AOM

User Guide

Issue 01

Date 2023-11-17

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 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

Category	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.

Category	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 rules, and configure alarm noise reduction. 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, they can

Category	Description
	rectify faults in time to avoid service loss.

Category	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

Category	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.

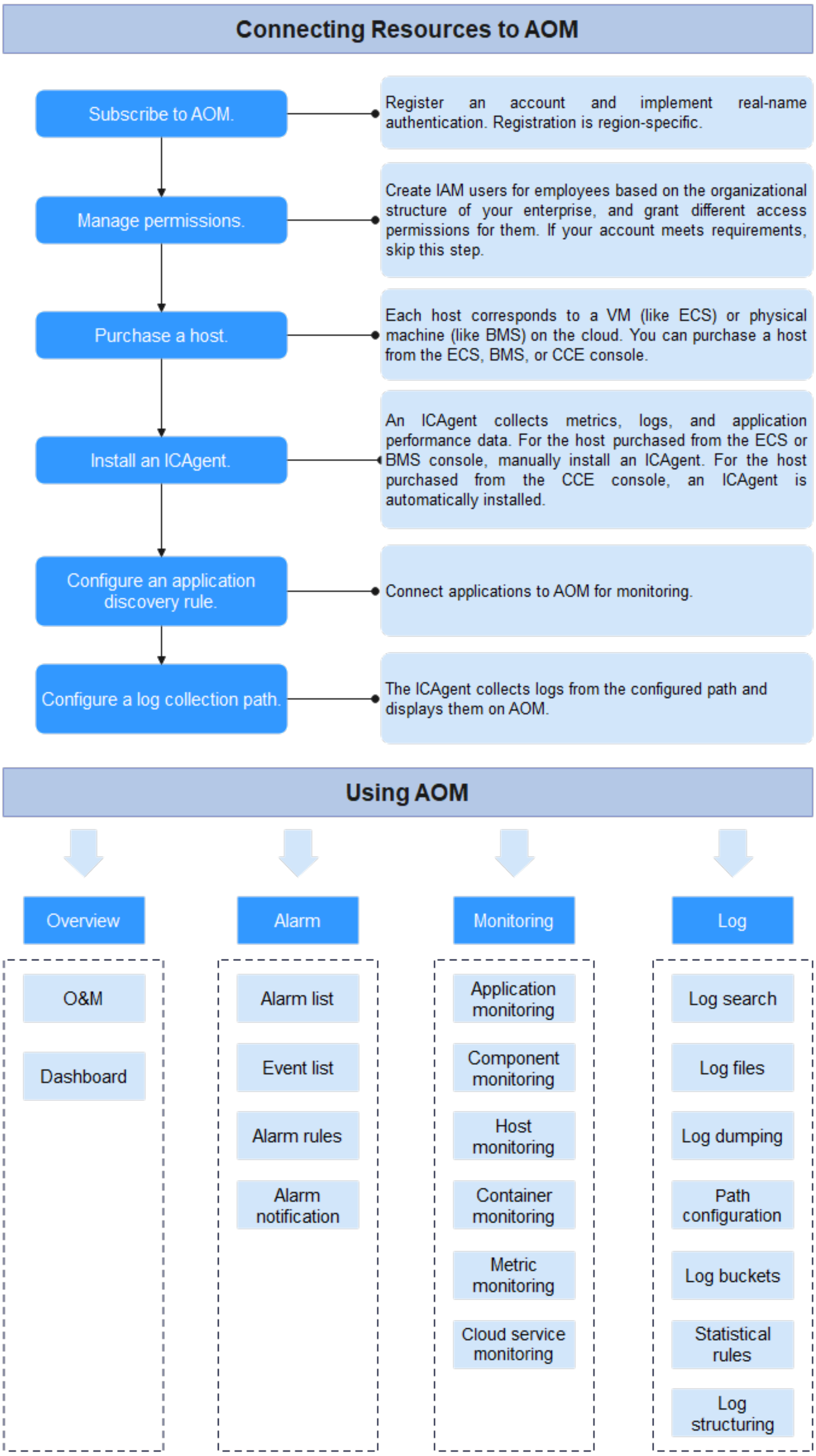
Category	Description
Log	Functions such as log search, log file, log dump, and path configuration are provided. ● Log search AOM enables you to quickly query logs, and locate faults based on log sources and contexts. ● Log files You can quickly view log files of component instances to locate faults. ● 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

Category	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. ● 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. ● 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



Register an account and implement real-name authentication. Registration is region-specific.

Create IAM users for employees based on the organizational structure of your enterprise, and grant different access permissions for them. If your account meets requirements, skip this step.

Each host corresponds to a VM (like ECS) or physical machine (like BMS) on the cloud. You can purchase a host from the ECS, BMS, or CCE console.

An ICAgent collects metrics, logs, and application performance data. For the host purchased from the ECS or BMS console, manually install an ICAgent. For the host purchased from the CCE console, an ICAgent is automatically installed.

Connect applications to AOM for monitoring.

The ICAgent collects logs from the configured path and displays them on AOM.

1. (Mandatory) **Subscribe to AOM**.
2. (Optional) Create IAM users 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 **Monitoring Overview**, **Alarm Management**, **Resource Monitoring**, and **Log Management** to perform routine O&M.

2 Subscribing to AOM

Before subscribing to AOM, register a **HUAWEI ID**.

Subscribing to AOM

AOM resources are region-specific and cannot be used across regions. Select a region (such as CN-Hong Kong and AP-Bangkok) 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 **Application** > **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. Note that you can only switch the pay-per-use edition back to the basic edition once in 24 hours, and resources beyond the basic edition will be deleted.

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 chapter describes how to use **Identity and Access Management (IAM)** for fine-grained permissions control for your AOM resources. 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 a cloud account or service to perform professional and efficient O&M on your AOM resources.

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

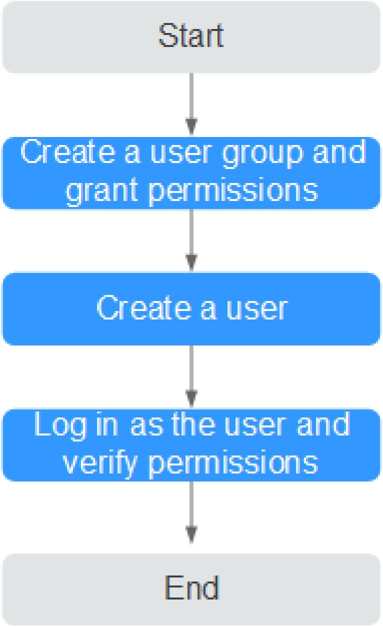
This section describes the procedure for granting permissions (see **Figure 3-1**).

Prerequisites

Learn about the permissions (see **AOM Permissions**) supported by AOM and choose policies or roles according to your requirements. For the permissions of other services, see **System Permissions**.

Process

Figure 3-1 Process for granting AOM permissions


Start
Create a user group and grant permissions
Create a user
Log in as the user and verify permissions
End

1. **Create a user group and assign permissions**.

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

2. **Create an IAM user**.

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

3. **Log in** and verify 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 about how to create custom policies, see **Creating a Custom Policy**. For example custom policies, see the following description.

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"
                        ]
                }
        ]
}
```

3.3 Cloud Service Authorization

Grant permissions to access Resource Management Service (RMS), Log Tank Service (LTS), Cloud Container Engine (CCE), Cloud Container Instance (CCI), Cloud Eye, Distributed Message Service (DMS), and Elastic Cloud Server (ECS) in one click. The setting takes effect for the entire AOM service.

Prerequisites

The **aom_admin_trust** agency has been created on IAM. For details, see **Creating an Agency**.

Procedure

Step 1 Log in to the AOM console and choose **Configuration Management** > **Service Authorization**.

Step 2 In the upper right corner of the cloud service authorization page, click **Authorize** to grant permissions to access the preceding cloud services in one click.

If **Cancel Authorization** is displayed in the upper right corner of the page, you have the permissions to access the preceding cloud services.

----End

4 Connecting Resources to AOM

4.1 Installing an ICAgent (Huawei Cloud Host)

ICAgents collect metrics, logs, and application performance data in real time. For hosts purchased from the ECS or BMS console, you need to manually install the ICAgent. For hosts purchased from the CCE console, the ICAgent is automatically installed.

Prerequisites

- Before installing an 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.
- An ICAgent process needs to be installed and run by the **root** user.

Installation Methods

There are two methods to install an 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 an 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 condition is met: An ICAgent has never been installed on your server.

Method	Scenario
Inherited installation	This method is used when the following conditions are met: You have multiple servers where an ICAgent is to be installed. One server is bound to an EIP, but others are not. An 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 an ICAgent on the remaining servers. See **Inherited Installation**.

Initial Installation

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

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

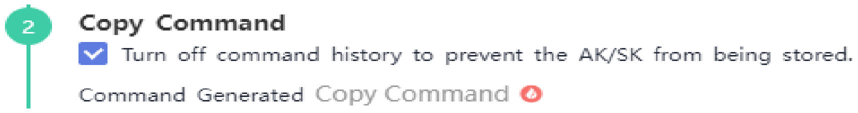
- If you have obtained the AK/SK, skip this step.
- If you have not obtained an AK/SK, **obtain them first**.

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

Step 3 Select **Other: custom hosts**, and 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



2 Copy Command

☑ Turn off command history to prevent the AK/SK from being stored.

Command Generated Copy Command

Step 5 Generate the ICAgent installation command, and copy and run it to install an 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 is successfully installed, choose **Configuration Management** > **Agent Management** in the navigation pane on the left, and select **Other: custom hosts** to view the ICAgent status of the server.
- 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 Installing an ICAgent (Non-Huawei Cloud Host)

Prerequisites

- You have purchased an Elastic Cloud Server (ECS) as a jump server.
- The ECS meets the requirements listed in **OSs and versions supported by AOM** and supports the AMD64 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.

Precautions

When you install an ICAgent on a non-Huawei Cloud server, the jump server forwarding command generated by the system does not contain any domain name. That is, the ICAgent cannot be installed using a domain name.

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 4-2**.

Table 4-2 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.

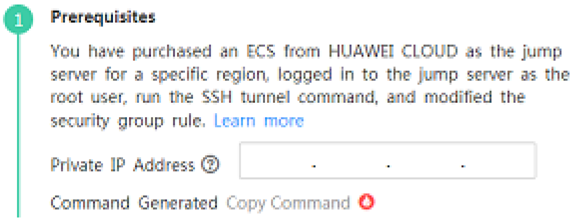
Step 2 Log in to the AOM console. In the navigation pane, choose **Configuration Management** > **Agent Management**.

Step 3 Select **Other: custom hosts**, 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 4-2**, enter a private IP address to generate the jump server forwarding command.

Figure 4-2 Private IP address of the jump server



1 **Prerequisites**

You have purchased an ECS from HUAWEI CLOUD as the jump server for a specific region, logged in to the jump server as the root user, run the SSH tunnel command, and modified the security group rule. Learn more

Private IP Address ⓘ . . .

Command Generated Copy Command

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 is located.

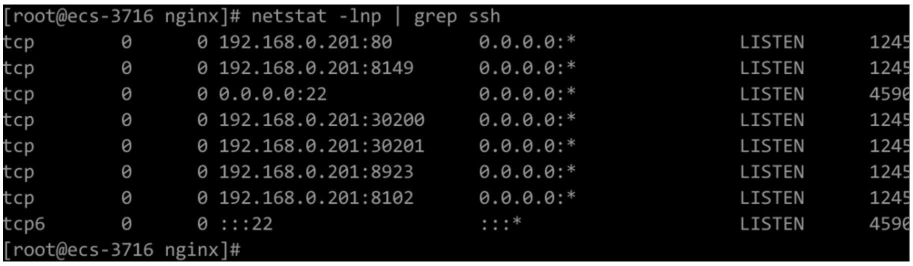
2. Click **Copy Command** to copy the jump server forwarding command.
3. Log in as the **root** user to the jump server and run the SSH tunnel forwarding command:

```
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 4-3** are returned, TCP ports are enabled.

Figure 4-3 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

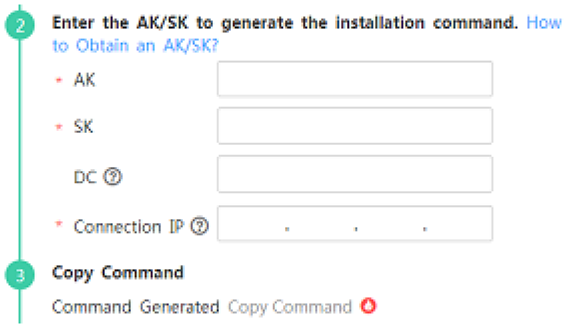
- Enter **http://***Jump server IP address* in the address bar of a browser. If the access is successful, the security group rule has taken effect.
- If the jump server powers off and restarts, run the preceding command again.

Step 5 **Obtain an AK/SK**.

Step 6 Generate and copy the ICAgent installation command.

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

Figure 4-4 Obtaining the AK/SK



2 Enter the AK/SK to generate the installation command. How to Obtain an AK/SK?

* AK

* SK

DC

* Connection IP . . .

3 Copy Command

Command Generated Copy Command

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

4.3 ICAgent Version Description

Table 4-3 ICAgent version description

Version	Description
5.12.135	● Solved the 0% CPU usage issue. ● Solved the missing container network metrics of containerd nodes in CCE 1.23 clusters. ● Supported collection of disk partition metrics of EulerOS 2.5.
5.12.133	Supported multi-line collection of standard container output logs.
5.12.130	Supported direct ingestion of CCE logs to LTS.
5.12.120	● Supported setting of the maximum number of process handles. ● Supported changing of the LTS PodLB domain name.
5.12.111	Added thread metrics and fixed the issue that the LVS disk partition metrics fail to be obtained.
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 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.

4.4 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 an 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 an 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 4-4**. 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 4-4 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**.

Filtering Rule	Example
If the **CMD** value of a process starts with **[** and ends with **]**, the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose **PID** is **2** is not discovered by AOM because its **CMD** value is **[kthreadd]**.
If the **CMD** value of a process starts with **(** and ends with **)**, the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose **PID** is **3** is not discovered by AOM because its **CMD** value is **(ksoftirqd/0)**.
If the **CMD** value of a process starts with **/sbin/**, the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose **PID** is **1148** is not discovered by AOM because its **CMD** value starts with **/sbin/**.

Built-in Discovery Rules

AOM provides two built-in discovery rules: **Sys_Rule** and **Default_Rule**. These rules are executed on all hosts, including hosts added later. The priority of **Sys_Rule** is higher than that of **Default_Rule**. That is, **Sys_Rule** is executed on the host first. If **Sys_Rule** is met, **Default_Rule** is not executed. Otherwise, **Default_Rule** is executed. Rule details are as follows:

Sys_Rule (cannot be disabled)

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

- Priorities for determining the application name:
  a. Use the value of the **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, **rule-test**.
2. Select a typical host, for example, **host-test**, to check whether the application discovery rule is valid. The hosts that execute the rule will be configured in **Step 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 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 4-5** if needed.

Table 4-5 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.

4.5 Configuring Log Collection Paths

4.5.1 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.

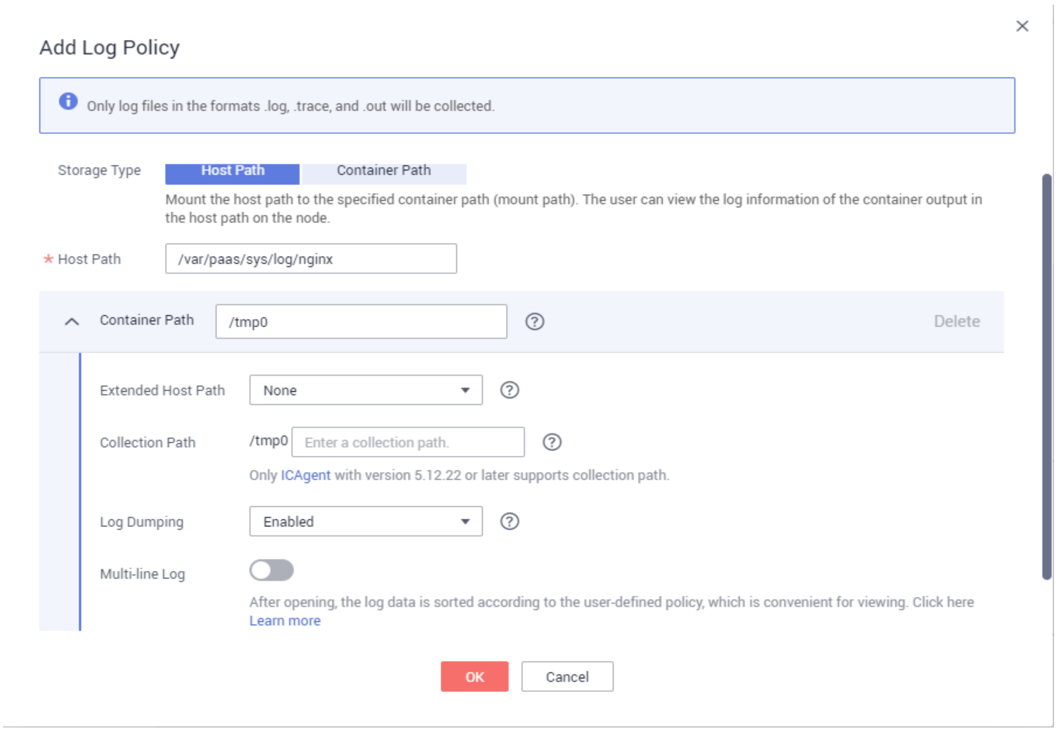
Procedure

Adding a Log Policy on CCE

Step 1 When creating a workload on the CCE console, add a container. Then, expand **Log Policies**.

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

Figure 4-5 Adding a log policy



Add Log Policy

Only log files in the formats .log, .trace, and .out will be collected.

Storage Type: Host Path | Container Path

Mount the host path to the specified container path (mount path). The user can view the log information of the container output in the host path on the node.

* Host Path: /var/paas/sys/log/nginx

Container Path: /tmp0 Delete

Extended Host Path: None

Collection Path: /tmp0 Enter a collection path.

Only ICAgent with version 5.12.22 or later supports collection path.

Log Dumping: Enabled

Multi-line Log

After opening, the log data is sorted according to the user-defined policy, which is convenient for viewing. Click here Learn more

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 4-6 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**

Parameter	Description
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. Mount the volume to an empty directory. If the directory is not empty, ensure that there are no files that affect container startup. Otherwise, the files will be replaced, causing container startup failures or workload creation failures. – If the volume is mounted to a high-risk directory, 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.
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.

- **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 4-7 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	

Parameter	Description
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. Mount the volume to an empty directory. If the directory is not empty, ensure that there are no files that affect container startup. Otherwise, the files will be replaced, causing container startup failures or workload creation failures. – If the volume is mounted to a high-risk directory, 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

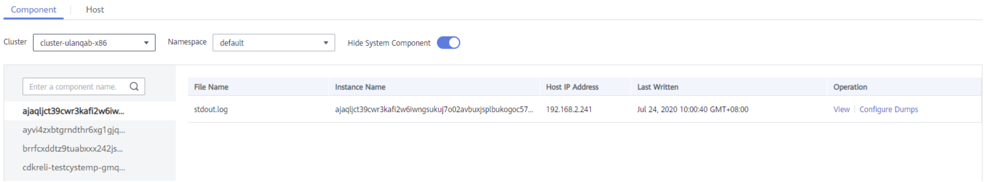
Viewing Container Logs

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 4-6 Viewing container log files

  Cluster: cluster-ulanqab-x86
  Namespace: default
  Hide System Component

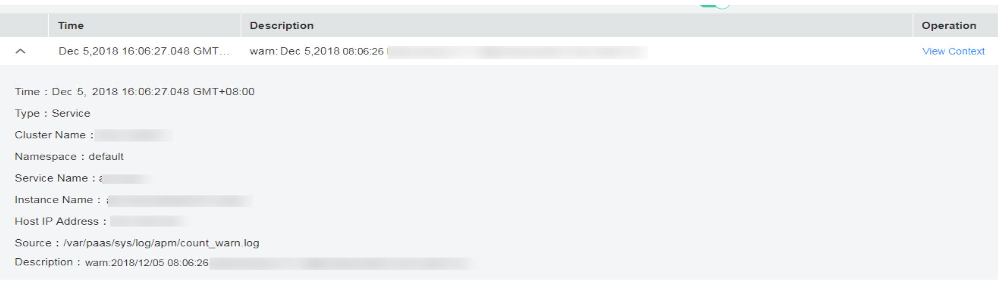
  ajaqljct39cwr3kafi2w6iw...
  ayvi4zxbtgrndthr6xg1gjq...
  brrfcxddtz9tuabxxx242js...
  cdkreli-testcystemp-gmq...

File Name	Instance Name	Host IP Address	Last Written	Operation
stdout.log	ajaqljct39cwr3kafi2w6iwngsukuj7o02avbuxjsplbukogoc57...	192.168.2.241	Jul 24, 2020 10:00:40 GMT+08:00	View | Configure Dumps

- **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 4-7 Viewing and analyzing container logs



	Time	Description	Operation
^	Dec 5,2018 16:06:27.048 GMT...	warn: Dec 5,2018 08:06:26 [redacted]	View Context

Time : Dec 5, 2018 16:06:27.048 GMT+08:00

Type : Service

Cluster Name : [redacted]

Namespace : default

Service Name : [redacted]

Instance Name : [redacted]

Host IP Address : [redacted]

Source : /var/paas/sys/log/apm/count_warn.log

Description : warn:2018/12/05 08:06:26 [redacted]

4.5.2 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 an ICAgent on a VM according to **Installing an 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

- Ensure that your VMs are ECSs or BMSs running Linux.
- 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.
- For ECSs in the same resource set, logs will be collected based on the latest log collection configuration. AOM and LTS log collection configurations cannot take effect at the same time. For example, if you set log collection paths in AOM for ECSs, the previous LTS collection configurations of all ECSs under the resource set become invalid.
- When configuring the collection path of VM logs, do not use the log paths for mapping container service logs to VMs. Otherwise, the collected VM logs may be overwritten by container logs.

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.

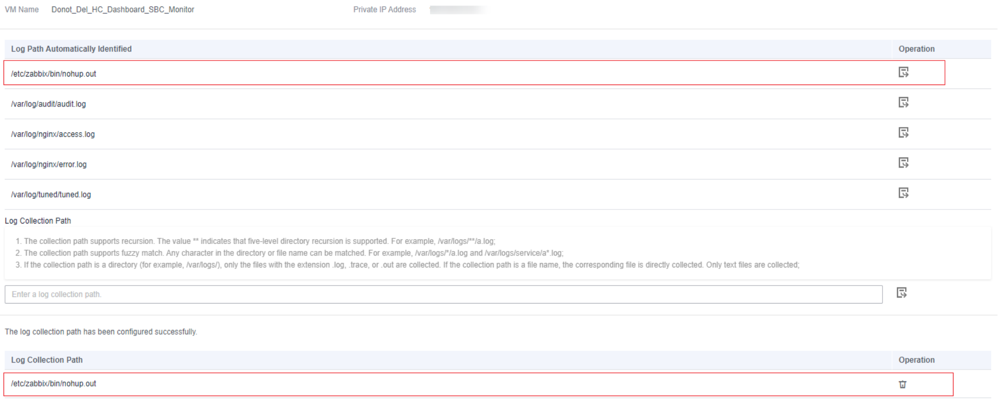
You can use the paths automatically identified by the ICAgent or manually configure paths.

- **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 4-8 Using the paths automatically identified by the ICAgent



VM Name Donot_Del_HC_Dashboard_SBC_Monitor Private IP Address [redacted]

Log Path Automatically Identified	Operation
/etc/zabbix/bin/nohup.out	⎘
/var/log/audit/audit.log	⎘
/var/log/nginx/access.log	⎘
/var/log/nginx/error.log	⎘
/var/log/tuned/tuned.log	⎘

Log Collection Path

1. The collection path supports recursion. The value ** indicates that five-level directory recursion is supported. For example, /var/logs/**/a.log;
2. The collection path supports fuzzy match. Any character in the directory or file name can be matched. For example, /var/logs/*/a.log and /var/logs/service/a*.log;
3. If the collection path is a directory (for example, /var/logs/), only the files with the extension .log, .trace, or .out are collected. If the collection path is a file name, the corresponding file is directly collected. Only text files are collected;

Enter a log collection path. ⎘

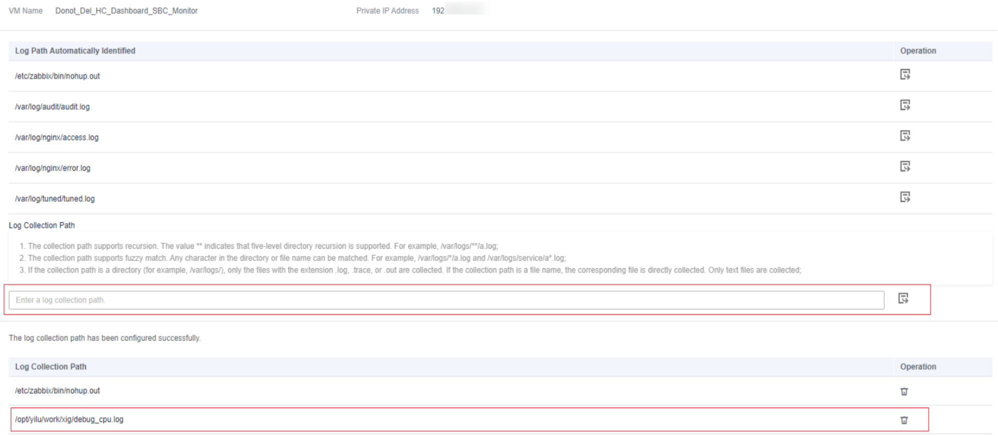
The log collection path has been configured successfully.

Log Collection Path	Operation
/etc/zabbix/bin/nohup.out	🗑

- **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 4-9 Manually configuring log collection paths



VM Name Donot_Del_HC_Dashboard_SBC_Monitor Private IP Address 192[redacted]

Log Path Automatically Identified	Operation
/etc/zabbix/bin/nohup.out	⎘
/var/log/audit/audit.log	⎘
/var/log/nginx/access.log	⎘
/var/log/nginx/error.log	⎘
/var/log/tuned/tuned.log	⎘

Log Collection Path

1. The collection path supports recursion. The value ** indicates that five-level directory recursion is supported. For example, /var/logs/**/a.log;
2. The collection path supports fuzzy match. Any character in the directory or file name can be matched. For example, /var/logs/*/a.log and /var/logs/service/a*.log;
3. If the collection path is a directory (for example, /var/logs/), only the files with the extension .log, .trace, or .out are collected. If the collection path is a file name, the corresponding file is directly collected. Only text files are collected;

Enter a log collection path. ⎘

The log collection path has been configured successfully.

