zooming in a metric graph	Click  in the upper right corner of the metric graph.
Drilling down blue texts	Click the blue texts, such as **Host**, **Application**, or **Component** to drill down to the details page.

5.2 Dashboard

With a dashboard, different graphs such as line graphs and digit graphs are displayed on the same screen, which lets you view comprehensive monitoring data.

For example, you can add key metrics of important resources to the dashboard for real-time monitoring. You can also compare the same metric for different resources on one GUI. In addition, you can add routine O&M metrics to the dashboard so that you can perform routine check without re-selecting metrics when you re-open AOM.

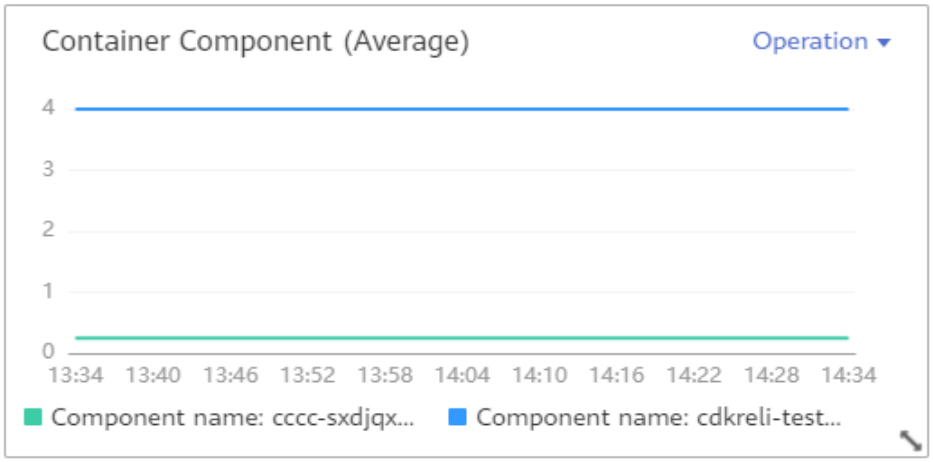
Before creating a dashboard, learn the types of graphs that can be added to the dashboard for accurate resource monitoring. The following graphs can be added to the dashboard:

Metric Data Graphs (Including Line and Digit Graphs)

- **Line graph**: displays the metric data trend by time. Use this type of graph to monitor the metric data trend of one or more resources in a period.

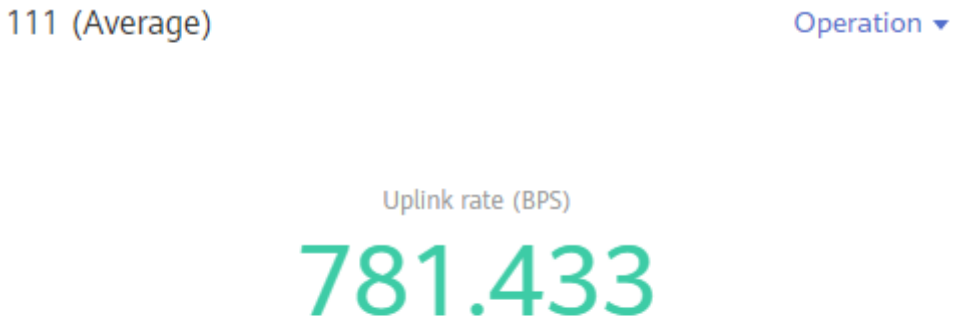
  You can use a line graph to compare the same metric of different resources. The following figure shows the total CPU cores of different components.

Figure 5-10 Line graph



- **Digit graph**: displays the latest value of a metric in real time.
  The following figure shows the average uplink rate (BPS) of a component.

  Figure 5-11 Digit graph

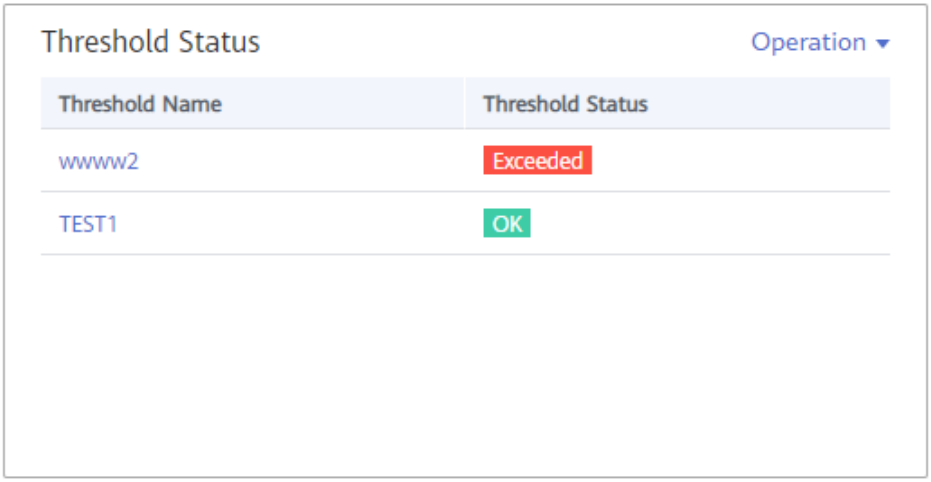
  

Health Status Graphs (Including Threshold, Host, and Component Status Graphs)

The status of thresholds, hosts, and components can be displayed. The status of one or more threshold rules, hosts, or components can be added to one graph for monitoring.

- **Threshold-crossing status graph**: monitors the status of threshold rules in real time.

Figure 5-12 Threshold-crossing status graph

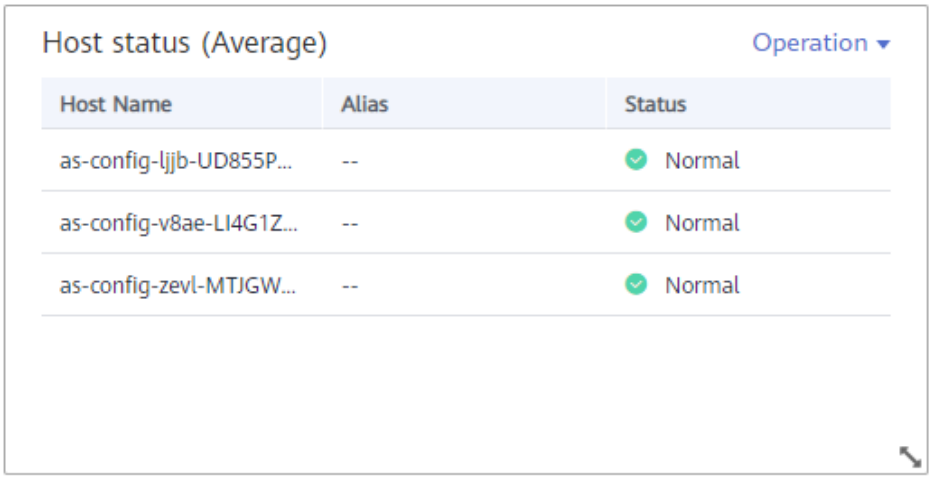


NOTE

Before adding a threshold-crossing status graph, ensure that you have created a threshold rule. Otherwise, such a graph cannot be added.

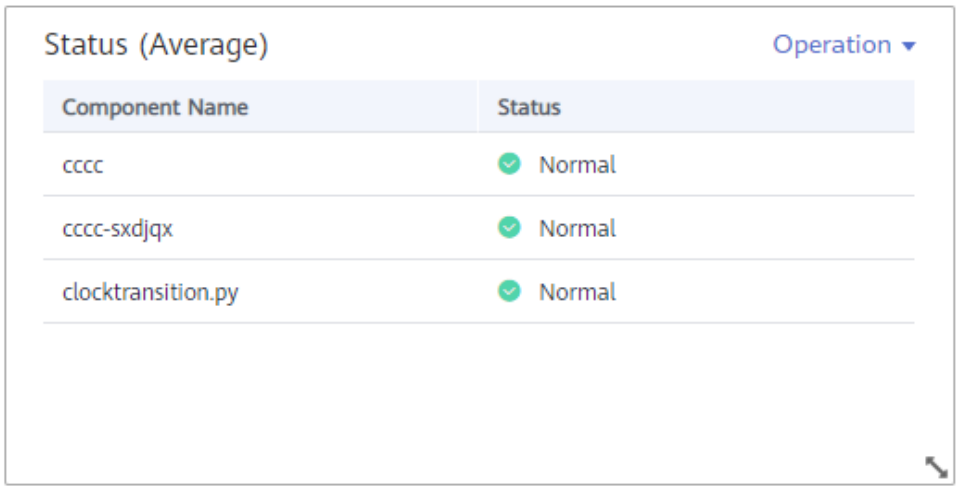
- **Host status graph**: monitors the host status in real time.

Figure 5-13 Host status graph



- **Component status graph**: monitors the component status in real time.

Figure 5-14 Component status graph

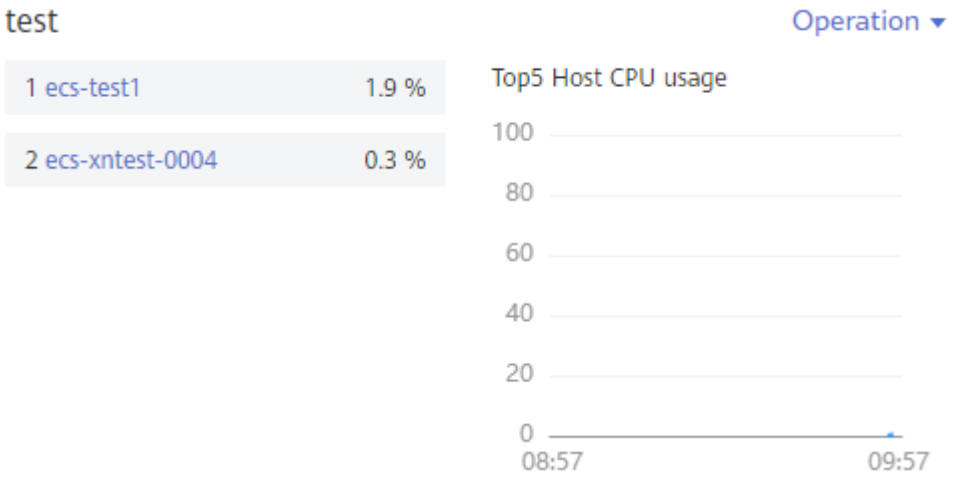


Top N Resource Graphs

For top N resource graphs, the statistical unit is a cluster and statistical objects are resources such as hosts, components, or instances in the cluster. A top N resource graph shows the top N resources in a cluster in a visualized manner. Both the top 5 and top 15 resources can be displayed. By default, the top 5 resources are displayed. After the graph is zoomed in, the top 15 resources are displayed.

To quickly 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. The following figure shows the top 5 hosts with the highest CPU usage.

Figure 5-15 Top N resource graph



NOTE

- By default, the top 5 resources are displayed. To view the top 15 resources, click **Top 15 xxx**, double-click the graph, or click **View Larger** in the **Operation** column.
- To monitor the top 5 resources among all clusters, view them on the **O&M** page. Alternatively, add the corresponding graph on the **O&M** page to the dashboard.
- You can customize the title of the top N resource graph. By default, the title is **resource type(cluster name)**.

Precautions

- A maximum of 50 dashboards can be created in a region.
- A maximum of 20 graphs can be added to a dashboard.
- A maximum of 10 resources can be added to a line graph, and resources can be selected across clusters.
- Only one resource can be added to a digit graph.
- A maximum of 10 threshold rules can be added to a threshold-crossing status graph.
- A maximum of 10 hosts can be added to a host status graph.
- A maximum of 10 components can be added to a component status graph.

Creating a Dashboard

Step 1 In the navigation pane, choose **Overview** > **Dashboard**.

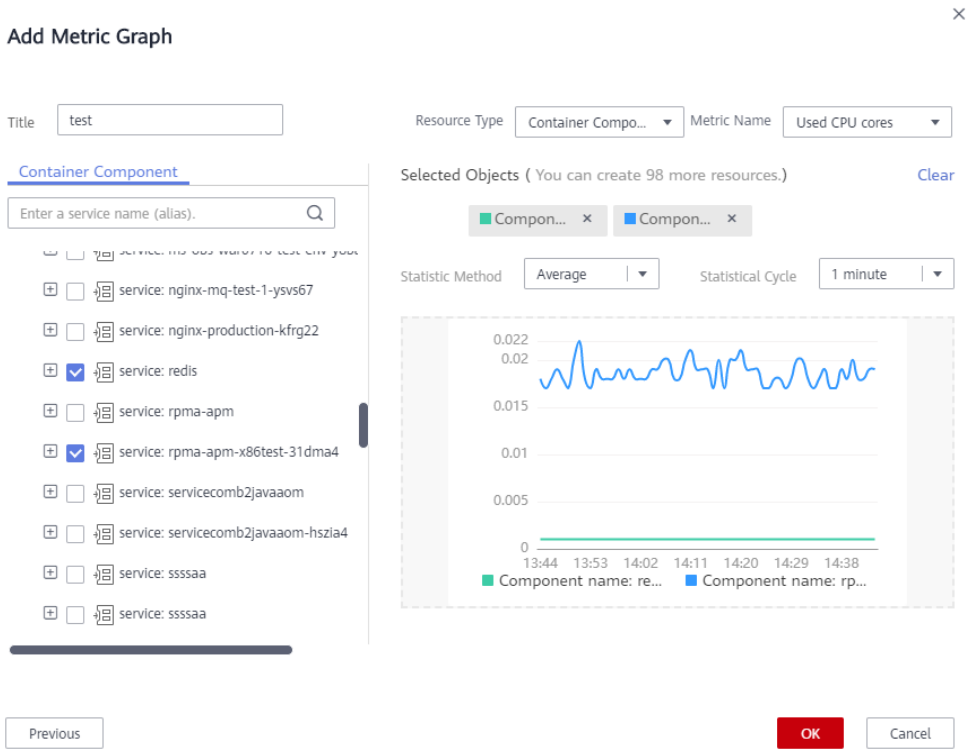
Step 2 On the **Dashboard** page, click **Create Dashboard**. In the displayed **Create Dashboard** dialog box, enter a dashboard name and click **OK**.

Step 3 Add a metric graph to the dashboard. The dashboard supports the following graphs: line graphs, digit graphs, threshold-crossing status graphs, host status graphs, and component status graphs. Select a graph that is appropriate for your requirements.

The following shows how to add a line graph to a dashboard:

1. On the **Dashboard** page, click **Add Metric Graph**. In the displayed **Select Which to Add** dialog box, click **Create** below **Metric Data**.
2. Select the type of the graph: In the displayed **Add Metric Graph** dialog box, select **Line graph** and then click **Next**.
3. Select the metrics and set **Statistic Method** and **Statistical Cycle**, and click **OK**.

Figure 5-16 Creating a dashboard



Step 4 Click **Save** in the upper right corner of the **Dashboard** page.

NOTE

Enable **Auto Refresh** ( ) in the upper right corner of the **Dashboard** page so that all graphs in the dashboard can be refreshed automatically.

- On (default)

  Data in the dashboard will be automatically refreshed each minute.
- Off

  Data in the dashboard will not be automatically refreshed.

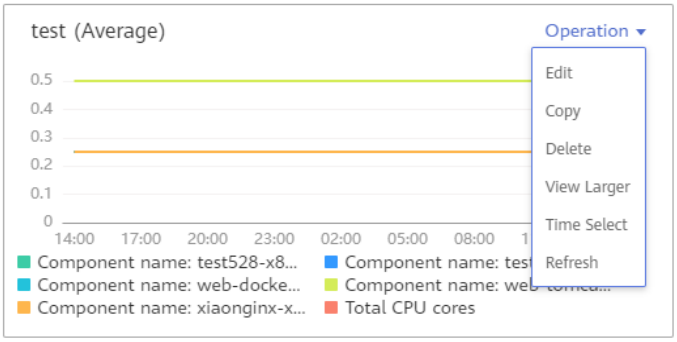
----End

More Operations

After creating a dashboard, perform the operations listed in **Table 5-2** if needed.

Table 5-2 Related operations

Object	Operation	Description
Dashboard	Save as	Click **More** in the upper right corner, and choose **Save As**, **Rename**, or **Delete** from the drop-down list.
	Rename	
	Delete	

Object	Operation	Description
	Export a monitoring report	Click **Export Monitoring Report** to export a line graph in the dashboard as a CSV file to a local PC.
Graph	Add	Click **Add Metric Graph** to add a line graph, digit graph, threshold-crossing status graph, host status graph, or component status graph to the dashboard.
	Edit Copy Delete Zoom in Time select Refresh	Choose **Edit**, **Copy**, **Delete**, and **View Larger** (only a line graph can be enlarged) from the **Operation** column. The **Time Select** option is available only in a line graph. This option allows you to set a temporary time range and statistical cycle so that you can view the resource data within a specified time range. **Figure 5-17** Operations on a graph  **NOTE** In the dashboard, when resources such as hosts and components are deleted, graphs created for these resources are not automatically deleted. To improve system performance, manually delete unnecessary graphs.
	Resize	Move the cursor to the lower right corner of a graph. When the cursor changes to ↘, hold down your left mouse button to resize the graph.
	Reposition	Put the cursor at the blank area in the upper or lower part of a graph, and drag and drop it to the desired position.

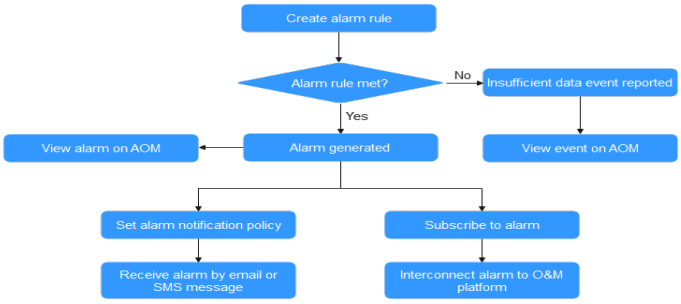
6 Alarm Management

6.1 Alarm Management

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

Before using the alarm management function, ensure that you have installed the ICAgent according to **Installing the ICAgent**. **Figure 6-1** shows how to use this function.

Figure 6-1 Alarm management process



6.2 Static Threshold Rules

6.2.1 Creating a Static Threshold Rule

This function is available in regions except AP-Singapore, CN-Hong Kong, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN South-Shenzhen.

You can set threshold conditions for resource metrics by setting static threshold rules. If a metric value meets the threshold condition, a threshold alarm will be generated. If no metric data is reported, an insufficient data event will be generated.

When AOM is interconnected with **Simple Message Notification (SMN)** and you set **a notification policy** on the SMN console, notifications are sent by email or Short Message Service (SMS) message if the status of the static threshold rule changes (**Exceeded**, **OK**, or **Insufficient**). In this way, you can identify and handle exceptions at the earliest time.

Creation Methods

Static threshold rules are classified into single- and multi-resource static threshold rules based on the mapping between resources and rules.

- **Single-resource static threshold rules:** Resources and rules have a many-to-many relationship. When multiple resources are monitored, multiple rules are generated after the creation is complete. Each resource can be monitored by using an independent rule.

  To monitor resources separately, you are advised to use this method. For details, see **Directly Creating Static Threshold Rules**.
- **Multi-resource static threshold rules:** Resources and rules have a many-to-one relationship. When multiple resources are monitored, only one rule is generated after the creation is complete. Multiple resources are monitored by the same rule.

  To monitor multiple resources in a centralized manner, you are advised to use this method.
  - Based on O&M experience, AOM provides default multi-resource threshold rules for key metrics (including CPU usage, physical memory usage, host status, and service status) of all hosts and services. You can create default multi-resource threshold rules in one click. For details, see **Creating Multi-Resource Threshold Rules**.
  - If default multi-resource threshold rules cannot meet requirements, use static threshold templates to create rules. For details, see **Using Templates to Create Static Threshold Rules**. Static threshold templates are used for creating multi-resource static threshold rules. For details on how to create a static threshold template, see **Creating a Static Threshold Template**.

Precautions

- You can create a maximum of 1000 static threshold rules. If the number of static threshold rules reaches 1000, delete unnecessary rules and create new ones.
- Setting a notification policy

If you want to send notifications by email or Short Message Service (SMS) message when the static threshold rule status (**Exceeded**, **Normal**, or **Insufficient**) changes, set a notification policy on the Simple Message Notification (SMN) console according to the following procedure. If you do not need to receive email or SMS notifications, skip the following operations. The procedure is as follows:

a. Create a topic according to **Creating a Topic**.

b. Set a topic policy according to **Configuring Topic Policies**.

   Select **APM** for **Services that can publish messages to this topic**. If **APM** is not selected, notifications cannot be sent.

c. Add a subscriber, that is, the email or SMS message recipient, for the topic according to **Adding a Subscription**.

Directly Creating Static Threshold Rules

Step 1 Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Threshold Rules**. Then, click **Add Threshold** in the upper right corner.

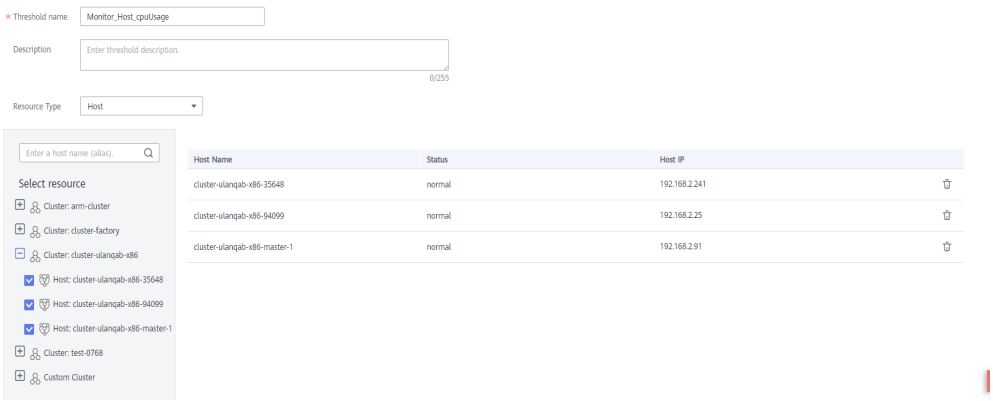
Step 2 Customize static threshold rules.

1. Select a resource: Enter a threshold name, select **Custom creation** for **Creation Mode**, select a resource type, select the resource to be monitored from the resource tree, and click **Next**.

   NOTE

   - You can select a maximum of 100 resources from the resource tree.
   - When multiple resources are selected, multiple single-resource static threshold rules will be created after the creation is complete. Each resource is monitored by a single-resource static threshold rule. A rule name consists of the threshold rule name you enter in the **Threshold name** text box, and a sequence number ranging from 0 to 9. The earlier a resource is selected, the smaller its number.

   Figure 6-2 Selecting resources



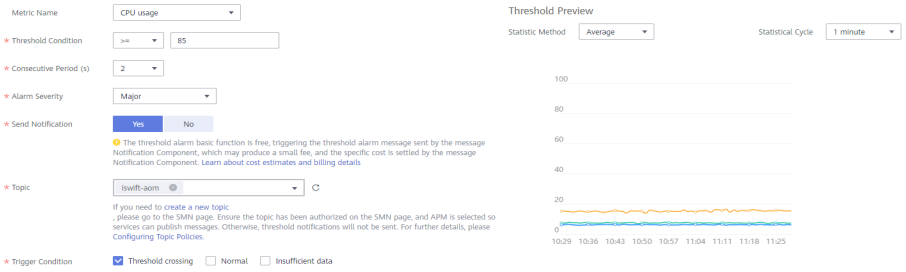
2. Define a threshold: Select the metric to be monitored, and set parameters such as **Threshold Condition**, **Consecutive Period**, **Alarm Severity**, **Statistic Method**, and **Send Notification**.

NOTE

- **Threshold Condition**: trigger condition of a threshold alarm. A threshold condition consists of two parts: determination condition (≥, ≤, >, or <) and threshold value. For example, after **Threshold Condition** is set to **> 85**, if the actual metric value exceeds 85, a threshold alarm is generated.
- **Consecutive Period**: If a metric value meets the threshold condition for a specified number of consecutive periods, a threshold alarm is generated.
- **Statistic Method**: method used to measure metric values.
- **Statistical Cycle**: interval at which metric data is collected.
- **Send Notification**: whether to send notifications by email or SMS message when the static threshold rule status (**Exceeded**, **Normal**, or **Insufficient**) changes.
  - If you want to receive email or SMS notifications, select **Yes**, set **a notification policy**, select a created topic, and select a trigger scenario.
  - If you do not need to receive notifications by email or SMS message, select **No**.
- **Trigger Scenario**: condition for sending a notification.

  You can select multiple trigger conditions. For example, to receive notifications if the threshold status changes to **Exceeded**, select **Threshold crossing**. To receive notifications upon any threshold status change, select all trigger conditions.

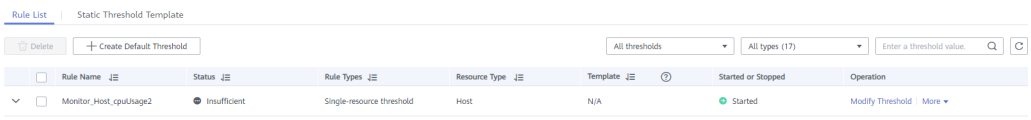
Figure 6-3 Customizing a threshold



Step 3 Click **Submit**. As shown in the following figure, multiple single-resource static threshold rules are created. One resource corresponds to one rule. Each resource can be monitored by using an independent rule.

A single-resource static threshold rule monitors a host. If the CPU usage of the host exceeds 85%, a threshold alarm is generated on the alarm page. You can choose **Alarm Center** > **Alarm List** in the navigation pane and view the alarm in the alarm list. If the host meets the preset notification policy, an email or SMS message will be sent.

Figure 6-4 Creating a single-resource static threshold rule



----End

Using Templates to Create Static Threshold Rules

Before creating a static threshold, ensure that a static threshold template has been created according to **Creating a Static Threshold Template**.

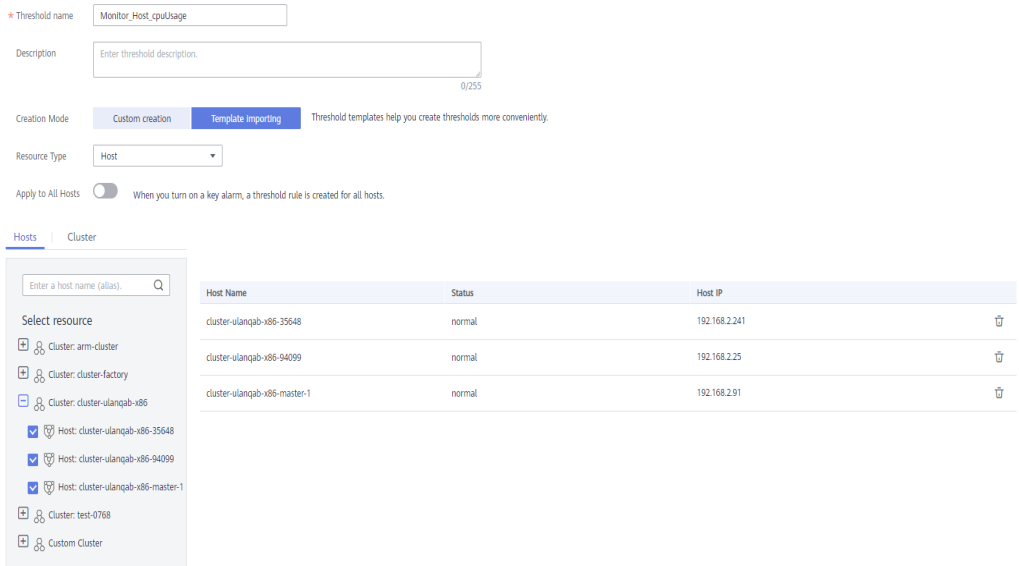
Step 1 Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Threshold Rules**. Then, click **Add Threshold** in the upper right corner.