Log Collection Path	Operation
/etc/zabbix/bin/nohup.out	🗑
/opt/yilu/work/xig/debug_cpu.log	🗑

Step 3 Click **OK**.

----End

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

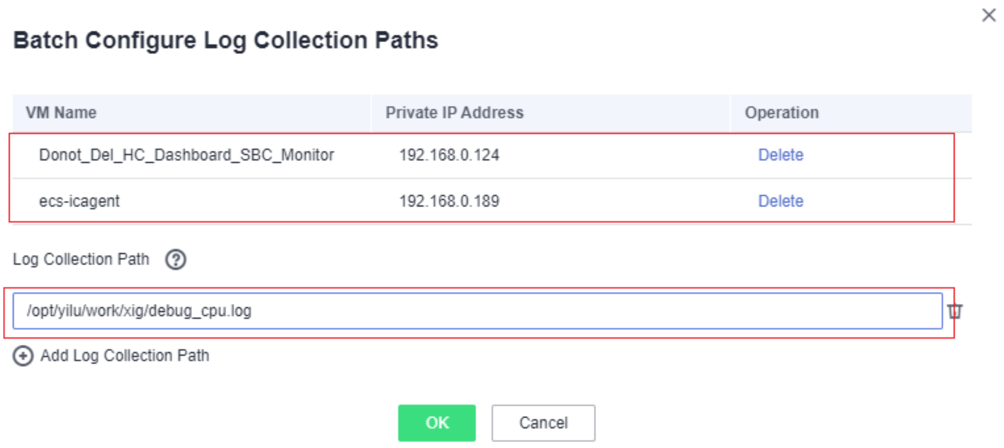
You can configure log collection paths for multiple VMs in batches. When your service is deployed on multiple VMs, you can configure log collection paths in batches to reduce workload.

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 4-10 Configuring log collection paths in batches



Batch Configure Log Collection Paths

VM Name	Private IP Address	Operation
Donot_Del_HC_Dashboard_SBC_Monitor	192.168.0.124	Delete
ecs-icagent	192.168.0.189	Delete

Log Collection Path: /opt/yilu/work/xig/debug_cpu.log

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. For details, see **Viewing 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**.

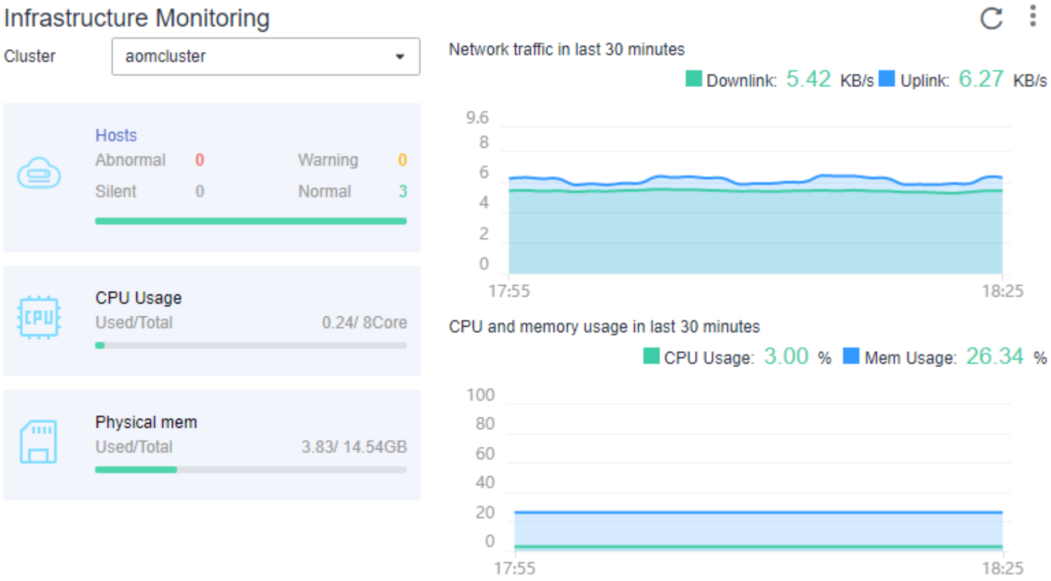
5 Monitoring Overview

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



Infrastructure Monitoring

Cluster: aomcluster

Hosts
Abnormal 0 | Warning 0
Silent 0 | Normal 3

CPU Usage
Used/Total 0.24/ 8Core

Physical mem
Used/Total 3.83/ 14.54GB

Network traffic in last 30 minutes
🟩 Downlink: 5.42 KB/s 🟦 Uplink: 6.27 KB/s

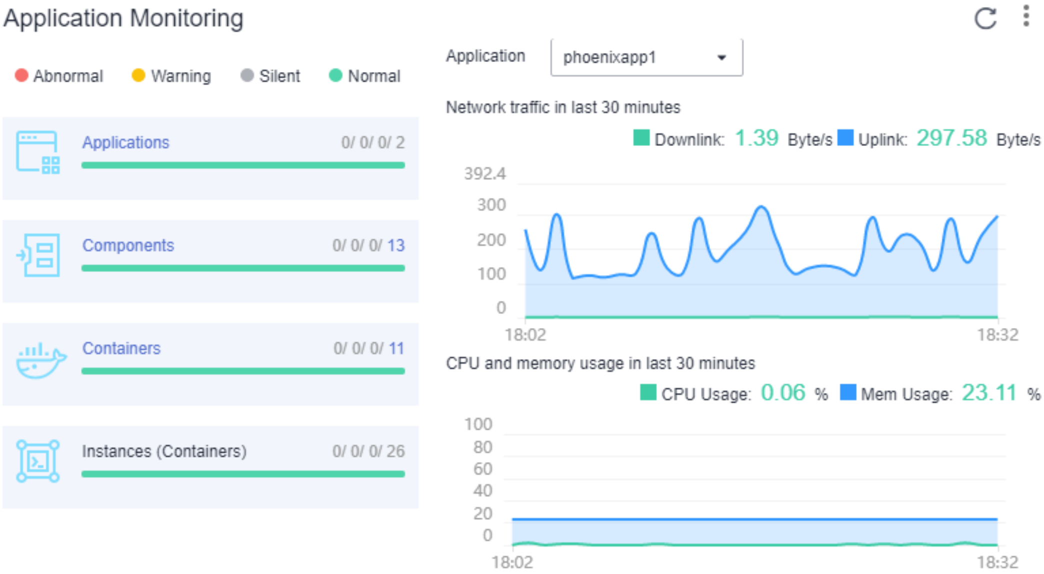
CPU and memory usage in last 30 minutes
🟩 CPU Usage: 3.00 % 🟦 Mem Usage: 26.34 %

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 in the last 30 minutes. 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 30 minutes. 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



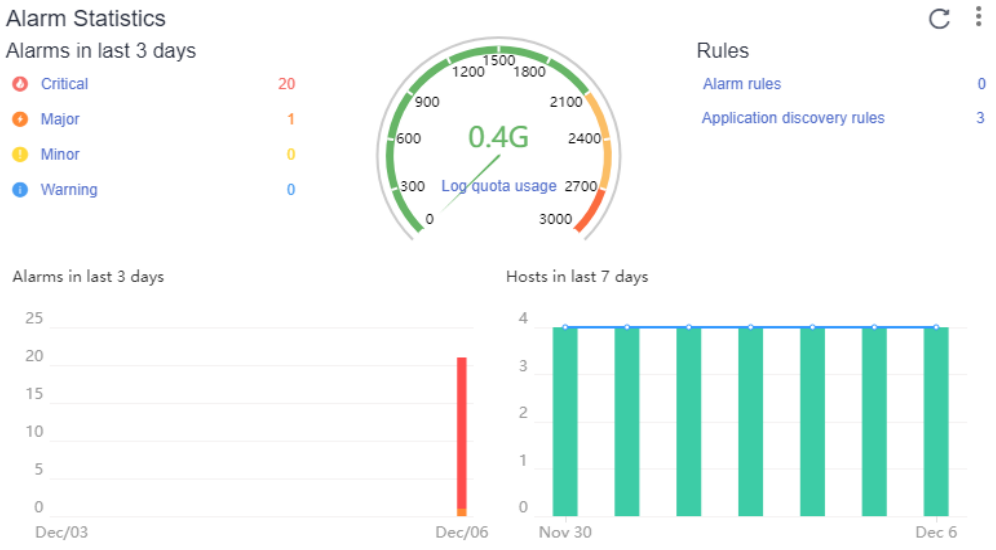
Application phoenixapp1

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 in the last 30 minutes. 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 30 minutes. 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



Alarm Statistics

Alarms in last 3 days

Critical	20
Major	1
Minor	0
Warning	0

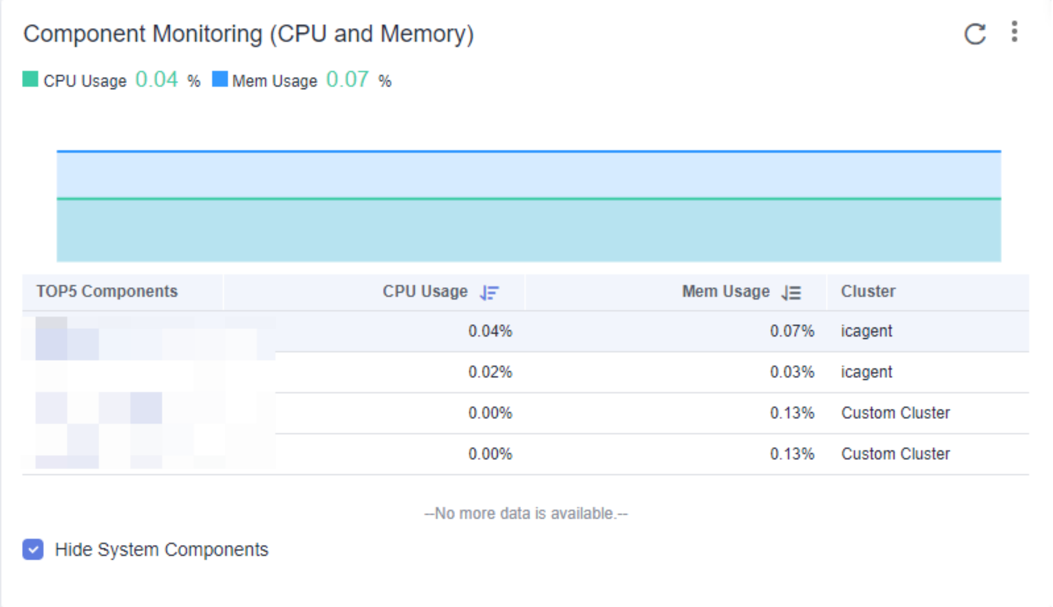
Rules

Alarm rules	0
Application discovery rules	3

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

Component Monitoring (CPU and Memory) Card

Figure 5-4 Component monitoring (CPU and memory)



Component Monitoring (CPU and Memory)

🟩 CPU Usage 0.04 % 🟦 Mem Usage 0.07 %

TOP5 Components	CPU Usage	Mem Usage	Cluster
[redacted]	0.04%	0.07%	icagent
[redacted]	0.02%	0.03%	icagent
[redacted]	0.00%	0.13%	Custom Cluster
[redacted]	0.00%	0.13%	Custom Cluster

--No more data is available.--

☑ Hide System Components

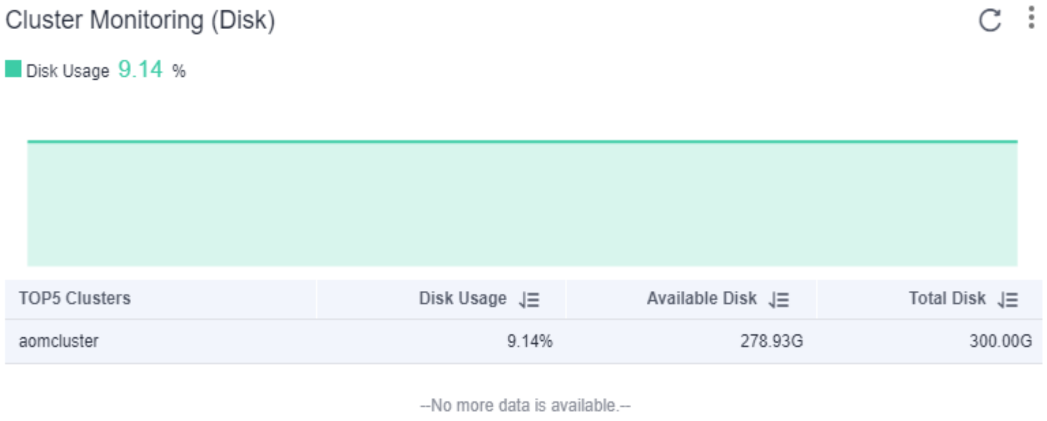
This card mainly displays:

- 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.
- You can select **Hide system components** in the lower left corner.

Cluster Monitoring (Disk) Card

Figure 5-5 Cluster monitoring (disk)



Cluster Monitoring (Disk)

🟩 Disk Usage 9.14 %

TOP5 Clusters	Disk Usage	Available Disk	Total Disk
aomcluster	9.14%	278.93G	300.00G

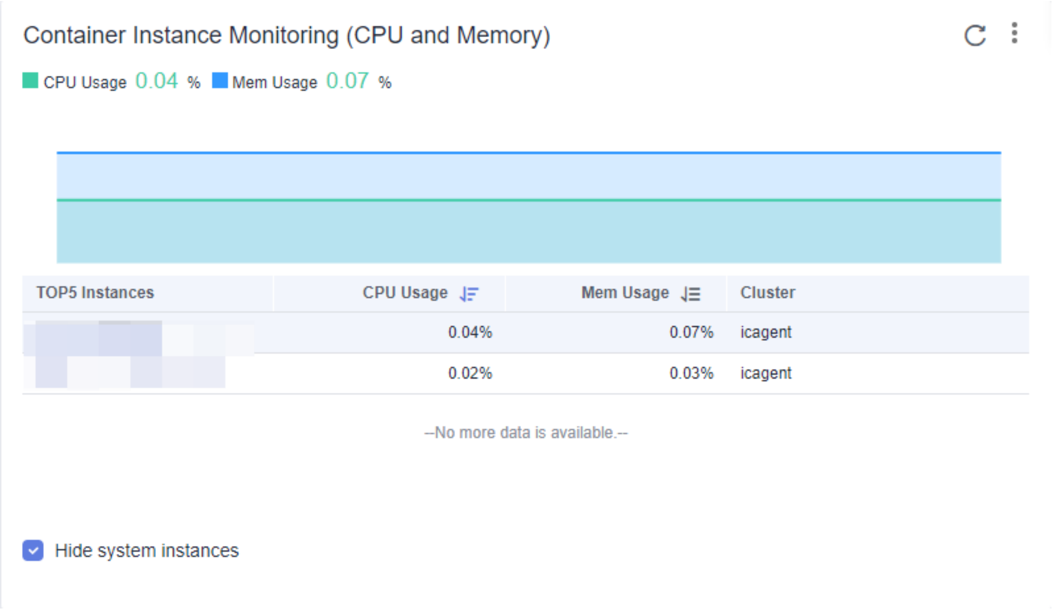
--No more data is available.--

This card mainly displays:

- The top 5 clusters with high disk usage in the last minute.
- Trend graph of the disk usage of the selected cluster in the last hour. The value of each point in the graph indicates the disk usage of the cluster in one minute.
- Disk usage of the selected cluster at the latest time point, which is displayed above the trend graph.

Container Instance Monitoring (CPU and Memory) Card

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



Container Instance Monitoring (CPU and Memory)

🟩 CPU Usage 0.04 % 🟦 Mem Usage 0.07 %

TOP5 Instances	CPU Usage	Mem Usage	Cluster
[redacted]	0.04%	0.07%	icagent
[redacted]	0.02%	0.03%	icagent

--No more data is available.--

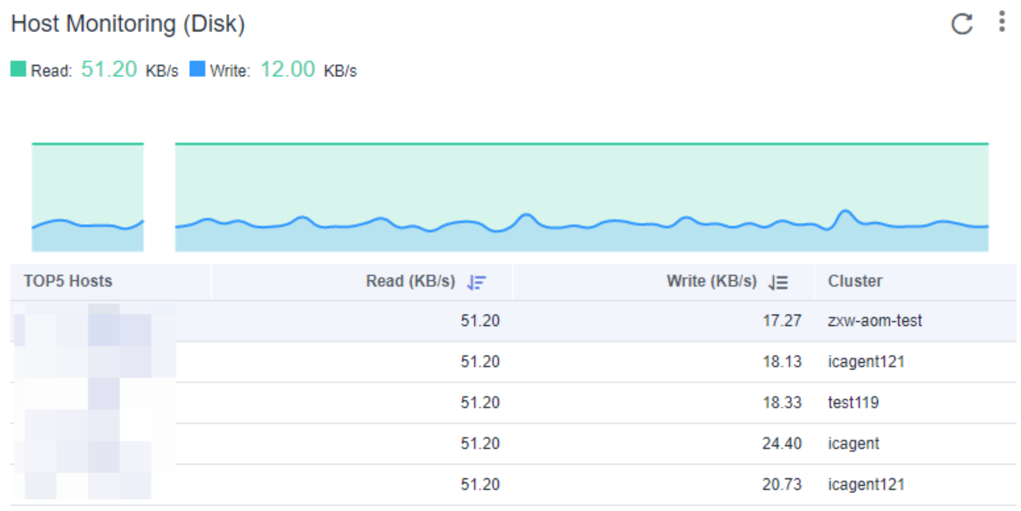
☑ Hide system instances

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.
- You can select **Hide system instances** in the lower left corner.

Host Monitoring (Disk) Card

Figure 5-7 Host monitoring (disk)



Host Monitoring (Disk)

🟩 Read: 51.20 KB/s 🟦 Write: 12.00 KB/s

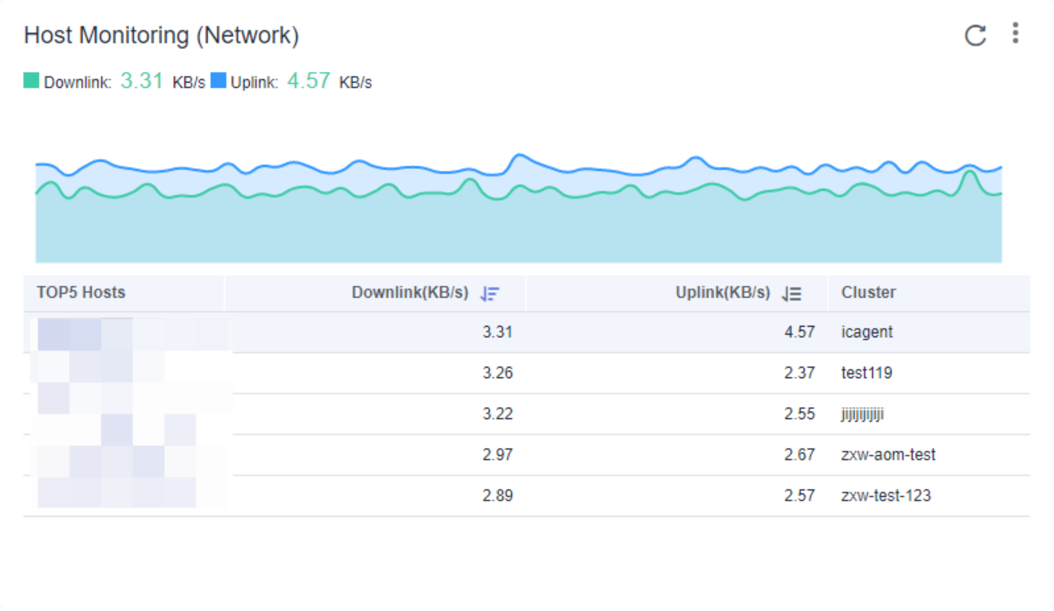
TOP5 Hosts	Read (KB/s)	Write (KB/s)	Cluster
[redacted]	51.20	17.27	zxw-aom-test
[redacted]	51.20	18.13	icagent121
[redacted]	51.20	18.33	test119
[redacted]	51.20	24.40	icagent
[redacted]	51.20	20.73	icagent121

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)



Host Monitoring (Network)

🟩 Downlink: 3.31 KB/s 🟦 Uplink: 4.57 KB/s

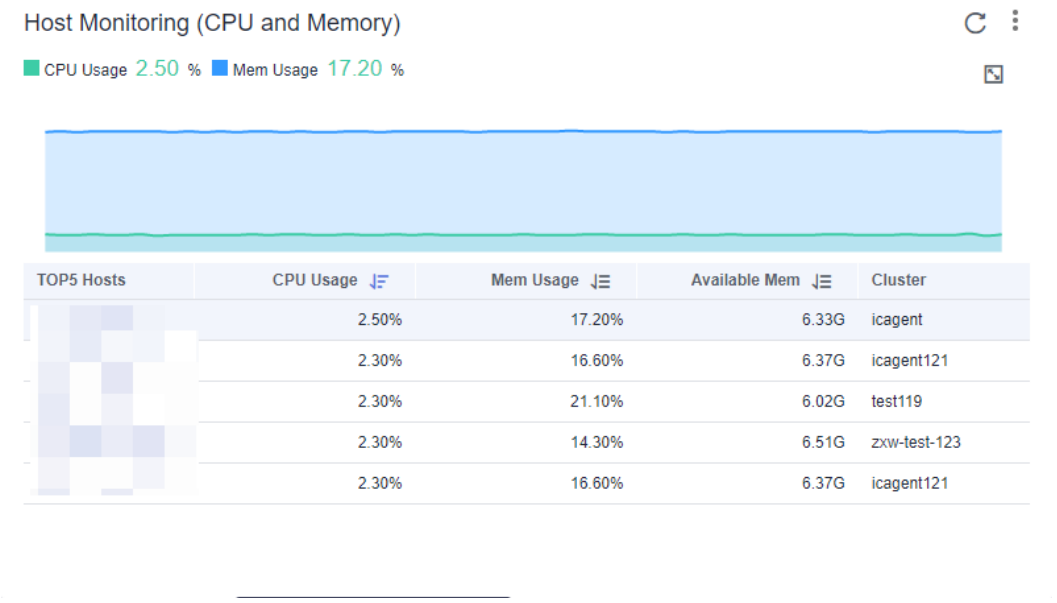
TOP5 Hosts	Downlink(KB/s)	Uplink(KB/s)	Cluster
[redacted]	3.31	4.57	icagent
[redacted]	3.26	2.37	test119
[redacted]	3.22	2.55	jijijijijiji
[redacted]	2.97	2.67	zxw-aom-test
[redacted]	2.89	2.57	zxw-test-123

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.

Host Monitoring (CPU and Memory) Card

Figure 5-9 Host monitoring (CPU and memory)



Host Monitoring (CPU and Memory)

🟩 CPU Usage 2.50 % 🟦 Mem Usage 17.20 %

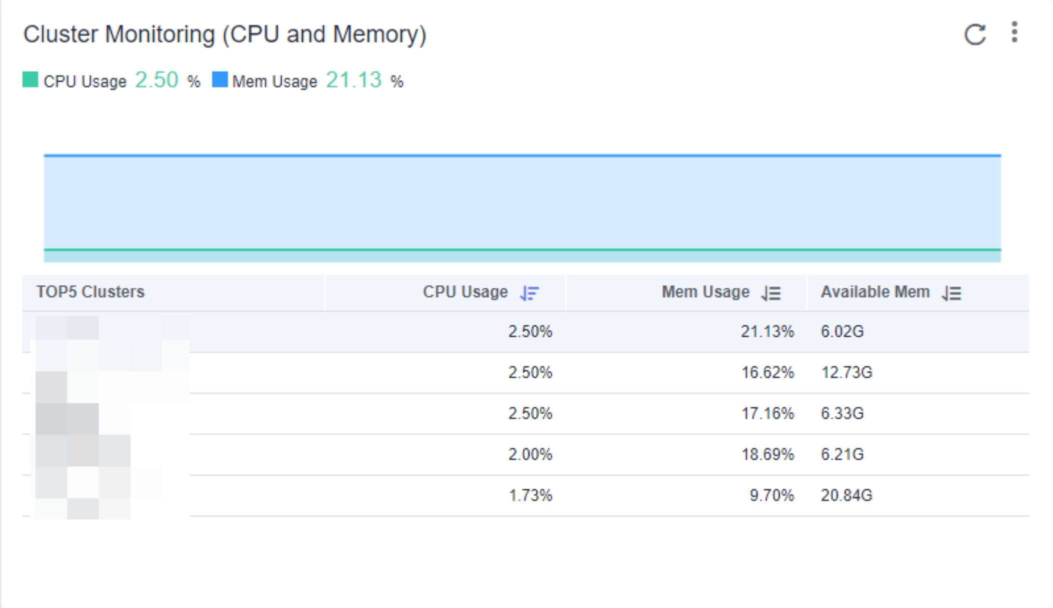
TOP5 Hosts	CPU Usage	Mem Usage	Available Mem	Cluster
[redacted]	2.50%	17.20%	6.33G	icagent
[redacted]	2.30%	16.60%	6.37G	icagent121
[redacted]	2.30%	21.10%	6.02G	test119
[redacted]	2.30%	14.30%	6.51G	zxw-test-123
[redacted]	2.30%	16.60%	6.37G	icagent121

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.

Cluster Monitoring (CPU and Memory) Card

Figure 5-10 Cluster monitoring (CPU and memory)



Cluster Monitoring (CPU and Memory)

🟩 CPU Usage 2.50 % 🟦 Mem Usage 21.13 %

TOP5 Clusters	CPU Usage	Mem Usage	Available Mem
[redacted]	2.50%	21.13%	6.02G
[redacted]	2.50%	16.62%	12.73G
[redacted]	2.50%	17.16%	6.33G
[redacted]	2.00%	18.69%	6.21G
[redacted]	1.73%	9.70%	20.84G

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.

Operation	Description
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.