Step 2 Select a resource: Enter a threshold rule name, select **Template importing** for **Creation Mode**, select a resource type, select the resource to be monitored from the resource tree, and click **Next**.

NOTE

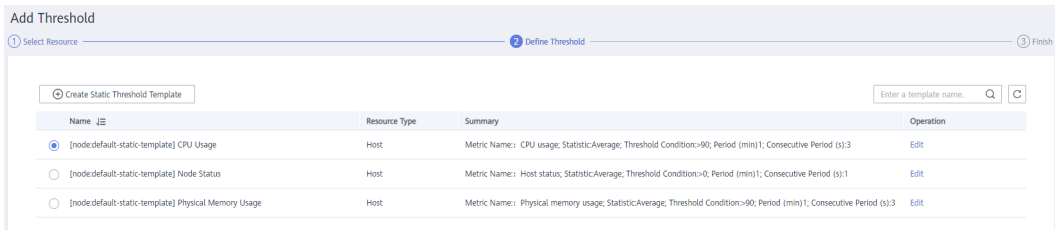
- When the option below **Resource Type** is disabled (that is, ): Select up to 100 resources from the resource tree.
- When the option below **Resource Type** is enabled (that is, ): If **Resource Type** is **Host**, all hosts will be monitored. If **Resource Type** is **Component**, all components will be monitored. Your setting also applies to hosts and components added later.

Figure 6-5 Selecting the resource to be monitored



Step 3 Select the static threshold template you have created.

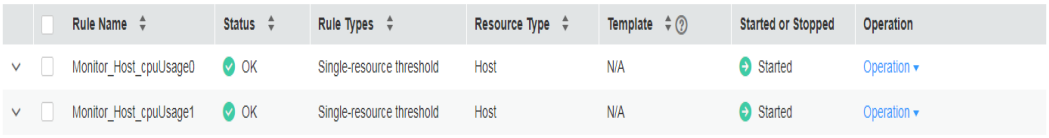
Figure 6-6 Selecting the static threshold template



Step 4 Click **Submit**. As shown in the following figure, a multi-resource static threshold rule is created. Click ⌄ to monitor the same metric of multiple resources.

In the displayed host list, if the CPU usage of a host exceeds 85%, a threshold alarm is generated on the **Alarm List** page. You can choose **Alarm Center** > **Alarm List** in the navigation pane and view the alarm. If any host meets the preset notification policy, an email or SMS message will be sent.

Figure 6-7 Creating a static threshold rule



----End

Creating Multi-Resource Threshold Rules

Step 1 Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Threshold Rules**.

Step 2 On the **Rule List** tab page, click **Create Default Threshold**.

AOM will automatically create six static threshold templates. You can click the **Static Threshold Template** tab to view the templates. For details, see **Creating Default Static Threshold Templates**. In addition, AOM will automatically create six default multi-resource threshold rules based on these templates. The monitored objects are all hosts or services, as shown in **Figure 6-7**. For example, click ⌄ next to **[node:default-static-rule] CPU Usage** to monitor the CPU usage of all hosts.

If you add hosts or services later, AOM automatically applies the rules to them.

Figure 6-8 Creating default multi-resource threshold rules

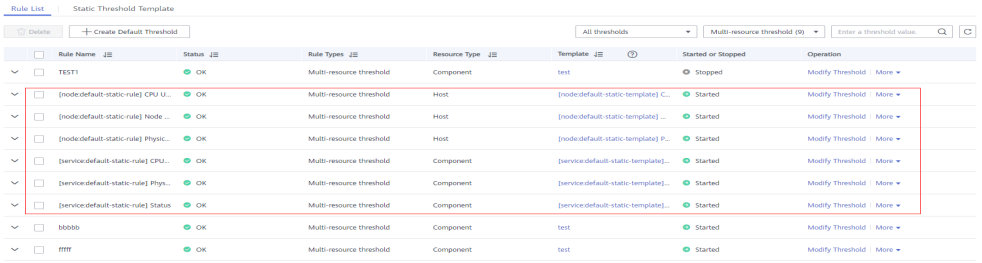


Table 6-1 Description of default multi-resource threshold rules

Rule/Template	Resource	Metric	Default Configuration
• Rule: [node: default-static-rule] CPU Usage • Template: [node: default-static-template] CPU Usage	Host	CPU usage	Statistic Method: Average; Threshold Condition: > 90%; Consecutive Periods: 3; Statistical Cycle: 1 minute; Alarm

Rule/Template	Resource	Metric	Default Configuration
• Rule: [node: default-static-rule] Physical Memory Usage • Template: [node: default-static-template] Physical Memory Usage		Physical memory usage	Severity: Major; Send Notification: No
• Rule: [node: default-static-rule] Node Status • Template: [node: default-static-template] Node Status		Host status	Statistic Method: Average; Threshold Condition: > 0; Consecutive Periods: 1; Statistical Cycle: 1 minute; Alarm Severity: Major; Send Notification: No
• Rule: [service: default-static-rule] CPU Usage • Template: [service: default-static-template] CPU Usage	Component	CPU usage	Statistic Method: Average; Threshold Condition: > 90%; Consecutive Periods: 3; Statistical Cycle: 1 minute; Alarm Severity: Major; Send Notification: No
• Rule: [service: default-static-rule] Physical Memory Usage • Template: [service: default-static-template] Physical Memory Usage		Physical memory usage	
• Rule: [service: default-static-rule] Status • Template: [service: default-static-template] Status		Component status	Statistic Method: Average; Threshold Condition: > 0; Consecutive Periods: 1; Statistical Cycle: 1 minute; Alarm Severity: Major; Send Notification: No

----End

More Operations

After creating threshold rules, perform the operations listed in **Table 6-2** if needed.

Table 6-2 Related operations

Operation	Description
Modifying a static threshold rule	Choose **Modify Threshold** in the **Operation** column.
Deleting a static threshold rule	• To delete a static threshold rule, choose **More** > **Delete** in the **Operation** column. • To delete one or more static threshold rules, select them and click **Delete** above the rule list.
Starting or stopping a static threshold rule	• Choose **More** > **Start** in the **Operation** column. • Choose **More** > **Stop** in the **Operation** column. **NOTE** Single-resource static threshold rules cannot be started or stopped.
Searching for a static threshold rule	You can search for a rule by rule name, description, or metric name. Simply enter a keyword in the search box in the upper right corner and click  .
Viewing an alarm	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 Center** > **Alarm List** to view the alarm.
Viewing an event	When no metric data of a resource is reported during the configured consecutive periods, the system reports an insufficient data event. In the navigation pane, choose **Alarm Center** > **Event List** to view the event.

6.2.2 Creating a Static Threshold Template

This function is available in regions except CN-Hong Kong, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN South-Shenzhen.

Static threshold templates are used for creating multi-resource static threshold rules. For details about how to create such rules, see **Using Templates to Create Static Threshold Rules**.

Precautions

- You can create a maximum of 50 static threshold templates. If the maximum number has been reached, delete unnecessary templates and create new ones.
- Setting a notification policy

  If you want to send notifications by email or Short Message Service (SMS) message when the static threshold rule status (**Exceeded**, **Normal**, or

Insufficient) changes, set a notification policy on the Simple Message Notification (SMN) console according to the following procedure. If you do not need to receive email or SMS notifications, skip the following operations. The procedure is as follows:

a. Create a topic according to **Creating a Topic**.

b. Set a topic policy according to **Configuring Topic Policies**.

   Select **APM** for **Services that can publish messages to this topic**. If **APM** is not selected, notifications cannot be sent.

c. Add a subscriber, that is, the email or SMS message recipient, for the topic according to **Adding a Subscription**.

Creation Method

- Creating static threshold templates in one click: AOM provides default static threshold templates for key metrics (including the CPU usage, physical memory usage, host status, and service status) of all hosts and services, greatly reducing configuration workloads. For details, see **Creating Default Static Threshold Templates**.
- Customizing static threshold templates: If the default static threshold templates cannot meet requirements, customize a static threshold template according to **Customizing Static Threshold Templates**.

Creating Default Static Threshold Templates

Step 1 Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Threshold Rules**.

Step 2 On the **Rule List** tab page, click **Create Default Threshold**.

Figure 6-9 Default static threshold templates

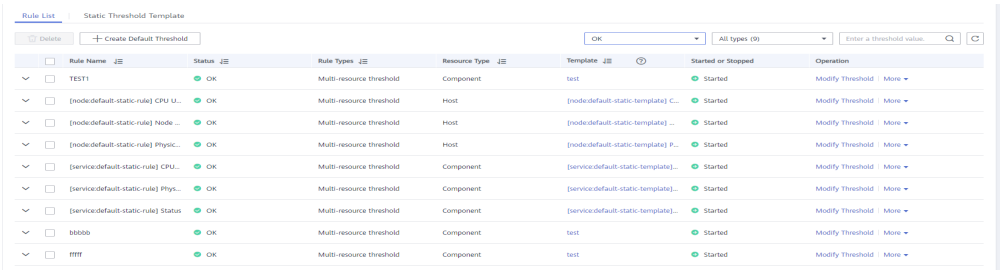


Table 6-3 Description of default static threshold templates

Template/Rule	Resource	Metric	Default Settings
• Template: [node: default-static-template] CPU Usage • Rule: [node: default-static-rule] CPU Usage	Host	CPU usage	Statistic Method: Average; Threshold Condition: > 90%; Consecutive Periods: 3; Statistical Cycle: 1 minute; Alarm Severity: Major; Send Notification: No

Template/Rule	Resource	Metric	Default Settings
• Template: [node: default-static-template] Physical Memory Usage • Rule: [node: default-static-rule] Physical Memory Usage		Physical memory usage	
• Template: [node: default-static-template] Node Status • Rule: [node: default-static-rule] Node Status		Host status	Statistic Method: Average; Threshold Condition: > 0; Consecutive Periods: 1; Statistical Cycle: 1 minute; Alarm Severity: Major; Send Notification: No
• Template: [service: default-static-template] CPU Usage • Rule: [service: default-static-rule] CPU Usage	Component	CPU usage	Statistic Method: Average; Threshold Condition: > 90%; Consecutive Periods: 3; Statistical Cycle: 1 minute; Alarm Severity: Major; Send Notification: No
• Template: [service: default-static-template] Physical Memory Usage • Rule: [service: default-static-rule] Physical Memory Usage		Physical memory usage	
• Template: [service: default-static-template] Status • Rule: [service: default-static-rule] Status		Component status	Statistic Method: Average; Threshold Condition: > 0; Consecutive Periods: 1; Statistical Cycle: 1 minute; Alarm Severity: Major; Send Notification: No

NOTE

Default static threshold templates can be deleted or modified. To recreate default static threshold templates after deleting them, click **Create Default Threshold** again.

----End

Customizing Static Threshold Templates

Step 1 Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Threshold Rules**.

Step 2 Click the **Static Threshold Template** tab, and then click **Create Static Threshold Template**.

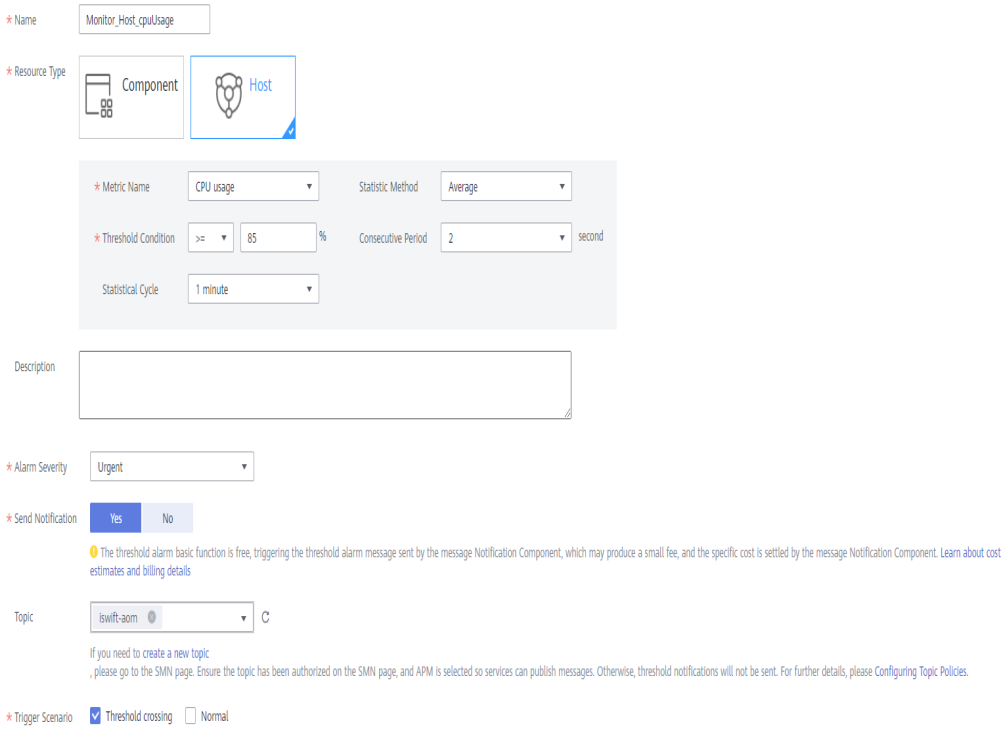
Step 3 Customize a static threshold template.

Enter a template name, select a resource type, set parameters such as **Name**, **Statistic Method**, and **Threshold Condition**, select an alarm severity, and determine whether to send notifications.

NOTE

- **Statistic Method**: method used to measure metric values.
- **Threshold Condition**: trigger condition of a threshold alarm. A threshold condition consists of two parts: determination condition (≥, ≤, >, or <) and threshold value. For example, after **Threshold Condition** is set to **> 85**, if the actual metric value exceeds 85, a threshold alarm is generated.
- **Consecutive Period**: If a metric value meets the threshold condition for a specified number of consecutive periods, a threshold alarm is generated.
- **Statistical Cycle**: interval at which metric data is collected.
- **Send Notification**: whether to send notifications by email or SMS message when the static threshold rule status (**Exceeded**, **Normal**, or **Insufficient**) changes.
  - If you want to receive email or SMS notifications, select **Yes**, set **a notification policy**, select a created topic, and select a trigger scenario.
  - If you do not need to receive notifications by email or SMS message, select **No**.
- **Trigger Scenario**: condition for sending a notification. You can select multiple trigger conditions. For example, to receive a notification when the threshold status changes to **Exceeded**, select the **Threshold crossing** trigger scenario.

Figure 6-10 Customizing a static threshold template



Step 4 Click **Create**.

----End

More Operations

After creating a static threshold template, perform the operations listed in **Table 6-4** if needed.

Table 6-4 Related operations

Operation	Description
Using a static threshold template to create a multi-resource static threshold rule	Click **Create Threshold** in the **Operation** column. For details, see **Using Templates to Create Static Threshold Rules**.
Modifying a static threshold template	Click **Edit** in the **Operation** column.
Deleting a static threshold template	• To delete a static threshold template, click **Delete** in the **Operation** column. • To delete one or more static threshold templates, select them and click **Delete** above the template list.
Searching for a static threshold template	Enter a template name in the search box in the upper right corner and click  .

6.3 Alarm Rules

6.3.1 Overview

This function is available in AP-Singapore, CN-Hong Kong, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN South-Shenzhen.

By setting alarms rules, you can define event conditions for services or threshold conditions for resource metrics. If the resource data of a service meets the event condition, an event alarm will be generated. If a metric value meets the threshold condition, a threshold alarm will be generated. If no metric data is reported, an insufficient data event will be generated.

Alarm rules are classified into static threshold rules and event alarm rules. Generally, static threshold rules are used to monitor the usage of resources such as hosts and components in real time. When there are too many resource usage alarms and notifications are sent too often, use an event alarm rule to identify a type of resource usage problems for simplified notification.

The total number of static threshold rules and event alarm rules is 1000. If the number of alarm rules has reached the upper limit, delete unnecessary rules and create new ones.

6.3.2 Creating Static Threshold Rules

You can set threshold conditions for resource metrics by setting static threshold rules. If a metric value meets the threshold condition, a threshold alarm will be generated. If no metric data is reported, an insufficient data event will be generated.

Creation Methods

There are two creation methods: **Directly Creating Static Threshold Rules** and **Using Templates to Create Static Threshold Rules**. Only one rule is generated at a time. All resources are monitored using the same rule. To use the second method to create a static threshold rule, ensure that a static threshold template has been created according to **Creating Static Threshold Templates**.

Precautions

If you need AOM to send notifications by email or SMS message when the static threshold rule status (**Exceeded**, **OK**, **Insufficient**, or **Disabled**) changes, set an alarm action policy according to **Creating an Alarm Action Policy**.

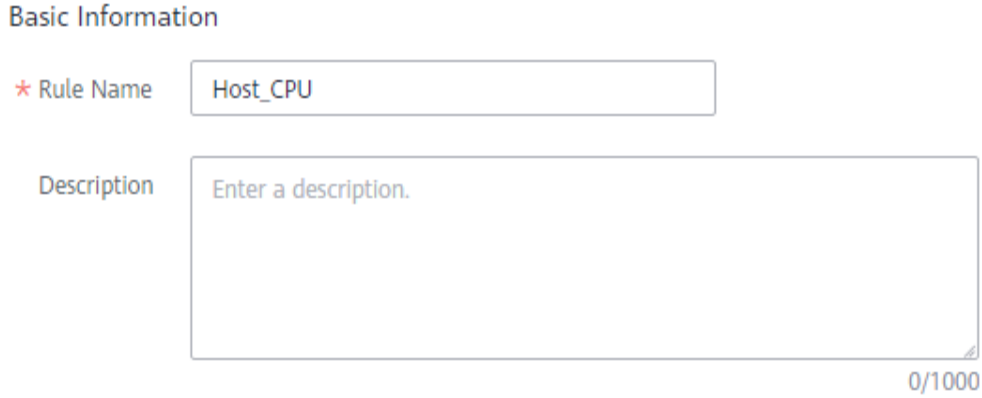
Directly Creating Static Threshold Rules

Step 1 Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Alarm Rules**. Then, click **Create Alarm Rule** in the upper right corner.

Step 2 Customize a static threshold rule.

1. Set basic information such as the rule name and description.

   Figure 6-11 Setting basic information

2. Set details about the rule.
   a. Set **Rule Type** to **Threshold alarm**.
   b. Select monitored objects. Use either of the following methods:
      - **Select resource object**: Click **Select Resource Object**, add objects by dimension or resource, and click **Confirm**.

NOTE

A threshold rule can monitor a maximum of 100 metrics.

- Command input: Both manual and auto inputs are supported.
  - Manual input: used when you know the metric name and IP address, and you are familiar with the Prometheus format.

    For example, to query the CPU usage of the host, run the **avg(label_replace(avg_over_time(aom_node_cpu_usage{hostID="81010a40-1682-41c1-9645-f0588ff9c0cf",nodeIP="192.168.1.210",clusterId = '00000000-0000-0000-0000-00000000'}[59999ms]), "__name__","aom_node_cpu_usage","","")) by(__name__,hostID,nodeIP)** command.

    NOTE

    For details about Prometheus commands, move the cursor to next to the search box and click **Learn more**.
  - Auto input: used when you do not know the metric information or are unfamiliar with the Prometheus format. The command can only be automatically filled when you switch from the **Metric Monitoring** page.

    Specifically, choose **Monitoring** > **Metric Monitoring** in the navigation pane. Then, click **Add Metric** and select **Dimension** or **Resource** for **Add By**. Select up to 12 metrics to monitor. Next, click in the **Operation** column. The system automatically switches to the threshold rule creation page and fills the Prometheus command for your metric.

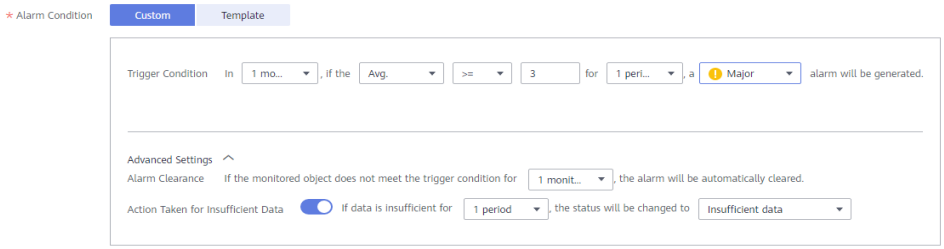
c. Set an alarm condition. Click **Custom** and set information such as statistical periods, consecutive periods, and threshold condition. **Table 6-5** describes the parameters.

Table 6-5 Alarm condition parameters

Category	Parameter	Description
Trigger Condition	Statistical Periods	Interval at which metric data is collected. By default, only one period is measured. A maximum of five periods can be measured.
	Consecutive Periods	When the metric value meets the threshold condition for a specified number of consecutive periods, a threshold-crossing alarm will be generated.
	Statistic	Method used to measure metrics. Options: **Avg.**, **Min.**, **Max.**, **Sum**, and **Samples**.

Category	Parameter	Description
	Threshold Condition	Trigger condition of a threshold alarm. A threshold condition consists of two parts: operators (≥, ≤, >, and <) and threshold value. For example, after **Threshold Condition** is set to **> 85**, if the actual metric value exceeds 85, a threshold alarm is generated.
	Alarm Severity	Severity of a threshold alarm. Options: **Critical**, **Major**, **Minor**, and **Warning**.
Advanced Settings	Alarm Clearance	An alarm will be cleared if the monitored object does not meet the trigger condition within the monitoring period. By default, metrics in only one period are monitored. You can set up to five monitoring periods.
	Action Taken for Insufficient Data	Action to be taken when no metric data is generated or metric data is insufficient within the monitoring period. You can configure this option based on your requirements. By default, metrics in only one period are monitored. You can set up to five monitoring periods. Options: **Alarm**, **Insufficient data**, **Keep previous status**, and **Normal**.

Figure 6-12 Setting an alarm condition



d. Set alarm tags and annotations to group alarms. They can be associated with alarm noise reduction policies for sending notifications.

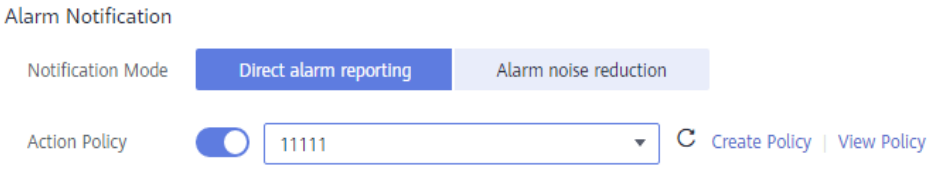
   Click **Add Tag** or **Add Annotation**.

3. Set an alarm notification policy. There are two alarm notification modes.
   - Direct alarm reporting: An alarm is directly sent when the alarm condition is met.

     You need to configure whether to enable an alarm action policy. After this function is enabled, the system sends alarm notifications based on the associated SMN topic and message template. If the existing alarm action policies cannot meet the requirements, click **Create Policy** to add

one. For details about how to set an alarm action policy, see **Creating an Alarm Action Policy**.

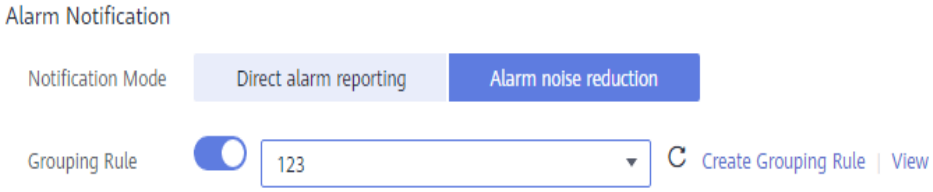
Figure 6-13 Selecting the direct alarm reporting mode



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

  Select a grouping rule to reduce alarm noise. If existing grouping rules cannot meet your requirements, click **Create Grouping Rule** to create one. For details, see **Grouping Rules**.

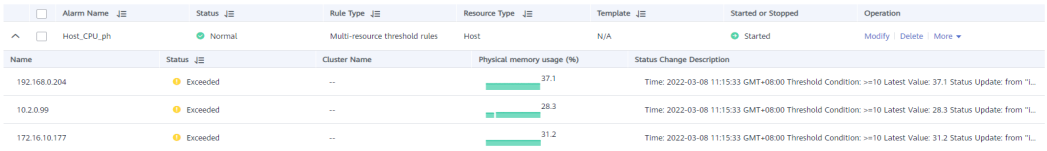
Figure 6-14 Selecting the alarm noise reduction mode



Step 3 Click **Create Now**. As shown in the following figure, a static threshold rule is created. Click ⌄ to monitor the same metric of multiple resources in batches.

In the expanded list, if the physical memory usage of a host exceeds 10%, a threshold alarm is generated on the alarm page. To view the alarm, go to the AOM console and choose **Alarm Center** > **Alarm List** in the navigation pane. If a host meets the preset notification policy, the system sends an alarm notification to the specified personnel by email, SMS, or WeCom.

Figure 6-15 Creating a static threshold rule



----End

Using Templates to Create Static Threshold Rules

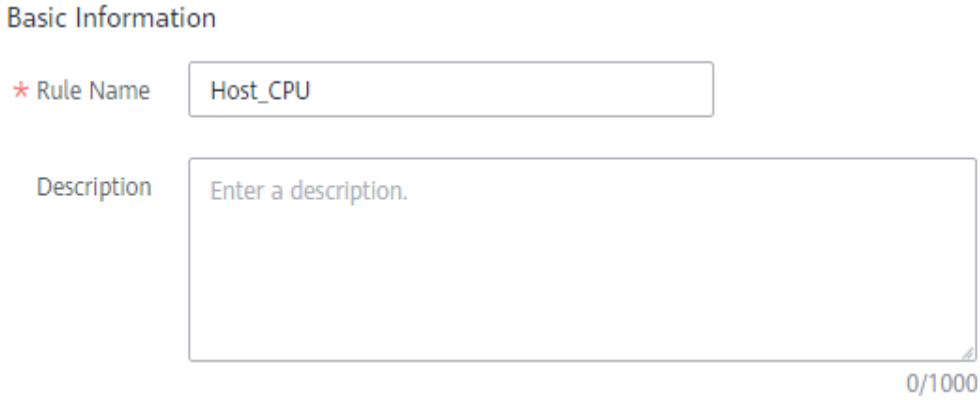
Before creating a static threshold, ensure that a static threshold template has been created according to **Creating Static Threshold Templates**.

Step 1 Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Alarm Rules**. Then, click **Create Alarm Rule** in the upper right corner.

Step 2 Customize a static threshold rule.

1. Set basic information such as the rule name and description.

Figure 6-16 Setting basic information



2. Set details about the rule.
   a. Set **Rule Type** to **Threshold alarm**.
   b. Select monitored objects. When a template is used to create a threshold rule, you can select metrics only by dimension or resource. The command input mode is not supported.
   c. Set an alarm condition. Click **Template**, select the created static threshold template from the drop-down list, and set parameters, such as **Alarm Clearance** and **Action Taken for Insufficient Data**.

Figure 6-17 Setting an alarm condition

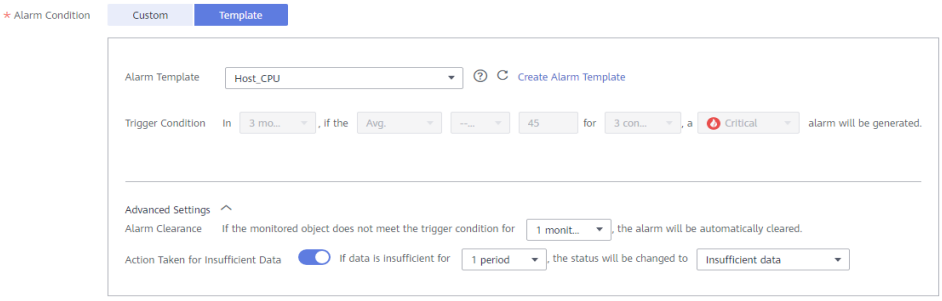


Table 6-6 Alarm condition parameters

Category	Parameter	Description
Alarm Template	-	Select the static threshold template you have created. If the existing templates do not meet your requirements, click **Create Alarm Template** to create one. For details, see **Creating Static Threshold Templates**.
Trigger Condition	-	The system automatically imports the preset trigger condition in the template. Note that the condition cannot be modified.