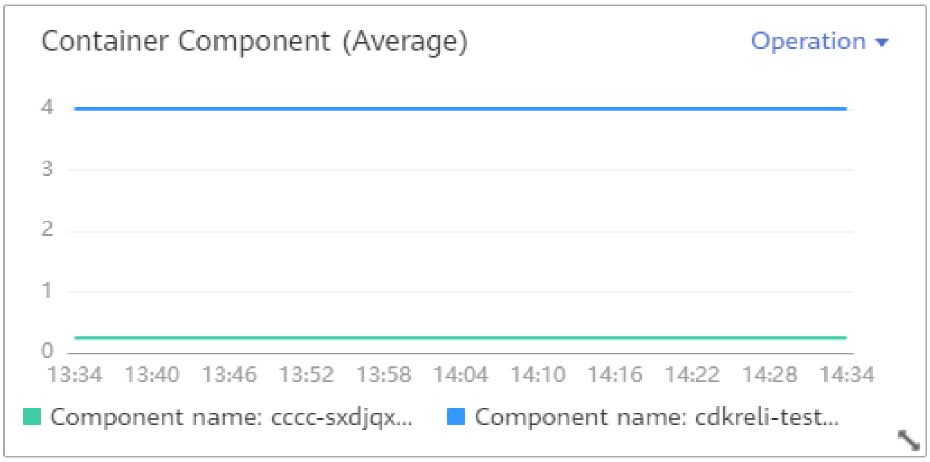
Before creating a dashboard, learn the types of graphs that can be added to the dashboard for accurate resource monitoring. The following graphs can be added to the dashboard:

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.

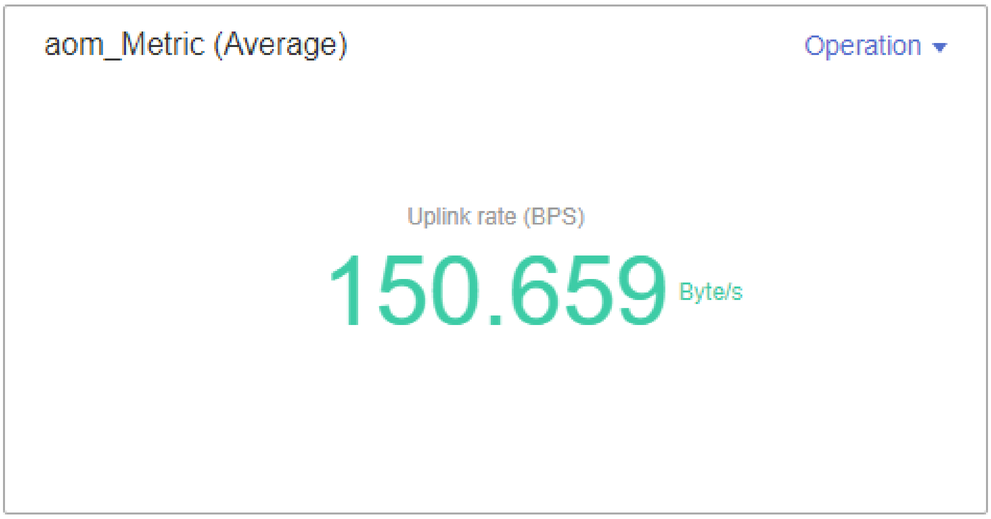
  Figure 5-11 Line graph

- **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 5-12 Digit graph

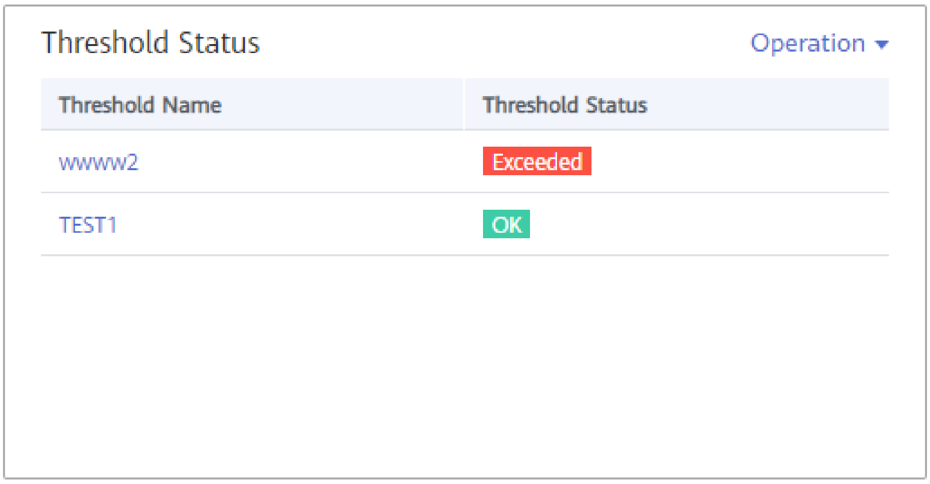


Health Status Graphs (Including Threshold, Host, and Component Status Graphs)

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 5-13 Threshold status graph



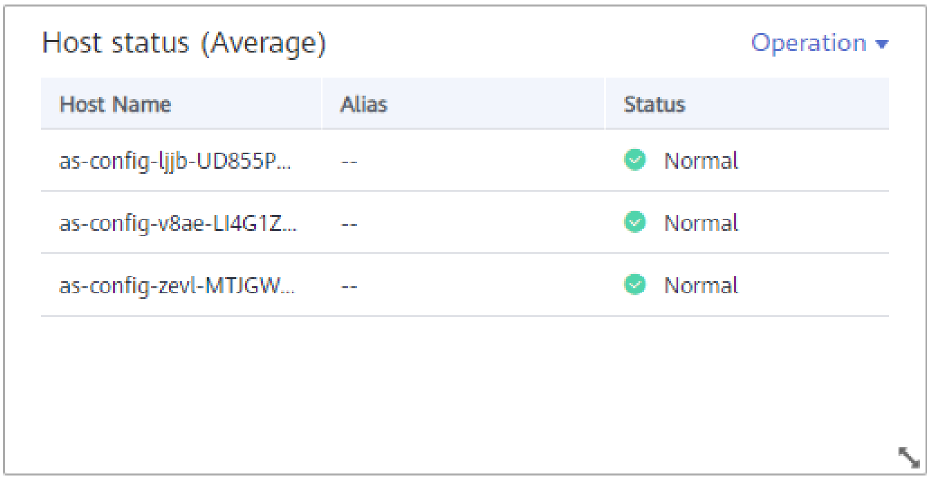
Threshold Name	Threshold Status
wwww2	Exceeded
TEST1	OK

NOTE

Before adding a threshold 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 5-14 Host status graph

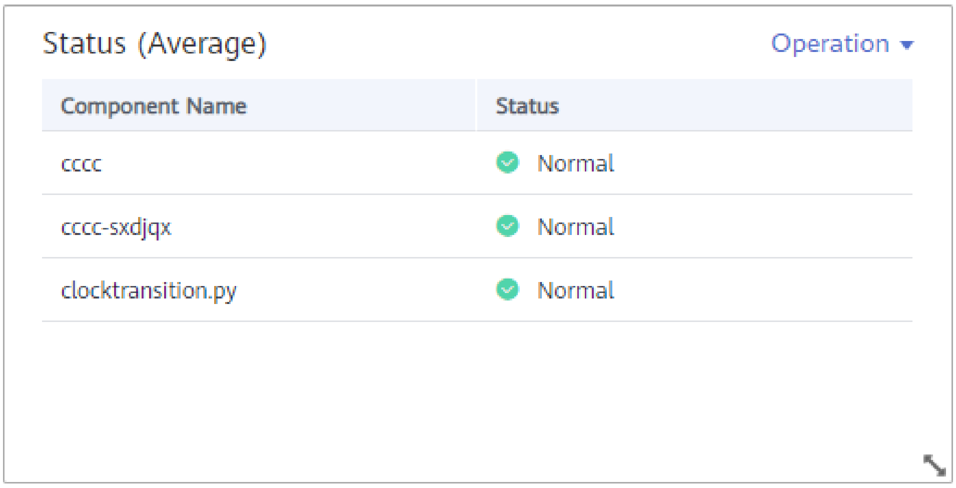


Host status (Average)

Host Name	Alias	Status
as-config-ljjb-UD855P...	--	✓ Normal
as-config-v8ae-LI4G1Z...	--	✓ Normal
as-config-zevl-MTJGW...	--	✓ Normal

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

Figure 5-15 Component status graph



Status (Average)

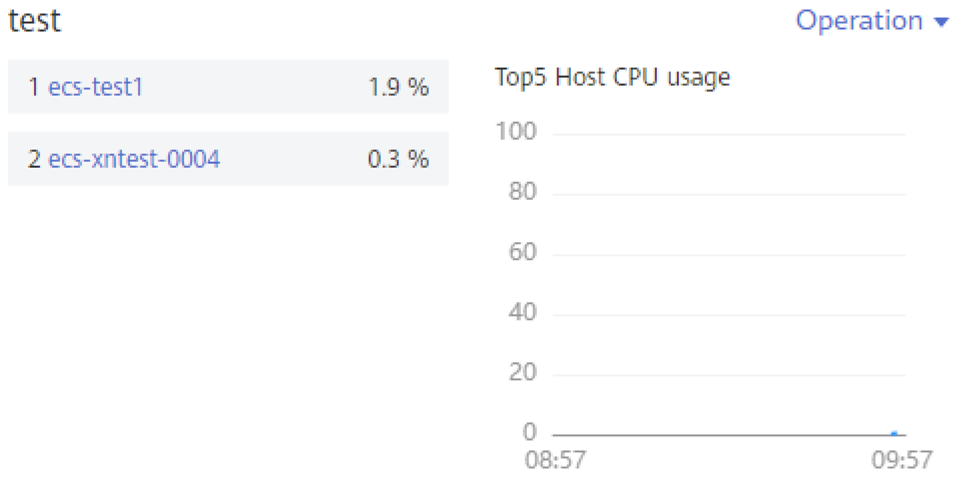
Component Name	Status
cccc	✓ Normal
cccc-sxdjqx	✓ Normal
clocktransition.py	✓ Normal

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 5-16 Top N resource graph



test

1 ecs-test1	1.9 %
2 ecs-xntest-0004	0.3 %

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**.

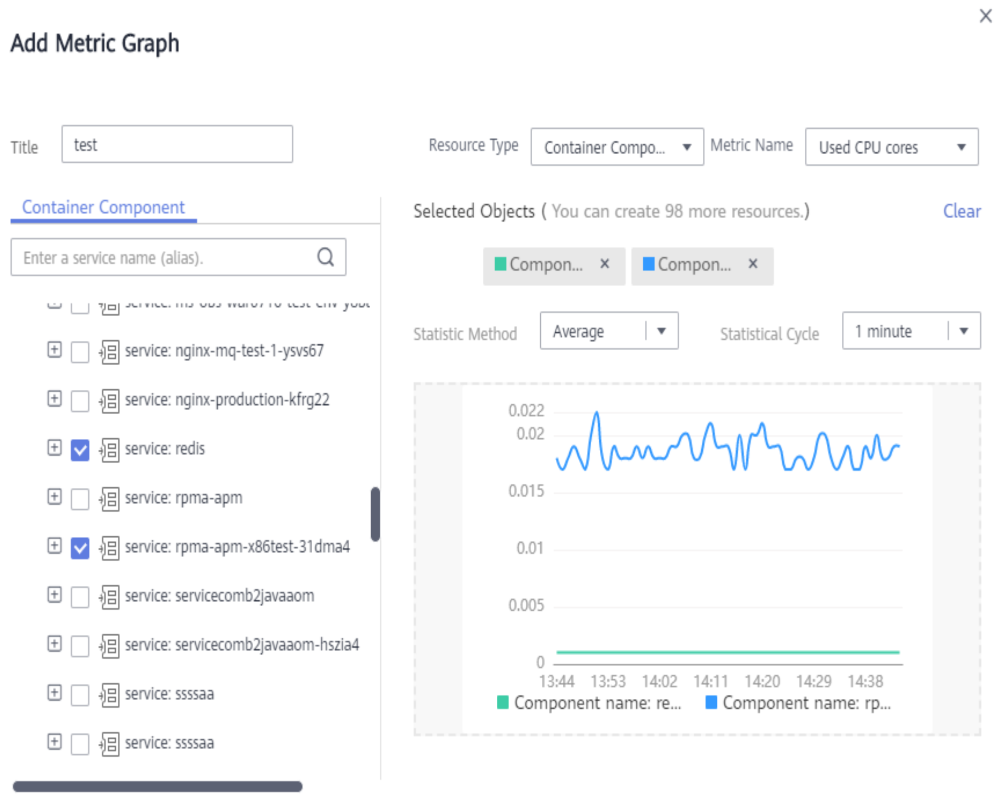
Step 2 On the **Dashboard** page, click **Create Dashboard**. In the displayed **Create Dashboard** dialog box, enter a dashboard name and click **OK**.

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 meets 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 **Statistical Mode** and **Statistical Cycle**, and click **OK**.

Figure 5-17 Adding a metric graph



Add Metric Graph

Title: test

Resource Type: Container Compo... ▾ Metric Name: Used CPU cores ▾

Container Component

Enter a service name (alias).

- ⊞ □ service: nginx-mq-test-1-ysvs67
- ⊞ □ service: nginx-production-kfrg22
- ⊞ ☑ service: redis
- ⊞ □ service: rpma-apm
- ⊞ ☑ service: rpma-apm-x86test-31dma4
- ⊞ □ service: servicecomb2javaaom
- ⊞ □ service: servicecomb2javaaom-hszia4
- ⊞ □ service: ssssaa
- ⊞ □ service: ssssaa

Selected Objects (You can create 98 more resources.) Clear

🟩 Compon... × 🟦 Compon... ×

Statistic Method: Average ▾ Statistical Cycle: 1 minute ▾

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.

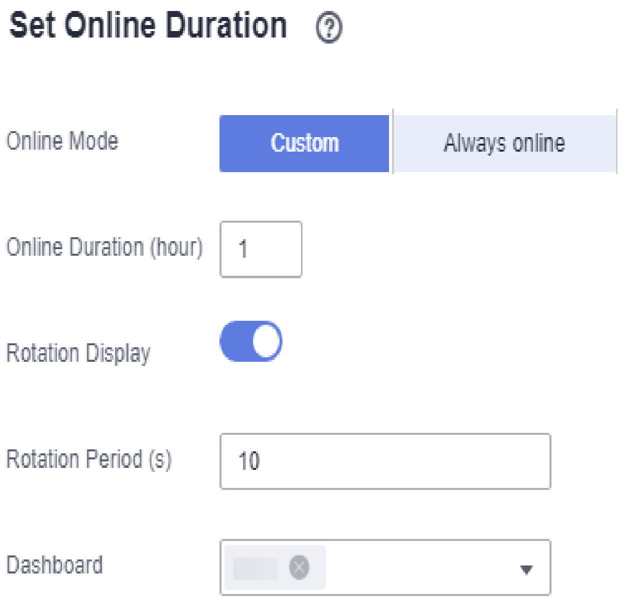
----End

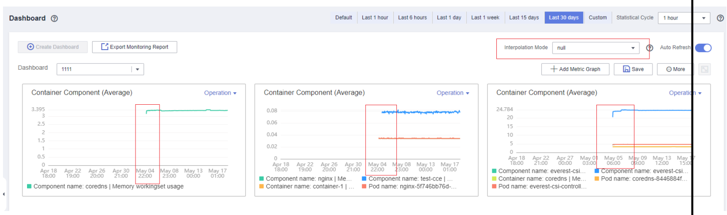
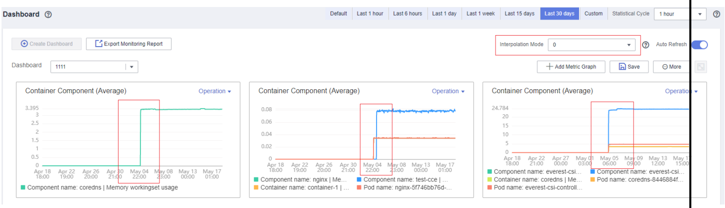
More Operations

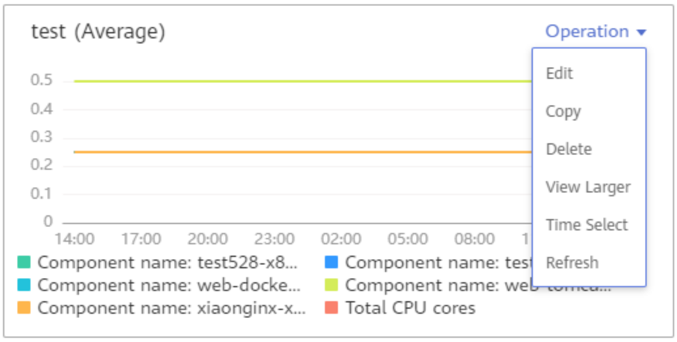
After creating a dashboard, perform the operations listed in **Table 5-2** if needed.

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	
	Export a monitoring report	Click **Export Monitoring Report** to export a line graph in the dashboard as a CSV file to a local PC.

Object	Operation	Description
	Set the full-screen online duration	1. Select the target dashboard and click ⤢ in the upper right corner of the **Dashboard** page. 2. In the dialogue box that is displayed, set the full-screen online duration. **Figure 5-18** Setting the online duration  Set Online Duration Online Mode: Custom | Always online Online Duration (hour): 1 Rotation Display Rotation Period (s): 10 Dashboard **NOTE** - **Custom**: The default online duration is 1 hour. You can enter 1–24 (unit: hour) in the text box. For example, if you enter **2** in the text box, the login page is automatically displayed 2 hours later. - **Always online**: The full-screen online duration is not restricted. That is, you can always implement full-screen monitoring and the login page will never be displayed. - **Rotation Period**: Set **Rotation Period** and **Dashboard** if rotation display is enabled. Range: 10s (default) to 120s. 3. Click **OK** to enter the full-screen mode.

Object	Operation	Description
	Set an interpolation mode	Click **Interpolation Mode** to set a mode for aggregating metric data. By default, AOM uses **null** to represent breakpoints in a metric graph. However, a metric graph with breakpoints is not suitable for reporting or presentation. To solve the problem, set **Interpolation Mode** to **0** or **null** to interpolate values. In this way, you can replace the missing metric data and avoid breakpoints. You can set **Interpolation Mode** to **null**, or **0**. ● **null**: Breakpoints are represented by **null** by default. See the following figure. **Figure 5-19** Graph when **Interpolation Mode** is **null**  Interpolation Mode null Dashboard Default Last 1 hour Last 6 hours Last 1 day Last 1 week Last 15 days Last 30 days Custom Statistical Cycle 1 hour Create Dashboard Export Monitoring Report Auto Refresh Dashboard 1111 Add Metric Graph Save More Container Component (Average) Operation Component name: coredns | Memory workingset usage Component name: nginx | Me... Component name: test-cce | ... Container name: container-1 | ... Pod name: nginx-5f746bb76d-... Component name: everest-csi... Container name: coredns | Me... Pod name: coredns-8446884f... Pod name: everest-csi-controll... ● **0**: Breakpoints are indicated by **0**. See the following figure. **Figure 5-20** Graph when **Interpolation Mode** is **0**  Interpolation Mode 0 Dashboard Default Last 1 hour Last 6 hours Last 1 day Last 1 week Last 15 days Last 30 days Custom Statistical Cycle 1 hour Create Dashboard Export Monitoring Report Auto Refresh Dashboard 1111 Add Metric Graph Save More Container Component (Average) Operation Component name: coredns | Memory workingset usage Component name: nginx | Me... Component name: test-cce | ... Container name: container-1 | ... Pod name: nginx-5f746bb76d-... Component name: everest-csi... Container name: coredns | Me... Pod name: coredns-8446884f... Pod name: everest-csi-controll...
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.

Object	Operation	Description
	Edit	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 5-21** Operations on a graph  test (Average) Operation Edit Copy Delete View Larger Time Select Refresh 0.5 0.4 0.3 0.2 0.1 0 14:00 17:00 20:00 23:00 02:00 05:00 08:00 Component name: test528-x8... Component name: tes Component name: web-docke... Component name: we Component name: xiaonginx-x... Total CPU cores **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.
	Copy	
	Delete	
	Zoom in	
	Time select	
	Refresh	
	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.

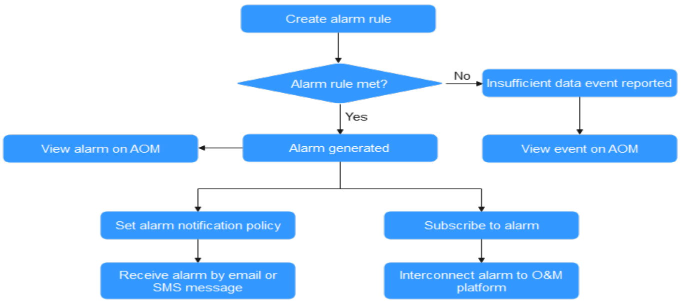
6 Alarm Management

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 an ICAgent**. **Figure 6-1** shows how to use this function.

Figure 6-1 Alarm management process


Create alarm rule
Alarm rule met?
No
Insufficient data event reported
Yes
View alarm on AOM
Alarm generated
View event on AOM
Set alarm notification policy
Subscribe to alarm
Receive alarm by email or SMS message
Interconnect alarm to O&M platform

6.2 Alarm Rules (Old)

6.2.1 Adding Threshold Rules

This function is available in AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago.

You can set threshold conditions for resource metrics by setting 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 threshold rule changes (**Exceeded**, **OK**, or **Insufficient**). In this way, you can identify and handle exceptions at the earliest time.

Precautions

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

  If you want to send notifications by email or SMS message when the threshold rule status (**Exceeded**, **Normal**, or **Insufficient**) changes, set a notification policy on the 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**.

  b. **Set a topic policy**.

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

  c. **Add a subscription to a topic**.

Creating a Threshold Rule

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 a threshold rule.

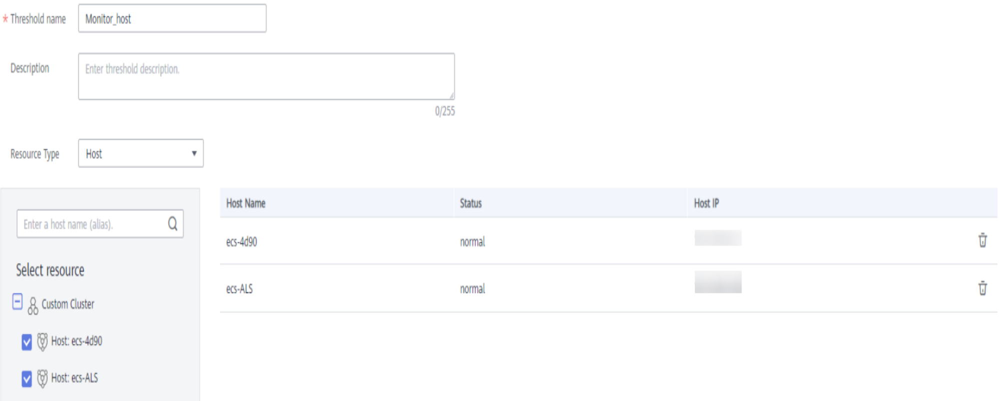
1. Select resources: Enter a threshold name, select a resource type, select the resources to be monitored from the resource tree, and click **Next**.

   NOTE

   – You can select a maximum of 100 resources from the resource tree.

   – When multiple resources are selected, multiple single-resource threshold rules will be created after the creation is complete. Each resource is monitored by a single-resource 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



* Threshold name: Monitor_host

Description: Enter threshold description.

0/255

Resource Type: Host ▾

Enter a host name (alias).

Select resource

⊟ Custom Cluster

☑ Host: ecs-4d90

☑ Host: ecs-ALS

Host Name	Status	Host IP
ecs-4d90	normal	[redacted]
ecs-ALS	normal	[redacted]

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 Periods**: 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 threshold rule status (**Exceeded**, **Normal**, or **Insufficient**) changes.

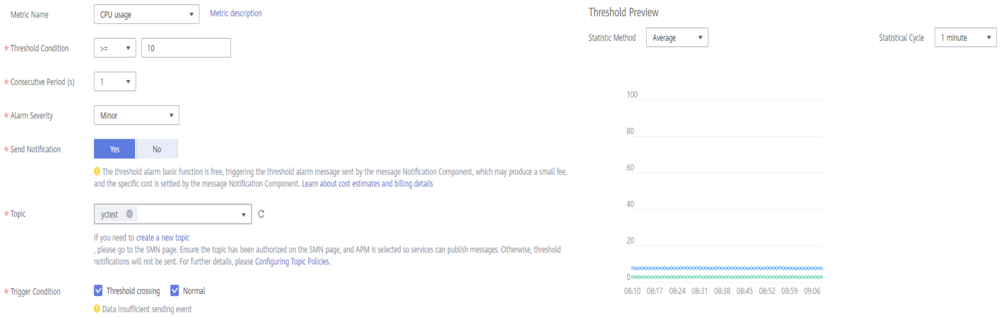
     ■ If you want to receive email or SMS notifications, select **Yes**, set **a notification policy**, select a created topic, and select a trigger scenario.

     ■ 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



Metric Name: CPU usage ▾ Metric description

* Threshold Condition: >= ▾ 10

* Consecutive Period (s): 1 ▾

* Alarm Severity: Minor ▾

* Send Notification: Yes | No

The threshold alarm basic function is free, triggering the threshold alarm message sent by the message Notification Component, which may produce a small fee, and the specific cost is settled by the message Notification Component. Learn about cost estimates and billing details

* Topic: yctest ▾

If you need to create a new topic
, please go to the SMN page. Ensure the topic has been authorized on the SMN page, and APM is selected so services can publish messages. Otherwise, threshold notifications will not be sent. For further details, please Configuring Topic Policies.

* Trigger Condition: ☑ Threshold crossing ☑ Normal

Data insufficient sending event

Threshold Preview

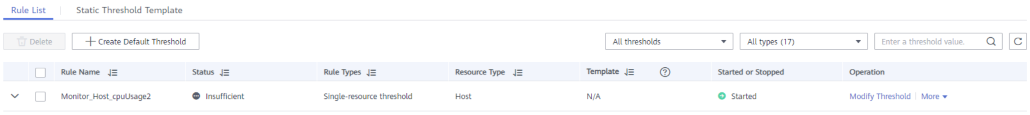
Statistic Method: Average ▾

Statistical Cycle: 1 minute ▾

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

A single-resource 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 threshold rule



	Rule Name	Status	Rule Types	Resource Type	Template	Started or Stopped	Operation
□	Monitor_Host_cpuUsage2	● Insufficient	Single-resource threshold	Host	N/A	● Started	Modify Threshold | More

----End

More Operations

After creating threshold rules, perform the operations listed in **Table 6-1** if needed.

Table 6-1 Related operations

Operation	Description
Modifying a threshold rule	Choose **Modify Threshold** in the **Operation** column.
Deleting a threshold rule	● To delete a threshold rule, choose **More** > **Delete** in the **Operation** column. ● To delete one or more threshold rules, select them and click **Delete** above the rule list.
Searching for a 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.

6.3 Alarm Rules (New)

6.3.1 Overview

This function is available in CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, and AP-Singapore.

By setting alarms rules, you can define event conditions for services or threshold conditions for resource metrics. An event alarm is generated when the resource data of a service meets the event condition. A threshold alarm is generated when the metric data of a resource meets the threshold condition. An insufficient data event is generated when no metric data is reported.

Alarm rules are classified into threshold rules and event alarm rules. Generally, threshold rules are used to monitor the usage of resources such as hosts and components in the environment in real time. When there are too many resource usage alarms and 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 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 Alarm Tags and Annotations

When creating alarm rules, you can set alarm tags and annotations. Tags are attributes that can be used to identify alarms. They are applied to the alarm noise reduction scenario. Annotations are attributes that cannot be used to identify alarms. They are applied to scenarios such as alarm notification and message templates.

Alarm Tags

- Alarm tags can apply to grouping rules, suppression rules, and silence rules. The alarm management system manages alarms and notifications based on the tags.
- Each tag is in "key:value" format and can be customized. The key and value can contain only letters, digits, and underscores (_) and cannot start with an underscore (_). You can create up to 10 custom tags.
- If you set a tag when creating an alarm rule, the tag is automatically added as an alarm attribute when an alarm is triggered.
- In the message template, the **$event.metadata.key1** variable specifies the tag. For details, see **Table 6-13**.

Alarm Annotations

- Annotations are attributes that cannot be used to identify alarms. They are applied to scenarios such as alarm notification and message templates.

- Each annotation is in "key:value" format and can be customized. The key and value can contain only letters, digits, and underscores (_) and cannot start with an underscore (_). You can create up to 10 custom annotations.
- In the message template, the **$event.annotations.key2** variable specifies the annotation. For details, see **Table 6-13**.

6.3.3 Creating a Threshold Rule

You can set threshold conditions for resource metrics by setting 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 Threshold Rules** and **Using Templates to Create 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 threshold rules, ensure that a static threshold template has been created according to **Creating a Static Threshold Template**.

Precautions

- If you need AOM to send email or SMS notifications when the threshold rule status (**Exceeded**, **Normal**, **Insufficient**, or **Disabled**) changes, set an alarm action rule according to **Creating an Alarm Action Rule**.
- If you use a threshold rule to monitor the same metric of multiple resources in batches, pay attention to the following:
  - If the metric status of a resource is **Exceeded**, the status of the threshold rule is also **Exceeded**.
  - If the metric status of one or more resources is **Insufficient** or **Normal**, the status of the threshold rule is **Normal**.

Directly Creating 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 Set a threshold rule.

1. Set basic information such as the rule name and description.
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 objects: Click **Select Resource Object**, add objects by dimension or resource, and click **Confirm**.

NOTE

- ○ A threshold rule can monitor up to 100 pieces of metric data.
- ○ If you enable **Apply to All** (●) when selecting objects to monitor, an alarm rule will be created for all metrics of the type you select under an application or service. For example, if you select **CCE/Host/Host/CPU Usage** and enable **Apply to All**, an alarm rule will be created for all hosts in CCE.
- ○ Click **Edit resource objects** to modify the selected resource object.

- ■ 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 command **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)**.

    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.

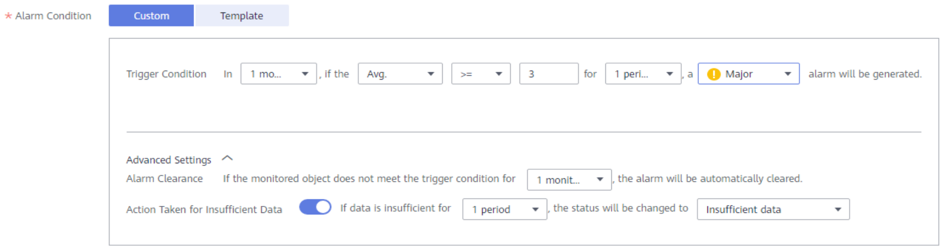
c. Set an alarm condition. Click **Custom** and set information such as **Statistical Period**, **Consecutive Periods**, and **Threshold Criterion**. **Table 6-2** describes the parameters.

Table 6-2 Alarm condition parameters

Category	Parameter	Description
Trigger Condition	Statistical Period	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.

Category	Parameter	Description
	Statistic	Method used to measure metrics. Options: **Avg.**, **Min.**, **Max.**, **Sum**, and **Samples**.
	Threshold Condition	Trigger condition of a threshold alarm. A threshold condition consists of two parts: operators (≥, ≤, >, and <) and threshold value. For example, after **Threshold Criterion** is set to **> 85**, if the actual metric value exceeds 85, a threshold alarm is generated. Move the cursor to the graph area above the alarm condition. The ID, IP address, and unit of the current metric are displayed.
	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 set 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 6-5 Setting an alarm condition



* Alarm Condition: Custom | Template

Trigger Condition: In 1 mo... , if the Avg. >= 3 for 1 peri... , a Major alarm will be generated.

Advanced Settings

Alarm Clearance: If the monitored object does not meet the trigger condition for 1 monit... , the alarm will be automatically cleared.

Action Taken for Insufficient Data: If data is insufficient for 1 period , the status will be changed to Insufficient data

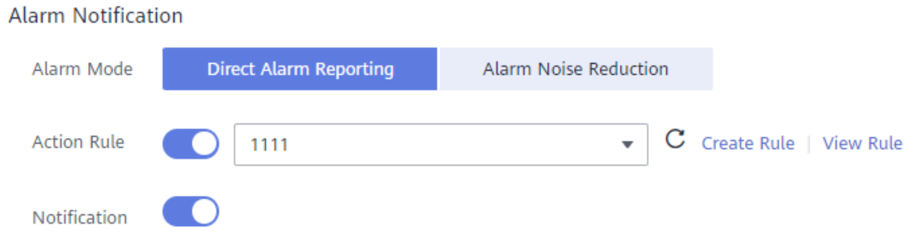
d. Set alarm tags and annotations to group alarms. They can be associated with alarm noise reduction policies for sending alarm notifications. For details, see **Alarm Tags and Annotations**.

   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.
  1. Specify whether to enable an alarm action rule. After an alarm action rule is enabled, the system sends notifications based on the associated SMN topic and message template. If the existing alarm action rules cannot meet your requirements, click **Create Rule** to create one. For details, see **Creating an Alarm Action Rule**.
  2. After an alarm action rule is selected, specify whether to enable alarm clearance notification. After alarm clearance notification is enabled, if the alarm clearance condition set in **Advanced Settings > Alarm Clearance** is met, alarm clearance notifications are sent based on the selected action rule.

Figure 6-6 Selecting the direct alarm reporting mode



Alarm Notification

Alarm Mode: Direct Alarm Reporting | Alarm Noise Reduction

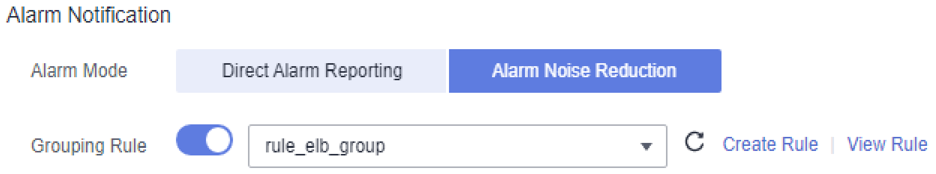
Action Rule: 1111

Notification

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

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

Figure 6-7 Selecting the alarm noise reduction mode



Alarm Notification

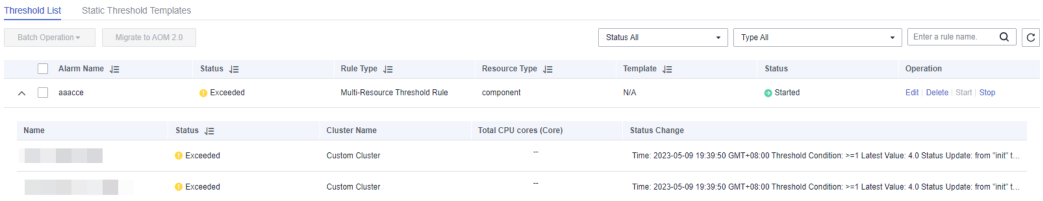
Alarm Mode: Direct Alarm Reporting | Alarm Noise Reduction

Grouping Rule: rule_elb_group

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

In the expanded list, if the metric data of a host meets the preset alarm condition, 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 or SMS.

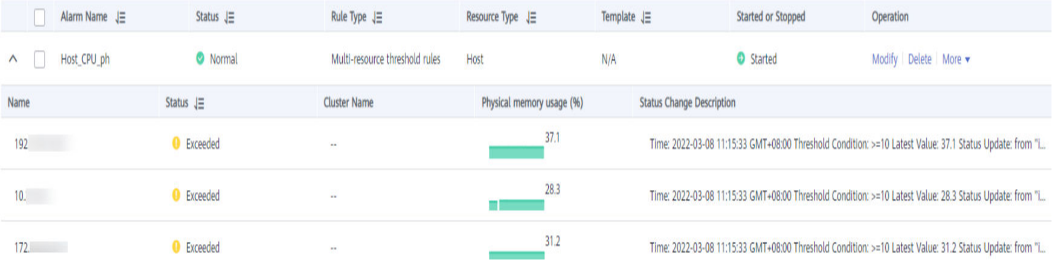
Figure 6-8 Creating a threshold rule



Alarm Name	Status	Rule Type	Resource Type	Template	Status	Operation
aaacce	Exceeded	Multi-Resource Threshold Rule	component	N/A	Started	Edit | Delete | Start | Stop

Name	Status	Cluster Name	Total CPU cores (Core)	Status Change
[redacted]	Exceeded	Custom Cluster	--	Time: 2023-05-09 19:39:50 GMT+08:00 Threshold Condition: >=1 Latest Value: 4.0 Status Update: from "init" t...
[redacted]	Exceeded	Custom Cluster	--	Time: 2023-05-09 19:39:50 GMT+08:00 Threshold Condition: >=1 Latest Value: 4.0 Status Update: from "init" t...

Figure 6-9 Creating a threshold rule



	Alarm Name	Status	Rule Type	Resource Type	Template	Started or Stopped	Operation
^ □	Host_CPU_ph	Normal	Multi-resource threshold rules	Host	N/A	Started	Modify | Delete | More ▾

Name	Status	Cluster Name	Physical memory usage (%)	Status Change Description
192[redacted]	Exceeded	--	37.1	Time: 2022-03-08 11:15:33 GMT+08:00 Threshold Condition: >=10 Latest Value: 37.1 Status Update: from "i...
10.[redacted]	Exceeded	--	28.3	Time: 2022-03-08 11:15:33 GMT+08:00 Threshold Condition: >=10 Latest Value: 28.3 Status Update: from "i...
172.[redacted]	Exceeded	--	31.2	Time: 2022-03-08 11:15:33 GMT+08:00 Threshold Condition: >=10 Latest Value: 31.2 Status Update: from "i...

----End

Using Templates to Create Threshold Rules

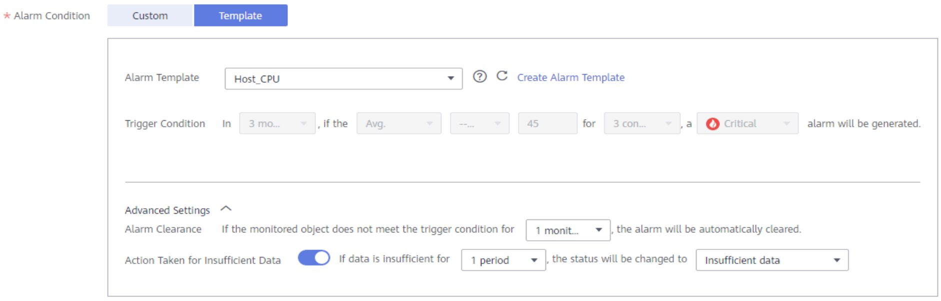
Before creating threshold rules, ensure that a static threshold template has been created according to **Creating a Static Threshold Template**.

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

Step 2 Set a threshold rule.

1. Set basic information such as the rule name and description.
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 6-10 Setting an alarm condition



* Alarm Condition: Custom | Template

Alarm Template: Host_CPU ▾ — Create Alarm Template

Trigger Condition: In 3 mo... , if the Avg. --... 45 for 3 con... , a Critical alarm will be generated.

Advanced Settings ^

Alarm Clearance: If the monitored object does not meet the trigger condition for 1 monit... , the alarm will be automatically cleared.

Action Taken for Insufficient Data: ● If data is insufficient for 1 period , the status will be changed to Insufficient data

Table 6-3 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 a Static Threshold Template**.
Trigger Condition	-	The system automatically imports the preset trigger condition in the template. Note that the condition cannot be modified.
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 set 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 alarm notifications.

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

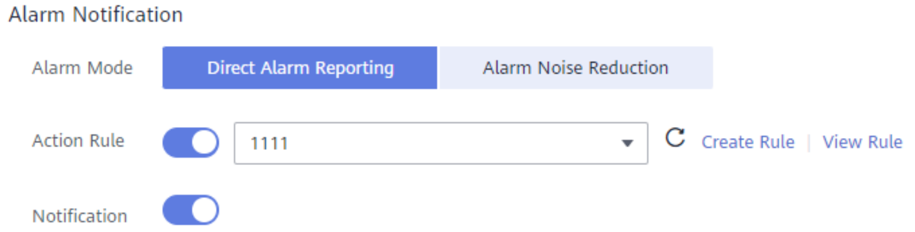
3. Set an alarm notification policy. There are two alarm notification modes.

– **Direct Alarm Reporting**: An alarm is directly sent when the alarm condition is met.

i. Specify whether to enable an alarm action rule. After an alarm action rule is enabled, the system sends notifications based on the associated SMN topic and message template. If the existing alarm action rules cannot meet your requirements, click **Create Rule** to create one. For details, see **Creating an Alarm Action Rule**.

ii. After an alarm action rule is selected, specify whether to enable alarm clearance notification. After alarm clearance notification is enabled, if the alarm clearance condition set in **Advanced Settings > Alarm Clearance** is met, alarm clearance notifications are sent based on the selected action rule.

Figure 6-11 Selecting the direct alarm reporting mode



Alarm Notification

Alarm Mode: **Direct Alarm Reporting** | Alarm Noise Reduction

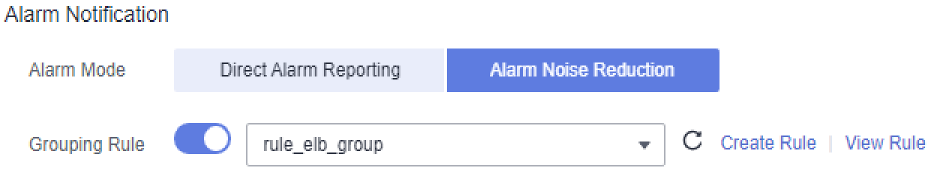
Action Rule: ● 1111 ▾ — Create Rule | View Rule

Notification: ●

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

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

Figure 6-12 Selecting the alarm noise reduction mode



Alarm Notification

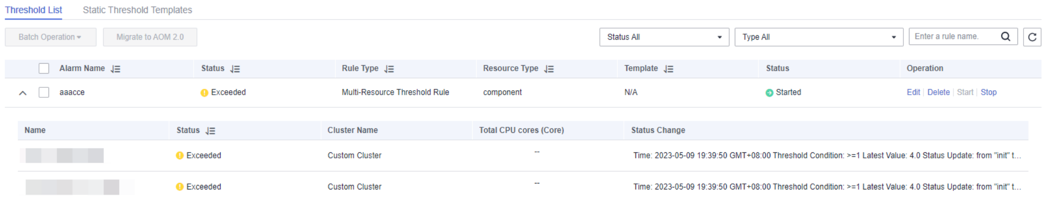
Alarm Mode: Direct Alarm Reporting | **Alarm Noise Reduction**

Grouping Rule: ● rule_elb_group ▾ — Create Rule | View Rule

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

In the expanded list, if the metric data of a host meets the preset alarm condition, 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 or SMS.

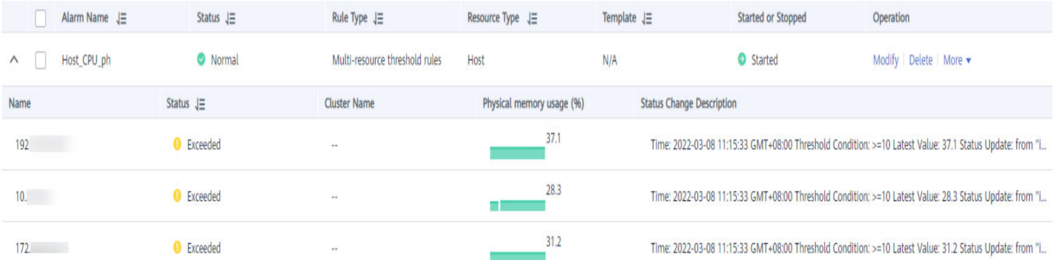
Figure 6-13 Creating a threshold rule



	Alarm Name	Status	Rule Type	Resource Type	Template	Status	Operation
∧	aaacce	Exceeded	Multi-Resource Threshold Rule	component	N/A	Started	Edit | Delete | Start | Stop

Name	Status	Cluster Name	Total CPU cores (Core)	Status Change
[redacted]	Exceeded	Custom Cluster	--	Time: 2023-05-09 19:39:50 GMT+08:00 Threshold Condition: >=1 Latest Value: 4.0 Status Update: from "init" t...
[redacted]	Exceeded	Custom Cluster	--	Time: 2023-05-09 19:39:50 GMT+08:00 Threshold Condition: >=1 Latest Value: 4.0 Status Update: from "init" t...

Figure 6-14 Creating a threshold rule



	Alarm Name	Status	Rule Type	Resource Type	Template	Started or Stopped	Operation
∧	Host_CPU_ph	Normal	Multi-resource threshold rules	Host	N/A	Started	Modify | Delete | More ▾

Name	Status	Cluster Name	Physical memory usage (%)	Status Change Description
192[redacted]	Exceeded	--	37.1	Time: 2022-03-08 11:15:33 GMT+08:00 Threshold Condition: >=10 Latest Value: 37.1 Status Update: from "i...
10.[redacted]	Exceeded	--	28.3	Time: 2022-03-08 11:15:33 GMT+08:00 Threshold Condition: >=10 Latest Value: 28.3 Status Update: from "i...
172.[redacted]	Exceeded	--	31.2	Time: 2022-03-08 11:15:33 GMT+08:00 Threshold Condition: >=10 Latest Value: 31.2 Status Update: from "i...

----End

More Operations

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

Table 6-4 Related operations

Operation	Description
Editing a threshold rule	Click **Edit** in the **Operation** column.
Deleting threshold rules	● To delete a threshold rule, click **Delete** in the **Operation** column. ● To delete one or more threshold rules, select the check boxes before them and click **Delete** above the rule list.
Migrating threshold rules	To migrate one or more threshold rules, select the check boxes before them and click **Migrate to AOM 2.0** above the rule list. **NOTICE** ● Migration cannot be undone. Exercise caution when performing this operation. ● If the threshold rules to be migrated depend on alarm templates, the corresponding alarm templates will also be migrated.
Starting or stopping a threshold rule	Click **Start** or **Stop** in the **Operation** column. **NOTE** Single-resource threshold rules cannot be started or stopped.
Searching for a 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 the threshold condition 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.

6.3.4 Creating a Static Threshold Template

Ensure that a static threshold template is available if you want to create threshold rules based on a 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**.

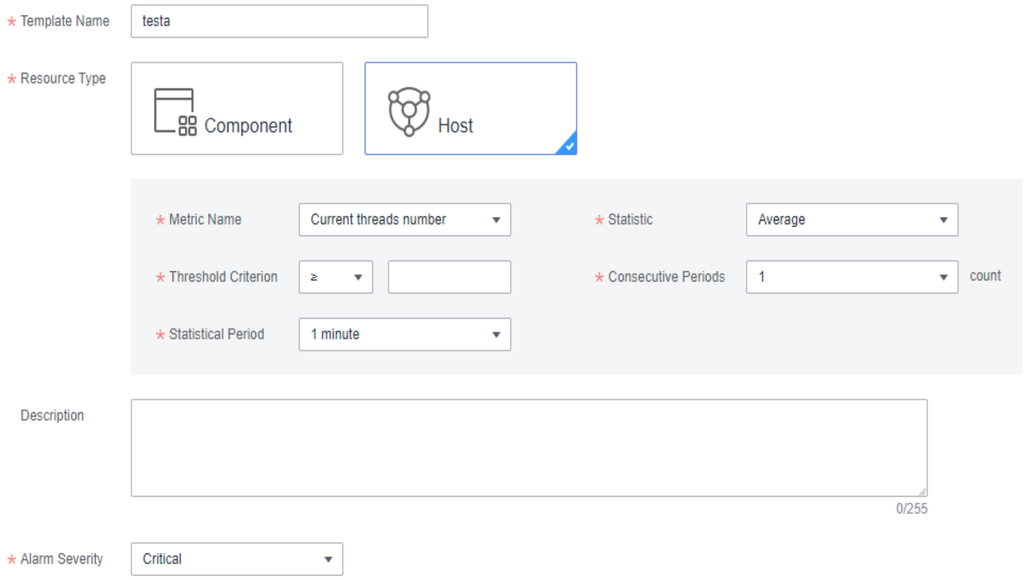
Step 3 Customize a static threshold template.

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

NOTE

- **Statistic**: method used to measure metric values.
- **Threshold Criterion**: trigger condition of a threshold alarm. It consists of two parts: determination condition (≥, ≤, >, or <) and threshold value. For example, after **Threshold Criterion** 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.
- **Alarm Severity**: includes **Critical**, **Major**, **Minor**, and **Warning**.

Figure 6-15 Customizing a static threshold template



* Template Name: testa

* Resource Type: Component | Host (selected)

* Metric Name: Current threads number

* Statistic: Average

* Threshold Criterion: ≥

* Consecutive Periods: 1 count

* Statistical Period: 1 minute

Description: 0/255

* Alarm Severity: Critical

Step 4 Click **Create**.

----End

More Operations

After creating a static threshold template, perform the operations listed in **Table 6-5** if needed.

Table 6-5 Related operations

Operation	Description
Using a static threshold template to create a multi-resource threshold rule	Click **Create Rule** in the **Operation** column. For details, see **Using Templates to Create Threshold Rules**.
Editing 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 🔍.

6.3.5 Creating an Event Alarm Rule

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

Precautions

If you want to receive email or SMS notifications when the resource data meets the event condition, set an alarm action rule according to **Creating an Alarm Action Rule**.

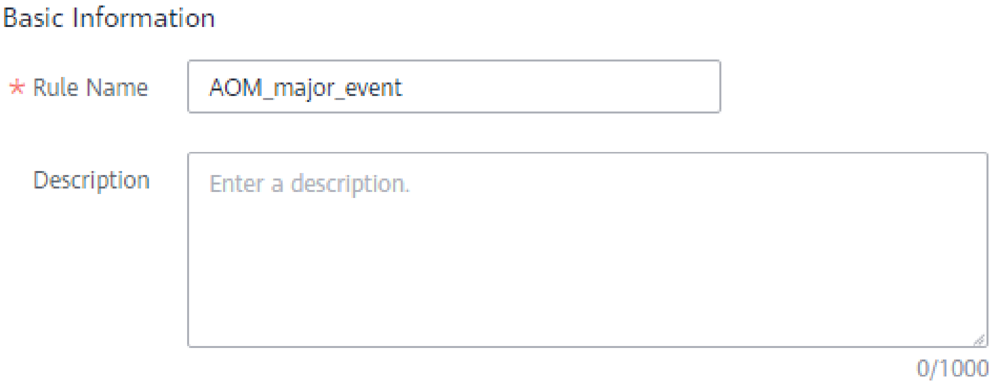
Procedure

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 6-16 Setting basic information



Basic Information

* Rule Name: AOM_major_event

Description: Enter a description.

0/1000

2. Set details about the rule.

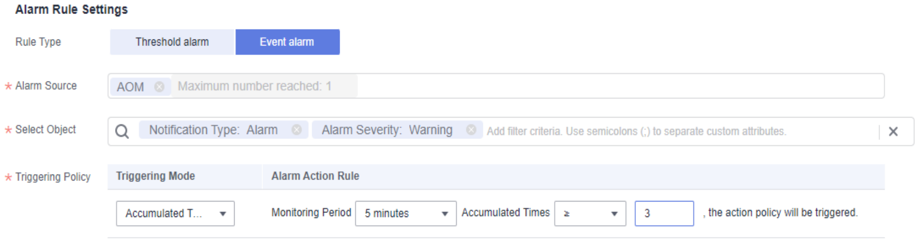
   a. Set **Rule Type** to **Event alarm**.

   b. Set the alarm source, trigger object, and trigger policy.

Table 6-6 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.
Trigger Policy	Policy for triggering event alarms. ▪ **Accumulated Triggering**: An alarm action rule is triggered when the accumulated number of times you preset is reached in a monitoring period. ▪ **Immediate Triggering**: An alarm is generated immediately when the filter criterion is met.

Figure 6-17 Setting an alarm rule



Alarm Rule Settings

Rule Type: Threshold alarm | Event alarm

* Alarm Source: AOM ⊗ Maximum number reached: 1

* Select Object: Notification Type: Alarm ⊗ Alarm Severity: Warning ⊗ Add filter criteria. Use semicolons (;) to separate custom attributes.

* Triggering Policy

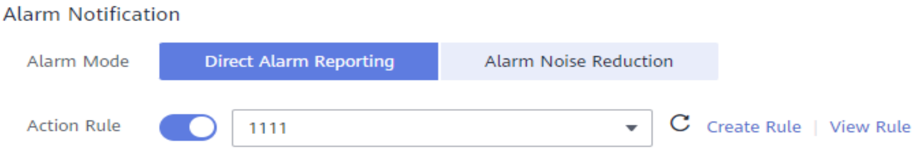
Triggering Mode	Alarm Action Rule
Accumulated T... ▾	Monitoring Period 5 minutes ▾ Accumulated Times ≥ ▾ 3 , the action policy will be triggered.