Category	Parameter	Description
Advanced Settings	Alarm Clearance	An alarm will be cleared if the monitored object does not meet the trigger condition within the monitoring period. By default, metrics in only one period are monitored. You can set up to five monitoring periods.
	Action Taken for Insufficient Data	Action to be taken when no metric data is generated or metric data is insufficient within the monitoring period. You can configure this option based on your requirements. By default, metrics in only one period are monitored. You can set up to five monitoring periods. Options: **Alarm**, **Insufficient data**, **Keep previous status**, and **Normal**.

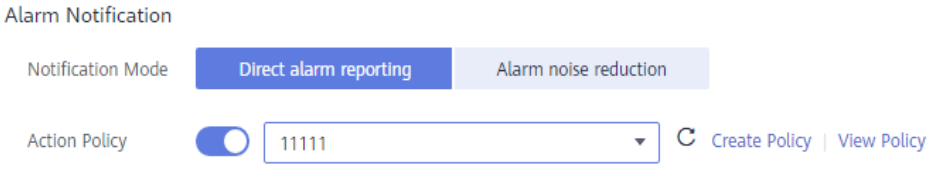
d. Set alarm tags and annotations to group alarms. They can be associated with alarm noise reduction policies for sending notifications.

   Click **Add Tag** or **Add Annotation**.

3. Set an alarm notification policy. There are two alarm notification modes.
   - Direct alarm reporting: An alarm is directly sent when the alarm condition is met.

     You need to configure whether to enable an alarm action policy. After this function is enabled, the system sends alarm notifications based on the associated SMN topic and message template. If the existing alarm action policies cannot meet the requirements, click **Create Policy** to add one. For details about how to set an alarm action policy, see **Creating an Alarm Action Policy**.

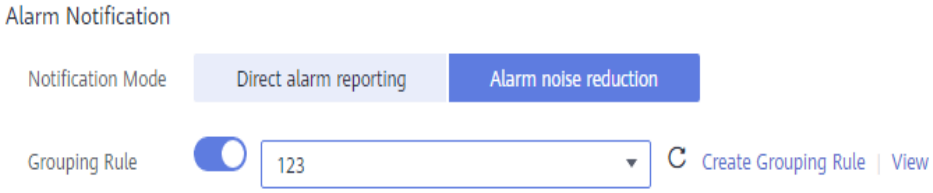
     Figure 6-18 Selecting the direct alarm reporting mode

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

     Select a grouping rule to reduce alarm noise. If existing grouping rules cannot meet your requirements, click **Create Grouping Rule** to create one. For details, see **Grouping Rules**.

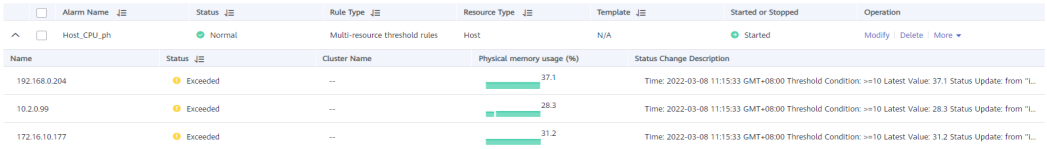
Figure 6-19 Selecting the alarm noise reduction mode



Step 3 Click **Create Now**. As shown in the following figure, a static threshold rule is created. Click ⌄ to monitor the same metric of multiple resources in batches.

In the expanded list, if the physical memory usage of a host exceeds 10%, a threshold alarm is generated on the alarm page. To view the alarm, go to the AOM console and choose **Alarm Center** > **Alarm List** in the navigation pane. If a host meets the preset notification policy, the system sends an alarm notification to the specified personnel by email, SMS, or WeCom.

Figure 6-20 Creating a static threshold rule



----End

More Operations

After creating static threshold rules, perform the operations listed in **Table 6-7** if needed.

Table 6-7 Related operations

Operation	Description
Modifying a static threshold rule	Click **Modify** in the **Operation** column.
Deleting a static threshold rule	• To delete a static threshold rule, click **Delete** in the **Operation** column. • To delete one or more static threshold rules, select them and click **Delete** above the rule list.
Starting or stopping a static threshold rule	Choose **More** > **Start** or **Stop** in the **Operation** column. **NOTE** Single-resource static threshold rules cannot be started or stopped.
Searching for a static threshold rule	You can search for a rule by rule name, description, or metric name. Simply enter a keyword in the search box in the upper right corner and click 🔍.

Operation	Description
Viewing an alarm	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 Center** > **Alarm List** to view the alarm.
Viewing an event	When no metric data of a resource is reported during the configured consecutive periods, the system reports an insufficient data event. In the navigation pane, choose **Alarm Center** > **Event List** to view the event.

6.3.3 Creating Static Threshold Templates

Before creating a static threshold rule, create a static threshold template.

Precautions

You can create a maximum of 50 static threshold templates. If the maximum number has been reached, delete unnecessary templates and create new ones.

Procedure

Step 1 Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Alarm Rules**.

Step 2 Click the **Static Threshold Templates** tab, and then click **Create**.

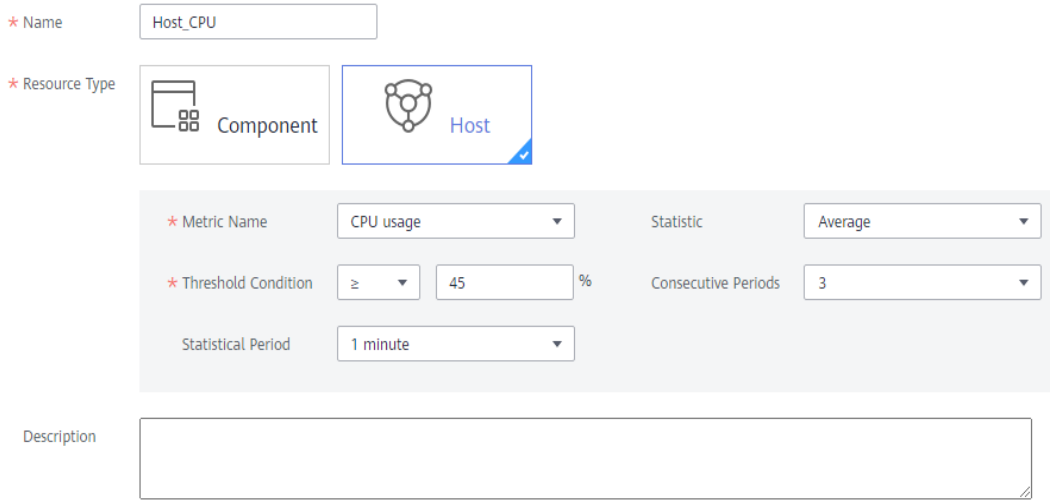
Step 3 Customize a static threshold template.

Enter a template name, select a resource type, and set parameters such as **Name**, **Statistic**, and **Threshold Condition**.

NOTE

- **Statistic**: method used to measure metric values.
- **Threshold Condition**: trigger condition of a threshold alarm. A threshold condition consists of two parts: determination condition (≥, ≤, >, or <) and threshold value. For example, after **Threshold Condition** is set to **> 85**, if the actual metric value exceeds 85, a threshold alarm is generated.
- **Consecutive Periods**: If a metric value meets the threshold condition for a specified number of consecutive periods, a threshold alarm is generated.
- **Statistical Period**: interval at which metric data is collected.

Figure 6-21 Customizing static threshold templates



Step 4 Click **Create**.

----End

More Operations

After creating a static threshold template, perform the operations listed in **Table 6-8** if needed.

Table 6-8 Related operations

Operation	Description
Using a static threshold template to create a multi-resource static threshold rule	Click **Create Threshold** in the **Operation** column. For details, see **Using Templates to Create Static Threshold Rules**.
Modifying a static threshold template	Click **Modify** in the **Operation** column.
Deleting a static threshold template	• To delete a static threshold template, click **Delete** in the **Operation** column. • To delete one or more static threshold templates, select them and click **Delete** above the template list.
Searching for a static threshold template	Enter a template name in the search box in the upper right corner and click .

6.3.4 Creating an Event Alarm Rule

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

Precautions

If you want to receive notifications by email or SMS message when the resource data of a service meets the event condition, set an alarm action policy according to **Creating an Alarm Action Policy**.

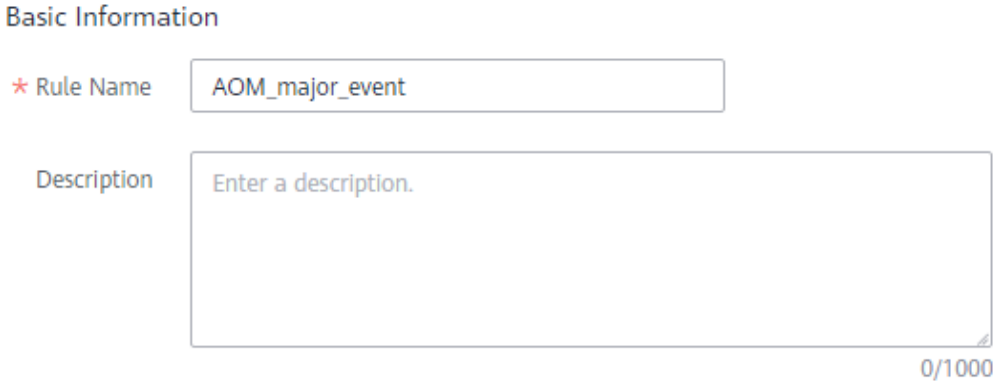
Procedure

Step 1 Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Alarm Rules**. Then, click **Create Alarm Rule** in the upper right corner.

Step 2 Set an event alarm rule.

1. Set basic information such as the rule name and description.

   Figure 6-22 Setting basic information

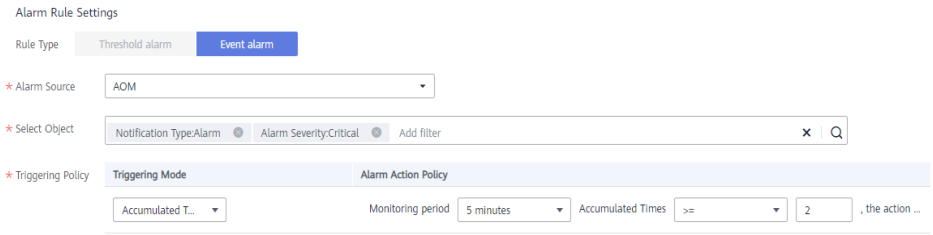
2. Set details about the rule.
   a. Set **Rule Type** to **Event alarm**.
   b. Set the alarm source, trigger object, and trigger policy.

   Table 6-9 Alarm rule parameters

Parameter	Description
Alarm Source	Name of the service for which an event alarm is reported. You can select a service from the service list.
Trigger 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.

Parameter	Description
Trigger Policy	Policy for triggering event alarms. ■ Accumulated triggering: An alarm action policy is triggered when the preset accumulated number of times has been reached in a monitoring period. ■ Immediate triggering: An alarm is generated immediately when the filter criterion is met.

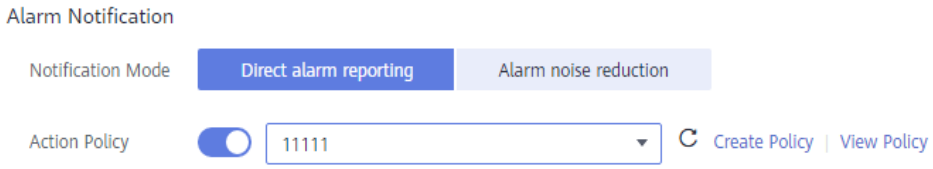
Figure 6-23 Setting an alarm rule



3. Set an alarm notification policy. There are two alarm notification modes.
   - Direct alarm reporting: An alarm is directly sent when the alarm condition is met.

     You need to configure whether to enable an alarm action policy. After this function is enabled, the system sends alarm notifications based on the associated SMN topic and message template. If the existing alarm action policies cannot meet the requirements, click **Create Policy** to add one. For details about how to set an alarm action policy, see **Creating an Alarm Action Policy**.

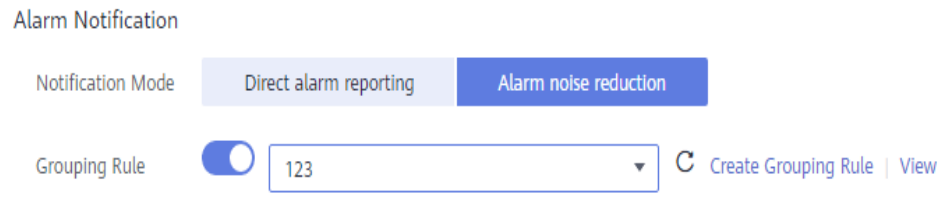
     Figure 6-24 Selecting the direct alarm reporting mode

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

     Select a grouping rule to reduce alarm noise. If existing grouping rules cannot meet your requirements, click **Create Grouping Rule** to create one. For details, see **Grouping Rules**.

     Figure 6-25 Selecting the alarm noise reduction mode

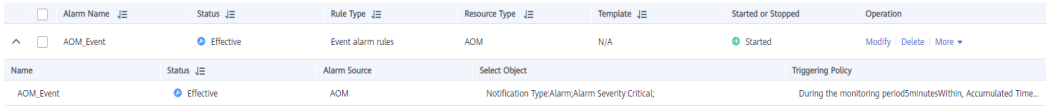
     

Step 3 Click **Create Now**. An event alarm rule is created, as shown in **Figure 6-26**.

This rule monitors critical alarm events of AOM. When the AOM resources meet the preset event alarm condition, critical alarms are generated on the alarm page.

In the navigation pane, choose **Alarm Center** > **Alarm List** to view the alarm. When a service event meets the preset notification policy, the system sends an alarm notification to the specified personnel by email, SMS, or WeCom.

Figure 6-26 Event alarm rule



----End

Related Operations

After creating an event alarm rule, perform the operations listed in **Table 6-10** if needed.

Table 6-10 Related operations

Operation	Description
Modifying an event alarm rule	Click **Modify** in the **Operation** column.
Deleting an event alarm rule	• To delete an event alarm rule, click **Delete** in the **Operation** column. • To delete one or more event alarm rules, select them and click **Delete** above the rule list.
Starting or stopping an event alarm rule	Choose **More** > **Start** or **Stop** in the **Operation** column.
Searching for an event alarm rule	You can search for a rule by rule name, description, or metric name. Simply enter a keyword in the search box in the upper right corner and click  .

6.4 Creating Notification Rules

This function is available in regions except AP-Singapore, CN-Hong Kong, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN South-Shenzhen.

AOM supports alarm notification. You can use this function by creating notification rules. When alarms are reported due to an exception in AOM or an external service, alarm information can be sent to specified personnel by email or

Short Message Service (SMS) message. In this way, these personnel can rectify faults in time to avoid service loss.

If no notification rules exist, no alarm notifications will be sent. In this case, you can only view alarms on the **Alarm List** page in the AOM console.

Procedure

After notification rules are created, SMS messages or emails are sent when the notification rules are met.

Step 1 Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Notification Rules**. Then, click **Create Notification Rule** in the upper right corner.

Step 2 Click **Create SMN Topic** and set a notification policy on the Simple Message Notification (SMN) console when AOM is interconnected with SMN. If you have already configured a notification policy, skip this step.

1. Create a topic according to **Creating a Topic**.

   For example, create a topic named **Topic1**.

2. Set a topic policy according to **Configuring Topic Policies**.

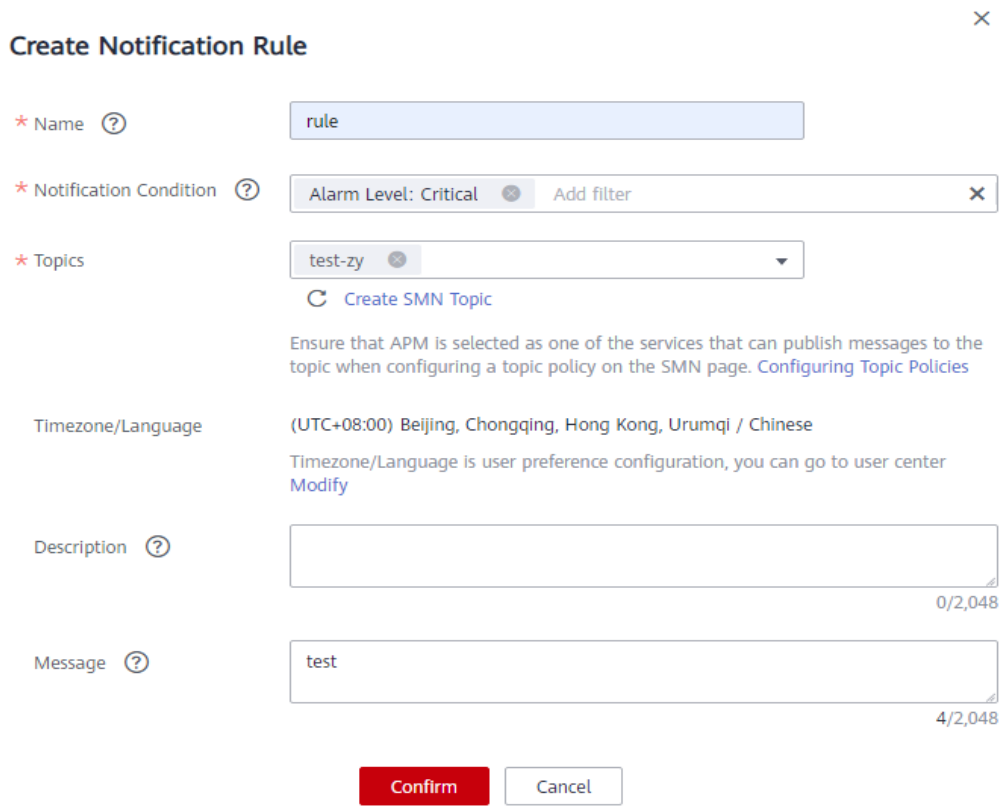
   Select **APM** for **Services that can publish messages to this topic**. If **APM** is not selected, notifications cannot be sent.

3. Add a subscriber, that is, the email or SMS message recipient, for the topic according to **Adding a Subscription**. SMN can send alarm notifications to subscribers in real time.

   For example, enter the email addresses of O&M personnel.

Step 3 Create a notification rule. Specifically, enter the rule name, select the notification condition, select the topic created in **Step 2**, select the time zone and language as required, enter the notification message, and click **Confirm**, as shown in **Figure 6-27**.

Figure 6-27 Creating a notification rule



After a notification rule is created, the O&M personnel will receive an email or SMS notification when this rule is met.

----End

More Operations

After creating a notification rule, perform the operations listed in **Table 6-11** if needed.

Table 6-11 Related operations

Operation	Description
Modifying a notification rule	Click in the **Operation** column.
Enabling or disabling a notification rule	Click **Enable** or **Disable** in the **Operation** column.

Operation	Description
Deleting a notification rule	• To delete a notification rule, click in the **Operation** column. • To delete one or more notification rules, select them and click **Delete** above the rule list.
Searching for a notification rule	Enter a rule name in the search box in the upper right corner and click .

6.5 Viewing Alarms

Procedure

Step 1 In the navigation pane, choose **Alarm Center** > **Alarm List**.

Step 2 View alarms on the **Alarm List** page.

1. Set a time range to view alarms. There are two methods to set a time range:

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

   Method 2: Specify the start time and end time to customize a time range. You can specify up to 15 days.

2. Set filter criteria and click to view the alarms generated in the time period.

Step 3 Perform the operations listed in **Table 6-12** as required.

Table 6-12 Operations

Operation	Method	Description
Viewing alarm statistics	View alarm statistics that meet filter criteria within a specific time range through a bar graph.	-
Clearing alarms	In the alarm list, click in the **Operation** column of the target alarm.	• You can clear alarms after the problems that cause them are resolved. • You can view the alarms that have been cleared on the **History** tab page.
Viewing alarm details	View alarm details in the **Alarm Detail** column.	-

----End

6.6 Viewing Events

Events generally carry some important information, informing you of the changes of AOM or an external service. Such changes do not necessarily cause exceptions. Events do not need to be handled.

Procedure

Step 1 In the navigation pane, choose **Alarm Center** > **Event List**.

Step 2 View events on the **Event List** page.

1. Set a time range to view events. There are two methods to set a time range:

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

   Method 2: Specify the start time and end time to customize a time range. You can specify up to 15 days.

2. Set filter criteria and click to view the events generated in the time period.

Step 3 Perform the operations listed in **Table 6-13** as required.

Table 6-13 Operations

Operation	Method	Description
Viewing event statistics	View event statistics that meet filter criteria within a specific time range through a bar graph.	-

----End

6.7 Alarm Action Policies

6.7.1 Overview

AOM allows you to customize alarm action policies. You can create an alarm action policy to associate an SMN topic and a message template. You can also customize notification content by using a message template. After an alarm action policy is created, choose **Alarm Center** > **Alarm Noise Reduction** in the navigation pane. Then, click the **Grouping Rules** tab and click **Create**. On the displayed page, specify an alarm action policy.

NOTE

This function is available only in AP-Singapore, CN-Hong Kong, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN South-Shenzhen. If you need this function, **submit a service ticket** to enable it.

6.7.2 Creating an Alarm Action Policy

Prerequisites

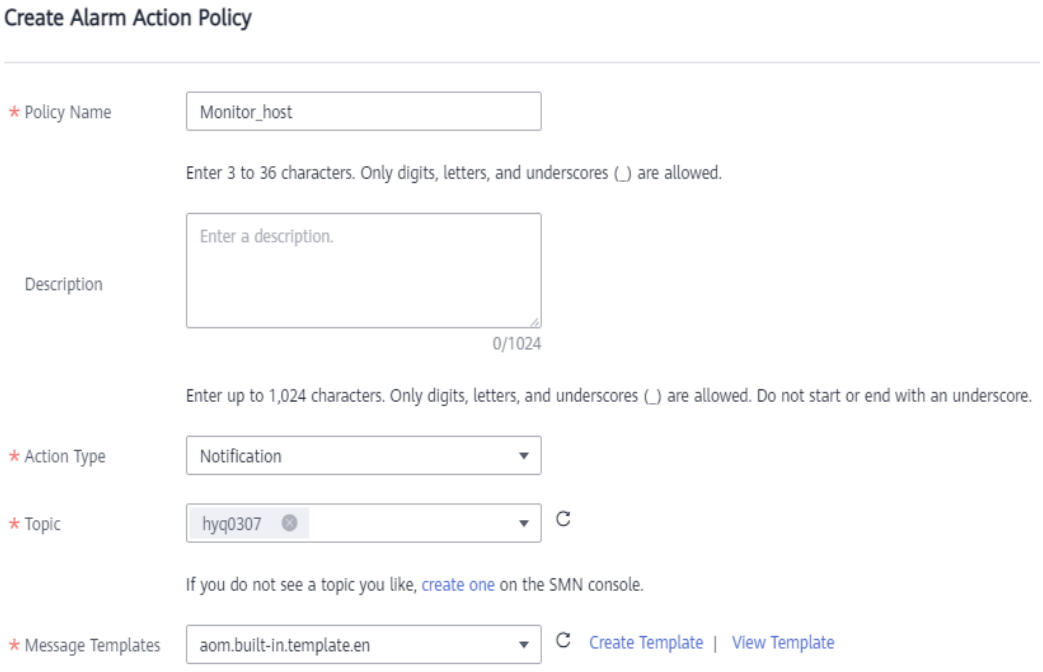
- A topic has been created according to **Creating a Topic**.
- A topic policy has been set according to **Configuring Topic Policies**.
- **APM** has been selected for **Services that can publish messages to this topic**. If **APM** is not selected, notifications cannot be sent.
- A subscriber, that is, the email or SMS message recipient has been added for the topic according to **Adding a Subscription**.

Procedure

Step 1 Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Alarm Action Policies**. On the displayed page, click **Create** in the upper left corner.

Step 2 Set parameters such as **Policy Name**, and click **Confirm**. **Figure 6-28** shows the details.

Figure 6-28 Creating an alarm action policy



NOTE

- You can select one or more topics. If there is no topic you want to select, create one on the SMN page. For details, see **Creating a Topic**.
- If there is no message template you want to select, click **Create Template** to create one. For details, see **Creating a Message Template**.

----End

6.7.3 Creating a Message Template

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

Procedure

Step 1 Log in to the AOM console and choose **Alarm Center** > **Alarm Action Policies** in the navigation pane. On the displayed page, click the **Message Templates** tab.

Step 2 Click **Create**. Alternatively, select a created message template and click **Copy** in the **Operation** column.

1. Enter a template name.
2. Enter a template description.
3. Select a language. (Only simplified Chinese and English are supported.)
4. Customize the template content. (Default fields are automatically filled when a message template is created.)

NOTE

1. You can create up to 100 message templates. If the number of templates exceeds the upper limit, delete unnecessary templates and create new ones.
2. There are two default message templates. If you do not customize any message template, notifications will be sent based on default templates. The default templates cannot be deleted or edited.
3. In addition to default message fields, the message template also allows you to customize fields. You need to define values for custom fields for event alarm reporting. For details about how to call related APIs, see the description of event alarm APIs. For details about the parameters, see the alarm reporting structs in the following message template.
4. Custom fields support the JSONPath format. Example: **$event.metadata.case1** or **$event.metadata.case[0]**.
5. In the upper right corner of the **Body** area, click **Add Variables** to add required variables.
6. If you select **Email**, you can click **Preview** to view the final effect.

Table 6-14 Variables in the default message template

Variable	Description	Definition
Notification Type	Type selected when a notification rule is created, which can be **Alarm** or **Event**.	${event_type}
Severity	Alarm or event severity, which can be **Critical**, **Major**, **Minor**, or **Warning**.	${event_severity}
Name	Name of the alarm or event that triggers the notification rule.	$event.metadata.event_name

Variable	Description	Definition
Occurred	Time when the alarm or event is triggered.	${starts_at}
Source	Name of the service corresponding to the alarm or event that triggers the notification rule.	$event.metadata.resource_provider
Resource Type	Type of the resource selected when you customize a threshold rule or define alarm reporting.	$event.metadata.resource_type
Resource Identifier	Resource that triggers the alarm or event.	${resources}
Custom tag	Extended tag.	$event.metadata.key1
Possible Cause	Cause of the alarm. For non-custom reporting, "NA" is displayed.	${alarm_probableCause_zh}
Suggestion	Suggestion on how to handle the alarm. For non-custom reporting, "NA" is displayed.	${alarm_fix_suggestion_zh}
Custom annotation	Extended annotation.	$event.annotations.key2

Alarm reporting structs corresponding to the message template

```
{
   "events": [{
      "starts_at": 1579420868000,       //${starts_at}
            "ends_at": 1579420868000,
      "timeout": 60000,
      "resource_group_id": "5680587ab6*******755c543c1f",
      "metadata": {
         "event_name": "test",          //${metadata.event_name}
         "event_severity": "Major",     //${metadata.event_severity}
         "event_type": "alarm",         //${metadata.event_type}
         "resource_provider": "ecs",    //${metadata.resource_provider}
         "resource_type": "vm",         //${metadata.resource_type}
         "resource_id": "ecs123",
         "key1": "Custom field"           //$event.metadata.key1
      },
      "annotations": {
         "alarm_probableCause_zh_cn": "possible cause",     //${annotations.alarm_probableCause_zh}
         "alarm_fix_suggestion_zh_cn": "fix suggestion",    //${annotations.alarm_fix_suggestion_zh}
         "key2": "Custom field"    //$event.annotations.key2
      }
   }]
}
```

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

----End

6.8 Alarm Noise Reduction

6.8.1 Overview

NOTE

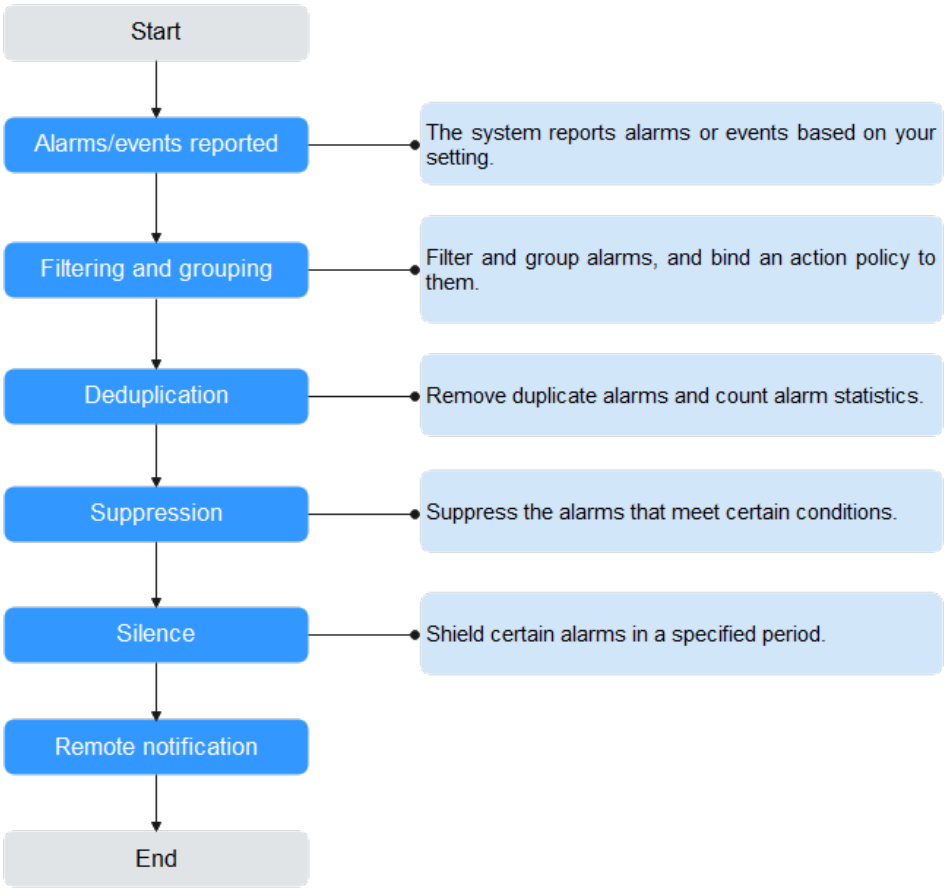
This function is available only in AP-Singapore, CN-Hong Kong, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN South-Shenzhen. If you need this function, **submit a service ticket** to enable it.

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

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

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

Figure 6-29 Alarm noise reduction process



You need to manually create grouping, suppression, and silence rules. For details, see the following description.

NOTE

1. This module is used only for message notification. All triggered alarms and events can be viewed on the **Alarm List** and **Event List** pages.
2. All conditions of alarm noise reduction rules are obtained from **metadata** in alarm structs. You can use the default fields or customize your own fields.

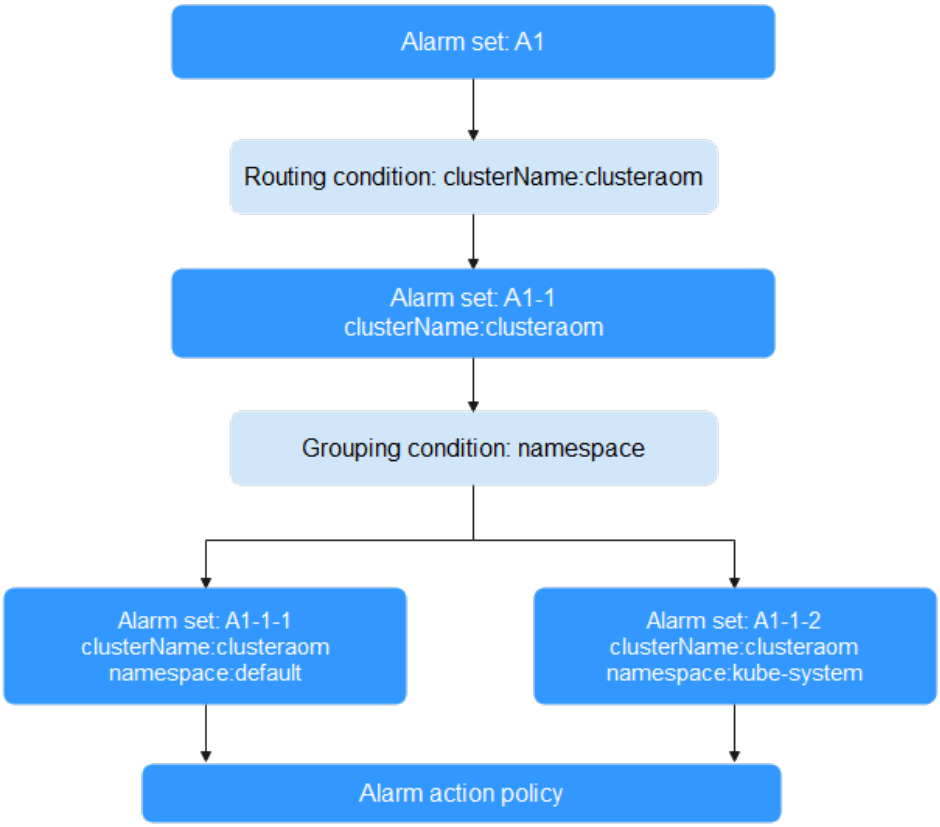
```
{
   "starts_at" : 1579420868000,
   "ends_at" : 1579420868000,
   "timeout" : 60000,
   "resource_group_id" : "5680587ab6*******755c543c1f",
   "metadata" : {
     "event_name" : "test",
     "event_severity" : "Major",
     "event_type" : "alarm",
     "resource_provider" : "ecs",
     "resource_type" : "vm",
     "resource_id" : "ecs123" ,
     "key1" : "value1"   //Custom alarm reporting field
 },
   "annotations" : {
     "alarm_probableCause_en_us": " Possible causes",
     "alarm_fix_suggestion_en_us": "Handling suggestion"
  }
}
```

6.8.2 Grouping Rules

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

As shown in **Figure 6-30**, when the routing condition is set to **clusterName: clusteraom**, the system filters alarm subsets whose **clusterName** is **clusteraom**. Then, the system groups the alarm subsets based on the grouping condition, and combines the grouped alarms based on the initial wait time, batch processing interval, and repeat interval. Then the combined alarms can be associated with action policies to trigger alarm notifications.

Figure 6-30 Alarm grouping process



Creating a Grouping Rule

Step 1 In the navigation pane, choose **Alarm Center** > **Alarm Noise Reduction**. Then, choose **Grouping Rules**.

Step 2 Click **Create** and set parameters such as **Rule Name**, **Inherited Rule**, and **Routing Condition**. For details, see **Table 6-15**.

Figure 6-31 Creating a grouping rule

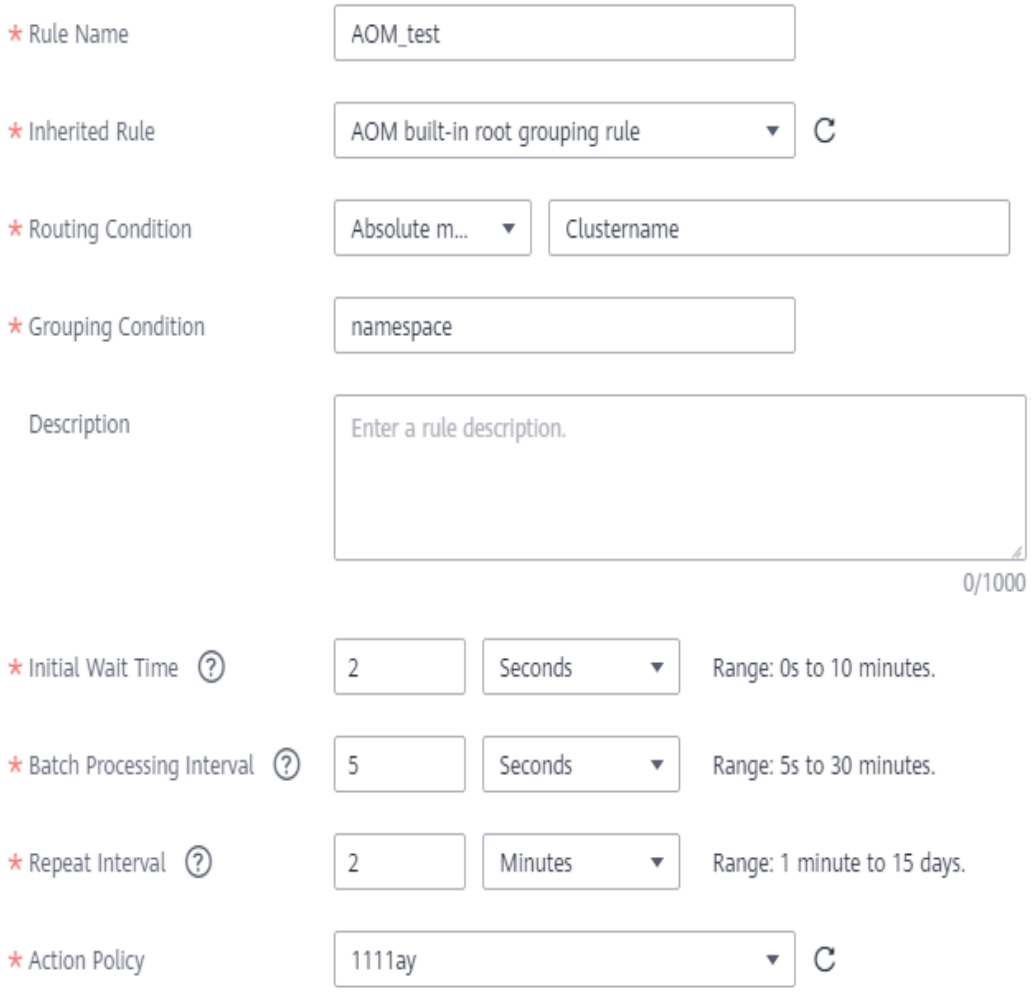
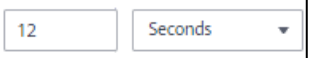


Table 6-15 Grouping rule parameters

Parameter	Description	Example
Rule Name	Rule name, which can contain up to 100 characters and cannot start or end with an underscore (_). Only letters, digits, and underscores are allowed.	ruleName
Inherited Rule	A grouping rule can inherit the routing and grouping conditions of a notification rule. AOM built-in grouping rule is a root rule, with no routing or grouping condition being set. If you do not want to inherit any rule, select this option.	AOM built-in root grouping rule

Parameter	Description	Example
Routing Condition	The system will filter the alarms that meet the routing condition. If the routing condition is set to **event_severity:Critical**, alarms whose **event_severity** is **Critical** will be filtered.	event_severity:Critical, event_type:alarm
Grouping Condition	The system will group alarms based on specified fields. Alarms in the same group are aggregated for sending one notification. The grouping condition can be an existing or a custom alarm field.	event_severity, event_type
Description	Description of a grouping rule.	-
Initial Wait Time	Time for a newly created or modified rule to take effect. The value ranges from 0s to 10 minutes. The recommended value is 15s.	
Batch Processing Interval	Period in which alarms will be combined for batch processing. The batch processing interval cannot be shorter than the initial wait time. The value ranges from 5s to 30 minutes. The recommended value is 60s. If this parameter is set to 1 minute, a batch of alarms and events are processed each minute.	
Repeat Interval	Period in which duplicate alarms will be sent only once. The value ranges from 1 minute to 15 days. The recommended value is 1 hour. If this parameter is set to 1 hour and the alarm or event is not cleared within 1 hour, the notification will be sent again.	
Action Policy	An action policy is related to the SMN message to be sent and custom template. For details, see **Alarm Action Policies**.	-

Step 3 Click **OK**.

----End

More Operations

After creating a grouping rule, perform the operations listed in **Table 6-16** if needed.

Table 6-16 Related operations

Operation	Description
Editing a grouping rule	Click **Modify** in the **Operation** column.
Delete a grouping 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.
Searching for a grouping rule	Enter a rule name in the search box in the upper right corner and click  .

6.8.3 Suppression Rules

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

Precautions

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

Creating a Suppression Rule

Step 1 Log in to the AOM console. Choose **Alarm Center** > **Alarm Noise Reduction** in the navigation pane and click the **Suppression Rules** tab. Then, click **Create**.

Step 2 Set information such as **Rule Name** and **Match Condition**.

Figure 6-32 Creating a suppression rule

NOTE

Match condition refers to the type of alarms which trigger suppression. Suppressed object refers to the type of alarms to be suppressed.

Specify the match condition and suppressed object using one of the following formats:

- "key1:value1,key2:value2". Match the value corresponding to the key to determine a suppressed object.
- "key1,key2". Match the key to determine the suppressed object. All values under the key are covered.
- "key1,key2,key3:value3". Determine the suppressed object by using the preceding two methods.

  "key:value" pairs must be separated by commas (,). The relationship between "key:value" pairs is "AND". That is, all conditions specified by setting "key:value" pairs must be met.

Step 3 Click **OK**.

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

----End

More Operations

After creating a suppression rule, perform the operations listed in **Table 6-17** if needed.

Table 6-17 Related operations

Operation	Description
Modifying a suppression rule	Click **Modify** in the **Operation** column.

Operation	Description
Deleting a suppression 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.
Searching for a suppression rule	Enter a rule name in the search box in the upper right corner and click  .

Using a suppression rule

For example, the alarm severities are **Critical**, **Major**, **Minor**, and **Warning** in descending order. If the match condition is set to **event_severity:Major** and the suppressed object is set to **event_severity:Minor**, minor alarms will be suppressed when major alarms are reported.

6.8.4 Silence Rules

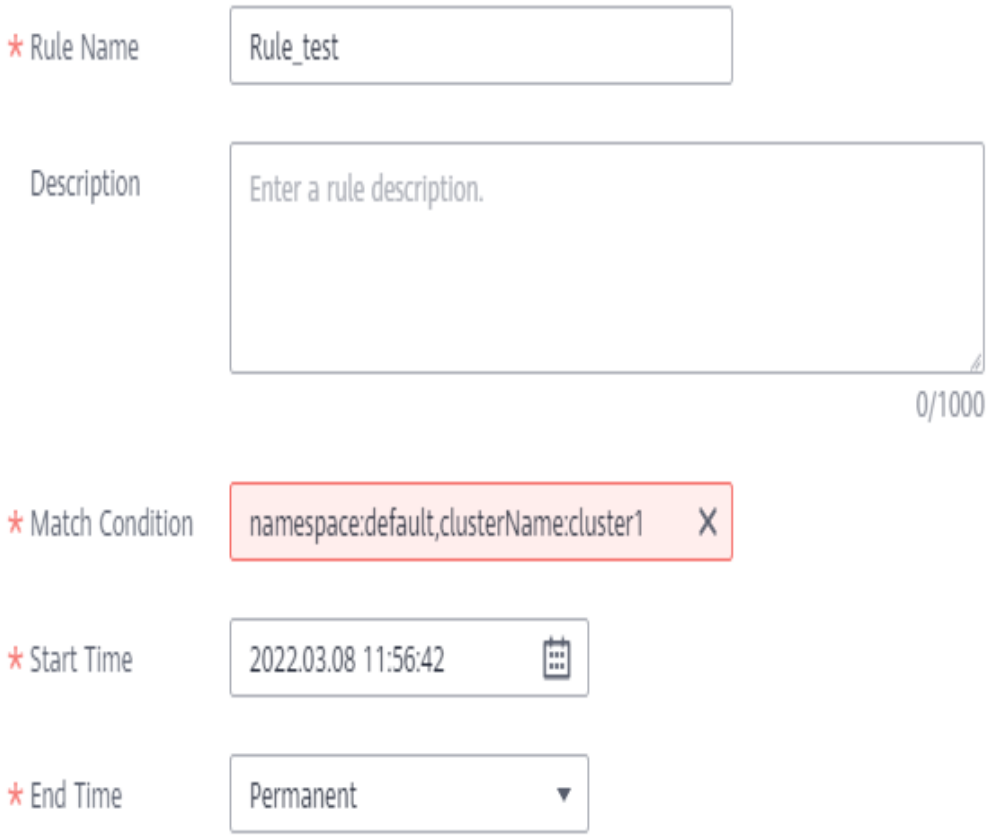
AOM supports alarm silence. You can shield alarm notifications in a specified period. A silence rule takes effect immediately after it is created.

Creation Method

Step 1 Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Alarm Noise Reduction** and click the **Silence Rules** tab. On the displayed page, click **Create**.

Step 2 Set information such as **Rule Name** and **Match Condition**.

Figure 6-33 Creating a silence rule



NOTE

Any alarm notifications that meet the match condition will be shielded. You can set a match condition in one of the following formats:

- "key1:value1,key2:value2". Match the value corresponding to the key to determine a suppressed object.
- "key1,key2". Match the key to determine the suppressed object. All values under the key are covered.
- "key1,key2,key3:value3". Determine the suppressed object by using the preceding two methods.

  "key:value" pairs must be separated by commas (,). The relationship between "key:value" pairs is "AND". That is, all conditions specified by setting "key:value" pairs must be met.

The "key:value" pairs in the match condition are obtained from **metadata** in the alarm message body. Example:

```
{
   "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"
 },
"annotations" : {
      "alarm_probableCause_en_us": " Possible causes",
      "alarm_fix_suggestion_en_us": "Handling suggestion"
 }
}
```

Step 3 Click **OK**.

----End

More Operations

After creating a silence rule, perform the operations listed in **Table 6-18** if needed.

Table 6-18 Related operations

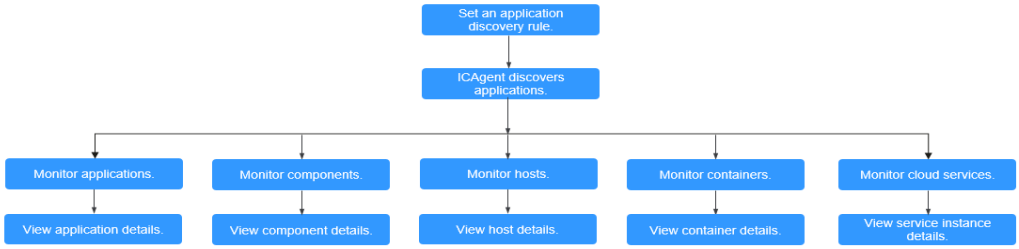
Operation	Description
Modifying a silence rule	Click **Modify** in the **Operation** column.
Deleting a silence rule	• To delete a single rule, click **Delete** in the **Operation** column in the row that contains the rule, and then click **Yes** on the displayed page. • To delete one or more rules, select them, click **Delete** above the rule list, and then click **Yes** on the displayed page.
Searching for a silence rule	Enter a rule name in the search box in the upper right corner and click .

7 Resource Monitoring

7.1 Resource Monitoring Description

For the applications that meet **Built-in Discovery Rules**, they will be automatically discovered after the ICAgent is installed. For the applications that cannot be discovered using built-in rules, customize your own rules.

Figure 7-1 Resource monitoring process



7.2 Application Monitoring

An application is a group of identical or similar components divided based on service requirements. Applications are categorized into system applications and custom applications. The former are discovered based on built-in rules while the latter are discovered based on custom rules.

Applications are defined to facilitate component O&M. The definition methods of applications are as follows:

On the application discovery page of AOM, configure information to create an application. For details, see **Configuring Application Discovery Rules**. You can customize an application name or add a system application name.

Procedure

Step 1 In the navigation pane, choose **Monitoring** > **Application Monitoring**.

NOTE

Set filter criteria above the application list to filter applications.

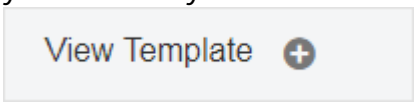
Step 2 Click an application. On the details page that is displayed, manage and monitor components in batches by application.

You can also view the component list, host list, and alarm analysis result of the current application.

Step 3 During routine O&M, you can monitor various metrics of applications on the **View Monitor Graphs** tab page.

- **Creating a view template**

  AOM provides default view templates (such as **Application Template**) that you can modify. You can also click the plus sign (+) in

  to customize a view template.

- **Adding a metric graph**

  – You can click  to add a line graph or 

  to add a digit graph to the view template. You can also delete, move, and copy metric graphs in the view template. For details, see **Dashboard**.

- **Adding to a dashboard**

  On the application details page, click the **View Monitor Graphs** tab, and choose **More** > **Add To Dashboard** in the upper right corner to add the view template to the dashboard for monitoring.

Step 4 Perform the following operations if needed:

- **Adding an application**

  For identical or similar components that are discovered by default discovery rules or that are not installed with Application Performance Management (APM) probes, you can group them logically, that is, add them to the same application for monitoring.

  In the upper right corner of the **Application Monitoring** page, click **Create Application**. On the displayed page, add a custom application discovery rule. For details, see **Configuring Application Discovery Rules**. You can monitor the application after adding it. AOM can display O&M information by component. For details, see **Component Monitoring**.

----End

7.3 Component Monitoring

Components refer to the services that you deploy, including containers and common processes. For example, a workload on the Cloud Container Engine (CCE) is a component, and the Tomcat running on the VM is also a component.

The component list displays the type, CPU usage, memory usage, and alarm status of each component, helping you learn their running status. You can click a component name to learn more information about the component. AOM supports

drill-down from a component to an instance, and then to a container. By viewing the status of each layer, you can implement dimensional monitoring for components.

Step 1 In the navigation pane, choose **Monitoring** > **Component Monitoring**.

- The component list displays information such as **Component Name**, **Status**, **Application**, **Deployment Mode**, and **Application Discovery Rules**.
- Click  in the upper right corner and select **Hide system component**.
- Set filter criteria above the component list to filter components.

Step 2 Perform the following operations as required:

- **Adding an alias**

  If a component name is complex and difficult to identify, you can add an alias for the component.

  Click **Add alias** in the **Operation** column to add an alias.

- **Adding a tag**

  Tags are identifiers of components. You can distinguish system components from non-system ones 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). You can click  in the upper right corner to select or deselect **Hide system component**. In addition, AOM allows you to customize tags to facilitate component management.

  In the component list, click **Add tags** in the **Operation** column of the component, enter a tag, click  and **OK** to add a tag. You can also mark the component as a system component.

  NOTE

  - The **Tags** column of the component list is hidden by default. You can click  in the upper right corner and select or deselect **Tags** to show or hide tags.
  - **Application Discovery Rules**:
    - **Sys_Rule**: AOM automatically discovers components based on the built-in application discovery rule named **Sys_Rule**. For details, see **Built-in Discovery Rules**.
    - **Default_Rule**: AOM automatically discovers components based on the built-in application discovery rule named **Default_Rule**. For details, see **Built-in Discovery Rules**.
    - Custom rules: Their names are customized and not fixed. Applications are discovered based on custom rules.

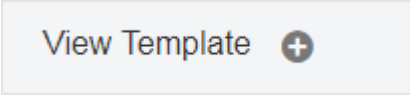
Step 3 Set filter criteria to search for the desired component.

Step 4 Click the component name. The **Component Details** page is displayed.

- On the **Instance List** tab page, view the instance details.

NOTE

Click an instance name to monitor the resource usage and health status.

- On the **Host List** tab page, view the host details.
- On the **Alarm Analysis** tab page, view the alarm details.
- Click the **View Monitor Graphs** tab to monitor the metrics of the component.
  - AOM provides default view templates (such as **Service Template**) that can be modified. You can also click the plus sign (+) in 

to customize a view template.
  - You can click  to add a line graph or  to add a digit graph to the view template. You can also delete, move, and copy metric graphs in the view template. For details, see **Dashboard**.

  a. On the component details page, click the **View Monitor Graphs** tab, and choose **More** > **Add To Dashboard** in the upper right corner to add the view template to the dashboard for monitoring.

----End

7.4 Host Monitoring

Hosts include the Elastic Cloud Server (ECS) and Bare Metal Server (BMS). AOM monitors the hosts purchased during Cloud Container Engine (CCE) or ServiceStage cluster creation and those directly purchased. Ensure that hosts meet operating system (OS) and version requirements, and the ICAgent is installed on them according to **Installing the ICAgent**. Otherwise, these hosts cannot be monitored by AOM. In addition, the hosts support both IPv4 and IPv6 addresses.

AOM monitors common system devices such as disks and file systems, and resource usage and health status of hosts and service processes or instances running on them.

Precautions

- A maximum of five tags can be added to a host, and each tag must be unique.
- The same tag can be added to different hosts.
- For hosts created on the CCE or ServiceStage console, you cannot select clusters or create aliases for them.
- 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, and power off or shut down of the host, or a threshold alarm is reported on the host.

Procedure

Step 1 In the navigation pane, choose **Monitoring** > **Host Monitoring**.

To view the host list more easily, you can:

- Click  in the upper right corner and select **Hide master host**.
- Set filter criteria above the host list to filter hosts.

Step 2 Perform the following operations as required:

- **Adding an alias**

  If a host name is too complex, you can add a simple alias.

  In the host list, click **Add alias** in the **Operation** column.

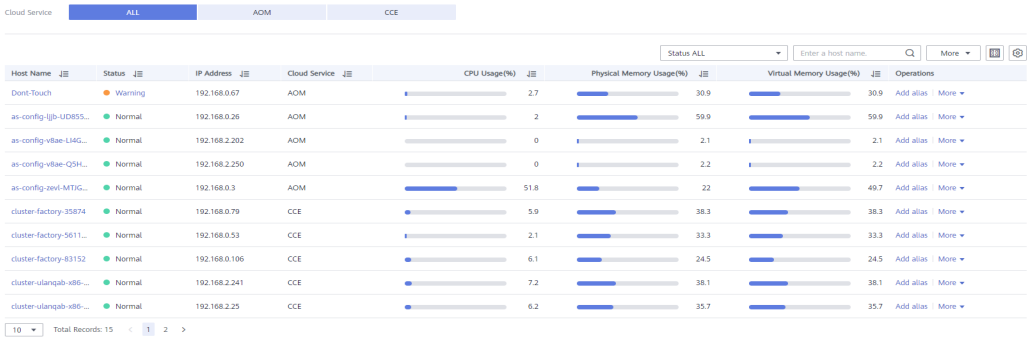
- **Adding a tag**

  A tag is the identifier of a host. You can manage and classify hosts by tag. After a tag is added, you can quickly identify, select, or search for a host.

  In the host list, choose **More** > **Add tags** in the **Operation** column, enter a tag, and click  and **OK**. The **Tags** column of the host list is hidden by default. You can click  in the upper right corner and select or deselect **Tags** to show or hide tags.

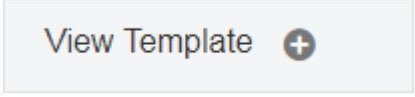
Step 3 Set filter criteria to search for the desired host.

Figure 7-2 Host list



Step 4 Click the host name to enter the **Host Details** page. In the instance list, monitor the resource usage and health status of instances. In addition, click the **View Monitor Graphs** tab to monitor the metrics of the host.

- **Creating a view template**

  AOM provides default view templates (such as **Host Template**) that you can modify. You can also click the plus sign (+) in 

to customize a view template.

- **Adding a metric graph**

  – You can click  to add a line graph or  to add a digit graph to the view template. You can also delete, move, and copy metric graphs in the view template. For details, see **Dashboard**.