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 rule. After this function is enabled, the system sends alarm notifications based on the associated SMN topic and message template. If the existing alarm action rules cannot meet your requirements, click **Create Rule** to create one. For details, see **Creating an Alarm Action Rule**.

  Figure 6-18 Selecting the direct alarm reporting mode

  Alarm Notification

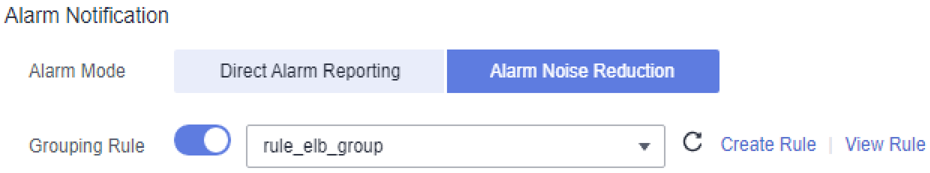
  Alarm Mode: Direct Alarm Reporting | Alarm Noise Reduction

  Action Rule: 1111

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

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

  Figure 6-19 Selecting the alarm noise reduction mode

  Alarm Notification

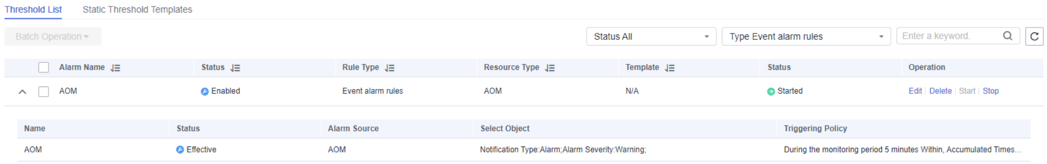
  Alarm Mode: Direct Alarm Reporting | Alarm Noise Reduction

  Grouping Rule: rule_elb_group

Step 3 Click **Create Now**. An event alarm rule is created, as shown in the following figure.

This rule monitors critical alarm events of AOM. When a service event meets the preset notification policy, the system sends an alarm notification to specified personnel by email or SMS.

Figure 6-20 Event alarm rule



Threshold List | Static Threshold Templates

Batch Operation | Status All | Type Event alarm rules | Enter a keyword.

	Alarm Name	Status	Rule Type	Resource Type	Template	Status	Operation
^	AOM	Enabled	Event alarm rules	AOM	N/A	Started	Edit | Delete | Start | Stop

Name	Status	Alarm Source	Select Object	Triggering Policy
AOM	Effective	AOM	Notification Type:Alarm;Alarm Severity:Warning;	During the monitoring period 5 minutes Within, Accumulated Times...

----End

Related Operations

After creating an event alarm rule, perform the operations listed in **Table 6-7** if needed.

Table 6-7 Related operations

Operation	Description
Editing an event alarm rule	Click **Edit** in the **Operation** column.
Deleting event alarm rules	● To delete an event alarm rule, click **Delete** in the **Operation** column. ● To delete one or more event alarm rules, select the check boxes before them and click **Delete** above the rule list.
Migrating event alarm rules	To migrate one or more event alarm rules, select the check boxes before them and click **Migrate to AOM 2.0** above the rule list. **NOTICE** Migration cannot be undone. Exercise caution when performing this operation.
Starting or stopping an event alarm rule	Click **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 AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago.

AOM supports alarm notification. You can create 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, they 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**.

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

2. **Set a topic policy**.

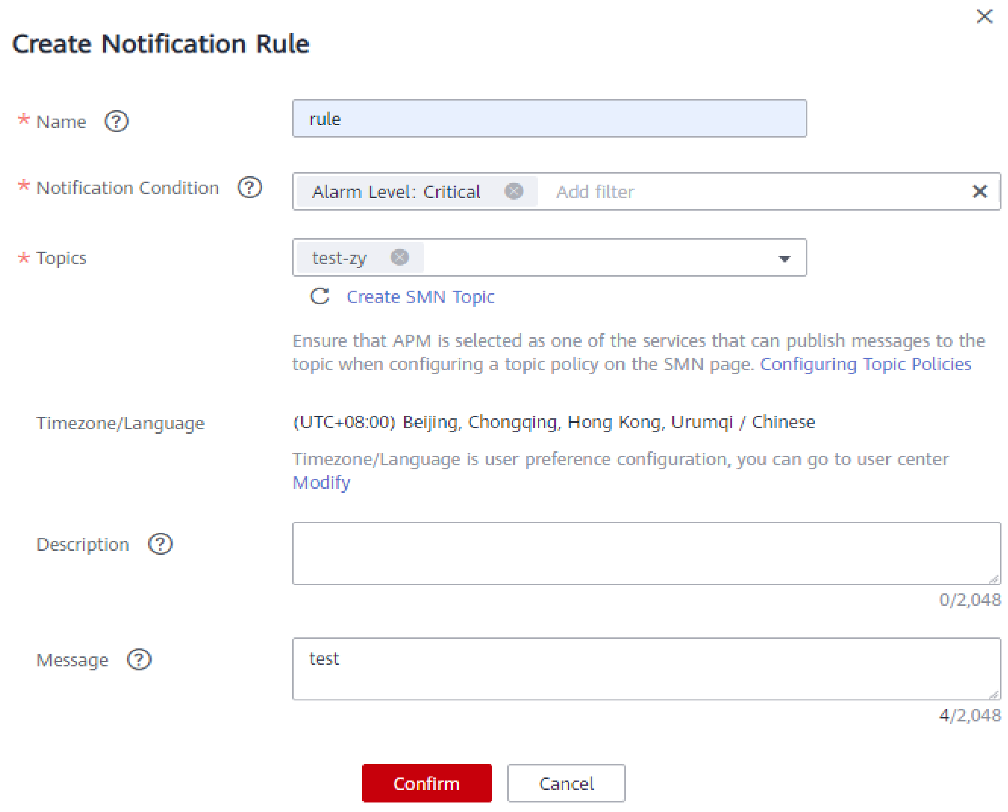
   Select **APM** for **Services that can publish messages to this topic**. If **APM** is not selected, notifications cannot be sent.

3. **Add a subscription to a topic**. SMN can then 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 6-21**.

Figure 6-21 Creating a notification rule



Create Notification Rule

* Name: rule

* Notification Condition: Alarm Level: Critical

* Topics: test-zy

Ensure that APM is selected as one of the services that can publish messages to the topic when configuring a topic policy on the SMN page. Configuring Topic Policies

Timezone/Language: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi / Chinese

Timezone/Language is user preference configuration, you can go to user center Modify

Description: 0/2,048

Message: test 4/2,048

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 6-8** if needed.

Table 6-8 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.
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 notification 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 31 days.

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

Step 3 Perform the operations listed in **Table 6-9** as required.

Table 6-9 Operations

Operation	Method	Description
Viewing alarm statistics	Click **Show Graph**, and view alarm statistics that meet filter criteria within a specific time range on a bar graph.	-

Operation	Method	Description
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 31 days.

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

Step 3 Perform the operations listed in **Table 6-10** as required.

Table 6-10 Operations

Operation	Method	Description
Viewing event statistics	Click **Show Graph**, and view event statistics that meet filter criteria within a specific time range on a bar graph.	-

----End

6.7 Alarm Action Rules

6.7.1 Overview

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

NOTE

This function is available in CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, and AP-Singapore. If you need this function, **submit a service ticket**.

6.7.2 Creating an Alarm Action Rule

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, an email or SMS message recipient has been added to the topic according to **Adding a Subscription to a Topic**.

Precaution

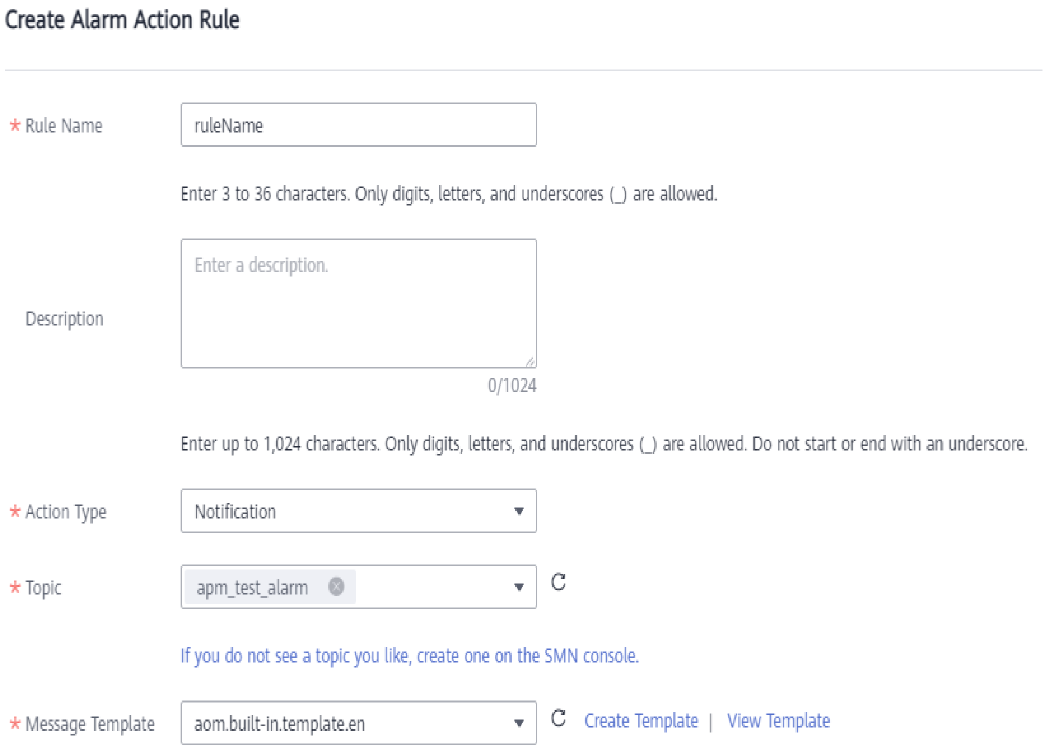
You can create a maximum of 1000 alarm action rules. If this number has been reached, delete unnecessary rules.

Procedure

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

Step 2 Set parameters such as **Rule Name** and **Action Type**.

Figure 6-22 Creating an alarm action rule



Create Alarm Action Rule

* Rule Name: ruleName

Enter 3 to 36 characters. Only digits, letters, and underscores (_) are allowed.

Description: Enter a description.

0/1024

Enter up to 1,024 characters. Only digits, letters, and underscores (_) are allowed. Do not start or end with an underscore.

* Action Type: Notification

* Topic: apm_test_alarm

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

* Message Template: aom.built-in.template.en

Table 6-11 Parameters for configuring an alarm action rule

Parameter	Description
Rule Name	Name of an action rule. Enter 1 to 100 characters, and do not start or end with an underscore (_) or hyphen (-) . Only digits, letters, hyphens, and underscores are allowed.
Description	Description of the action rule.
Action Type	Type of action that is associated with the SMN topic and message template. Select your desired action from the drop-down list. Currently, only **Notification** is supported.
Topic	SMN topic. Select your desired topic from the drop-down list. If there is no topic you want to select, create one on the SMN console.
Message Template	Notification message template. Select your desired template from the drop-down list. If there is no message template you want to select, create one by referring to **Creating a Message Template**.

Step 3 Click **OK**.

----End

More Operations

After an alarm action rule is created, you can perform operations described in **Table 6-12**.

Table 6-12 Related operations

Operation	Description
Modifying an alarm action rule	Click **Edit** in the **Operation** column.
Deleting an alarm action rule	● To delete a single rule, click **Delete** in the **Operation** column in the row that contains the rule, and then click **Yes** on the displayed page. ● To delete one or more rules, select them, click **Delete** above the rule list, and then click **Yes** on the displayed page. **NOTE** Before deleting an alarm action rule, you need to delete the alarm rule bound to the action rule.
Searching for an alarm action rule	Enter a rule name in the search box in the upper right corner and click 🔍.

6.7.3 Creating a Message Template

You can create message templates to customize notifications. When a preset notification rule is triggered, notifications can be sent to specified personnel by emails, SMS, WeCom, DingTalk, voice calls, HTTP, or HTTPS. If no message template is created, the default message template will be used.

Creating a Message Template

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

Step 2 On the **Message Templates** page, click **Create**.

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

- You can create up to 100 message templates. If the number of templates exceeds the upper limit, delete unnecessary templates and create new ones.
- 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.
- In addition to default fields, the message template also allows you to add custom fields. You need to define values for custom fields for event alarm reporting. For details about how to call related APIs, see **Alarm APIs**. For details about the parameters, see the alarm reporting structs in the following message template.
- Custom fields support the JSONPath format. Example: **$event.metadata.case1** or **$event.metadata.case[0]**.
- In the upper right corner of the **Body** area, click **Add Variables** to add required variables.
- If you select **Email**, you can click **Preview** to view the final effect. On the **Preview** page, change the message topic if necessary.

Table 6-13 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
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}

Variable	Description	Definition
Additional Info	Additional alarm description, such as the metric name and alarm rule status change.	${message}
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

```
{
    "event": {
        "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

More Operations

After creating a message template, you can perform the operations listed in **Table 6-14**.

Table 6-14 Related operations

Operation	Description
Editing a message template	Click **Edit** in the **Operation** column.
Copying a message template	Click **Copy** in the **Operation** column.

Operation	Description
Deleting a message template	● To delete a single message template, click **Delete** in the **Operation** column in the row that contains the template, and then click **Yes** on the displayed page. ● To delete one or more message templates, select them, and click **Delete** above the template list, and then click **Yes** on the displayed page. **NOTE** Before deleting a message template, you need to delete the alarm action rules bound to it.
Searching for a message template	Enter a template name in the search box in the upper right corner and click 🔍.

6.8 Alarm Noise Reduction

6.8.1 Overview

NOTE

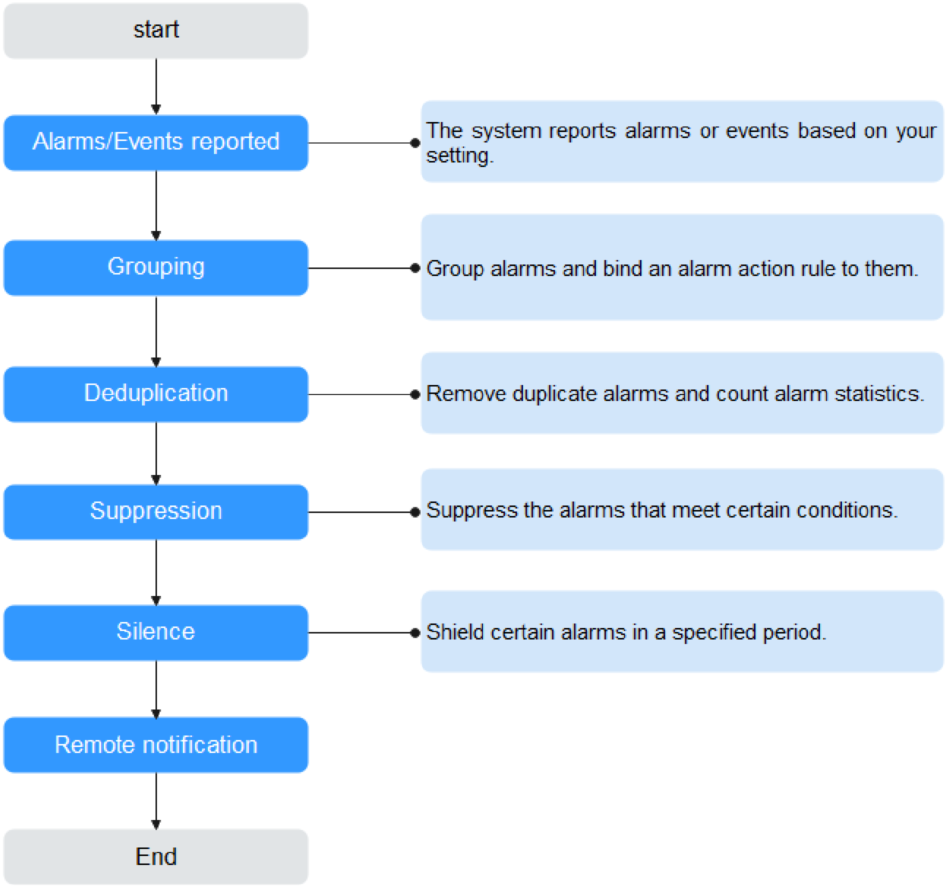
This function is available in CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, and AP-Singapore. If you need this function, **submit a service ticket**.

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 6-23 Alarm noise reduction process


start
Alarms/Events reported
The system reports alarms or events based on your setting.
Grouping
Group alarms and bind an alarm action rule to them.
Deduplication
Remove duplicate alarms and count alarm statistics.
Suppression
Suppress the alarms that meet certain conditions.
Silence
Shield certain alarms in a specified period.
Remote notification
End

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.

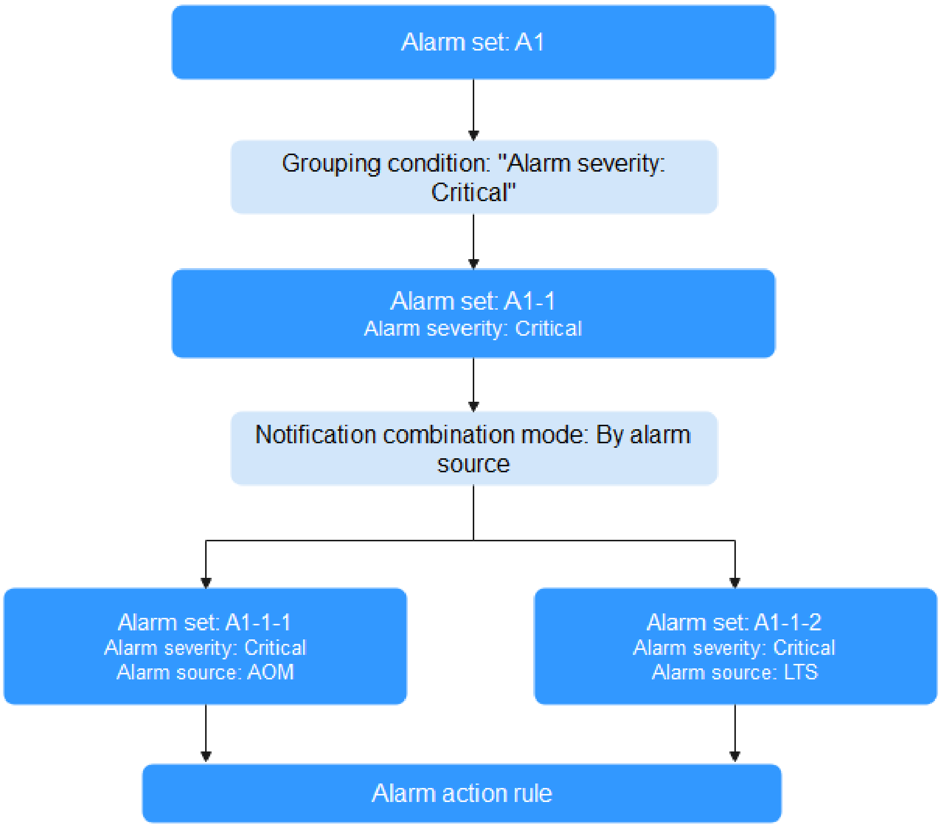
```
{
   "starts_at" : 1579420868000,
   "ends_at" : 1579420868000,
   "timeout" : 60000,
   "resource_group_id" : "5680587ab6*******755c543c1f",
   "metadata" : {
     "event_name" : "test",
     "event_severity" : "Major",
     "event_type" : "alarm",
     "resource_provider" : "ecs",
     "resource_type"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

6.8.2 Creating a Grouping Rule

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

As shown in **Figure 6-24**, when **Alarm Severity** under **Grouping Condition** is set to **Critical**, the system filters out the critical alarms, and then combines these alarms based on the specified mode. The combined alarms can then be associated with an action rule for sending notifications.

Figure 6-24 Grouping process



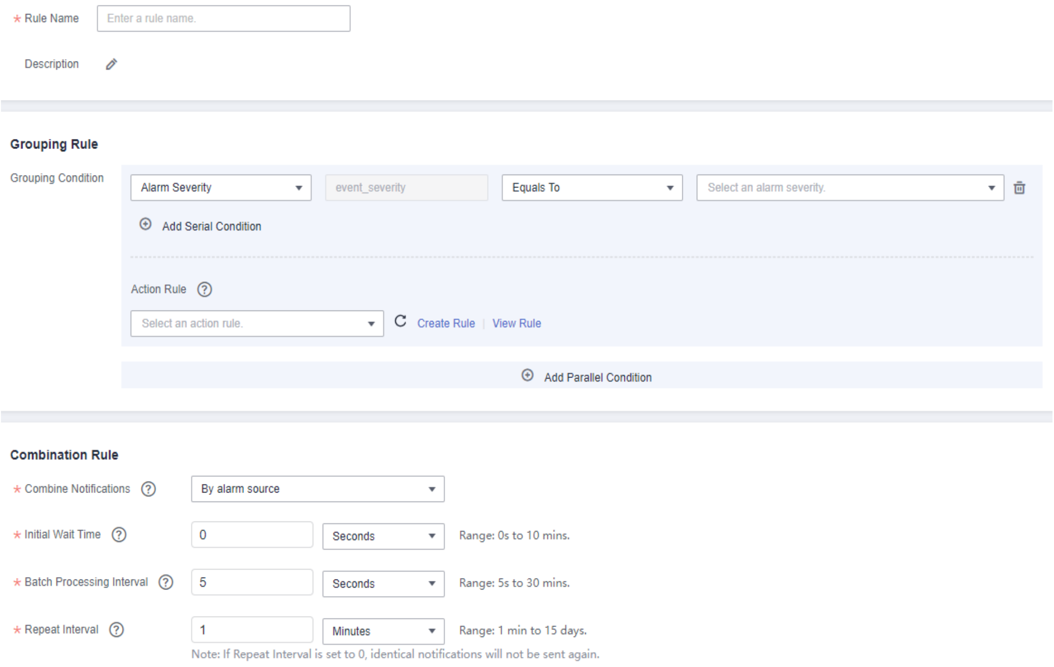
Creating a Grouping Rule

You can create up to 100 grouping rules.

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

Step 2 On the **Grouping Rules** tab page, click **Create** and set parameters such as the rule name and grouping condition. For details, see **Table 6-15**.

Figure 6-25 Creating a grouping rule



* Rule Name: Enter a rule name.

Description

Grouping Rule

Grouping Condition: Alarm Severity | event_severity | Equals To | Select an alarm severity.

Action Rule: Select an action rule.

Combination Rule

* Combine Notifications: By alarm source

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

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

* Repeat Interval: 1 Minutes Range: 1 min to 15 days.

Note: If Repeat Interval is set to 0, identical notifications will not be sent again.

Table 6-15 Setting a grouping rule

Category	Parameter	Description
-	Rule Name	Grouping rule name, which can contain up to 100 characters and cannot start or end with an underscore (_). Only letters, digits, and underscores are allowed.
	Description	Grouping rule description, which can contain up to 1024 characters.
Grouping rules	Grouping Condition	Conditions set to filter alarms. After alarms are filtered out, you can set alarm action rules for them. You can create a maximum of 10 parallel conditions, each of which can contain up to 10 serial conditions. One or more **alarm action rules** can be set for each parallel condition. Serial conditions are in the AND relationship whereas parallel conditions are in the OR relationship. An alarm must meet all serial conditions under one of the parallel conditions. For example, if three serial conditions (that is, **Alarm Severity** = **Critical**, **Alarm Severity** = **Major**, and **Provider** = **AOM**) are set under a parallel condition, critical and major AOM alarms are filtered out, and notification actions are performed based on the alarm action rule you set.

Category	Parameter	Description
Combination rules	Combine Notifications	Notifications for alarms with certain fields to be the same will be combined. Notifications can be combined: ● By alarm source ● By alarm source + severity ● By alarm source + all tags
	Initial Wait Time	Interval for sending an alarm notification after alarms are combined for the first time. It is recommended that the time be set to seconds to prevent alarm storms. Value range: 0s to 10 minutes. Recommended: 15s.
	Batch Processing Interval	Waiting time for sending an alarm notification after the combined alarm data changes. It is recommended that the time be set to minutes. If you want to receive alarm notifications as soon as possible, set the time to seconds. The change here refers to a new alarm or an alarm status change. Value range: 5s to 30 minutes. Recommended: 60s.
	Repeat Interval	Waiting time for sending an alarm notification after the combined alarm data becomes duplicate. It is recommended that the time be set to hours. The duplication means no new alarm is generated and no alarm status is changed. Other attributes such as titles and content may be changed. Value range: 0 minutes to 15 days. Recommended: 1 hour.

Step 3 Click **Create Now**.

----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
Modifying a grouping rule	Click **Modify** in the **Operation** column.

Operation	Description
Deleting a grouping rule	● To delete a single rule, click **Delete** in the **Operation** column in the row that contains the rule. ● To delete one or more rules, select them and click **Delete** above the rule list.
Searching for a grouping rule	Enter a rule name in the search box in the upper right corner and click 🔍.

6.8.3 Creating a Suppression Rule

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

Precautions

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

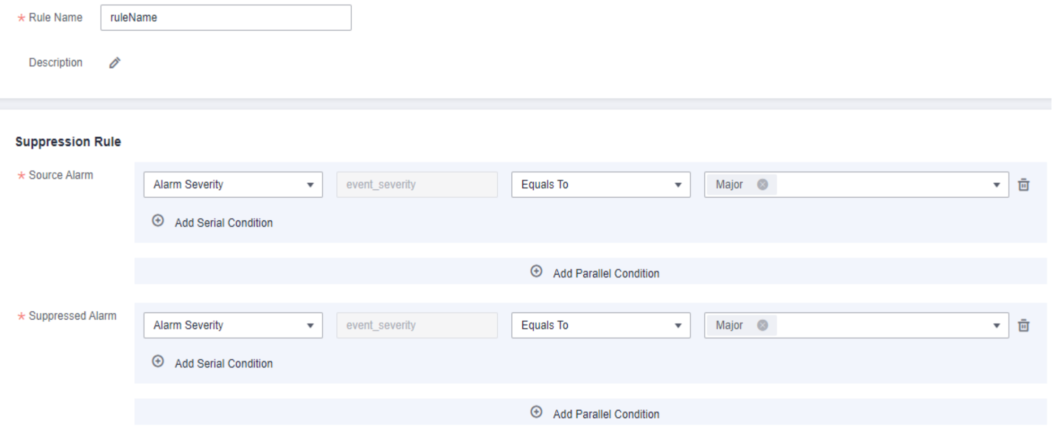
You can create up to 100 suppression rules.

Creating a Suppression Rule

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

Step 2 On the **Suppression Rules** tab page, click **Create** and set parameters such as the rule name and root alarm.

Figure 6-26 Creating a suppression rule



* Rule Name: ruleName

Description

Suppression Rule

* Source Alarm: Alarm Severity | event_severity | Equals To | Major

* Suppressed Alarm: Alarm Severity | event_severity | Equals To | Major

Table 6-17 Setting a suppression rule

Category	Parameter	Description
-	Rule Name	Suppression rule name, which can contain up to 100 characters and cannot start or end with an underscore (_). Only letters, digits, and underscores are allowed.
	Description	Suppression rule description, which can contain up to 1024 characters.
Suppression rules	Source Alarm	Alarm that triggers suppression. You can create up to 10 parallel conditions under **Source Alarm**, and up to 10 serial conditions under each parallel condition. Serial conditions are in the AND relationship whereas parallel conditions are in the OR relationship. An alarm must meet all serial conditions under one of the parallel conditions. For a serial condition, if **Alarm Severity** is set to **Critical**, critical alarms are filtered out as the root alarms.
	Suppressed Alarm	Alarm that is suppressed by the root alarm. Set parameters for the suppressed alarm in the same way that you set parameters for the source alarm. If **Serial Condition** of **Source Alarm** is set to **Critical** and that of **Suppressed Alarm** is set to **Warning**, warnings will be suppressed when critical alarms are generated.

Step 3 After you finish setting the parameters, click **Create Now**.

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

----End

More Operations

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

Table 6-18 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. ● To delete one or more rules, select them and click **Delete** above the rule list.
Searching for a suppression rule	Enter a rule name in the search box in the upper right corner and click 🔍.

6.8.4 Creating a Silence Rule

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

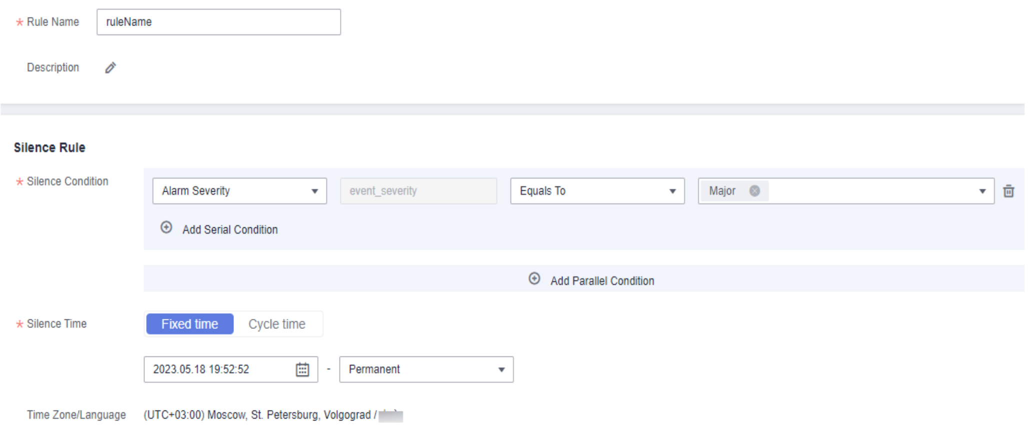
Creating a Silence Rule

You can create up to 100 silence rules.

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

Step 2 On the **Silence Rules** tab page, click **Create** and set parameters such as the rule name and silence condition.

Figure 6-27 Creating a silence rule



* Rule Name: ruleName

Description

Silence Rule

* Silence Condition: Alarm Severity | event_severity | Equals To | Major

Add Serial Condition

Add Parallel Condition

* Silence Time: Fixed time | Cycle time

2023.05.18 19:52:52 - Permanent

Time Zone/Language: (UTC+03:00) Moscow, St. Petersburg, Volgograd /

Table 6-19 Setting a silence rule

Category	Parameter	Description
-	Rule Name	Silence rule name, which can contain up to 100 characters and cannot start or end with an underscore (_). Only letters, digits, and underscores are allowed.

Category	Parameter	Description
	Description	Silence rule description, which can contain up to 1024 characters.
Silence rules	Silence Condition	Any alarm notifications that meet the silence condition will be shielded. You can create up to 10 parallel conditions under **Silence Condition**, and up to 10 serial conditions under each parallel condition. Serial conditions are in the AND relationship whereas parallel conditions are in the OR relationship. An alarm must meet all serial conditions under one of the parallel conditions. For a serial condition, if **Alarm Severity** is set to **Critical**, critical alarms are shielded.
	Silence Time	Time when alarm notifications are shielded. There are two options: ● Fixed time: Alarm notifications are shielded only in a specified period. ● Cycle time: Alarm notifications are shielded periodically.
	Time Zone/ Language	Time zone and language for which alarm notifications are shielded. The time zone and language configured in **Preferences** are selected by default. You can change them as required.

Step 3 Click **Create Now**.

----End

More Operations

After creating a silence rule, perform the operations listed in **Table 6-20** if needed.

Table 6-20 Related operations

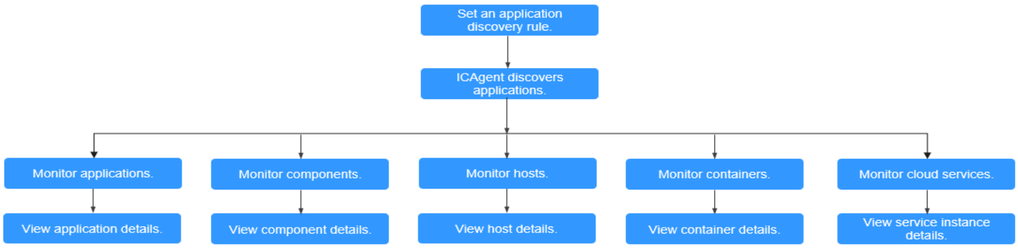
Operation	Description
Modifying a silence rule	Click **Modify** in the **Operation** column.
Deleting a silence rule	● To delete a single rule, click **Delete** in the **Operation** column in the row that contains the rule. ● To delete one or more rules, select them and click **Delete** above the rule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

7 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.

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

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 of the application in batches.

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

NOTE

In the upper right corner of the **Application Details** page, you can set a time range to query the component, host, or alarm information of the application. If no data exists within the time range, AOM automatically switches to the **Application Monitoring** page.

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 a default view template (**Application Template**) which can be modified. You can also click **View Template** to customize one.

- **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**. AOM also allows you to customize tags for easier component management.

  In the component list, click **Add tags** in the **Operation** column of the component, enter a tag, and 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.

NOTE

Components cannot be searched by alias.

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

NOTE

In the upper right corner of the **Component Details** page, you can set a time range to query the instance, host, or alarm information of the component. If no data exists within the time range, AOM automatically switches to the **Component Monitoring** page.

- 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 a default view template (**Service Template**) which can be modified. You can also click **View Template** to customize one.
  - 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 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 an 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** to add a tag. 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.
- **Synchronizing host data**

  In the host list, locate the target host and choose **More** > **Sync Host Data** in the **Operation** column to synchronize host data.

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

NOTE

Hosts cannot be searched by alias.

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.

NOTE

In the upper right corner of the **Host Details** page, you can set the time range to query the instance, GPU, NIC, and alarm information of the host. If no data exists within the time range, AOM automatically switches to the **Host Monitoring** page.

- **Creating a view template**

  AOM provides a default view template (**Host Template**) which can be modified. You can also click **View Template** to customize one.
- **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 **Instance List** tab to view the basic information such as the instance status and type. Click an instance to view its metrics on the details page.
- 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.
- Click the **Disk Partition** tab to view the disk partition type, size, and usage.

  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.

- CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, and AP-Singapore: 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.

- AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago: Search for a component or host and then select metrics, 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 in the upper part of the page, and analyze metric data from multiple dimensions.

Table 7-1 Metric parameters

Parameter	Description
Statistical Mode	Method used to measure metrics. Options: **Average**, **Minimum**, **Maximum**, **Sum**, and **SampleCount**. **NOTE** The number of samples equals to the count of data points.
Statistical Cycle	Interval at which metric data is collected. The statistical cycles that are available for you to select vary according to the time range.
Time Range	Time range in which metric data is collected. Options: **Last 30 minutes**, **Last 1 hour**, **Last 6 hours**, **Last 1 day**, **Last 1 week**, and **Custom**.
Refresh Frequency	Interval at which the metric data is refreshed. Options: **Refresh manually**, **30 seconds auto refresh**, **1 minute auto refresh**, and **5 minutes auto refresh**.

----End

More Operations

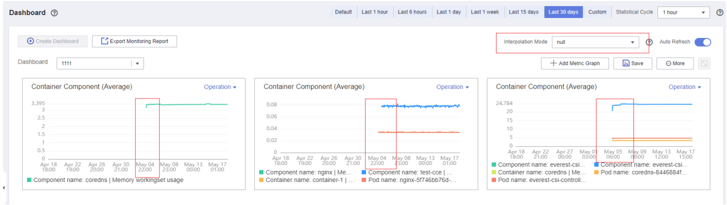
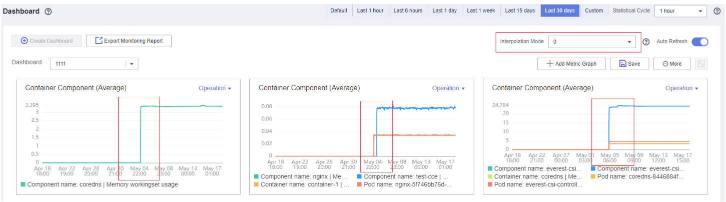
For CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, and AP-Singapore, see **Table 7-2**. For other regions, see **Table 7-3**.

Table 7-2 Related operations

Operation	Description
Hiding/ Showing metric data	After selecting a metric, click 👁 in the **Operation** column to hide the metric data in the current graph. To show the metric data again, click ⊘ in the **Operation** column. 👁 and ⊘ indicate the statuses of metric data.
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.
Exporting a monitoring report	Click **Export Report** to export a metric graph as a CSV file to your local PC.

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 threshold rule for it.
Exporting a monitoring report	Click **Export Report** to export a metric graph as a CSV file to your local PC.

Operation	Description
Setting an interpolation mode	Click **Interpolation Mode** to set a mode for aggregating metric data. By default, AOM uses **null** to represent breakpoints in a metric graph. However, a metric graph with breakpoints is not suitable for reporting or presentation. To solve the problem, set **Interpolation Mode** to **0** or **null** to interpolate values. In this way, you can replace the missing metric data and avoid breakpoints. You can set **Interpolation Mode** to **null**, or **0**. ● **null**: Breakpoints are represented by **null** by default. See the following figure. **Figure 7-2** Graph when **Interpolation Mode** is **null**  Dashboard; Last 30 days; Statistical Cycle 1 hour; Interpolation Mode null; Auto Refresh; Dashboard 1111 Default Last 1 hour Last 6 hours Last 1 day Last 1 week Last 15 days Last 30 days Custom Create Dashboard Export Monitoring Report Add Metric Graph Save More Container Component (Average) Operation Component name: coredns | Memory workingset usage ● **0**: Breakpoints are indicated by **0**. See the following figure. **Figure 7-3** Graph when **Interpolation Mode** is **0**  Dashboard; Last 30 days; Statistical Cycle 1 hour; Interpolation Mode 0; Auto Refresh; Dashboard 1111 Default Last 1 hour Last 6 hours Last 1 day Last 1 week Last 15 days Last 30 days Custom Create Dashboard Export Monitoring Report Add Metric Graph Save More Container Component (Average) Operation Component name: coredns | Memory workingset usage
Deleting a metric	Click 🗑 in the row where the metric is located.

7.7 Cloud Service Monitoring

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

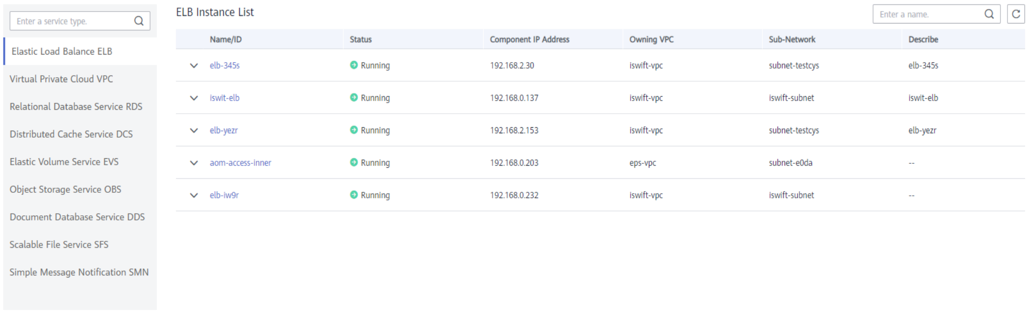
Currently, the following cloud services can be monitored:

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 (APIG), Graph Engine Service (GES), CloudTable, Cloud Data Migration (CDM), Data Warehouse Service (DWS), and IoT Device Access (IoTDA).

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 7-4 Monitoring cloud service status



Enter a service type.
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
Enter a name.

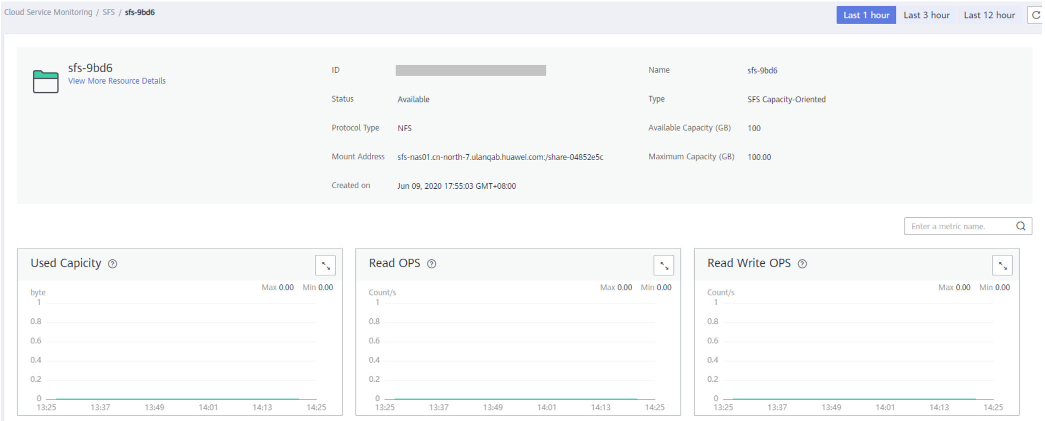
ELB Instance List

Name/ID	Status	Component IP Address	Owning VPC	Sub-Network	Describe
elb-345s	Running	192.168.2.30	iswift-vpc	subnet-testcys	elb-345s
iswit-elb	Running	192.168.0.137	iswift-vpc	iswift-subnet	iswit-elb
elb-yezr	Running	192.168.2.153	iswift-vpc	subnet-testcys	elb-yezr
aom-access-inner	Running	192.168.0.203	eps-vpc	subnet-e0da	--
elb-iw9r	Running	192.168.0.232	iswift-vpc	iswift-subnet	--

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 7-5 Monitoring cloud service metrics



sfs-9bd6

ID [redacted]

Status Available

Protocol Type NFS

Mount Address sfs-nas01.cn-north-7.ulanqab.huawei.com:/share-04852e5c

Created on Jun 09, 2020 17:55:03 GMT+08:00

Name sfs-9bd6

Type SFS Capacity-Oriented

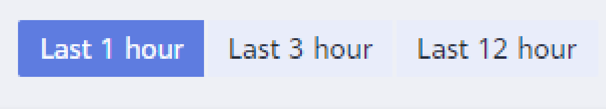
Available Capacity (GB) 100

Maximum Capacity (GB) 100.00

You can also perform the following operations:

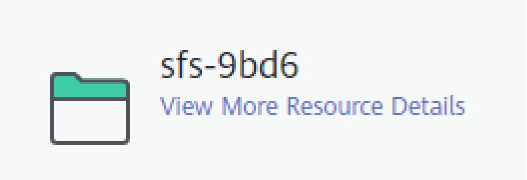
- In the upper right corner of a metric graph, click to enlarge the graph.
- In the upper right corner of the page, set a time range to view data.

Figure 7-6 Specifying different time segments



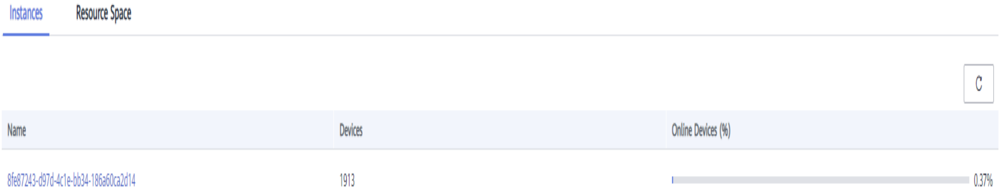
- Click **View More Resource Details** to go to the console of the corresponding service, as shown in the following figure.

Figure 7-7 Viewing more resource details



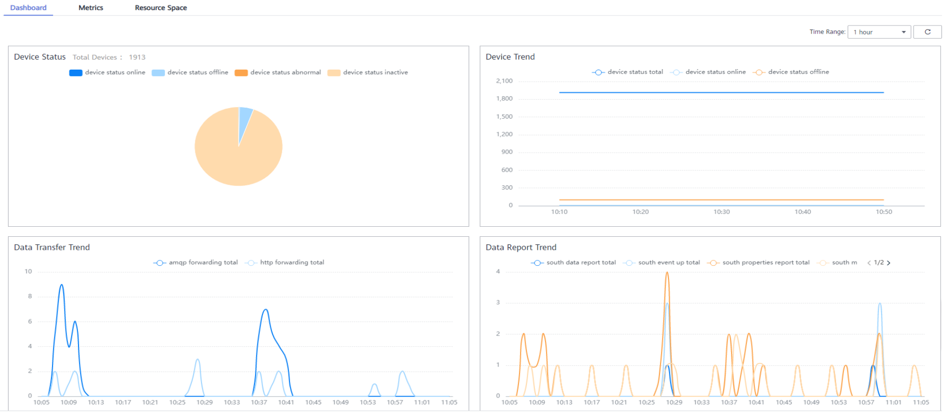
Monitoring IoTDA

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

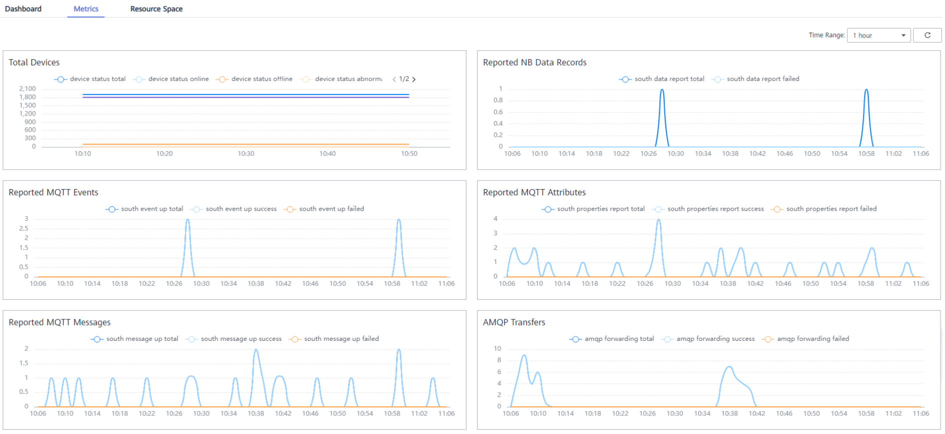


Name	Devices	Online Devices (%)
8fe87243-d97d-4c1e-bb34-186a60ca2d14	1913	0.37%

- 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.



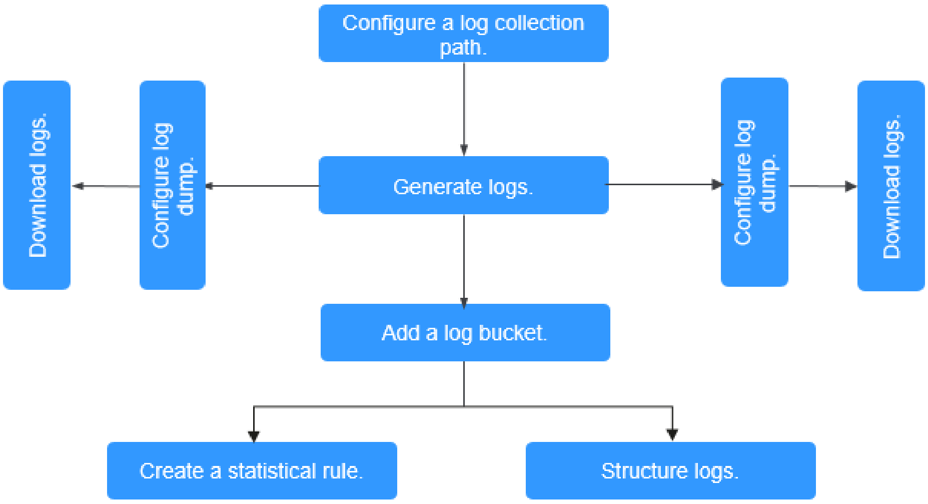
- Click an instance name and click the **Resource Space** tab to view the resource space of the current instance.

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. You can search for logs by component, system, or host.
   - For component logs, you can set filter criteria such as **Cluster**, **Namespace**, and **Component**. You can also click **Advanced Search** and set filter criteria such as **Instance**, **Host**, and **File Name**, and choose whether to enable **Hide System Component**.
   - For system logs, you can set filter criteria such as **Cluster** and **Host**.
   - For host logs, you can set filter criteria such as **Cluster** and **Host**.
2. Enter a keyword in the search box. Rules are as follows:
   - Enter 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.
   - Enter a keyword with a question mark (?) or an asterisk (*) for fuzzy match. Do not start a keyword with a question mark or an asterisk. For example, you can enter **ER?OR** or **ER*R**.
   - Enter search criteria containing search operator AND (&&) or OR (||). For example, enter **query logs&&erro*** or **query logs||error**.
   - For details about search rules, see **Search Syntax and Examples**.

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 (that is, the latest log is displayed at the end). ↓≡ indicates the descending order by time (that is, 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

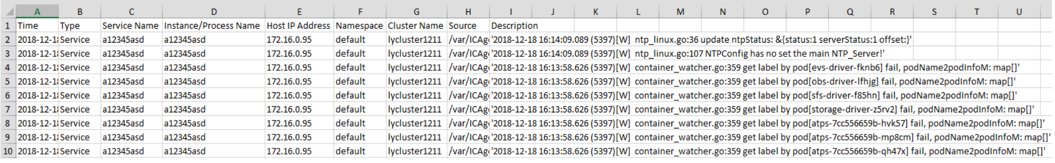
To ensure that tenant hosts and services run properly, some components (for example, kube-dns) provided by the system will run on the tenant hosts. The logs of these components are also queried during tenant log query.

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.

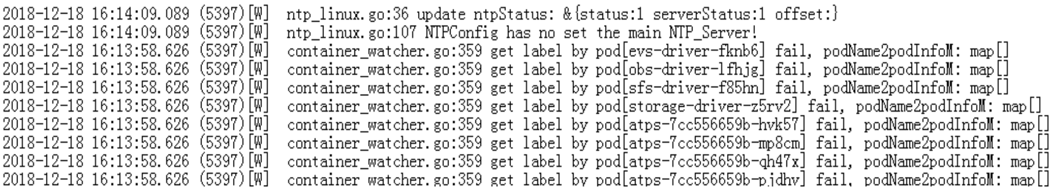
Logs can be exported in CSV or TXT format. You can select a format as required. If you select the CSV format, detailed information (such as log content, host IP address, and source) can be exported, as shown in **Figure 8-2**. If you select the TXT format, only log content can be exported, as shown in **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
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.