- **Adding to a dashboard**

  On the host details page, click the **View Monitor Graphs** tab, and choose **More** > **Add To Dashboard** in the upper right corner to add the view template to the dashboard for monitoring.

Step 5 Monitor common system devices such as the GPU and NIC of the host.

- Click the **GPUs** tab to view the basic information about the GPU of the host. Click a GPU to monitor its metrics on the **View Monitor Graphs** page.
- Click the **NIC** tab to view the basic information about the NIC of the host. Click a NIC to monitor its metrics on the **View Monitor Graphs** page.
- Click the **Disks** tab to view the basic information about the disk of the host. Click a disk to monitor its metrics on the **View Monitor Graphs** page.
- Click the **File System** tab to view the basic information about the file system of the host. Click a disk file partition to monitor its metrics on the **View Monitor Graphs** page.
- Click the **Alarm Analysis** tab to view the alarm details.

  NOTE

  Disk partitions are supported by CentOS 7.x and EulerOS 2.5.

----End

7.5 Container Monitoring

Container and component monitoring differs in their monitored objects. For component monitoring, workloads deployed using Cloud Container Engine (CCE), applications created using ServiceStage, and components deployed on Elastic Cloud Server (ECS) or Bare Metal Server (BMS) are monitored. For container monitoring, only workloads deployed using CCE and applications created using ServiceStage are monitored. For details, see **Component Monitoring**.

7.6 Metric Monitoring

The **Metric Monitoring** page displays metric data of each resource. You can monitor metric values and trends in real time, and create threshold rules for desired metrics. In this way, you can monitor services in real time and perform data correlation analysis.

Procedure

Step 1 In the navigation pane, choose **Monitoring** > **Metric Monitoring**.

Step 2 Select metrics.

- AP-Singapore, CN-Hong Kong, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN South-Shenzhen: click **Add Metric** and select up to 12 metrics by dimension or resource.

NOTE

A maximum of 100 metric data records can be displayed in a metric graph. If the number of displayed data records exceeds 100, no metrics can be added.

- Regions except AP-Singapore, CN-Hong Kong, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN South-Shenzhen: Enter the component or host name to search, or directly select up to 12 metrics from the resource tree.

Step 3 Set metric parameters according to **Table 7-1**, view the metric graph on the right, and analyze metric data from multiple dimensions.

Table 7-1 Metric parameters

Parameter	Description
Time Range	Time period when metrics are monitored.
Statistical Cycle	Interval at which metric data is collected.
Statistic Method	Method used to measure metrics. **NOTE** The number of samples equals to the count of data points.

----End

More Operations

For AP-Singapore, CN-Hong Kong, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN South-Shenzhen, see **Table 7-2**. For other regions, see **Table 7-3**.

Table 7-2 Related operations

Operation	Description
Hiding metric data	After selecting a metric, click in the **Operation** column to hide the metric data in the current graph.
Adding an alarm rule for a metric	After selecting a metric, click in the **Operation** column to create an alarm rule for it.
Copying metric data	After selecting a metric, click in the **Operation** column to copy the metric data.
Deleting one or more metrics	• To delete a metric, click in the **Operation** column. • To delete one or more metrics, select them and click **Delete** above the metric list.

Table 7-3 Related operations

Operation	Description
Adding a metric graph to a dashboard	Select a metric and click **Add to Dashboard** to add the metric graph to the dashboard.
Adding a threshold rule for a metric	After selecting a metric, click in the **Operation** column to create a static threshold rule for it.
Exporting a monitoring report	Click **Export Report** to export a metric graph as a CSV file to your local PC.
Deleting a metric	Click in the row where the metric is located.

7.7 Cloud Service Monitoring

AOM shows you the last six months of performance data curves to help you monitor your cloud service instances.

Currently, the following cloud services can be monitored:

Elastic Load Balance (ELB), Virtual Private Cloud (VPC), Relational Database Service (RDS), Distributed Cache Service (DCS), Elastic Volume Service (EVS), Object Storage Service (OBS), Document Database Service (DDS), Scalable File Service (SFS), Simple Message Notification (SMN), Distributed Message Service (DMS), Data Ingestion Service (DIS), Cloud Stream Service (CS), Distributed Database Middleware (DDM), API Gateway, Graph Engine Service (GES), CloudTable, Cloud Data Migration (CDM), Data Warehouse Service (DWS), and IoT Device Access (IoTDA).

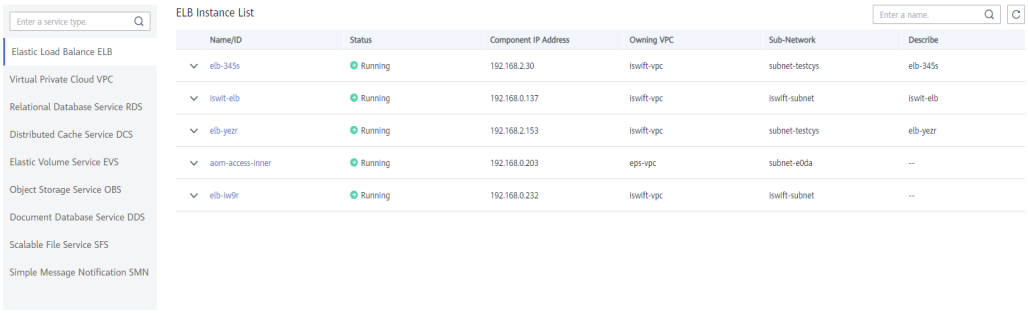
NOTE

IoTDA monitoring is supported only in AP-Singapore, CN-Hong Kong, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN South-Shenzhen.

Monitoring Cloud Service Status

After purchasing cloud services, you can monitor their status and other information on the **Cloud Service Monitoring** page of AOM without installing additional plug-ins.

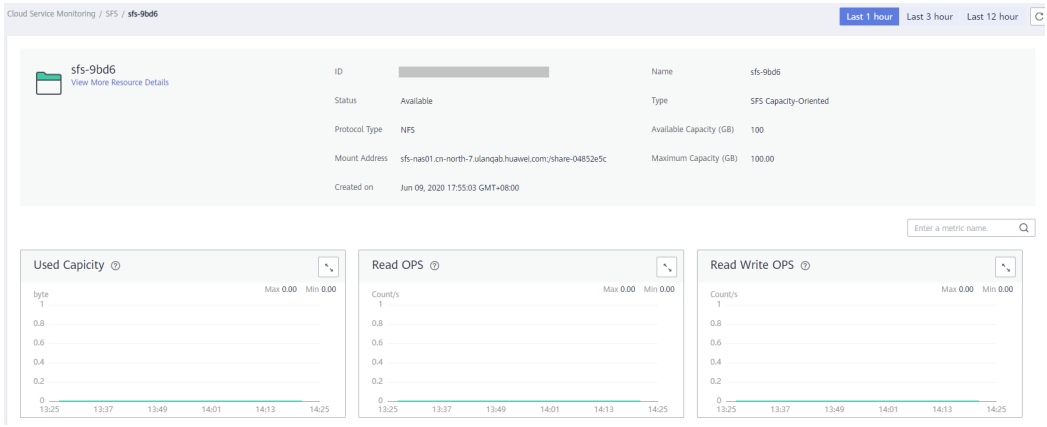
Figure 7-3 Monitoring cloud service status



Monitoring Cloud Service Metrics

Click a desired cloud service name. The service details page is displayed. You can view the metric graphs of the service.

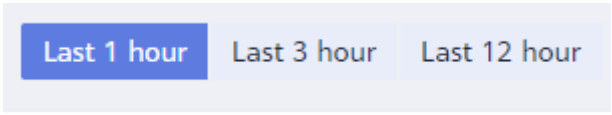
Figure 7-4 Monitoring cloud service metrics



You can also perform the following operations:

- In the upper right corner of a metric graph, click  to enlarge the graph.
- In the upper right corner of the page, set a time range to view data.

  Figure 7-5 Specifying different time segments

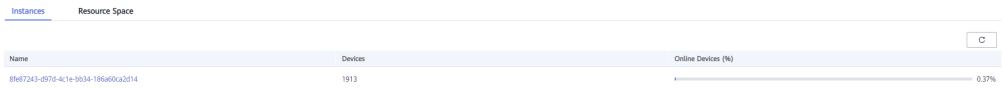
- Click **View More Resource Details** to go to the console of the corresponding service, as shown in the following figure.

  Figure 7-6 Viewing more resource details

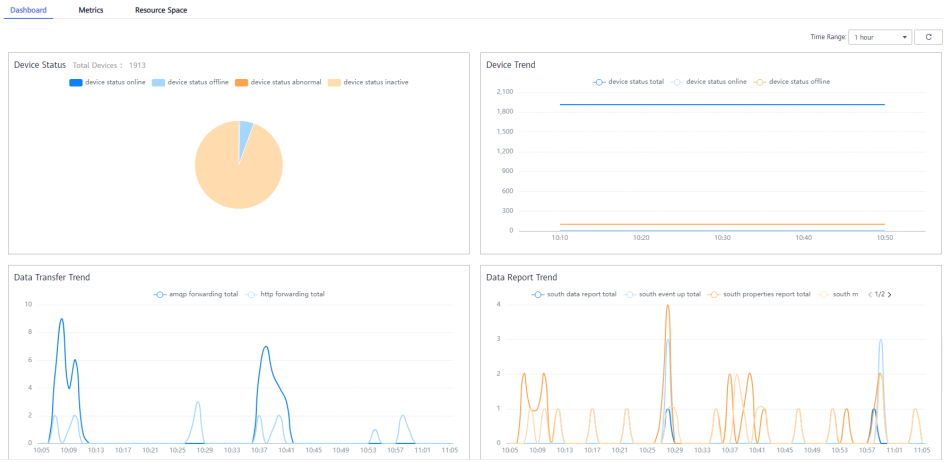
  

Monitoring IoTDA

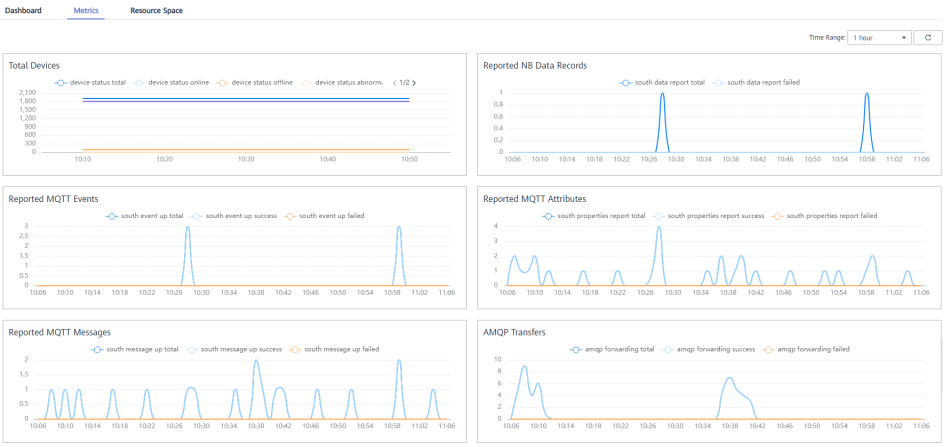
- Click the IoTDA service name. All instances and their resource spaces of your IoTDA service are displayed in the right pane.



- To monitor an IoTDA service instance, do as follows:
  - Click an instance name and click the **Dashboard** tab to view the key resources or metrics of the current instance.



  - Click an instance name and click the **Metrics** tab to view the curves of all reported metric data of the current instance.



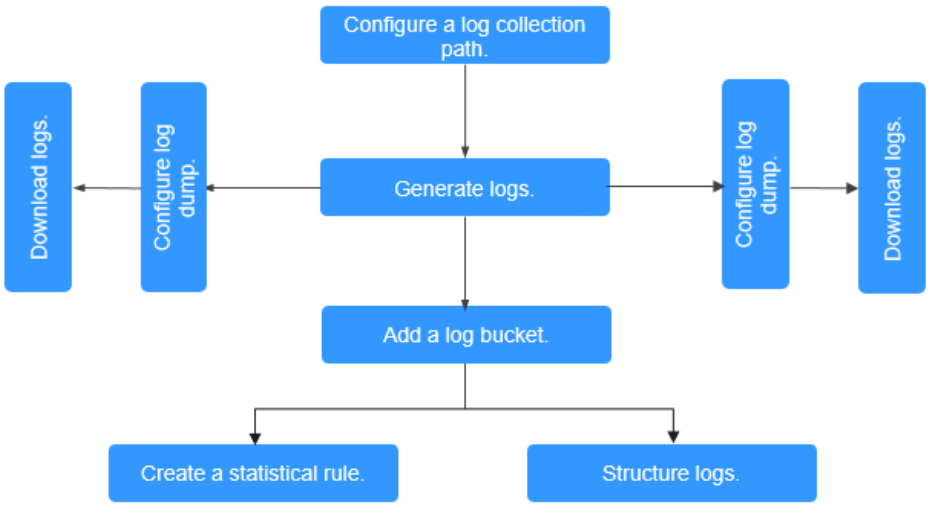
  - Click an instance name and click the **Resource Space** tab to view the resource space of the current instance.

8 Log Management

8.1 Log Management Description

AOM can collect and display container and VM logs. VM refers to an Elastic Cloud Server (ECS) or a Bare Metal Server (BMS) running Linux. Before collecting logs, ensure that you have configured a log collection path according to **Configuring Log Collection Paths**.

Figure 8-1 Log management process



8.2 Searching for Logs

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

Step 1 In the navigation pane, choose **Log** > **Log Search**.

Step 2 On the **Log Search** page, click the **Component**, **System**, or **Host** tab and set filter criteria as prompted.

NOTE

1. Enter a keyword between two adjacent delimiters for exact search. By **configuring delimiters**, you can divide the log content into multiple words and then enter these words to search for logs. If you are not sure whether there are adjacent delimiters, enter a keyword for fuzzy search.
2. Enter a keyword for fuzzy search. The keyword cannot start with an asterisk (*) or a question mark (?). For example, enter **ER?OR** or **ER*R**.
3. Enter content containing search operators AND (&&) or OR (||). For example, enter **query logs&&erro*** or **query logs||error**.

Step 3 View the search result of logs.

The search results are sorted based on the log collection time, and keywords in them are highlighted. You can click in the **Time** column to switch the sorting order.

indicates the default order. indicates the ascending order by time (the earliest log is displayed at the top). indicates the descending order by time (the latest log is displayed at the top).

1. Click on the left of the log list to view details.
2. AOM allows you to view the previous or next logs of a specified log by clicking **View Context** in the **Operation** column, facilitating fault locating. Therefore, you do not need to search for logs in raw files.
   - In the **Display Rows** drop-down list, set the number of rows that display raw context data of the log.

     NOTE

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

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

NOTE

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

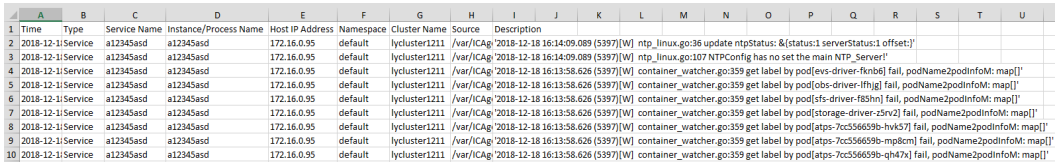
Step 4 (Optional) Click in the upper right corner on the **Log Search** page, select the file format, and export the search result to the local PC.

Logs are sorted according to the order set in **Step 3** 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 log content, host IP

address, and source can be exported, as shown in **Figure 8-2**. If you select the TXT format, only log content can be exported, as shown in **Figure 8-3**. Each row represents a log. If a log contains a large amount of content, you are advised to view the log using a text editor.

Figure 8-2 Exporting logs in CSV format



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1	Time	Type	Service Name	Instance/Process Name	Host IP Address	Namespace	Cluster Name	Source	Description												
2	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	'2018-12-18 16:14:09.089 (5397)[W] ntp_linux.go:36 update ntpStatus: &{status:1 serverStatus:1 offset:}'												
3	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	'2018-12-18 16:14:09.089 (5397)[W] ntp_linux.go:107 NTPConfig has no set the main NTP_Server!'												
4	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	'2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[evs-driver-fknb6] fail, podName2podInfoM: map[]'												
5	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	'2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[obs-driver-lfhjg] fail, podName2podInfoM: map[]'												
6	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	'2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[sfs-driver-f85hn] fail, podName2podInfoM: map[]'												
7	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	'2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[storage-driver-z5rv2] fail, podName2podInfoM: map[]'												
8	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	'2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[atps-7cc556659b-hvk57] fail, podName2podInfoM: map[]'												
9	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	'2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[atps-7cc556659b-mp8cm] fail, podName2podInfoM: map[]'												
10	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	'2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[atps-7cc556659b-qh47x] fail, podName2podInfoM: map[]'												

Figure 8-3 Exporting logs in TXT format

```
2018-12-18 16:14:09.089 (5397)[W]  ntp_linux.go:36 update ntpStatus: &{status:1 serverStatus:1 offset:}
2018-12-18 16:14:09.089 (5397)[W]  ntp_linux.go:107 NTPConfig has no set the main NTP_Server!
2018-12-18 16:13:58.626 (5397)[W]  container_watcher.go:359 get label by pod[evs-driver-fknb6] fail, podName2podInfoM: map[]
2018-12-18 16:13:58.626 (5397)[W]  container_watcher.go:359 get label by pod[obs-driver-lfhjg] fail, podName2podInfoM: map[]
2018-12-18 16:13:58.626 (5397)[W]  container_watcher.go:359 get label by pod[sfs-driver-f85hn] fail, podName2podInfoM: map[]
2018-12-18 16:13:58.626 (5397)[W]  container_watcher.go:359 get label by pod[storage-driver-z5rv2] fail, podName2podInfoM: map[]
2018-12-18 16:13:58.626 (5397)[W]  container_watcher.go:359 get label by pod[atps-7cc556659b-hvk57] fail, podName2podInfoM: map[]
2018-12-18 16:13:58.626 (5397)[W]  container_watcher.go:359 get label by pod[atps-7cc556659b-mp8cm] fail, podName2podInfoM: map[]
2018-12-18 16:13:58.626 (5397)[W]  container_watcher.go:359 get label by pod[atps-7cc556659b-qh47x] fail, podName2podInfoM: map[]
2018-12-18 16:13:58.626 (5397)[W]  container_watcher.go:359 get label by pod[atps-7cc556659b-pjdhv] fail, podName2podInfoM: map[]
```

----End

8.3 Viewing Log Files

You can quickly view log files of component instances to locate faults.

Step 1 In the navigation pane, choose **Log** > **Log Files**.

Step 2 On the page that is displayed, click the **Component** or **Host** tab and click a component or host name. Information such as the log file name and latest written time is displayed in the log file list on the right.

Step 3 Click **View** in the **Operation** column of the desired instance. **Table 8-1** describes how to view log file details. **Figure 8-5** shows log file details.

Table 8-1 Operations

Operation	Setup	Description
Setting a time range	Date	Click  to select a date.
	Time range	Click the desired time on the time axis to set a time range. You can select only one unit (5 minutes) each time.
Viewing log files	Clear	Click **Clear** to clear the logs displayed on the screen. Logs displayed on the screen will be cleared, but will not be deleted.

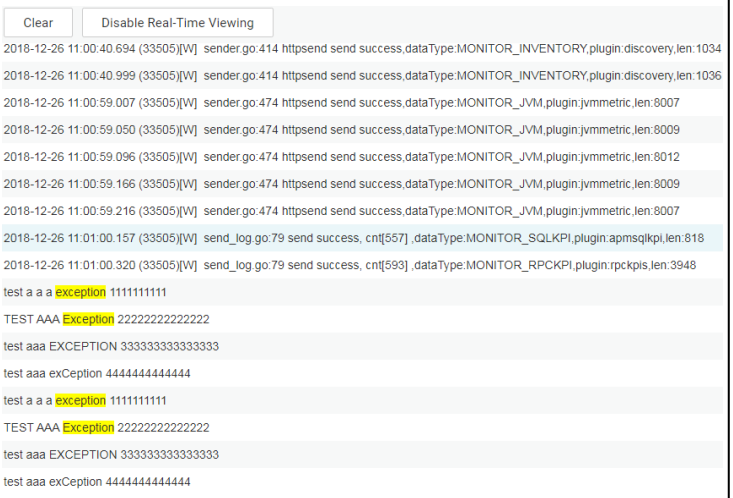
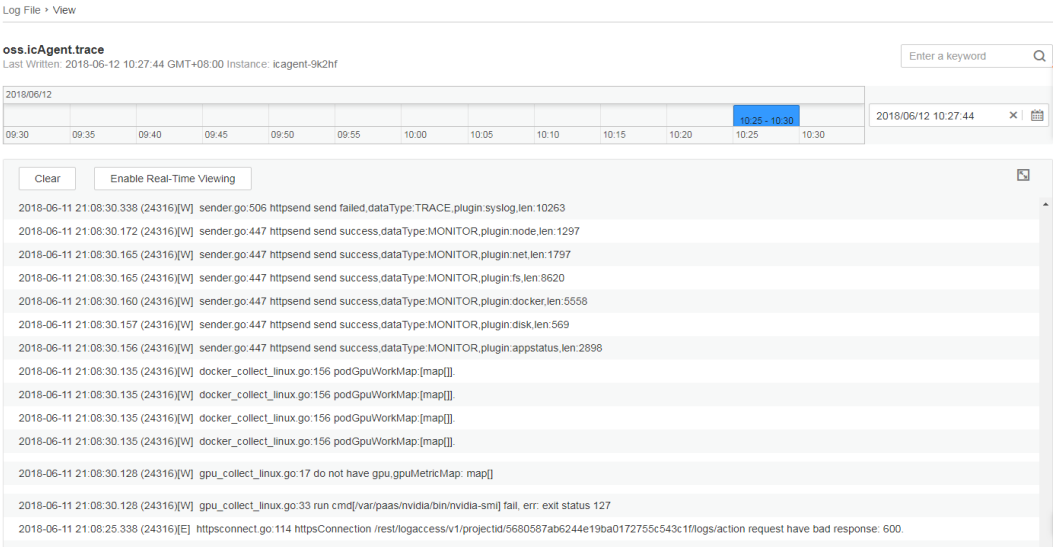
Operation	Setup	Description
	Viewing real-time logs	The real-time monitoring function is disabled by default. You can click **Enable Real-Time Viewing** as required. After this function is enabled, the latest written logs can be viewed. The **exception** in the log records the exceptions that occur during code running. When using logs to locate faults, pay attention to the **exception**. For real-time log viewing, AOM automatically highlights exception keywords in logs, facilitating fault locating. Such keywords are case-sensitive. For example, **exception** and **Exception** are highlighted, but keywords such as **EXCEPTION**, **exCeption**, and **EXception** are not highlighted, as shown in the following figure. **Figure 8-4** Viewing real-time logs 
	Maximized display	Click  to maximize a page. Components like the time axis are invisible on the screen. Click  again to cancel the maximized display.

Figure 8-5 Log file details



----End

8.4 Viewing Bucket Logs

AOM supports fine-grained log query. That is, you can view logs by bucket to obtain key service data and quickly locate problems.

Currently, in CN North-Beijing1, CN East-Shanghai2, and CN South-Guangzhou regions, you can query logs from multiple dimensions. You can query and analyze original logs, as well as structured logs based on SQL syntax.

Precautions

- Before viewing bucket logs, ensure that you have created at least one log bucket. Otherwise, you cannot view bucket logs.
- You can view bucket logs generated in the last seven days.

Viewing Original Logs

Step 1 Log in to the AOM console. In the navigation pane, choose **Log** > **Log Buckets**, and click the **Bucket Log** tab to view logs.

Step 2 Set filter criteria.

- **Select a log bucket**: Select a target log bucket from the drop-down list in the upper left corner.
- **Set a time range**: In the drop-down list in the upper right corner, select a time range, such as **Last 30 minutes**, **Last 1 hour**, or **Last 6 hours**. You can also select **Custom time range** to specify the start time and end time.
- **Enter a keyword**: Click the text box. All statistical rules and keywords of the bucket are displayed under the text box. Select a keyword. It is automatically displayed in the text box. Alternatively, enter a keyword directly in the text box.

NOTE

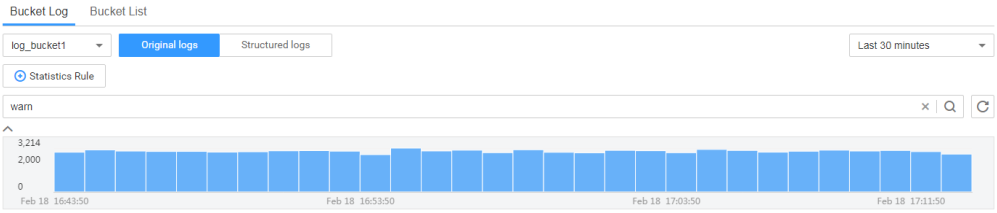
For common and complex keywords, click Statistics Rule and create statistical rules according to **Creating Statistical Rules**. In the subsequent query, you do not need to manually enter a keyword in the text box. Instead, you can directly click the text box and select a desired statistical rule and keyword. After a statistical rule is created, AOM counts the number of keywords and generates metrics accordingly. You can then monitor the metrics on the **Metric Monitoring** page.

Step 3 View the search result.

- **Viewing statistical data in a bar chart**

  The bar chart shows the number of logs that met the filter criteria set in step **Step 2** in different time periods. The horizontal axis represents the time and is divided into 30 rectangular blocks of the same size. The time duration indicated by each rectangle block is **selected time range/30**. For example, if the time range is 30 minutes, the time duration of each rectangle block is 1 minute. If the time range is set to 60 minutes, the time duration of each rectangle block is 2 minutes. The vertical axis represents the number of queried logs.

  Figure 8-6 Viewing statistical data in a bar chart

  When you hover over a rectangle block, the prompt displays the time range (start time and end time) and the number of logs that meet the filter criteria within the time range. When you click a rectangle block, the log list displays corresponding log details. To deselect the block, click .

- **Viewing log details in a log list**

  The log list displays the details of the logs that meet the filter criteria set in step **Step 2**.

  Figure 8-7 Viewing log details in a log list

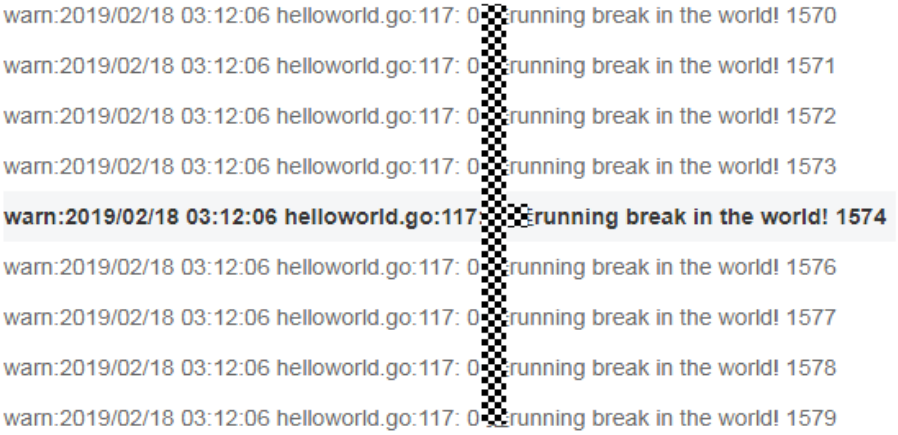
  

  You can also perform the following operations:

  – Click to view details of a selected log, such as the host IP address and source.

- Sort search results: Logs are sorted based on collection time in descending order by default. You can click in the **Collection Time** column to change the order. When you click the black triangle icon to sort logs by time in ascending order, the latest log is displayed at the end. When you click the black triangle icon to sort logs by time in descending order, the latest log is displayed at the top.
- View the context of a specified log: AOM allows you to view the previous or next logs of a specified log by clicking **View Context** in the **Operation** column, facilitating fault locating. Therefore, you do not need to search for logs in raw files.