Viewing Log Files

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

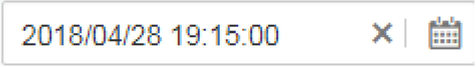
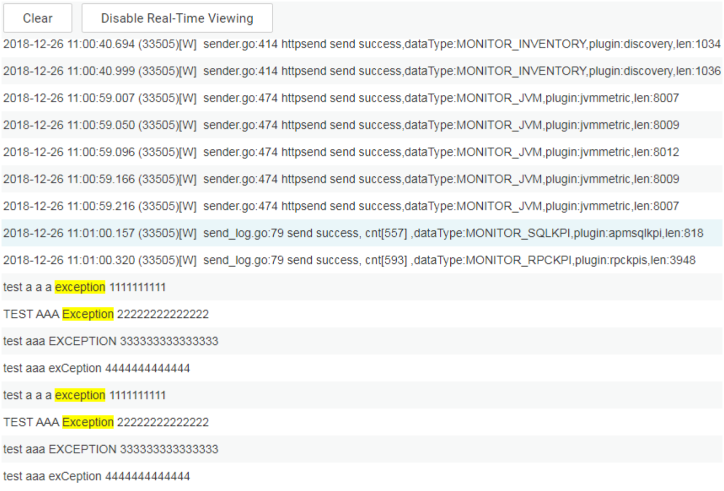
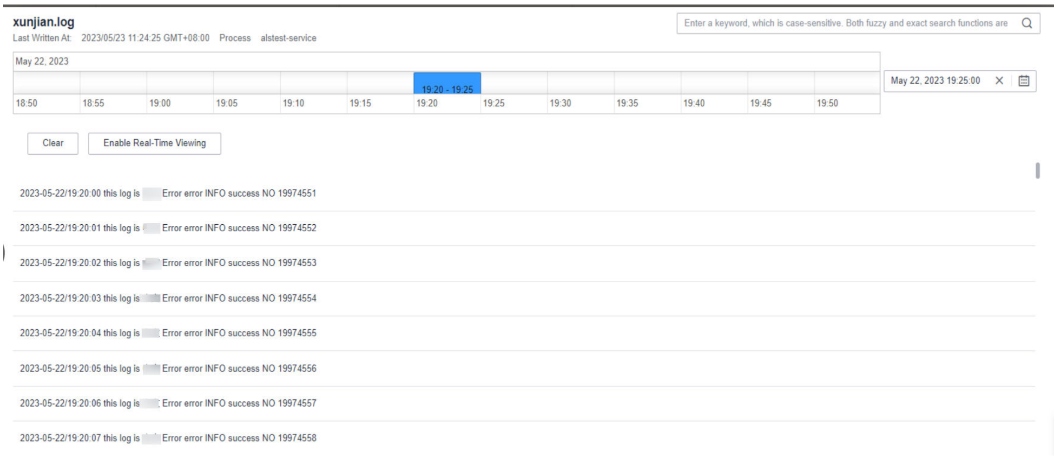
Operation	Setup	Description
Setting a time range	Date	Click  to select a date. 2018/04/28 19:15:00
	Time range	Click the desired time on the time axis to set a time range. You can select only one unit (5 minutes) each time.
Viewing log files	Clear	Click **Clear** to clear the logs displayed on the screen. Logs displayed on the screen will be cleared, but will not be deleted.
	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  2018-12-26 11:00:40.694 (33505)[W] sender.go:414 httpsend send success,dataType:MONITOR_INVENTORY,plugin:discovery,len:1034 2018-12-26 11:00:40.999 (33505)[W] sender.go:414 httpsend send success,dataType:MONITOR_INVENTORY,plugin:discovery,len:1036 2018-12-26 11:00:59.007 (33505)[W] sender.go:474 httpsend send success,dataType:MONITOR_JVM,plugin:jvmmetric,len:8007 2018-12-26 11:00:59.050 (33505)[W] sender.go:474 httpsend send success,dataType:MONITOR_JVM,plugin:jvmmetric,len:8009 2018-12-26 11:00:59.096 (33505)[W] sender.go:474 httpsend send success,dataType:MONITOR_JVM,plugin:jvmmetric,len:8012 2018-12-26 11:00:59.166 (33505)[W] sender.go:474 httpsend send success,dataType:MONITOR_JVM,plugin:jvmmetric,len:8009 2018-12-26 11:00:59.216 (33505)[W] sender.go:474 httpsend send success,dataType:MONITOR_JVM,plugin:jvmmetric,len:8007 2018-12-26 11:01:00.157 (33505)[W] send_log.go:79 send success, cnt[557] ,dataType:MONITOR_SQLKPI,plugin:apmsqlkpi,len:818 2018-12-26 11:01:00.320 (33505)[W] send_log.go:79 send success, cnt[593] ,dataType:MONITOR_RPCKPI,plugin:rpckpis,len:3948 test a a a exception 1111111111 TEST AAA Exception 22222222222222 test aaa EXCEPTION 333333333333333 test aaa exCeption 4444444444444 test a a a exception 1111111111 TEST AAA Exception 22222222222222 test aaa EXCEPTION 333333333333333 test aaa exCeption 4444444444444

Figure 8-5 Log file details


xunjian.log
Last Written At: 2023/05/23 11:24:25 GMT+08:00 Process alstest-service
Enter a keyword, which is case-sensitive. Both fuzzy and exact search functions are
May 22, 2023
19:20 - 19:25
18:50
18:55
19:00
19:05
19:10
19:15
19:20
19:25
19:30
19:35
19:40
19:45
19:50
May 22, 2023 19:25:00
Clear
Enable Real-Time Viewing

```
2023-05-22/19:20:00 this log is [redacted] Error error INFO success NO 19974551
2023-05-22/19:20:01 this log is [redacted] Error error INFO success NO 19974552
2023-05-22/19:20:02 this log is [redacted] Error error INFO success NO 19974553
2023-05-22/19:20:03 this log is [redacted] Error error INFO success NO 19974554
2023-05-22/19:20:04 this log is [redacted] Error error INFO success NO 19974555
2023-05-22/19:20:05 this log is [redacted] Error error INFO success NO 19974556
2023-05-22/19:20:06 this log is [redacted] Error error INFO success NO 19974557
2023-05-22/19:20:07 this log is [redacted] Error error INFO success NO 19974558
```

----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 Bucket 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

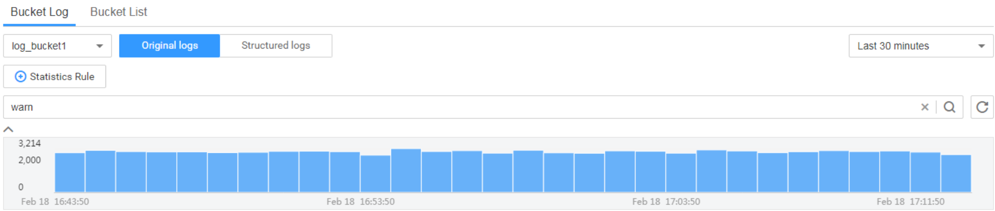
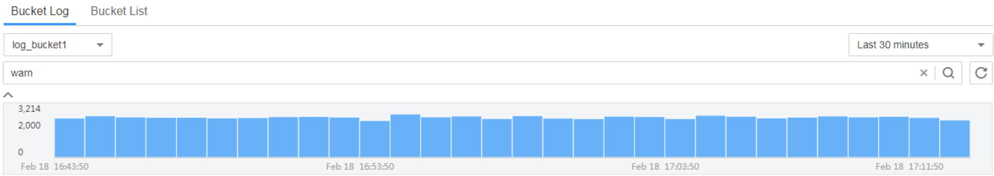


  Figure 8-7 Viewing statistical data in a bar chart

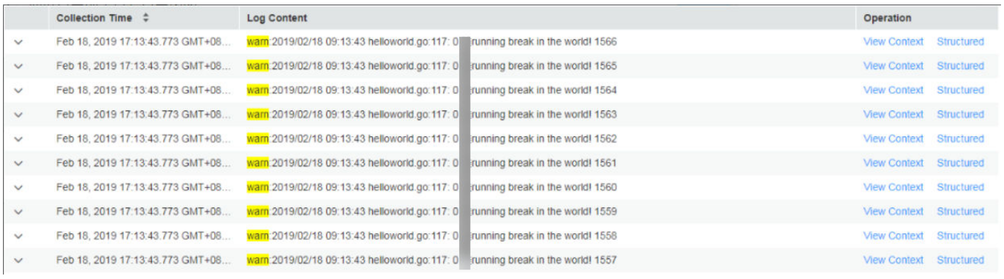


  When you hover over a rectangle block, the prompt displays the time range (start time and end time) and the number of logs that meet the filter criteria within the time range. When you click a rectangle block, the log list displays corresponding log details. To deselect the block, click ↻.

- **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 8-8 Viewing log details in a log list

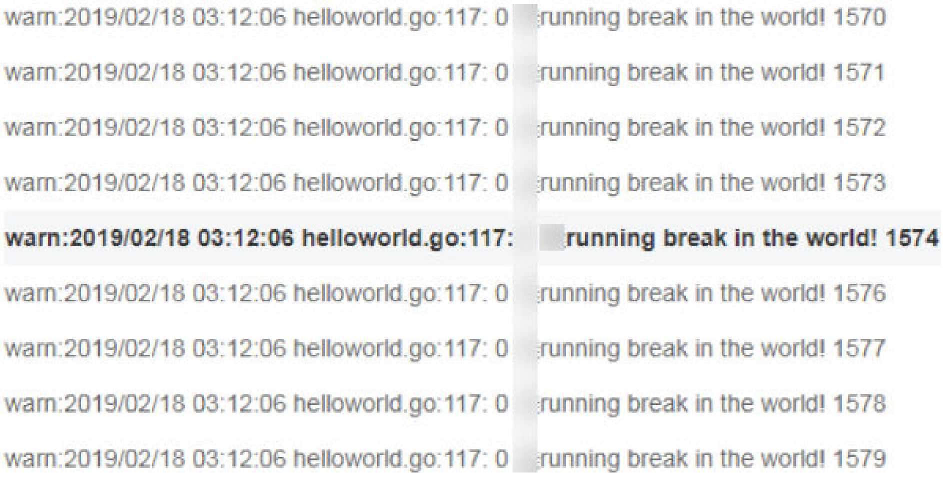


	Collection Time ⇕	Log Content	Operation
⌄	Feb 18, 2019 17:13:43.773 GMT+08...	warn:2019/02/18 09:13:43 helloworld.go:117: 0 [redacted] running break in the world! 1566	View Context Structured
⌄	Feb 18, 2019 17:13:43.773 GMT+08...	warn:2019/02/18 09:13:43 helloworld.go:117: 0 [redacted] running break in the world! 1565	View Context Structured
⌄	Feb 18, 2019 17:13:43.773 GMT+08...	warn:2019/02/18 09:13:43 helloworld.go:117: 0 [redacted] running break in the world! 1564	View Context Structured
⌄	Feb 18, 2019 17:13:43.773 GMT+08...	warn:2019/02/18 09:13:43 helloworld.go:117: 0 [redacted] running break in the world! 1563	View Context Structured
⌄	Feb 18, 2019 17:13:43.773 GMT+08...	warn:2019/02/18 09:13:43 helloworld.go:117: 0 [redacted] running break in the world! 1562	View Context Structured
⌄	Feb 18, 2019 17:13:43.773 GMT+08...	warn:2019/02/18 09:13:43 helloworld.go:117: 0 [redacted] running break in the world! 1561	View Context Structured
⌄	Feb 18, 2019 17:13:43.773 GMT+08...	warn:2019/02/18 09:13:43 helloworld.go:117: 0 [redacted] running break in the world! 1560	View Context Structured
⌄	Feb 18, 2019 17:13:43.773 GMT+08...	warn:2019/02/18 09:13:43 helloworld.go:117: 0 [redacted] running break in the world! 1559	View Context Structured
⌄	Feb 18, 2019 17:13:43.773 GMT+08...	warn:2019/02/18 09:13:43 helloworld.go:117: 0 [redacted] running break in the world! 1558	View Context Structured
⌄	Feb 18, 2019 17:13:43.773 GMT+08...	warn:2019/02/18 09:13:43 helloworld.go:117: 0 [redacted] running break in the world! 1557	View Context Structured

Perform the following operations if needed:

- 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 8-9 Viewing the context of a specified log



```
warn:2019/02/18 03:12:06 helloworld.go:117: 0 [redacted] running break in the world! 1570
warn:2019/02/18 03:12:06 helloworld.go:117: 0 [redacted] running break in the world! 1571
warn:2019/02/18 03:12:06 helloworld.go:117: 0 [redacted] running break in the world! 1572
warn:2019/02/18 03:12:06 helloworld.go:117: 0 [redacted] running break in the world! 1573
warn:2019/02/18 03:12:06 helloworld.go:117: [redacted] running break in the world! 1574
warn:2019/02/18 03:12:06 helloworld.go:117: 0 [redacted] running break in the world! 1576
warn:2019/02/18 03:12:06 helloworld.go:117: 0 [redacted] running break in the world! 1577
warn:2019/02/18 03:12:06 helloworld.go:117: 0 [redacted] running break in the world! 1578
warn:2019/02/18 03:12:06 helloworld.go:117: 0 [redacted] running break in the world! 1579
```

----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 periodical dump and one-off dump.

- **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 File Format	Options: **Custom file** and **Log bucket**.	Custom file
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 **Objects** page on the OBS console.
2. On the **Objects** tab page, find the log files stored in OBS, such as **192.168.0.74_var-paas-sys-log-apm-count_warn.log** and **192.168.0.74_var-paas-sys-log-apm-debug_erro.trace**.

   Paths of the log files dumped to the OBS bucket: Log file paths 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 File Format	Options: **Custom file** and **Log bucket**.	Custom file
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. ● If you select an unauthorized OBS bucket, LTS will take 15 minutes to authorize the ACL for the bucket. If your configuration fails, try again 15 minutes later. Exercise caution when modifying the bucket policy to prevent log dump failures.	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 to go to the **Objects** page on the OBS console.
2. On the **Objects** tab page, find the log file stored in OBS, for example, **/home/One-off Dump/log-group2_shard_0(custom).log**.

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

   Names of the log files dumped to the OBS bucket: 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.

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.

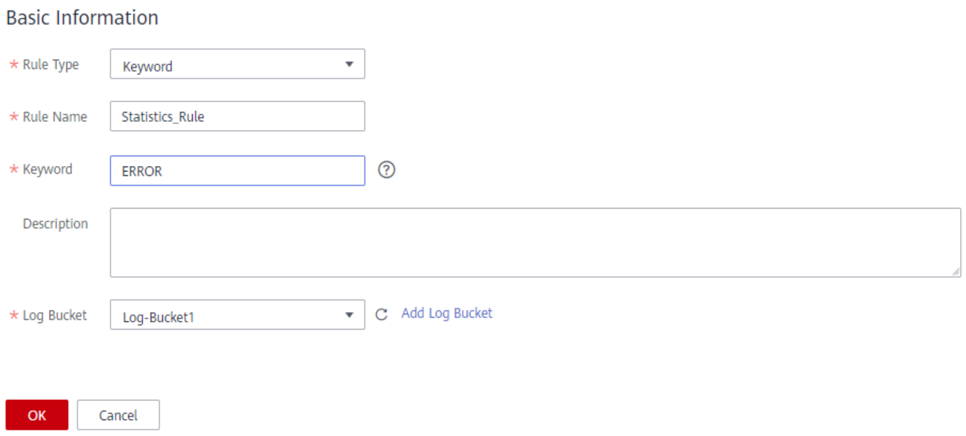
Procedure

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 8-10 Creating a statistical rule



Basic Information

* Rule Type: Keyword
* Rule Name: Statistics_Rule
* Keyword: ERROR
Description:
* Log Bucket: Log-Bucket1

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

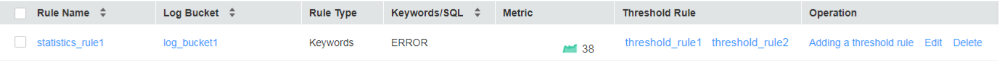
Step 3 (Optional) View the generated metric data.

- Method 1: View the metric data on the **Statistical Rules** page, as shown in **Figure 8-11**.

  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 8-11 Method 1



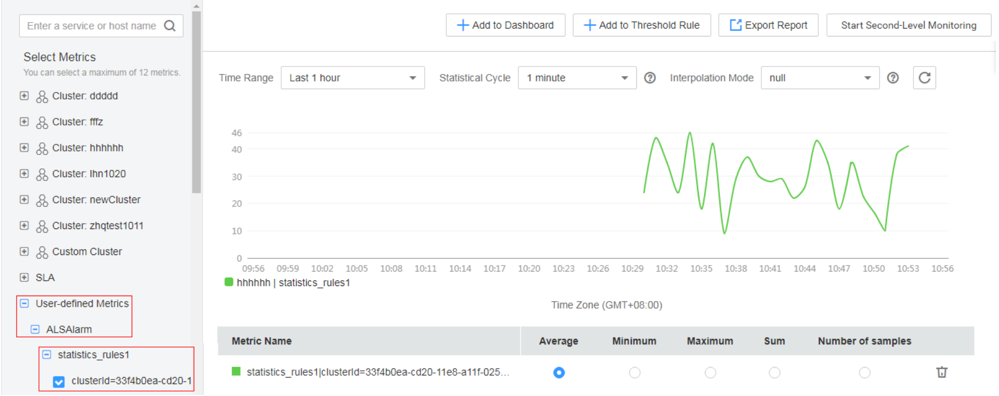
□	Rule Name	Log Bucket	Rule Type	Keywords/SQL	Metric	Threshold Rule	Operation
□	statistics_rule1	log_bucket1	Keywords	ERROR	38	threshold_rule1 threshold_rule2	Adding a threshold rule Edit Delete

- Method 2: View the metric data on the **Metric Monitoring** page, as shown in **Figure 8-12**.

  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 8-12 Method 2



Time Range: Last 1 hour

Statistical Cycle: 1 minute

Interpolation Mode: null

Metric Name	Average	Minimum	Maximum	Sum	Number of samples
statistics_rules1|clusterId=33f4b0ea-cd20-11e8-a11f-025...	●	○	○	○	○

----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

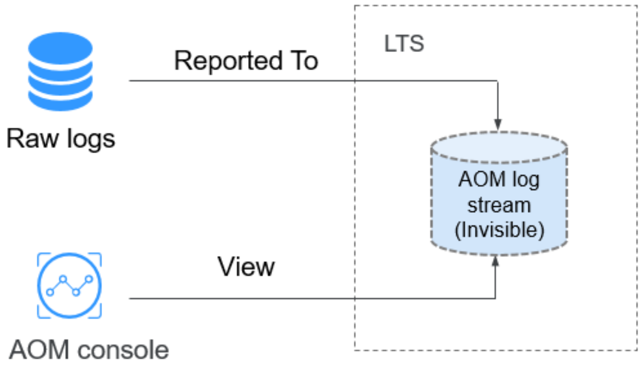
The function of connecting AOM logs to Log Tank Service (LTS) is currently restricted. If you need this function, **submit a service ticket**.

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

What Is Mapping?

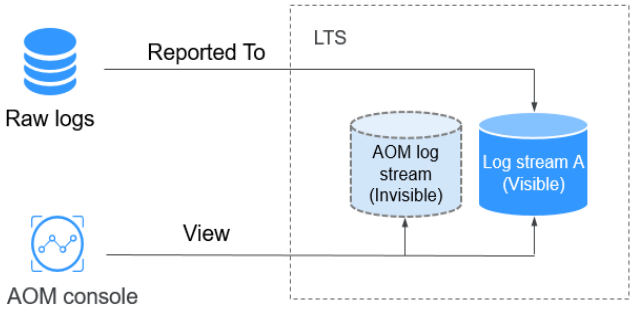
AOM logs exist in LTS in the form of a log stream, as shown in **Figure 8-13**. You can view raw logs in configured log collection paths on AOM, but cannot view the AOM log stream on LTS. You can create a mapping by adding an access rule on AOM. After the mapping is created, you can view and analyze AOM logs on LTS.

Figure 8-13 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 8-14**.

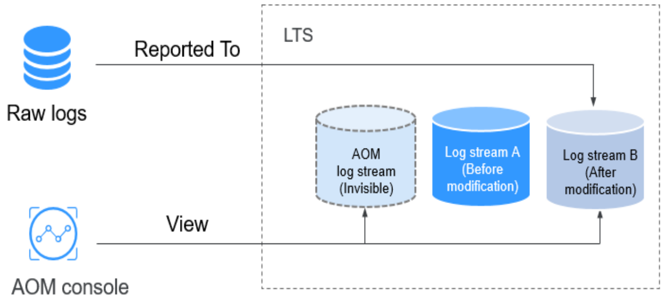
Figure 8-14 After mapping



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 8-15**.

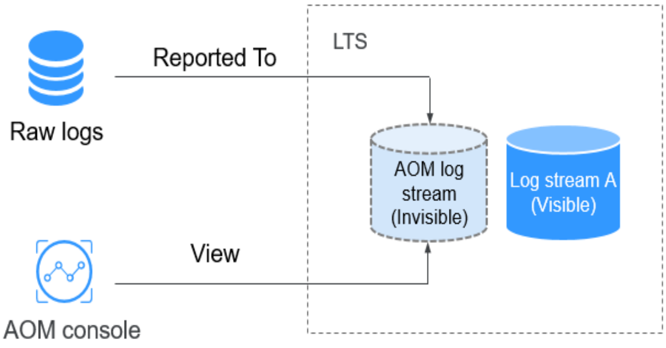
Figure 8-15 Modifying a mapping


Reported To
LTS
Raw logs
AOM log stream (Invisible)
Log stream A (Before modification)
Log stream B (After modification)
View
AOM console

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 8-16**. 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 8-16 Deleting a mapping



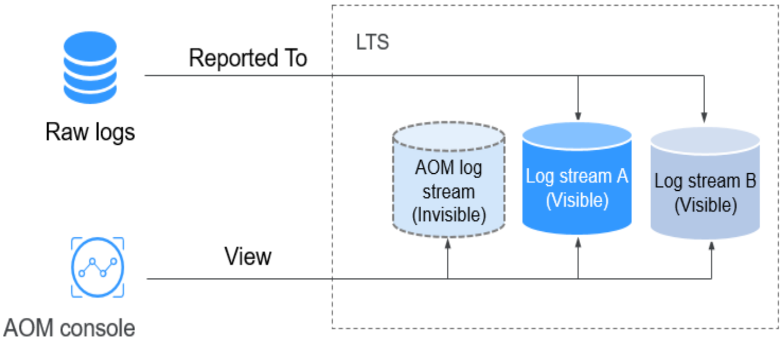
NOTE

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 8-17 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 also **configured a container log collection path**.

Adding Access Rules

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

Step 1 Log in to the AOM 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.

  NOTE

  If no log group or stream meets your requirements, click **Create Log Group** or **Create Log Stream** to create one. After creating a log stream, select an enterprise project.
- **Access by Workload**: Logs of the selected workload are connected to the specified log stream.
  a. **Rule Name**: Enter a 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.

    NOTE

    If no log group or stream meets your requirements, click **Create Log Group** or **Create Log Stream** to create one. After creating a log stream, select an enterprise project.

- **Automatic Mapping**: Workload logs are automatically connected to the generated log streams with the same names as the workloads.
  a. **Rule Name**: Enter a 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.

     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**.
  e. Set an access rule: Select a log group and an enterprise project, and specify a log stream prefix. A log stream will be generated based on the log stream prefix and workload name. By default, all logs of the selected workload are connected.

----End

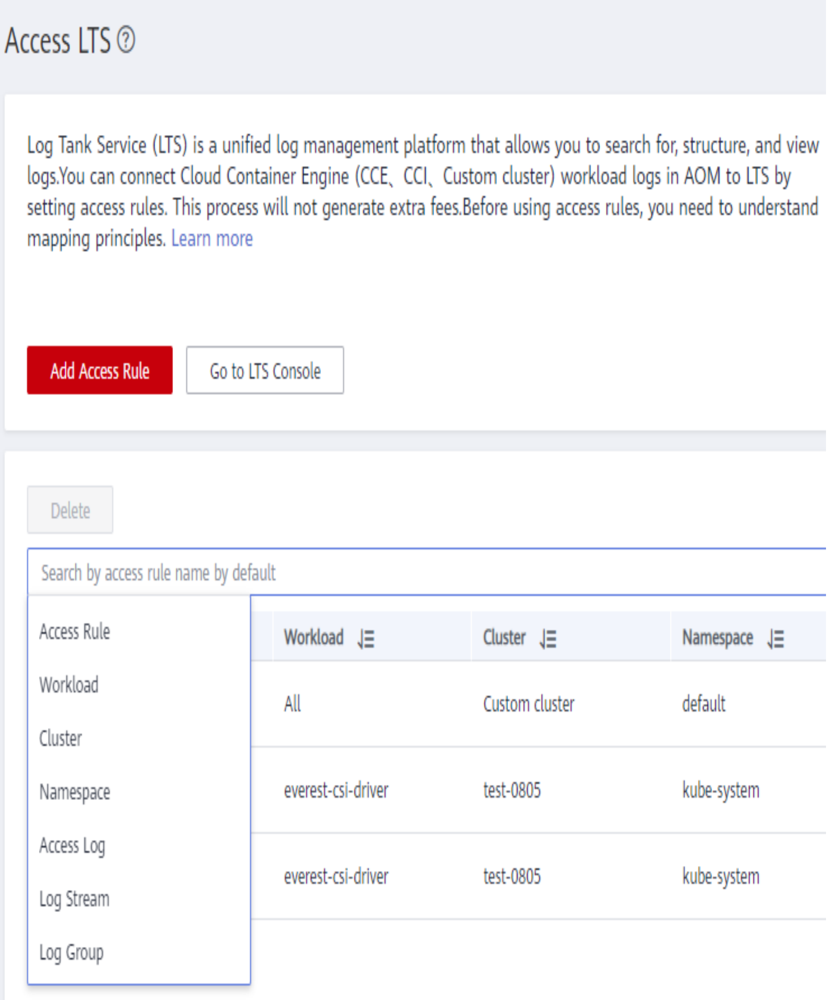
Managing Access Rules

On the **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 8-18 Selecting a search dimension



Access LTS ⓘ

Log Tank Service (LTS) is a unified log management platform that allows you to search for, structure, and view logs.You can connect Cloud Container Engine (CCE、CCI、Custom cluster) workload logs in AOM to LTS by setting access rules. This process will not generate extra fees.Before using access rules, you need to understand mapping principles. Learn more

Add Access Rule | Go to LTS Console

Delete

Search by access rule name by default

Access Rule
Workload
Cluster
Namespace
Access Log
Log Stream
Log Group

Workload	Cluster	Namespace
All	Custom cluster	default
everest-csi-driver	test-0805	kube-system
everest-csi-driver	test-0805	kube-system

- View

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

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

- Edit

  Click **Edit** in the **Operation** column to edit the access rule. For details about the impact of modifying an access rule, see **Modifying a Mapping**.

- Delete

  Click **Delete** in the **Operation** column to delete the access rule. Select one or more access rules and click **Delete** above the rule list.

  NOTE

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

9 Configuration Management

9.1 ICAgent Management (Huawei Cloud Host)

9.1.1 Installing an ICAgent

ICAgents collect metrics, logs, and application performance data in real time. For hosts purchased from the ECS or BMS console, you need to manually install the ICAgent. For hosts purchased from the CCE console, the ICAgent is automatically installed.

NOTE

AOM and LTS use the same ICAgent functions. All metric data collected by ICAgents will be reported to AOM for analysis and processing. However, for logs, only those matching the latest log collection configuration in the system will be collected.

For example, if you configure log collection paths in AOM for ECSs, the previous LTS collection configurations of all ECSs under the resource set become invalid.

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 an ICAgent, see **Installing an 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.

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

Prerequisites

Before installing an 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 an 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 an 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 condition is met: An ICAgent has never been installed on your server.
Inherited installation	This method is used when the following conditions are met: You need to install ICAgents on multiple servers. An 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 an ICAgent for the first time, perform the following operations:

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

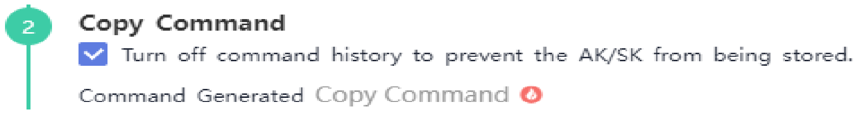
- If you have obtained the AK/SK, skip this step.
- If you have not obtained an AK/SK, **obtain them first**.