  Figure 8-8 Viewing the context of a specified log



- Perform log structuring: Click **Structure** in the **Operation** column and use this log as an example log to structure all logs in the bucket. For details, see Structuring Original Logs.

----End

Viewing Structured Logs

NOTICE

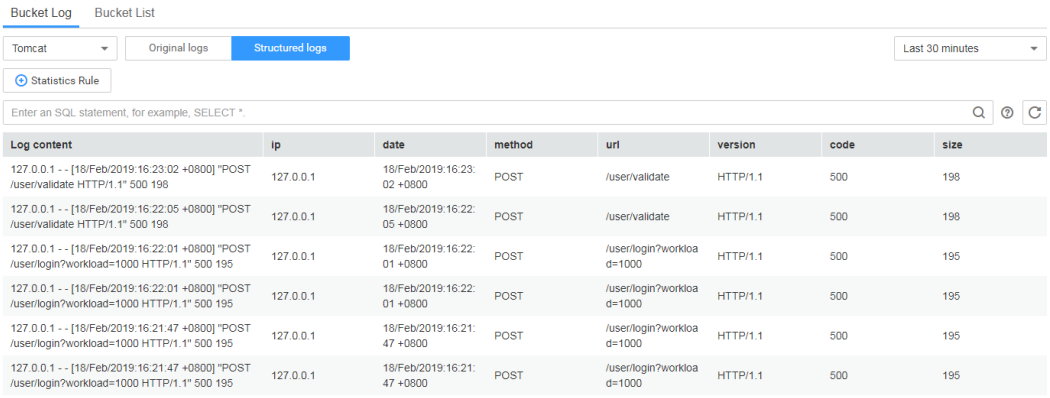
- This function only applies to CN North-Beijing1, CN East-Shanghai2, and CN South-Guangzhou regions.
- Before viewing structured logs, you need to structure original logs by adding extraction rules. Then you can query and analyze structured logs based on SQL syntax. For details, see Structuring Original Logs.
- After log structuring, wait about 1–2 minutes for SQL query and analysis.

The following shows how to locate faults in the Tomcat server through SQL query and analysis.

Step 1 Log in to the AOM console. In the navigation pane, choose **Log** > **Log Buckets**.

Step 2 Because SQL query is performed by log bucket, select a target log bucket on the **Bucket Log** tab page and click **Structured logs**.

Figure 8-9 Structured logs



Step 3 SQL query and analysis: Set a time range and filter criterion. Enter an SQL statement in the search box. For details about SQL statements supported by AOM, see SQL Query Syntax.

For example, to query the number of requests whose HTTP return code is greater than or equal to 500 in the last six hours, perform the following operations:

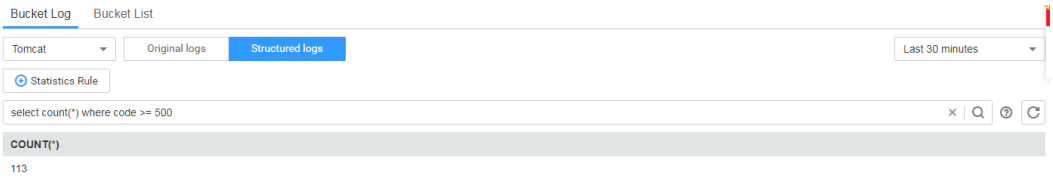
Select **Last 6 hours** from the drop-down list in the upper right corner and enter an SQL statement, such as **select count(*) where code >= 500** in the search box, as shown in **Figure 8-10**.

NOTE

- For common and complex SQL statements, click 

to create statistical rules. For details, see **Creating Statistical Rules**. In the subsequent query, you do not need to manually enter a keyword in the text box. Instead, you can directly click the text box and select a desired statistical rule and SQL statement. After statistical rules are created, AOM collects statistics on values returned by SQL statements and generates metrics. You can view the data trend in a metric graph.
- For the SQL statement which returns a single value, for example, **select count(*) where code >= 500**, statistical rules can be created. For the SQL statement which returns multiple values, for example, **select count(*) group by ip**, statistical rules cannot be created.

Figure 8-10 Using SQL statements to query data



----End

8.5 Adding Log Dumps

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

AOM offers both periodical and one-off dump modes. Select a model suited to your requirements.

- **Periodical dump**: Dump current logs in real time into an OBS bucket, divide 1-day logs based on the dump cycle, and dump logs of the same time segment into corresponding log files.

  To store logs for a long time, add a periodical dump. 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 there are a large number of logs and the export function cannot meet your needs, dump specified logs at one time according to **Adding One-Off Dumps**.

Adding Periodical Dumps

For example, 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 console. In the navigation pane, choose **Log** > **Log Dumps**.

Step 2 Click **Add Log Dump** in the upper right corner of the page. Then, set parameters according to **Table 8-2** and click **OK**.

Table 8-2 Periodical dump parameters

Parameter	Description	Example
Dump Mode	Options: **One-off dump** and **Periodical dump**.	Periodical 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. **NOTE** After a dump task is deleted, log groups will also be deleted.	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 that store logs. **NOTE** You must create an OBS bucket first. Click **View OBS** to create a bucket on the OBS console.	obs-store-test
OBS Bucket Directory	OBS bucket directory for storing logs.	/home/Periodical Dump

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

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

NOTE

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

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

Step 3 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 OBS console.
2. In the navigation pane, choose **Objects** and then click the **Objects** tab. On the page that is displayed, find the log files stored in the OBS bucket, 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 depend on the selected log types, as shown in **Table 8-3**.

Table 8-3 Paths of the log files dumped to the OBS bucket

Log Type	Log File Path
Component	**Bucket directory** > **Log group name** > **Cluster name** > **Component name** > **Log collection date** (format: **YYYY-MM-DD**) > **File ID** (format: **0X**) For example, **obs-store-test** > **home** > **Periodical Dump** > **log-group1** > **zhqtest0112n** > **als0320a** > **2019-03-22** > **03**.
Host	**Bucket directory** > **Log group name** > **CONFIG_FILE** > **default_appname** > **Log collection date** (format: **YYYY-MM-DD**) > **File ID** (format: **0X**)
System	**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, click **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 console. In the navigation pane, choose **Log** > **Log Dumps**.

Step 2 Click **Add Log Dump** in the upper right corner of the page. Then, set parameters according to **Table 8-4** and click **OK**.

Table 8-4 One-off dump parameters

Parameter	Description	Example
Dump Mode	Options: **One-off dump** and **Periodical dump**.	One-off dump

Parameter	Description	Example
Filter Criteria	Logs can be filtered by multiple criteria such as log collection time, log type, or namespace, so that you can dump the logs that meet specified criteria.	Set the log collection time to **Last 30 minutes**, select the **als0320a** component, and set the keyword to **warn**.
Log Group	Logs can be categorized into logical groups, so that you can dump them based on groups. **NOTE** After a dump task is deleted, log groups will also be deleted.	log-group2
Target OBS Bucket	OBS bucket that store logs. **NOTE** If no OBS bucket is available, click **View OBS** to create a bucket on the OBS console.	obs-store-test
OBS Bucket Directory	OBS bucket directory for storing logs. **NOTE** If this parameter is not set, 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 3 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 in the OBS console.
2. In the navigation pane, choose **Objects** and then click the **Objects** tab. On the page that is displayed, find the log files in the 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: The names of the log files depend on the value of **Dump File Format**. The log file is named in the format of "Log group name _shard_0(custom)", for example, **log-group2_shard_0(custom).log**.

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, click **Download As**.

----End

8.6 Creating Statistical Rules

Logs contain information such as system performance and services. For example, the number of the ERROR keywords indicates the system health, and the number of the BUY keywords indicates the service volume. You can create statistical rules to find such information. After statistical rules are created, AOM periodically counts keywords and generates metric data so that you can monitor system performance and service information in real time.

Currently, in CN North-Beijing1, CN East-Shanghai2 and CN South-Guangzhou regions, you can create statistical rules to count both keyword and SQL statistics. The difference lies in their statistical objects. Statistical objects of keywords are original logs and those of SQL statements are structured logs. In addition, statistical rules can only be created for an SQL statement which returns a single value. For example, for the **select count(*) where code >= 500** statement, statistical rules can be created; for the **select count(*) group by ip** statement, statistical rules cannot be created.

Precautions

A statistical rule takes effect by log bucket. Before creating a statistical rule, ensure that at least one log bucket has been created. A maximum of 5 statistical rules can be created for a log bucket.

Procedure

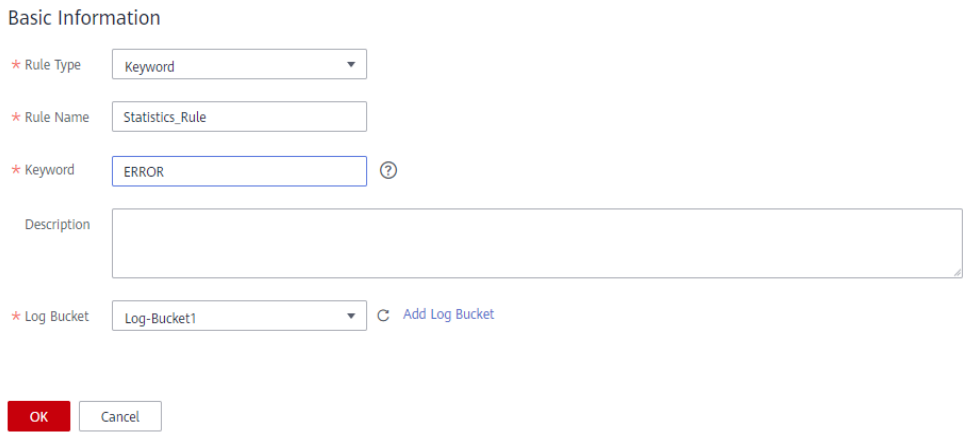
The following shows how to count keywords by creating a statistical rule:

Step 1 Log in to the AOM console. In the navigation pane, choose **Log** > **Statistical Rules**.

Step 2 Click **Create Statistical Rule** in the right corner of the page. Then, select a rule type, set a rule name and keyword, select the created log bucket, and click **OK**, as shown in the following figure.

A statistical rule takes effect by log bucket. AOM will periodically count the number of keywords in log files of a log bucket and generate log metrics.

Figure 8-11 Creating a statistical rule



After a statistical rule is created, a metric named after the rule will be generated.

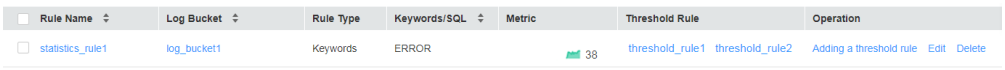
Step 3 (Optional) View the generated metric data.

- Method 1: View the metric data on the **Statistical Rules** page, as shown in **Figure 8-12**.

  The thumbnail of the **Metric** column displays the metric trend of the last hour (the statistical period is one minute). The number after the thumbnail is the last non-empty metric value on the thumbnail.

  To view more detailed metric data, double-click the thumbnail to zoom it in. To view the metric data for a different time, set the time range and statistical period in the upper area of the page. In addition, you can click **Adding a threshold rule** in the upper area of the page to add a threshold rule for the metric. AOM generates a threshold alarm when a metric value reaches the preset threshold so that you can handle exceptions at the earliest time.

  Figure 8-12 Method 1

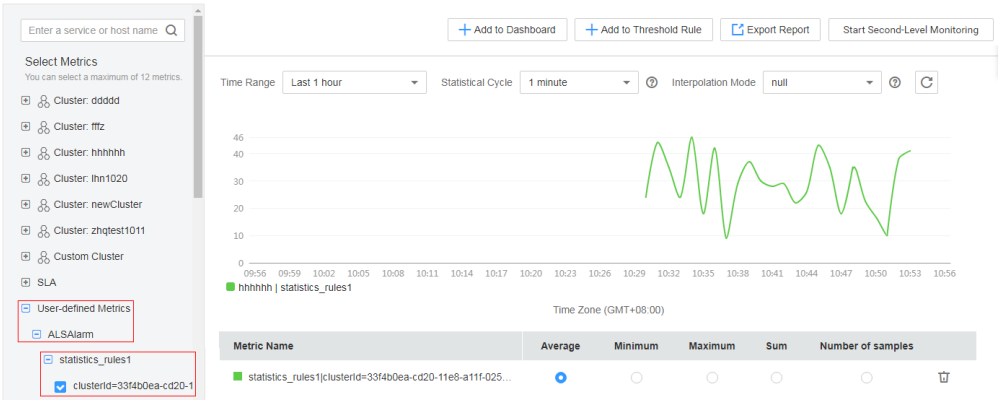
  

- Method 2: View the metric data on the **Metric Monitoring** page, as shown in **Figure 8-13**.

  In the navigation pane, choose **Monitoring** > **Metric Monitoring**. In the metric tree, choose **User-defined Metrics** > **ALSAlarm**, find the metric which is named after the statistical rule, and view the metric trend.

  In the upper right area of the **Metric Monitoring** page, you can add the metric to the dashboard, add a threshold rule, or export a monitoring report.

Figure 8-13 Method 2



----End

More Operations

After creating a statistical rule, perform the operations listed in **More Operations** if needed.

Table 8-5 Related operations

Operation	Description
Viewing a statistical rule	Click a statistical rule in the **Rule Name** column to view its details.
Viewing a threshold rule	The **Threshold Rule** column displays all threshold rules associated with the metrics generated by the statistical rule. Multiple threshold rules are separated by spaces. Click a threshold rule to view its details.
Adding a threshold rule	Click **Adding a threshold rule** in the **Operation** column to add a threshold rule for the metric generated by the statistical rule. AOM generates a threshold alarm when a metric value reaches the preset threshold so that you can handle exceptions at the earliest time.
Modifying a statistical rule	Click **Edit** in the **Operation** column.
Deleting a statistical rule	• To delete a statistical rule, click **Delete** in the **Operation** column. • To delete one or more statistical rules, select them and click **Delete** above the rule list. **NOTE** Deleting a statistical rule will not delete your log buckets or files.

8.7 Accessing LTS

8.7.1 Overview

NOTE

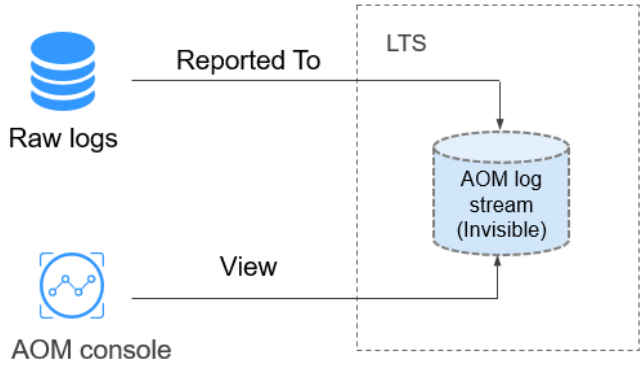
The function of connecting AOM logs to Log Tank Service (LTS) is currently restricted. If you want to use this function, **submit a service ticket**.

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

What Is Mapping?

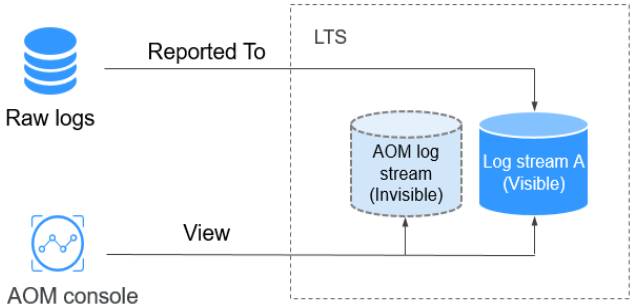
AOM logs exist in LTS in the form of a log stream, as shown in **Figure 8-14**. You can view raw logs in configured log collection paths on AOM, but cannot view the AOM log stream on LTS. You can create a mapping by adding an access rule on AOM. After the mapping is created, you can view and analyze AOM logs on LTS.

Figure 8-14 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 8-15**.

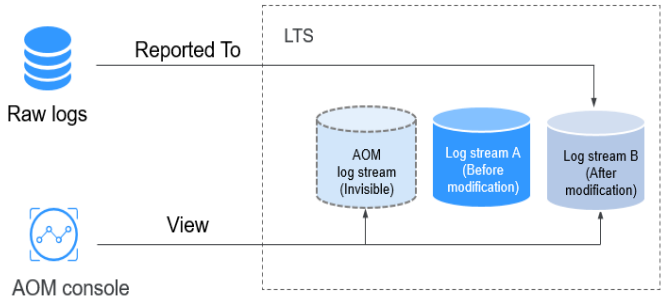
Figure 8-15 After mapping



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 8-16**.

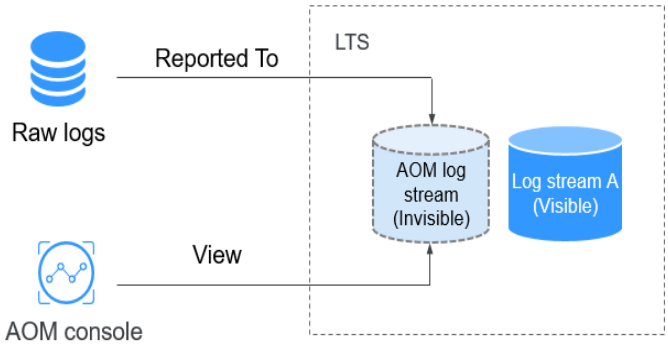
Figure 8-16 Modifying a mapping



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 8-17**. If the access rule is deleted but log stream A is not, you can still view the logs that have already been mapped on LTS.

Figure 8-17 Deleting a mapping



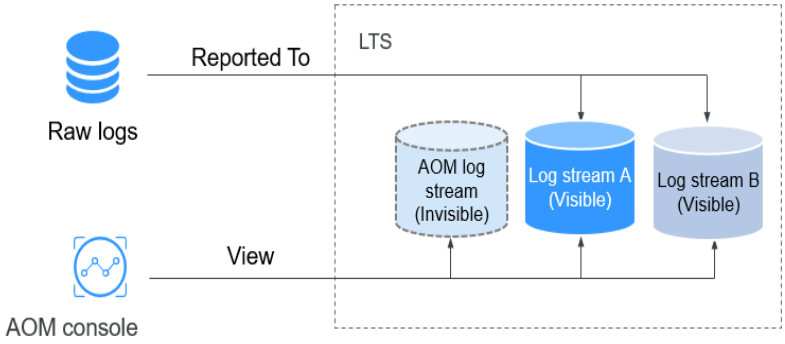
NOTE

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

Duplicate Mapping

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

Figure 8-18 Duplicate mapping



8.7.2 Managing Access Rules

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

Prerequisites

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

Adding 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 console. In the navigation pane, choose **Log** > **Access LTS**.

Step 2 Click **Add Access Rule**.

Step 3 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 custom rule name.
  b. **Cluster**: Select a cluster from the drop-down list.
  c. **Namespace**: Select a namespace from the drop-down list.
  d. **Workload**: Retain the default value **All**.
  e. **Container Name**: Select a container from the drop-down list box.
  f. Set an access rule.
     - **Access all logs**: If you select this option, select a log group and log stream.
     - **Specify log paths**: If you select this option, specify a log path and then select a log group and log stream.

- **Access by Workload**: Logs of the selected workload are connected to the specified log stream.
  a. **Rule Name**: Enter a custom rule name.
  b. **Cluster**: Select a cluster from the drop-down list.
  c. **Namespace**: Select a namespace from the drop-down list.
  d. **Workload**: Select one or more workloads from the drop-down list.
  e. **Container Name**: Select a container from the drop-down list box.
  f. Set an access rule.
     - **Access all logs**: If you select this option, select a log group and log stream.
     - **Specify log paths**: If you select this option, specify a log path and then select a log group and log stream.
- **Automatic Mapping**: Workload logs are automatically connected to the generated log streams with the same names as the workloads.
  a. **Rule Name**: Enter a custom rule name, for example, **test**. **Cluster**: Select a cluster from the drop-down list.
  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. **Access Rule**: Select a log group. A log stream with the same name as the workload is automatically generated. By default, all logs of the selected workload are connected.

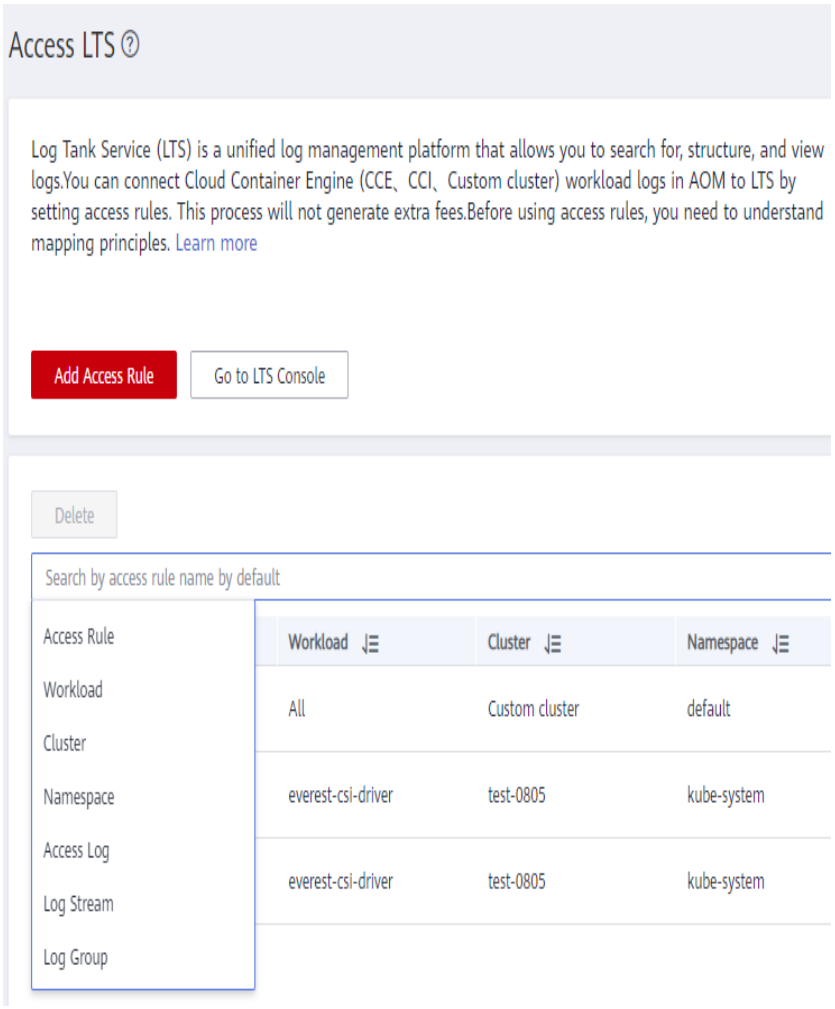
----End

Viewing and Managing Access Rules

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

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

Figure 8-19 Selecting a search dimension



- View

  You can view the created access rules on the **Access LTS** page. Click in the upper right corner of the search box to select the fields to display. Click a log group name in the **Log Group** column to go to the log group details page on the LTS console.

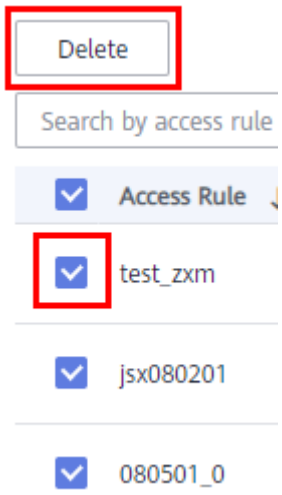
- Edit

  On the **Access LTS** page, click 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 **Access LTS** page, click in the **Operation** column to delete an access rule. You can also select and delete multiple rules in batches.

Figure 8-20 Deleting access rules in batches



NOTE

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

8.8 Container Log Collection Configuration

8.8.1 Adding Custom Tags

NOTE

This function is available only in CN East-Shanghai1.

By adding custom tags, you can view the custom tags on the log page. After AOM logs are connected to LTS, you can enter the keywords of the custom tags to search for logs.

1. **Edit the YAML file**. Specifically, add the following field under **spec:template:metadata:annotations:** in the YAML file of the workload:

   kubernetes.AOM.log.relabel: '{"key1":"value1", "key2":"value2"}

2. Restrictions on custom tags:

   a. A maximum of 16 "key:value" pairs can be set.

   b. The key or value can contain up to 64 characters.

   c. Custom tags are case insensitive and cannot be the same as default tags. For example, if the default tag is **po**, your custom tag cannot be **PO**, **Po**, or **pO**.

   Default tags:

   "podName", "appName", "containerName", "clusterId","clusterName", "serverlessPkg", "serverlessFunc", "projectId", "serviceID","nameSpace", "pid", "hostId", "hostName", "hostIP", "hostIPv6"

8.8.2 Standard Output Configuration

You can add a standard output tag to collect the standard output logs of the corresponding containers in a pod. Add the following field to **spec:template:metadata:annotations:** in the YAML file of the pod to specify the names of the containers whose data is to be collected:

kubernetes.AOM.log.stdout: '["container_name0", "container_name1"]'

The rules are as follows:

1. If the **kubernetes.AOM.log.stdout:** field does not exist, the standard output logs of all containers in the pod are collected by default. This rule is compatible with original scenarios.
2. If this field exists and its value is empty, that is, **kubernetes.AOM.log.stdout: '[]'**, the standard output logs of containers in the pod will not be collected.

Example:

```
spec:
  replicas: 1
  selector:
    matchLabels:
      app: als729
      version: v1
  template:
    metadata:
      creationTimestamp: null
      labels:
        app: als729
        version: v1
      annotations:
        kubernetes.AOM.log.relabel:
'{"key1":"value1","key2":"value2","key3":"value3","key4":"value4","key5":"value5","key6":"value6","key7":"val
ue7","key8":"value8","key9":"value9","key10":"value10","key11":"value11","key12":"value12","key13":"value1
3","key14":"value14","key15":"value16"}'
        kubernetes.AOM.log.stdout: '["container-0","container_name1"]'
```


9 Configuration Management

9.1 ICAgent Management (HUAWEI CLOUD Host)

9.1.1 Installing the ICAgent

ICAgent is used to collect metrics, logs, and application performance data. For servers that are directly purchased on the Elastic Cloud Server (ECS) or Bare Metal Server (BMS) console, manually install the ICAgent. For hosts purchased through Cloud Container Engine (CCE), the ICAgent is automatically installed.

The following table describes the ICAgent status.

Table 9-1 ICAgent status

Status	Description
Running	The ICAgent is running properly.
Uninstalled	The ICAgent is not installed. For details about how to install the ICAgent, see **Installing the ICAgent**.
Installing	The ICAgent is being installed. This operation takes about 1 minute to complete.
Installation failed	Failed to install the ICAgent. Uninstall the ICAgent according to **Uninstalling the ICAgent by Logging In to the Server** and then install it again.
Upgrading	The ICAgent is being upgraded. This operation takes about 1 minute to complete.
Upgrade failed	Failed to upgrade the ICAgent. Uninstall the ICAgent according to **Uninstalling the ICAgent by Logging In to the Server** and then install it again.
Offline	The ICAgent is abnormal due to network problems. Check and restore the network.

Status	Description
Abnormal	The ICAgent is abnormal. Contact technical support.

Prerequisites

Before installing the ICAgent, ensure that the time and time zone of the local browser are consistent with those of the server. If multiple servers are deployed, ensure that the local browser and multiple servers use the same time zone and time. Otherwise, metric data of applications and servers displayed on the UI may be incorrect.

Installation Methods

There are two methods to install the ICAgent. Note that the two methods are not applicable to container nodes created using ServiceStage or CCE. For container nodes, you do not need to manually install the ICAgent. Instead, you only need to perform certain operations when creating clusters or deploying applications.

For details, see **Table 9-2**.

Table 9-2 Installation methods

Method	Scenario
Initial installation	This method is used when the following conditions are met: 1. An Elastic IP Address (EIP) has been bound to the server. 2. The ICAgent has never been installed on the server.
Inherited installation	This method is used when the following conditions are met: You need to install the ICAgent on multiple servers. The ICAgent has been installed on one of the servers. All the servers are in the same VPC. If the servers are not in the same VPC, bind EIPs to them before using this installation method.

Initial Installation

After you apply for a server and install the ICAgent for the first time, perform the following operations:

Step 1 Obtain an Access Key ID/Secret Access Key (AK/SK).

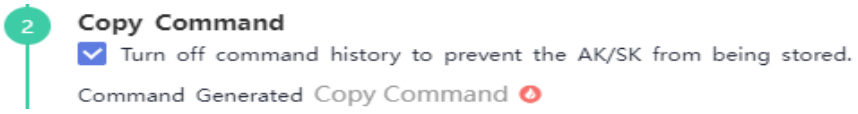
- If you have obtained the AK/SK, skip this step.
- If no AK/SK are available, obtain them first.

Step 2 In the navigation pane, choose **Configuration Management** > **Agent Management**.

Step 3 Select **Other: user-defined nodes**, click **Install ICAgent**, and set **Host** to **HUAWEI CLOUD host**.

Step 4 (Optional) To prevent your AK/SK from being disclosed, select the check box shown in the following figure to disable historical record collection.

Figure 9-1 Copying the ICAgent installation command



Step 5 Generate the ICAgent installation command, and copy and run it to install the ICAgent.

Step 6 After the ICAgent is installed, run the following command to enable historical record collection:

set -o history

NOTE

- If the message **ICAgent install success** is displayed, the ICAgent has been installed in the **/opt/oss/servicemgr/** directory. After the ICAgent has been installed, choose **Configuration Management** > **Agent Management** to view the ICAgent status.
- If the ICAgent fails to be installed, uninstall the ICAgent according to **Uninstalling the ICAgent by Logging In to the Server** and then install it again. If the problem persists, contact technical support.

----End

Inherited Installation

If the ICAgent has been installed on a server and the **ICProbeAgent.zip** installation package exists in the **/opt/ICAgent/** directory of this server, use this method to install the ICAgent on a remote server with a few clicks.

Step 1 Run the following command (***x.x.x.x*** indicates the server IP address) on the server where the ICAgent has been installed:

bash /opt/oss/servicemgr/ICAgent/bin/remoteInstall/remote_install.sh -ip x.x.x.x

Step 2 Enter the password of the **root** user as prompted.

NOTE

- If both the expect tool and the ICAgent have been installed on the server, the ICAgent will be installed on the remote server after the preceding command is executed. If the ICAgent has been installed on the server, but the Expect tool has not, enter the information as prompted for installation.
- Ensure that the **root** user can run the **SSH** or **SCP** command on the server where the ICAgent has been installed to remotely communicate with the server where the ICAgent is to be installed.
- If the message **ICAgent install success** is displayed, the ICAgent has been installed in the **/opt/oss/servicemgr/** directory. After the ICAgent has been installed, choose **Configuration Management** > **Agent Management** to view the ICAgent status.
- If the ICAgent fails to be installed, uninstall the ICAgent according to **Uninstalling the ICAgent by Logging In to the Server** and then install it again. If the problem persists, contact technical support.

----End

Inherited Batch Installation

If the ICAgent has been installed on a server and the **ICProbeAgent.zip** installation package exists in the **/opt/ICAgent/** directory of this server, use this method to install the ICAgent on multiple remote servers with a few clicks.

NOTICE

1. Ensure that you can run the **SSH** and **SCP** commands on the server where the ICAgent has been installed to communicate with the remote servers where the ICAgent is to be installed.
2. If you have installed the ICAgent in a server through an agency, you also need to set an agency for other servers where the ICAgent is to be installed.
3. Batch installation scripts depend on Python versions. You are advised to implement batch installation on hosts running Python 3.x. Python 2.x does not support batch installation.
4. Press **Enter** at the end of each line in the **iplist.cfg** file.

Prerequisites

The IP addresses and passwords of all servers on which the ICAgent is to be installed have been collected, sorted in the **iplist.cfg** file, and uploaded to the **/opt/ICAgent/** directory on the server where the ICAgent has been installed. The following is an example of the **iplist.cfg** file, where IP addresses and passwords are separated by spaces.

192.168.0.109 password (Set the password as required.)

192.168.0.39 password (Set the password as required.)

NOTE

- Because the **iplist.cfg** file contains sensitive information, you are advised to clear the information in time.
- If the passwords of all servers are the same, list IP addresses in the **iplist.cfg** file and enter the password during execution. If the password of an IP address is different from those of other IP addresses, enter the password next to this IP address.
- The batch installation function depends on Python 3.*. If the system displays a message indicating that Python cannot be found during the installation, install Python 3.* and try again.

Procedure

Step 1 Run the following command on the server where the ICAgent has been installed:

bash /opt/oss/servicemgr/ICAgent/bin/remoteInstall/remote_install.sh -batchModeConfig /opt/ICAgent/iplist.cfg

Enter the default password of the **root** user as prompted. If the passwords of all IP addresses have been configured in the **iplist.cfg** file, press **Enter** to skip this step. Otherwise, enter the default password.

```
batch install begin
Please input default passwd:
send cmd to 192.168.0.109
send cmd to 192.168.0.39
```



```
2 tasks running, please wait...
2 tasks running, please wait...
2 tasks running, please wait...
End of install agent: 192.168.0.39
End of install agent: 192.168.0.109
All hosts install icagent finish.
```

Wait until the message **All hosts install icagent finish.** is displayed, which indicates that the ICAgent has been installed on all the hosts listed in the configuration file.

Step 2 After the ICAgent has been installed, choose **Configuration Management** > **Agent Management** to view the ICAgent status.

----End

9.1.2 Upgrading the ICAgent

To ensure better collection experience, AOM will continuously upgrade ICAgent versions. When the system displays a message indicating that a new ICAgent version is available, perform the following operations:

NOTE

If the ICAgent has a critical bug, the system will upgrade the ICAgent version.

Step 1 In the navigation pane, choose **Configuration Management** > **Agent Management**.

Step 2 Select **Cluster: xxx** or **Other: user-defined nodes** from the drop-down list on the right of the page.

Step 3 Upgrade the ICAgent. If you select **Cluster: xxx** in **Step 2**, directly click **Upgrade ICAgent**. In this way, the ICAgent on all hosts in the cluster can be upgraded at one time. If you select **Other: user-defined nodes** in **Step 2**, select a desired host and then click **Upgrade ICAgent**.

Step 4 The upgrade takes about 1 minute to complete. When the ICAgent status changes from **Updating** to **Running**, the ICAgent has been upgraded.

NOTE

If the ICAgent state is abnormal after the upgrade or the upgrade fails, log in to the node and run the installation command to reinstall the ICAgent. The overwrite installation mode is supported. Therefore, you can reinstall the ICAgent without uninstallation.

----End

9.1.3 Uninstalling the ICAgent

If the ICAgent on a server is uninstalled, server O&M will be affected, making AOM functions unavailable. Exercise caution when performing this operation.

You can uninstall the ICAgent using either of the following methods:

- **Uninstalling the ICAgent on the AOM Console**: applies to the scenario where the ICAgent has been installed and needs to be uninstalled.
- **Uninstalling the ICAgent by Logging In to the Server**: applies to the scenario where the ICAgent fails to be installed and needs to be uninstalled.

- **Remotely Uninstalling the ICAgent**: applies to the scenario where the ICAgent has been installed and needs to be remotely uninstalled.
- **Uninstalling the ICAgent in Batches**: applies to the scenario where the ICAgent has been installed and needs to be uninstalled in batches.

Uninstalling the ICAgent on the AOM Console

Step 1 In the navigation pane, choose **Configuration Management** > **Agent Management**.

Step 2 Select **Other: user-defined nodes** from the drop-down list on the right of the page.

Step 3 Select one or more servers where the ICAgent is to be uninstalled, and click **Uninstall ICAgent**. In the **Uninstall ICAgent** dialog box, click **Yes**.

The uninstallation takes about 1 minute to complete. When the ICAgent status changes from **Uninstalling** to **Uninstall**, the ICAgent has been uninstalled.

----End

Uninstalling the ICAgent by Logging In to the Server

Step 1 Log in as the **root** user to the server where the ICAgent is to be uninstalled.

Step 2 Run the following command to uninstall the ICAgent:

bash /opt/oss/servicemgr/ICAgent/bin/manual/uninstall.sh;

Step 3 If the message **ICAgent uninstall success** is displayed, the ICAgent has been uninstalled.

----End

Remotely Uninstalling the ICAgent

In addition to the preceding method, you can use a method similar to **Inherited Installation** to remotely uninstall the ICAgent.

Step 1 Run the following command (***x.x.x.x*** indicates the server IP address) on the server where the ICAgent has been installed:

bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -ip x.x.x.x

Step 2 Enter the password of the **root** user as prompted.

NOTE

- If both the expect tool and the ICAgent have been installed on the server, the ICAgent will be uninstalled from the remote server after the preceding command is executed. If the ICAgent has been installed on the server, but the Expect tool has not, enter the information as prompted for installation.
- Ensure that the **root** user can run the **SSH** or **SCP** command on the server where the ICAgent has been installed to remotely communicate with the server where the ICAgent is to be uninstalled.
- If the message **ICAgent uninstall success** is displayed, the ICAgent has been uninstalled. After the ICAgent has been uninstalled, choose **Configuration Management** > **Agent Management** to view the ICAgent status.

----End

Uninstalling the ICAgent in Batches

If the ICAgent has been installed on a server and the **ICProbeAgent.zip** installation package exists in the **/opt/ICAgent/** directory of this server, use this method to uninstall the ICAgent from multiple remote servers in batches with a few clicks.

NOTICE

The servers must belong to the same Virtual Private Cloud (VPC) and network segment.

Prerequisites

The IP addresses and passwords of all servers from which the ICAgent is to be uninstalled have been collected, sorted in the **iplist.cfg** file, and uploaded to the **/opt/ICAgent/** directory on the server where the ICAgent has been installed. The following is an example of the **iplist.cfg** file, where IP addresses and passwords are separated by spaces.

192.168.0.109 password (Set the password as required.)

192.168.0.39 password (Set the password as required.)

NOTE

- Because the **iplist.cfg** file contains sensitive information, you are advised to clear the information in time.
- If the passwords of all servers are the same, list IP addresses in the **iplist.cfg** file and enter the password during execution. If the password of an IP address is different from those of other IP addresses, enter the password next to this IP address.
- You need to press **Enter** at the end of each line in the **iplist.cfg** file.

Procedure

Step 1 Run the following command on the server where the ICAgent has been installed:

bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -batchModeConfig /opt/ICAgent/iplist.cfg

Enter the default password of the **root** user as prompted. If the passwords of all IP addresses have been configured in the **iplist.cfg** file, press **Enter** to skip this step. Otherwise, enter the default password.

```
batch uninstall begin
Please input default passwd:
send cmd to 192.168.0.109
send cmd to 192.168.0.39
2 tasks running, please wait...
End of uninstall agent: 192.168.0.109
End of uninstall agent: 192.168.0.39
All hosts uninstall icagent finish.
```

Wait until the message **All hosts uninstall icagent finish.** is displayed, which indicates that the ICAgent has been uninstalled from all the hosts listed in the configuration file.

Step 2 After the ICAgent has been uninstalled, choose **Configuration Management** > **Agent Management** to view the ICAgent status.

----End

9.2 ICAgent Management (Non-HUAWEI CLOUD Host)

9.2.1 Installing the ICAgent

Prerequisites

- You have purchased an Elastic Cloud Server (ECS) as a jump server.
- The Operating System (OS) of the server meets the requirements in **Supported OSs** and supports the AMD64 processor architecture.
- The server has been bound to an Elastic IP Address (EIP). For details, see **Assigning an EIP and Binding It to an ECS**.
- Ensure that the time and time zone of the local browser are consistent with those of the ECS server.

Procedure

To install the ICAgent on a non-HUAWEI CLOUD server, purchase an ECS server from HUAWEI CLOUD as a jump server and perform the following operations:

NOTE

You are advised to use **CentOS 6.5 64bit** or later images. The minimum specification is **1 vCPU | 1 GB** and the recommended one is **2 vCPUs | 4 GB**.

Step 1 **Log in to the ECS** and modify its security group rule.

1. On the ECS details page, click the **Security Groups** tab.
2. On the security list page, click a security group name and click **Modify Security Group Rule**.
3. On the security group details page, click **Inbound Rules** and then **Add Rule**. On the page that is displayed, add a security group rule according to **Table 9-3**.

Table 9-3 Security group rule

Direction	Protocol	Port	Description
Inbound	TCP	8149, 8102, 8923, 30200, 30201, and 80	List of ports on the jump server to which the ICAgent sends data

NOTE

Enable ports 8149, 8102, 8923, 30200, 30201, and 80 in the inbound direction of the security group to ensure normal data communication between the non-HUAWEI CLOUD host and the jump server.

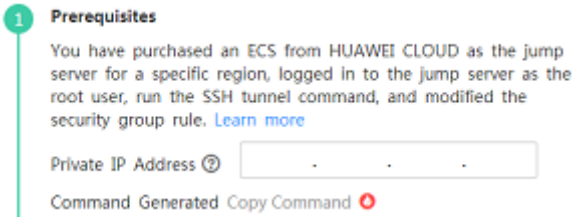
Step 2 Log in to the AOM console. In the navigation pane, choose **Configuration Management** > **Agent Management**.

Step 3 Select **Other: user-defined nodes**, click **Install ICAgent**, and set **Host** to **Non-HUAWEI CLOUD host**.

Step 4 Enable forwarding ports on the jump server.

1. As shown in **Figure 9-2**, enter a private IP address to generate the jump server forwarding command.

   Figure 9-2 Private IP address of the jump server

   NOTE

   The private IP address of the jump server refers to the internal IP address of the Virtual Private Cloud (VPC) where the jump server locates.

2. Click **Copy Command** to copy the jump server forwarding command.
3. Log in as the **root** user to the jump server and run the SSH tunnel forwarding command:

   ```
   ssh -f -N -L {ECS IP address}:8149:{ELB IP address}:8149 -L {ECS IP address}:8102:{ELB IP address}:8102 -L {ECS IP address}:8923:{ELB IP address}:8923 -L {ECS IP address}:30200:{ELB IP address}:30200 -L {ECS IP address}:30201:{ELB IP address}:30201 -L {ECS IP address}:80:icagent-{Region}.obs.{Region}.myhuaweicloud.com:80 {ECS IP address}
   ```

   Enter the password of the **root** user as prompted.
4. Run the **netstat –lnp | grep ssh** command to check whether corresponding ports are being listened to. If the results in **Figure 9-3** are returned, TCP ports are enabled.

Figure 9-3 Verification results of TCP ports

```
[root@ecs-3716 nginx]# netstat -lnp | grep ssh
tcp        0      0 192.168.0.201:80        0.0.0.0:*               LISTEN      1245
tcp        0      0 192.168.0.201:8149      0.0.0.0:*               LISTEN      1245
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      4590
tcp        0      0 192.168.0.201:30200     0.0.0.0:*               LISTEN      1245
tcp        0      0 192.168.0.201:30201     0.0.0.0:*               LISTEN      1245
tcp        0      0 192.168.0.201:8923      0.0.0.0:*               LISTEN      1245
tcp        0      0 192.168.0.201:8102      0.0.0.0:*               LISTEN      1245
tcp6       0      0 :::22                   :::*                    LISTEN      4590
[root@ecs-3716 nginx]#
```

NOTE

- Enter *http://IP address of the jump server ECS* in the address box of the browser. If the access is successful, the security group rule has taken effect.
- If the jump server powers off and restarts, run the preceding command again.

Step 5 Obtain an AK/SK according to **How Do I Obtain the AK/SK and Project ID?**

Step 6 Generate and copy the ICAgent installation command.

1. As shown in **Figure 9-4**, enter the **AK**, **SK**, **DC**, and **Connection IP** to generate the ICAgent installation command.

Figure 9-4 Obtaining the AK/SK

NOTE

- Ensure that the AK/SK are correct. Otherwise, the ICAgent cannot be installed.
- **DC**: Customize a DC name to query hosts more easily.
- **Connection IP**: For EIP connection, use the EIP of the jump server. For VPC peer connection, use the internal IP address of the VPC where the jump server is located.

2. Click **Copy Command** to copy the ICAgent installation command.

Step 7 Use a remote login tool to log in as the **root** user to the server where the ICAgent is to be installed and run the preceding command to install the ICAgent.

If the message **ICAgent install success** is displayed, the ICAgent has been installed in the **/opt/oss/servicemgr/** directory. After the ICAgent has been installed, choose **Configuration Management** > **Agent Management** to view the ICAgent status.

----End

9.2.2 Upgrading the ICAgent

To ensure better collection experience, AOM will continuously upgrade ICAgent versions. When the Linux system displays a message indicating that a new ICAgent version is available, perform the following operations:

Step 1 Log in to the AOM console. In the navigation pane, choose **Configuration Management** > **Agent Management**.

Step 2 Select **Cluster: xxx** or **Other: user-defined nodes** from the drop-down list on the right of the page.

Step 3 Upgrade the ICAgent. If you select **Cluster: xxx** in **Step 2**, directly click **Upgrade ICAgent**. In this way, the ICAgent on all hosts in the cluster can be upgraded at one time. If you select **Other: user-defined nodes** in **Step 2**, select a desired host and then click **Upgrade ICAgent**.

Step 4 The upgrade takes about 1 minute to complete. When the ICAgent status changes from **Updating** to **Running**, the ICAgent has been upgraded.

----End

9.2.3 Uninstalling the ICAgent

If the ICAgent on a server is uninstalled, server O&M will be affected, making topology and tracing functions unavailable. Exercise caution when performing this operation.

- **Uninstalling the ICAgent on the AOM Console**: applies to the scenario where the ICAgent has been installed and needs to be uninstalled.
- **Uninstalling the ICAgent by Logging In to the Server**: applies to the scenario where the ICAgent fails to be installed and needs to be uninstalled.

Uninstalling the ICAgent on the AOM Console

Step 1 Log in to the AOM console. In the navigation pane, choose **Configuration Management** > **Agent Management**.

Step 2 Select **Other: user-defined nodes** from the drop-down list on the right of the page.

Step 3 Select one or more servers where the ICAgent is to be uninstalled, and click **Uninstall ICAgent**. In the **Uninstall ICAgent** dialog box, click **Yes**.

The uninstallation takes about 1 minute to complete. When the ICAgent status changes from **Uninstalling** to **Uninstall**, the ICAgent has been uninstalled.

NOTE

To reinstall the ICAgent, wait for 5 minutes after it is uninstalled. Otherwise, the ICAgent may be automatically uninstalled again.

----End

Uninstalling the ICAgent by Logging In to the Server

Step 1 Log in as the **root** user to the server where the ICAgent is to be uninstalled.

Step 2 Run the following command to uninstall the ICAgent:

bash /opt/oss/servicemgr/ICAgent/bin/manual/uninstall.sh;

Step 3 If the message **ICAgent uninstall success** is displayed, the ICAgent has been uninstalled.

----End

9.3 Access Management

9.3.1 Overview

Access Management allows you to quickly connect monitoring data to AOM. This function determines whether to establish or delete network channels, and generate or revoke authentication credentials for reporting monitoring data.

NOTE

This function is available only in the following regions: CN North-Beijing1, CN North-Beijing2, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, Ulanqab1, and AP-Singapore.

By using the generated AccessCode as an authentication credential, you can remotely report native Prometheus metrics to AOM according to **Reporting Prometheus Data to AOM** and store time series data for a long time. You can also use AccessCode to query data in AOM according to **Viewing Metric Data in AOM Using Grafana**. AOM supports the following native Prometheus APIs:

APIs for querying Prometheus data:

- GET /v1/:project_id/api/v1/query
- GET /v1/:project_id/api/v1/query_range
- GET /v1/:project_id/api/v1/labels
- GET /v1/:project_id/api/v1/label/:label_name/values
- POST /v1/:project_id/api/v1/query
- POST /v1/:project_id/api/v1/query_range
- POST /v1/:project_id/api/v1/labels

When calling the preceding APIs, add **access_code** to the **Authorization** field in the request header.

Example: "Authorization: Bearer {access_code}" or "Authorization: Basic base64Encode("aom_access_code:{access_code}")"

API for reporting time series data: POST /v1/:project_id/push

NOTE

base64Encode means that parameters are encoded using Base64.

9.3.2 Reporting Prometheus Data to AOM

If you have deployed the open-source Prometheus, go to **Step 3**.

This section describes how to configure the **AccessCode** in the Prometheus configuration file and make the configuration take effect.

Prerequisites

You have purchased an ECS. For details, see **Elastic Cloud Server Getting Started**.

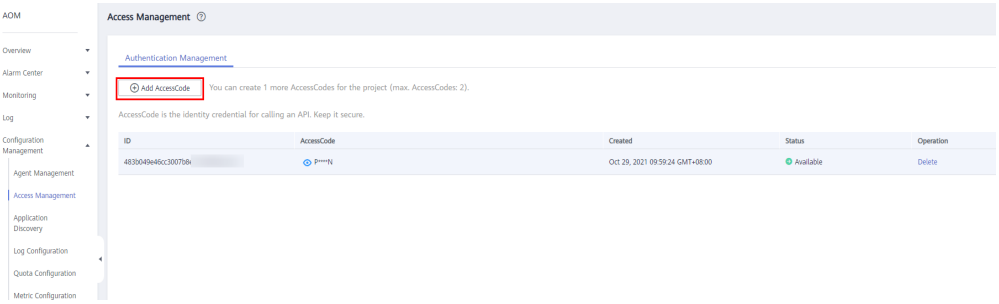
Procedure

Step 1 Install and start Prometheus. For details, see **Prometheus official documentation**.

Step 2 Add an AccessCode.

1. Log in to the AOM console. In the navigation pane, choose **Configuration Management** > **Access Management**.
2. On the **Authentication Management** tab page, click **Add AccessCode**.

Figure 9-5 Clicking **Add AccessCode**

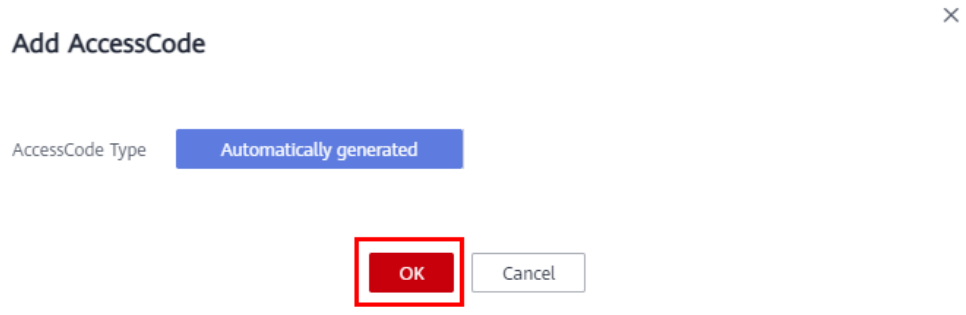


NOTE

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

3. In the dialog box that is displayed, click **OK** to add the AccessCode.

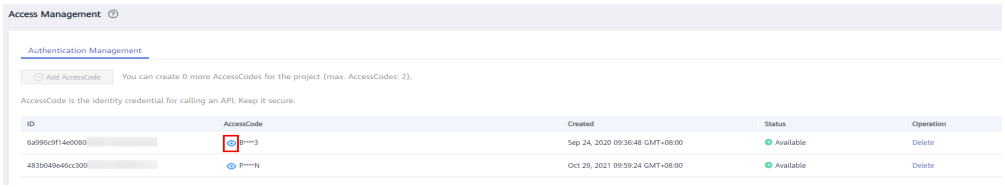
Figure 9-6 Adding an AccessCode



4. After the AccessCode is added, click to view the AccessCode on the **Authentication Management** tab page. To delete the AccessCode, click

Delete in the **Operation** column. Deleted AccessCodes cannot be recovered. Exercise caution when performing this operation.

Figure 9-7 Viewing the AccessCode



Step 3 Log in to the ECS and locate the Prometheus configuration file.

Run the following command:

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

Add the following configuration to the end of the **prometheus.yml** file:

- ```
  remote_write:
    - url: 'https://aom-internal-access.{region_name}.myhuaweicloud.com:8443/v1/{project_id}/push'
      tls_config:
        insecure_skip_verify: true
      bearer_token: '{access_code}'
  ```

Parameter description:

- **region_name**: domain name or IP address of the server bearing the REST service. **region_name** varies according to services in different regions. It can be obtained from **Regions and Endpoints**. For example, the **region_name** of AOM in CN North-Beijing1 is **cn-north-1**.
- **project_id**: project ID, which can be viewed in the project list on the **My Credentials** page.

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']
remote_write:
  - url: 'https://aom-internal-access.cn-north-1.myhuaweicloud.com:8443/v1/thisisyourprojectid/push'
    tls_config:
      insecure_skip_verify: true
    bearer_token: 'fVkvjOqghclARvZZEEWhwSwxesmKz5Efsx9vxZSNGCXEffcjPxxxxxx'
```

Step 4 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 **How Do I Switch to a Private DNS Server?**

Step 5 Restart Prometheus.

Step 6 Check whether data can be reported to AOM by referring to **Viewing Metric Data in AOM Using Grafana**.

----End

9.3.3 Viewing Metric Data in AOM Using Grafana

Prerequisites

- You have purchased an ECS. For details, see **Elastic Cloud Server Getting Started**.
- You have purchased an EIP and bound it to the ECS. For details, see **Elastic IP Getting Started**.

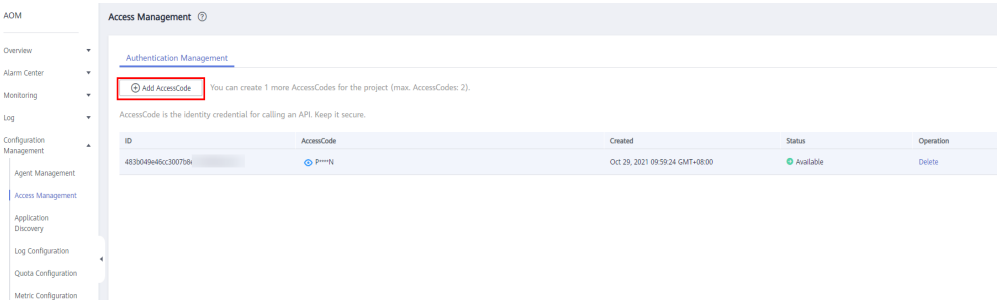
Procedure

Step 1 Install and start Grafana. For details, see the **Grafana official documentation**.

Step 2 Add an AccessCode.

1. Log in to the AOM console. In the navigation pane, choose **Configuration Management** > **Access Management**.
2. On the **Authentication Management** tab page, click **Add AccessCode**.

Figure 9-8 Clicking **Add AccessCode**

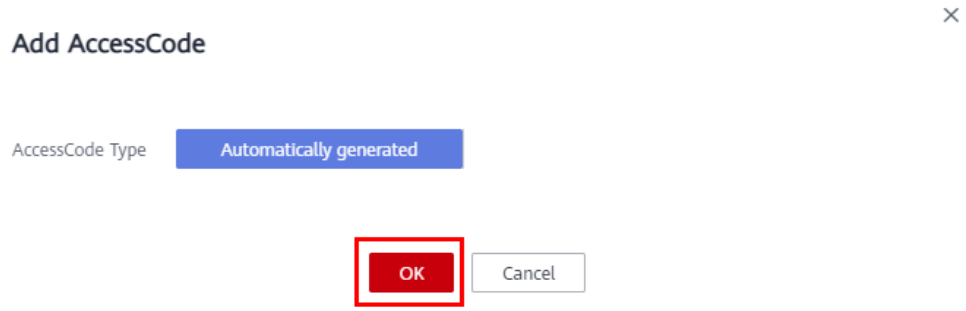


NOTE

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

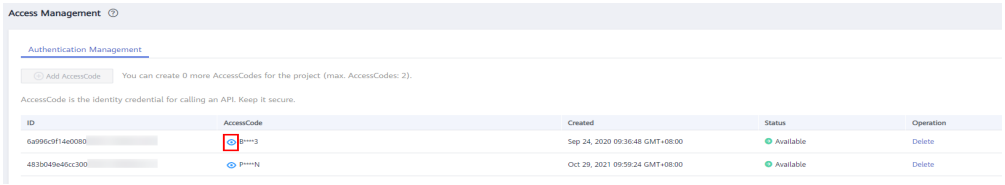
3. In the dialog box that is displayed, click **OK** to add the AccessCode.

Figure 9-9 Adding an AccessCode



4. After the AccessCode is added, click to view the AccessCode on the **Authentication Management** tab page. To delete the AccessCode, click **Delete** in the **Operation** column. Deleted AccessCodes cannot be recovered. Exercise caution when performing this operation.

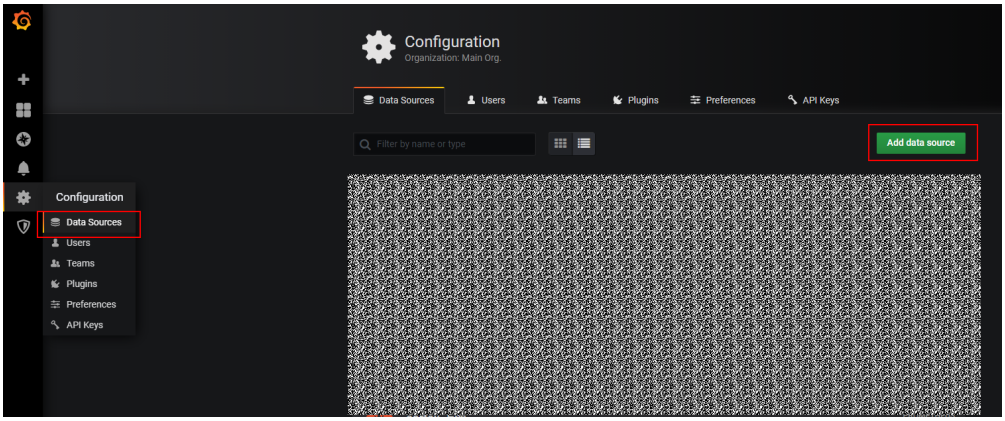
Figure 9-10 Viewing the AccessCode



Step 3 Configure Grafana.

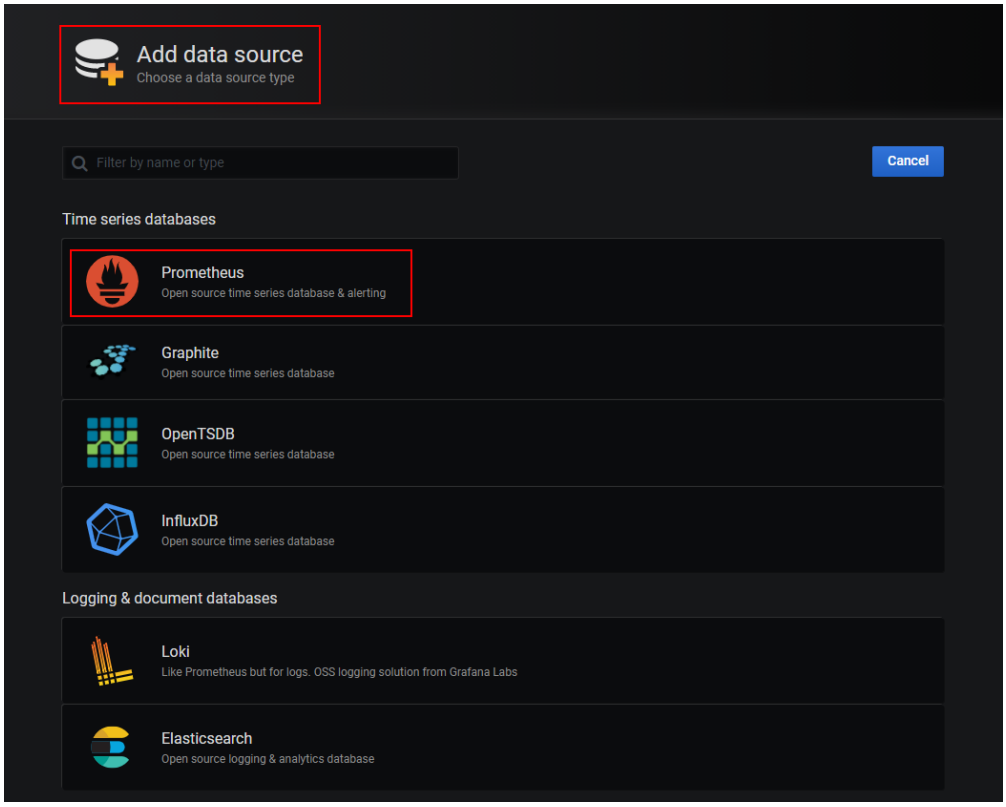
1. Log in to Grafana.
2. In the navigation pane, choose **Configuration** > **Data Sources**. Then, click **Add data source**.

Figure 9-11 Configuring Grafana



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

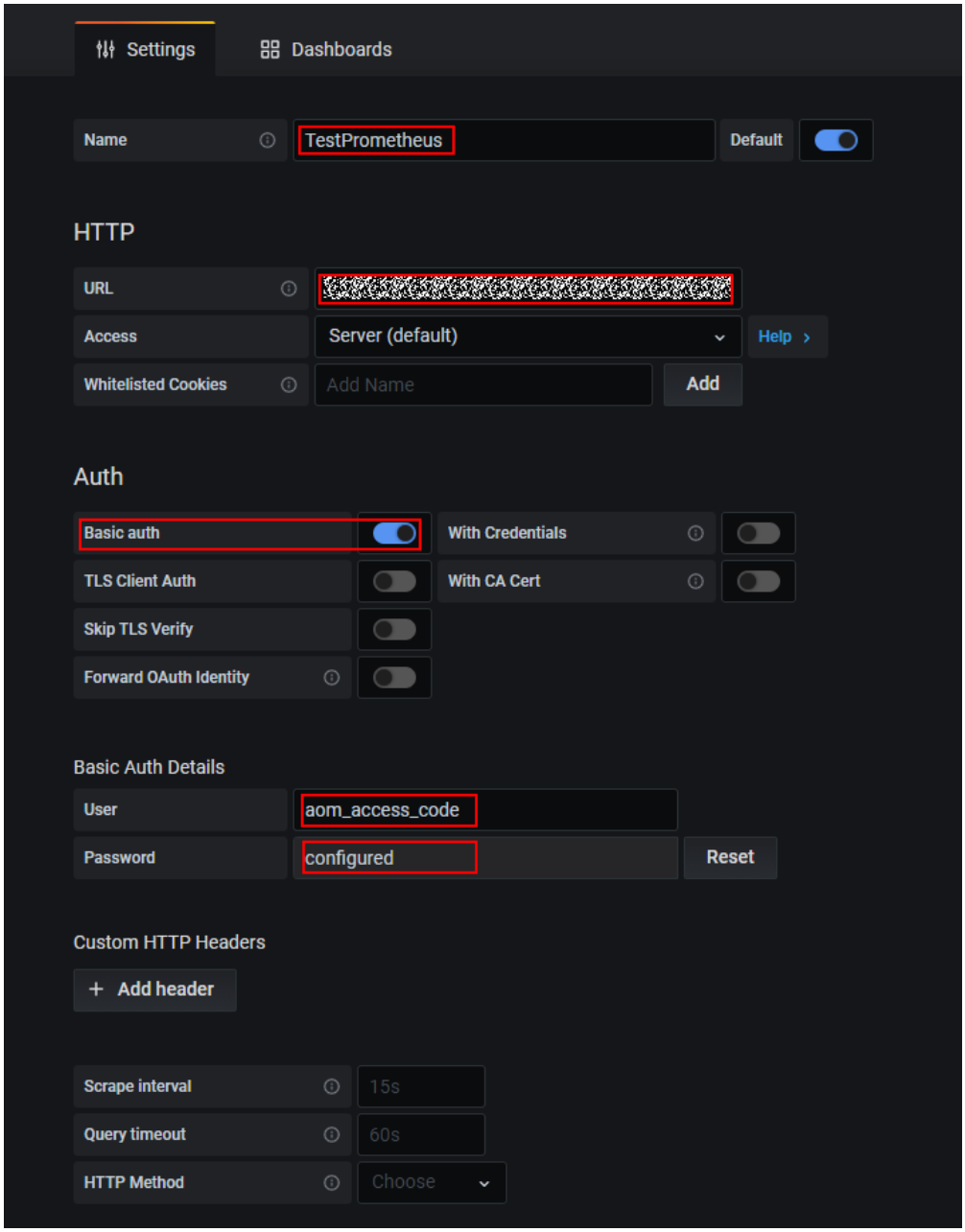
Figure 9-12 Entering the Prometheus configuration page



4. Set parameters according to the following figure.
   - **Password**: AccessCode generated in **Step 2**
   - **User**: aom_access_code
   - **URL**: {*URI-scheme*}://{*Endpoint*}/v1/{*project_id*}
     - **URI-scheme**: protocol used to transmit requests. Currently, all APIs use HTTPS.
     - **Endpoint**: domain name or IP address of the server bearing the REST service. The endpoint varies according to services in different regions. It can be obtained from **Regions and Endpoints**. For example, the endpoint of AOM in CN North-Beijing1 is **aom.cn-north-1.myhuaweicloud.com**.
     - **project_id**: project ID, which can be viewed in the project list on the **My Credentials** page.

   NOTE
   - The **Basic auth** and **Skip TLS Verity** options under **Auth** must be enabled.
   - AccessCodes correspond to project IDs. Confirm their mapping when entering information.

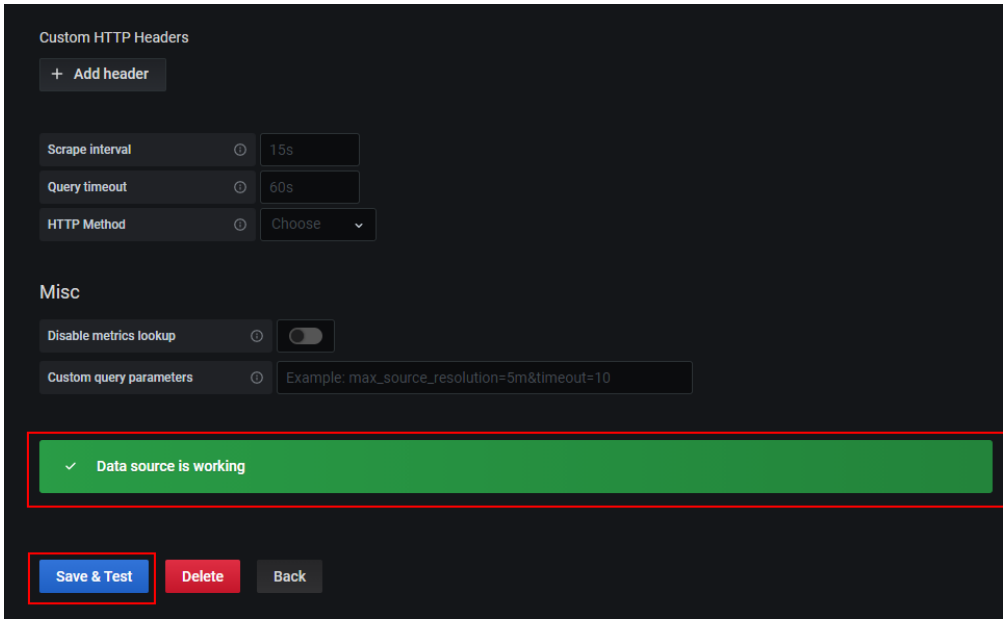
Figure 9-13 Configuring parameters



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 9-14 Checking whether the configuration is successful



----End

9.4 Log Configuration

9.4.1 Setting the Log Quota

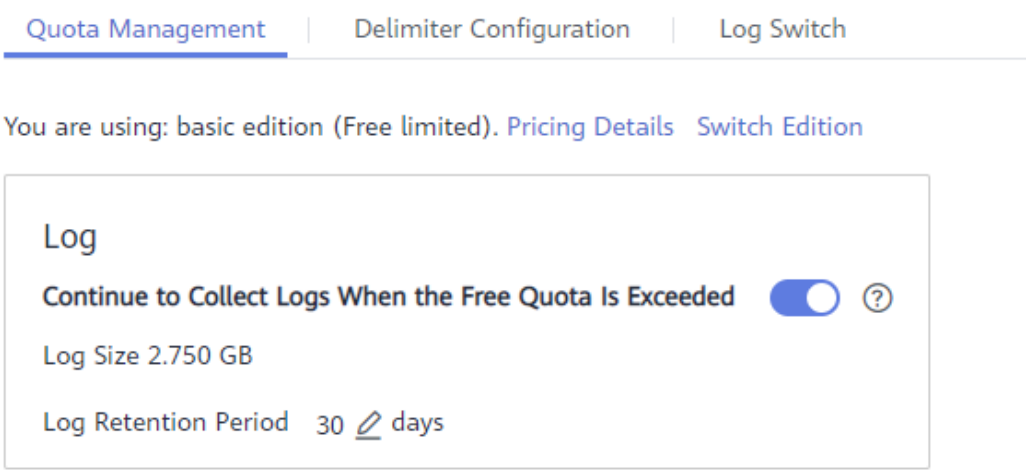
Step 1 Log in to the AOM console. In the navigation pane, choose **Configuration Management** > **Log Configuration**.

Step 2 On the **Quota Management** page, you can view the log size and retention period, and modify this period.

NOTICE

If you set a rule on AOM to connect logs to LTS, the log retention period you specify on the **Configuration Center** page will not take effect; instead, the log retention period set on LTS will be used.

Figure 9-15 Viewing log configuration



Log Retention Period: You can set this to 1–30 days.

----End

9.4.2 Configuring Delimiters

AOM enables you to divide the log content into multiple words for search by configuring delimiters. By default, AOM provides the following delimiters:

```
, '";=()[]{}@&<>/:\n\t\r
```

If default delimiters cannot meet requirements, customize delimiters according to the following procedure.

Precautions

Delimiters are applicable only to the logs generated after the time when the delimiters are configured. Earlier logs are processed based on earlier delimiters.

Procedure

Step 1 In the navigation pane, choose **Configuration Management** > **Log Configuration**, and click the **Delimiter Configuration** tab.

Step 2 Configure delimiters.

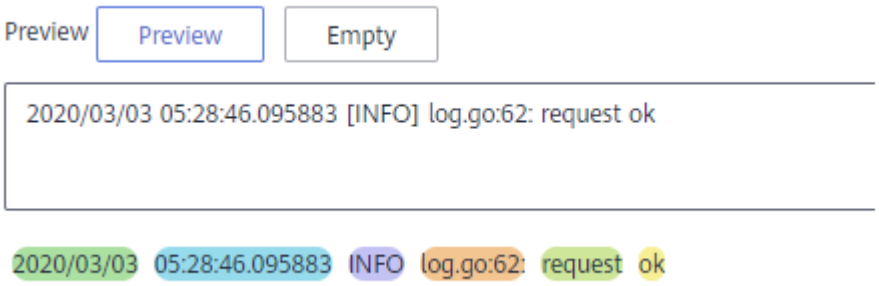
You can configure delimiters using the following methods: If you use both methods at the same time, the union set will be selected.

- Customize delimiters. Specifically, click , enter a delimiter in the text box, and click .
- Use ASCII code. Specifically, click **Add Special Delimiters**, enter the ASCII value according to **ASCII Comparison Table**, and click .

Step 3 Preview the log content.

Enter the log content to be previewed in the text box and click **Preview**. For example, if the comma (,) and brackets ([]) are used as delimiters, the preview effect is as follows:

Figure 9-16 Previewing the log content



Step 4 Confirm the configuration and click **OK**.

NOTE

Click **Reset** to restore the default configuration. Default delimiters are as follows:

```
, '";=()[]{}@&<>/:\n\t\r
```

----End

ASCII Comparison Table

Table 9-4 ASCII comparison table

ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character
0	NUL (Null)	32	Space	64	@	96	`
1	SOH (Start of heading)	33	!	65	A	97	a
2	STX (Start of text)	34	"	66	B	98	b
3	ETX (End of text)	35	#	67	C	99	c
4	EOT (End of transmission)	36	$	68	D	100	d
5	ENQ (Enquiry)	37	%	69	E	101	e

ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character
6	ACK (Acknowledge)	38	&	70	F	102	f
7	BEL (Bell)	39	'	71	G	103	g
8	BS (Backspace)	40	(	72	H	104	h
9	HT (Horizontal tab)	41	)	73	I	105	i
10	LF (Line feed)	42	*	74	J	106	j
11	VT (Vertical tab)	43	+	75	K	107	k
12	FF (Form feed)	44	,	76	L	108	l
13	CR (Carriage return)	45	-	77	M	109	m
14	SO (Shift out)	46	.	78	N	110	n
15	SI (Shift in)	47	/	79	O	111	o
16	DLE (Data link escape)	48	0	80	P	112	p
17	DC1 (Device control 1)	49	1	81	Q	113	q
18	DC2 (Device control 2)	50	2	82	R	114	r
19	DC3 (Device control 3)	51	3	83	S	115	s
20	DC4 (Device control 4)	52	4	84	T	116	t

ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character
21	NAK (Negative acknowledge)	53	5	85	U	117	u
22	SYN (Synchronous suspension)	54	6	86	V	118	v
23	ETB (End of transmission block)	55	7	87	W	119	w
24	CAN (Cancel)	56	8	88	X	120	x
25	EM (End of medium)	57	9	89	Y	121	y
26	SUB (Substitute)	58	:	90	Z	122	z
27	ESC (Escape)	59	;	91	[	123	{
28	FS (File separator)	60	<	92	/	124	|
29	GS (Group separator)	61	=	93	]	125	}
30	RS (Record separator)	62	>	94	^	126	~
31	US (Unit separator)	63	?	95	_	127	DEL (Delete)

9.4.3 Setting Log Collection

You can enable or disable log collection as required to reduce memory, database, and disk space usage.

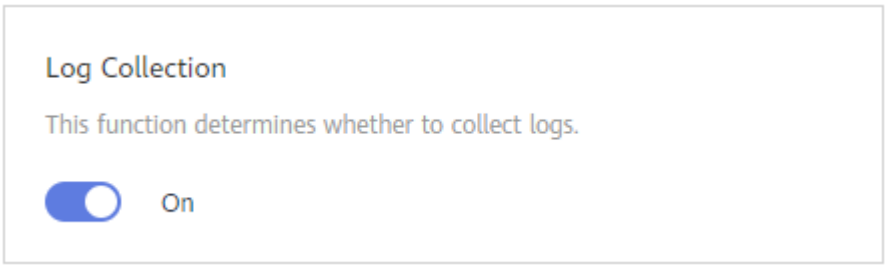
Procedure

Before enabling this function, ensure that you have installed the ICAgent on an Elastic Cloud Server (ECS) according to **Installing the ICAgent**.

Step 1 Log in to the AOM console. In the navigation pane, choose **Configuration Management** > **Log Configuration**. Then, click the **Log Switch** tab.

Step 2 Enable or disable log collection.

Figure 9-17 Setting log collection



NOTE

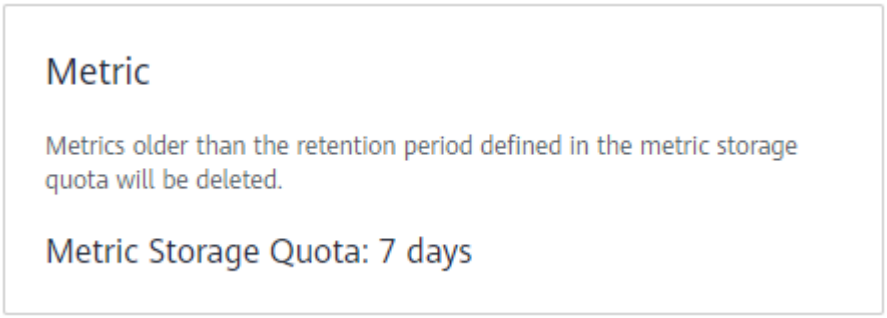
This function is enabled by default. If you do not need to collect logs, disable this function to reduce resource usage.

----End

9.5 Quota Configuration

You can change the metric quota by switching between the basic edition and pay-per-use edition. In the basic edition, limited functions are provided for free.

Figure 9-18 Configuring the quota



Earlier metrics will be deleted when the metric quota is exceeded.

9.6 Metric Configuration

You can enable the metric collection function to collect metrics (excluding SLA and custom metrics).

Before enabling this function, ensure that you have installed the ICAgent on an Elastic Cloud Server (ECS) according to **Installing the ICAgent**.

Step 1 Log in to the AOM console. In the navigation pane, choose **Configuration Management** > **Metric Configuration**.

Step 2 Enable or disable metric collection.

Figure 9-19 Configuring metric collection

NOTE

If you disable this function, no metric data will be updated.

----End

9.7 Data Subscription

AOM allows you to subscribe to metrics or alarms. After the subscription, data can be forwarded to custom Kafka or Distributed Message Service (DMS) topics for you to retrieve.

NOTICE

- Data subscription has not been opened to the public. If you want to use this function, **submit a service ticket**.
- A maximum of ten data subscription rules can be created.

Creating Subscription Rules

Step 1 Log in to the AOM console. In the navigation pane, choose **Configuration Management** > **Data Subscription**.

Step 2 Click **Create Subscription Rule** in the upper right corner. On the displayed page, set parameters and click **OK**.

You can set **Subscription Target Type** to **Custom Kafka** or **DMS** as required.

- If **Subscription Target Type** is set to **Custom Kafka**, set parameters based on **Table 9-5**.

Table 9-5 Subscription rule parameters

Parameter	Description	Example
Rule Name	Subscription rule name.	Enter **aom-kafka-test**.
Subscription Content	Options: **Metric** and **Alarm**.	Select **Metric**.
Subscription Target Type	Options: **Custom Kafka** and **DMS**.	Select **Custom Kafka**.
Subscription Target Address	Custom Kafka address, which needs to be connected to Internet. Each address must be in the format of "IPv4 address:port". If multiple addresses exist, separate them by commas (,). Example: **192.168.0.1:9092,192.168.0.2:9092**	Set this parameter as required.

a. (Optional) On the **Rule Details** page, click  to enable Kafka SASL_SSL and set parameters based on **Table 9-6**.

NOTE

AOM supports only Kafka SASL_SSL security authentication. If you have enabled Kafka SASL_SSL for instances, you also need to enable it on the **Rule Details** page.

Table 9-6 Setting Kafka SASL_SSL parameters

Parameter	Description	Example
User name	SASL username for instance access authentication.	demo
Password	SASL password for instance access authentication. Keep your password secure. The system cannot detect your password.	-
Client certificate	Use a client certificate in **.pem** format.	-

b. Click **Verify and Save Custom Kafka Configuration** to verify the connectivity of the custom Kafka instance.

c. Select a topic for transmitting data and click **OK**.

- If **Subscription Target Type** is set to **DMS**, set parameters based on **Table 9-7**.

Table 9-7 Subscription rule parameters

Parameter	Description	Example
Rule Name	Subscription rule name.	Enter **aom-kafka-test**.
Subscription Content	Options: **Metric** and **Alarm**.	Select **Metric**.
Subscription Target Type	Options: **Custom Kafka** and **DMS**.	Select **DMS**.
Instance	Select a DMS instance. If no DMS instance is available, click **Create DMS Instance** to create one.	Select **kafka-aom-7160**.

a. On the **Rule Details** page, click **Create a network connection channel**.

b. Verify the DMS instance connectivity.

Ensure that an inbound rule is added to allow traffic from source IP address 198.19.128.0/20 on port 9011. To set a security group rule, do as follows:

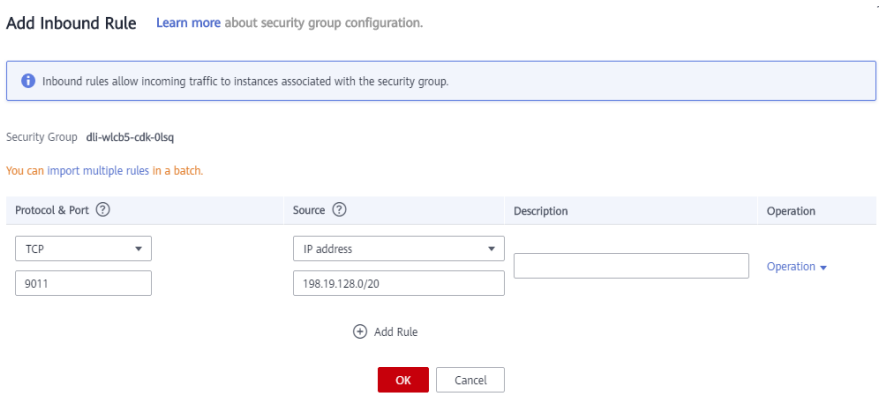
i. Log in to the management console.

ii. Click ☰ in the upper left corner and choose **Networking** > **Virtual Private Cloud**.

iii. In the navigation pane, choose **Access Control** > **Security Groups**. Then, locate the security group corresponding to the DMS instance and click **Manage Rule** in the **Operation** column.

iv. On the **Inbound Rules** tab page, click **Add Rule** to allow the network traffic from source IP address 198.19.128.0/20 on port 9011.

Figure 9-20 Adding an inbound rule



c. Click **Verify and Save DMS Configuration Information**.

d. Select a topic for transmitting data and click **OK**.

----End

Data Subscription Format

- Metric data example (in JSON format)

```
package metric

type MetricDatas struct {
  Metrics   []Metrics `json:"metrics"`
  ProjectId string    `json:"project_id"`
}

type Metrics struct {
  Metric      Metric  `json:"metric"`
  Values      []Value `json:"values"`
  CollectTime int64   `json:"collect_time"`
}

type Metric struct {
  Namespace  string      `json:"namespace"`
  Dimensions []Dimension `json:"dimensions"`
}

type Value struct {
  Value           interface{} `json:"value"`
  Type            string      `json:"type"`
  Unit            string      `json:"unit"`
  StatisticValues string      `json:"statisticvalues"`
  MetricName      string      `json:"metric_name"`
}

type Dimension struct {
  Name  string `json:"name"`
  Value string `json:"value"`
}
```

- Kafka message example

```
key:,
value:{"metrics":[{"metric":{"namespace":"PAAS.NODE","dimensions":
[{"name":"nodeName","value":"cn-north-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":"cn-north-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_id":"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 9-8 Alarm parameters

Parameter	Type	Description
events	Array of objects. For details, see **Table 9-9**.	Event or alarm details.
project_id	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 9-9 EventModel

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 (unit: ms) at which an alarm is automatically cleared. For example, if the duration is one 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 with the string-type attribute. Options: **Critical**, **Major**, **Minor**, and **Info**. ● **event_type**: Event type, which is an enumerated value with the string-type attribute. Options: **event** and **alarm**. ● **resource_provider**: Name of a cloud service corresponding to an event, which is a string. ● **resource_type**: Resource type corresponding to an event, which is a string. ● **resource_id**: Resource ID corresponding to an event, which is a string.
annotations	Object	Additional field for an event or alarm, which can be left blank.
attach_rule	Object	Reserved field for an event or alarm, which can be left blank.

Follow-up Operations

After the data subscription rule is created, AOM will send data to your custom Kafka or DMS topic so that you can retrieve the subscribed metrics or alarms.

10