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

Step 3 Select **Other: custom hosts**, 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



2 Copy Command

☑ Turn off command history to prevent the AK/SK from being stored.

Command Generated Copy Command

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

- Inherited installation is not supported when ICAgents are installed using an IAM agency.
- If both the expect tool and the ICAgent have been installed on the server, an ICAgent will be installed on the remote server after the preceding command is executed. If an 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 an ICAgent has been installed to remotely communicate with the server where an 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 an 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 ICAgents on multiple remote servers with a few clicks.

NOTICE

1. Ensure that you can run the **SSH** and **SCP** commands on the server where an ICAgent has been installed to communicate with the remote servers where an ICAgent is to be installed.
2. If you have installed an ICAgent in a server through an agency, you also need to set an agency for other servers where an 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.
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 an 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 an 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.
- Batch installation depends on Python 3.x. If the system displays a message indicating that Python cannot be found during the installation, install Python and try again.
- Before the installation, check whether the Python command file exists. If the file does not exist, create a soft link.

Procedure

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

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

Enter the preset 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 preset 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: custom hosts** 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: custom hosts** in **Step 2**, select a desired host and then click **Upgrade ICAgent**.

Step 4 (CN North-Beijing 4, CN East-Shanghai 1, CN East-Shanghai 2, and CN-South Guangzhou) Select a target version from the drop-down list and click **OK**.

Step 5 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: custom hosts** 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 **OK**.

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 ECS meets the requirements listed in **OSs and versions supported by AOM** and supports the AMD64 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.

Precautions

When you install an ICAgent on a non-Huawei Cloud server, the jump server forwarding command generated by the system does not contain any domain name. That is, the ICAgent cannot be installed using a domain name.

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.

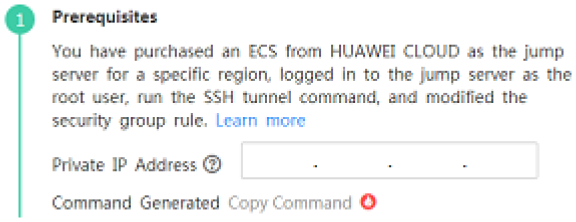
Step 2 Log in to the AOM console. In the navigation pane, choose **Configuration Management** > **Agent Management**.

Step 3 Select **Other: custom hosts**, 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



1 **Prerequisites**

You have purchased an ECS from HUAWEI CLOUD as the jump server for a specific region, logged in to the jump server as the root user, run the SSH tunnel command, and modified the security group rule. Learn more

Private IP Address ⓘ . . .

Command Generated Copy Command

NOTE

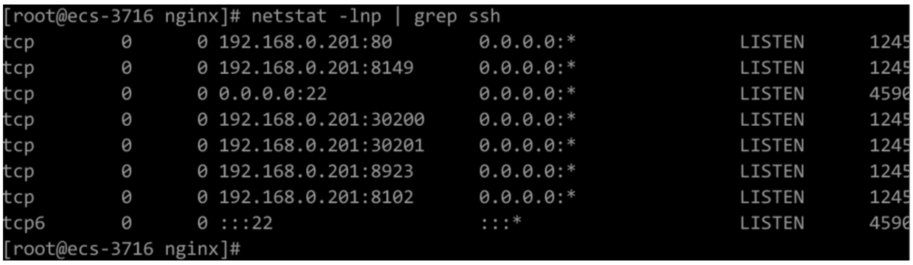
The private IP address of the jump server refers to the internal IP address of the Virtual Private Cloud (VPC) where the jump server is located.

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      4596
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      4596
[root@ecs-3716 nginx]#
```

NOTE

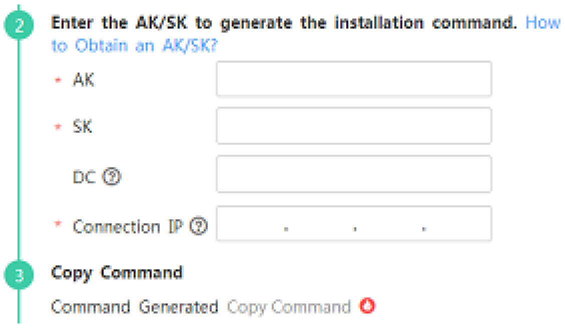
- Enter **http://***Jump server IP address* in the address bar of a browser. If the access is successful, the security group rule has taken effect.
- If the jump server powers off and restarts, run the preceding command again.

Step 5 **Obtain an AK/SK**.

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



2 Enter the AK/SK to generate the installation command. How to Obtain an AK/SK?

* AK

* SK

DC ?

* Connection IP ?

3 Copy Command

Command Generated Copy Command

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: custom hosts** 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: custom hosts** 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: custom hosts** 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 **OK**.

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 access code 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 the access code 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 **access code** 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

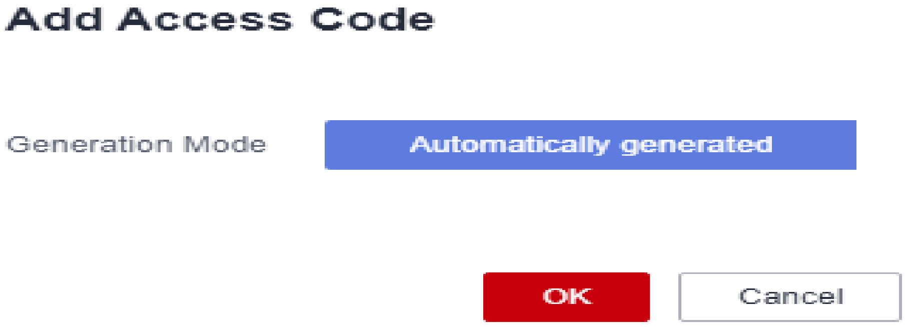
Step 1 Install and start Prometheus. For details, see **Prometheus official documentation**.

Step 2 Add an access code.

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

2. Click **Add AccessCode**.

Figure 9-5 Adding an access code



Add Access Code

Generation Mode: Automatically generated

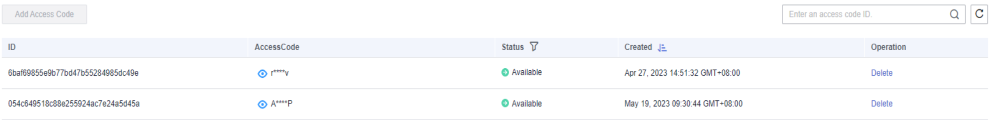
OK | Cancel

NOTE

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

3. In the dialog box that is displayed, click **OK** to add the access code.
4. After the access code is added, click 👁 to view it. To delete the access code, click **Delete** in the **Operation** column. Deleted access codes cannot be recovered. Exercise caution when performing this operation.

Figure 9-6 Viewing the access code



Add Access Code

Enter an access code ID.

ID	AccessCode	Status	Created	Operation
6baf69855e9b77bd47b55284985dc49e	👁 r****v	Available	Apr 27, 2023 14:51:32 GMT+08:00	Delete
054c649518c88e255924ac7e24a5d45a	👁 A****P	Available	May 19, 2023 09:30:44 GMT+08:00	Delete

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}.{Site domain name suffix}: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.
- *Site domain name suffix*: suffix of a site domain name, for example, **myhuaweicloud.com**.
- **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.{region_name}.{Site domain name suffix}:8443/v1/{project_id}/
push'
    tls_config:
      insecure_skip_verify: true
    bearer_token: 'fVkvjOqghcIARvZZEEWhwSwxesmKz5Efsx9vxZSNGCXEffcjPxxxxxx'
```

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**.

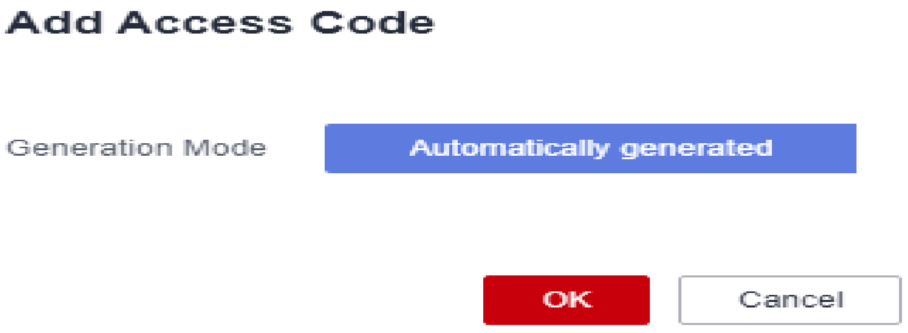
Procedure

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

Step 2 Add an access code.

1. Log in to the AOM console. In the navigation pane, choose **Configuration Management** > **Access Management**.
2. Click **Add AccessCode**.

Figure 9-7 Adding an access code



Add Access Code

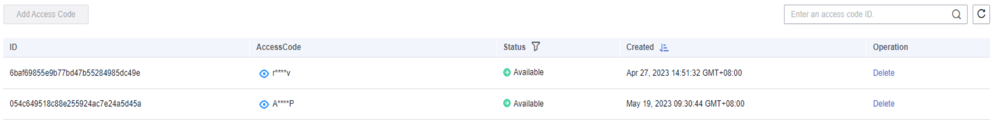
Generation Mode: Automatically generated

NOTE

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

3. In the dialog box that is displayed, click **OK** to add the access code.
4. After the access code is added, click 👁 to view it. To delete the access code, click **Delete** in the **Operation** column. Deleted access codes cannot be recovered. Exercise caution when performing this operation.

Figure 9-8 Viewing the access code

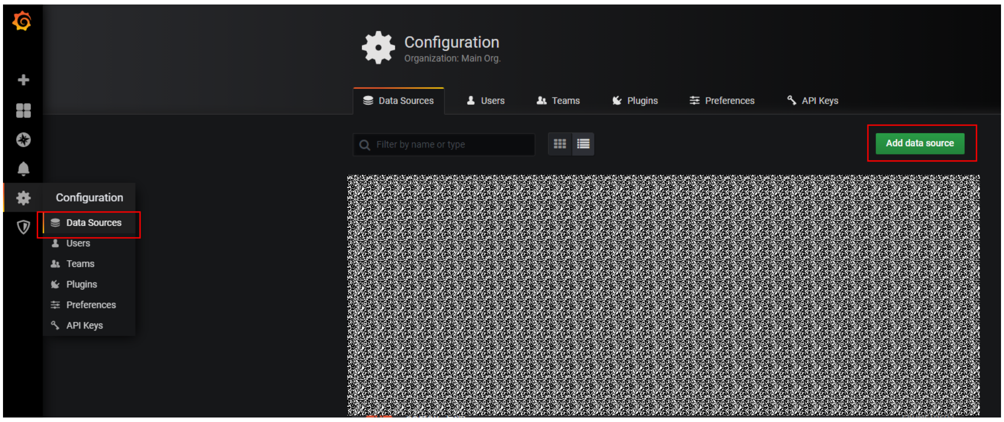


ID	AccessCode	Status	Created	Operation
6baf69855e9b77bd47b55284985dc49e	👁 r****v	Available	Apr 27, 2023 14:51:32 GMT+08:00	Delete
054c649518c88e255924ac7e24a5d45a	👁 A****P	Available	May 19, 2023 09:30:44 GMT+08:00	Delete

Step 3 Configure Grafana.

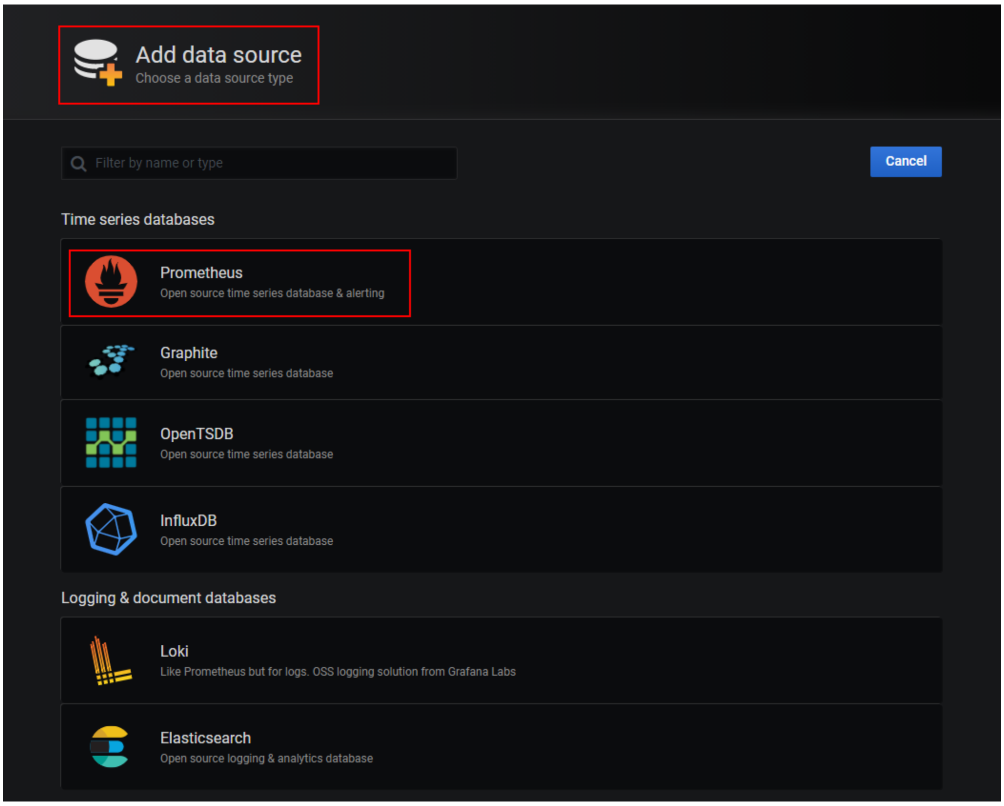
1. Log in to Grafana.
2. In the navigation pane, choose **Configuration** > **Data Sources**. Then, click **Add data source**.

Figure 9-9 Configuring Grafana



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

Figure 9-10 Entering the Prometheus configuration page



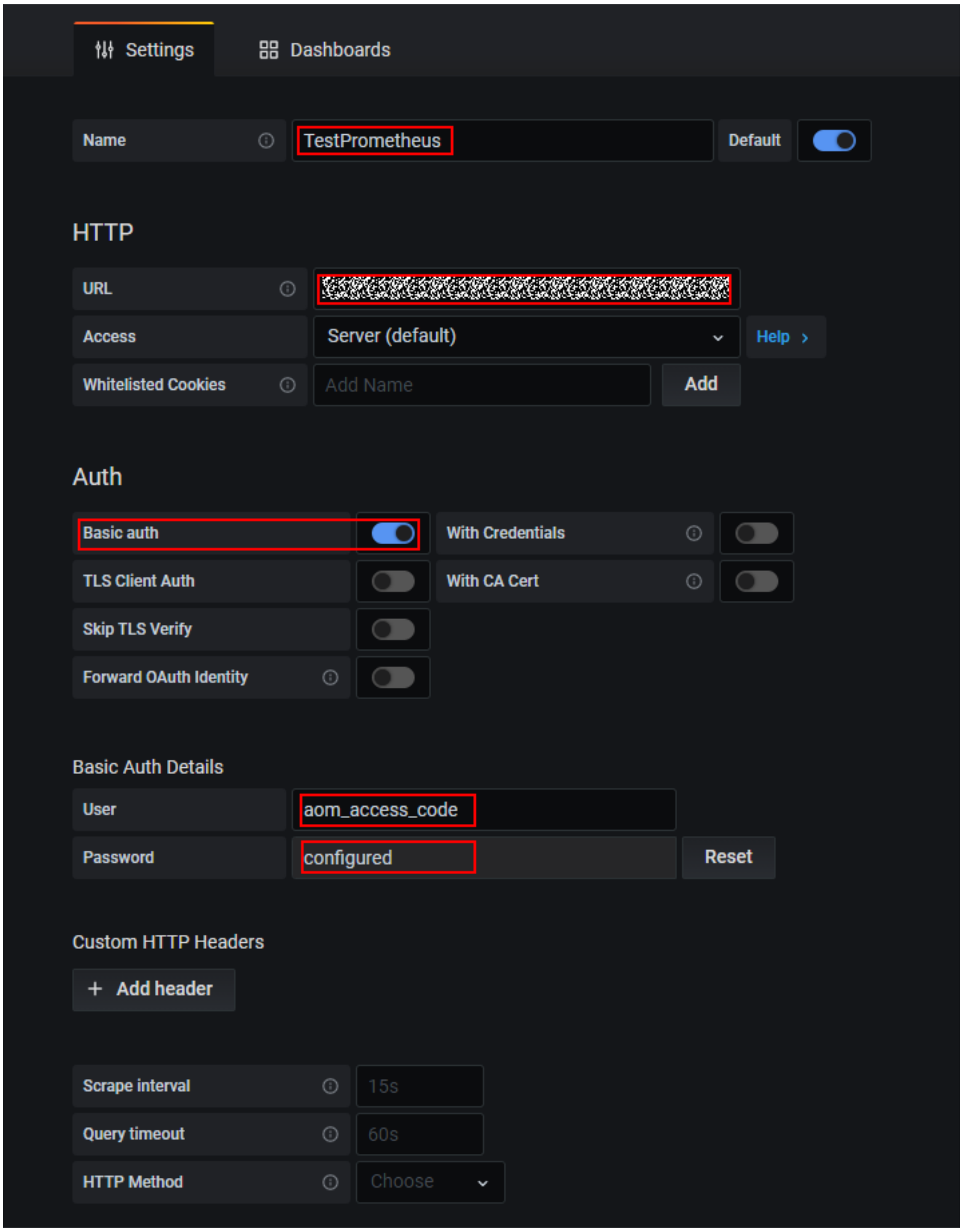
Add data source
Choose a data source type
Filter by name or type
Cancel
Time series databases
Prometheus
Open source time series database & alerting
Graphite
Open source time series database
OpenTSDB
Open source time series database
InfluxDB
Open source time series database
Logging & document databases
Loki
Like Prometheus but for logs. OSS logging solution from Grafana Labs
Elasticsearch
Open source logging & analytics database

4. Set parameters according to the following figure.
   - **Password**: access code 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.
     - **project_id**: project ID, which can be viewed in the project list on the **My Credentials** page.

NOTE

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

Figure 9-11 Configuring parameters



Name: TestPrometheus
Default: on

HTTP

URL: [redacted]
Access: Server (default)
Whitelisted Cookies: Add Name

Auth

Basic auth: on
With Credentials: off
TLS Client Auth: off
With CA Cert: off
Skip TLS Verify: off
Forward OAuth Identity: off

Basic Auth Details

User: aom_access_code
Password: configured

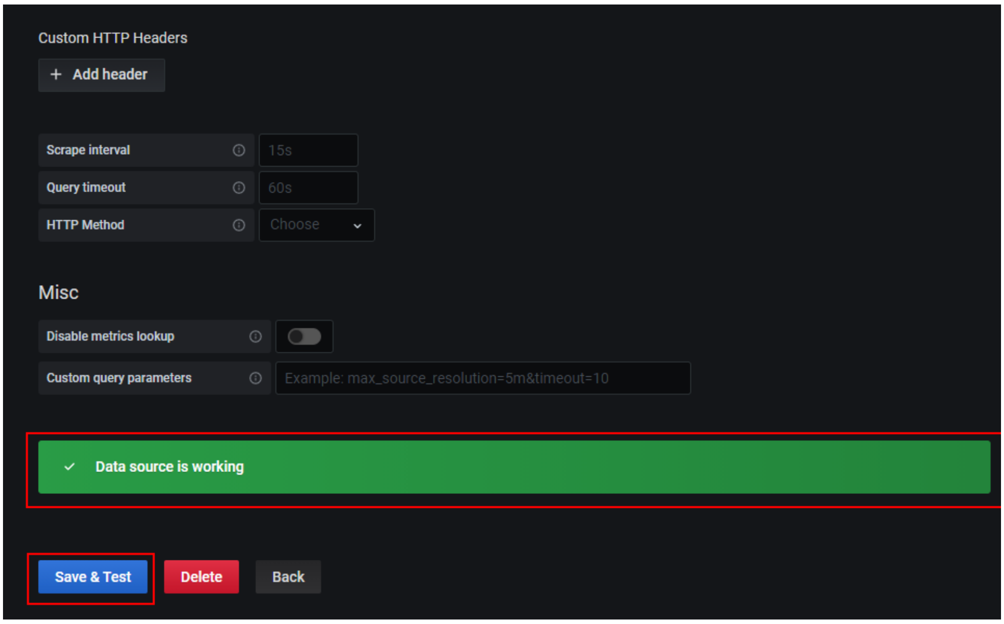
Custom HTTP Headers

Scrape interval: 15s
Query timeout: 60s
HTTP Method: Choose

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 9-12 Checking whether the configuration is successful



Custom HTTP Headers

Scrape interval: 15s

Query timeout: 60s

HTTP Method: Choose

Misc

Disable metrics lookup

Custom query parameters: Example: max_source_resolution=5m&timeout=10

✓ Data source is working

----End

9.4 Log Configuration

9.4.1 Setting the Log Quota

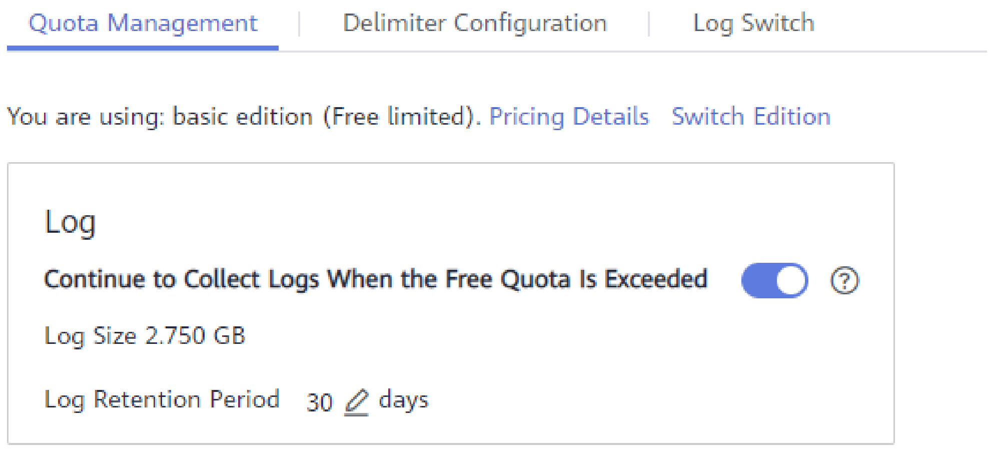
Step 1 Log in to the AOM console. In the navigation pane, choose **Configuration Management** > **Log Configuration**.

Step 2 On the **Quota Management** page, view the log size and retention 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 9-13 Viewing the log quota



You are using: basic edition (Free limited). Pricing Details Switch Edition

Log

Continue to Collect Logs When the Free Quota Is Exceeded

Log Size 2.750 GB

Log Retention Period 30 days

Log Retention Period: 30 days (maximum). You can change the value as required.

----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.

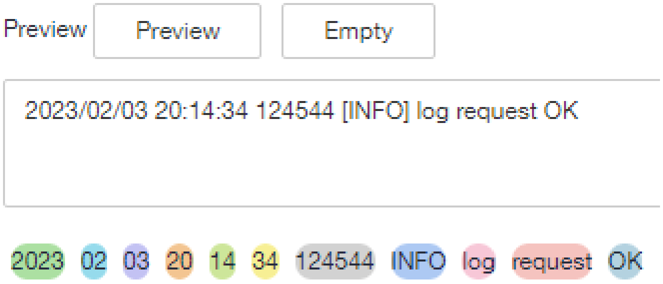
You can configure delimiters using the following methods: If you use both methods at the same time, the union set will be selected.

- 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 9-14 Previewing the log content



```
2023/02/03 20:14:34 124544 [INFO] log request OK
```

2023 02 03 20 14 34 124544 INFO log request OK

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
6	ACK (Acknowledge)	38	&	70	F	102	f

ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character
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
21	NAK (Negative acknowledge)	53	5	85	U	117	u

ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character
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.

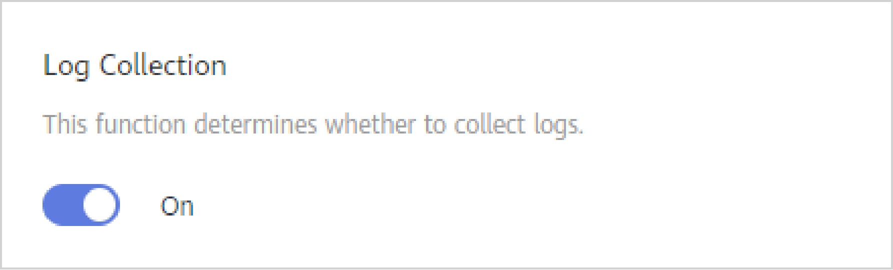
Configuring Log Collection

Before enabling this function, ensure that you have installed the ICAgent on an Elastic Cloud Server (ECS) according to **Installing an 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 9-15 Configuring log collection



Log Collection

This function determines whether to collect logs.

On

NOTE

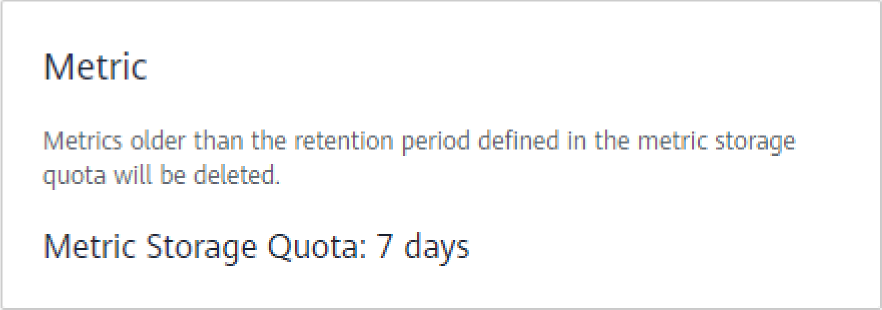
- The log collection function is enabled by default. If you do not need to collect logs, disable this function to reduce resource usage.
- After the log collection function is disabled, ICAgents will stop collecting logs, and this function on the LTS console will also be disabled.

----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 9-16 Configuring the quota



Metric

Metrics older than the retention period defined in the metric storage quota will be deleted.

Metric Storage Quota: 7 days

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

9.6 Metric Configuration

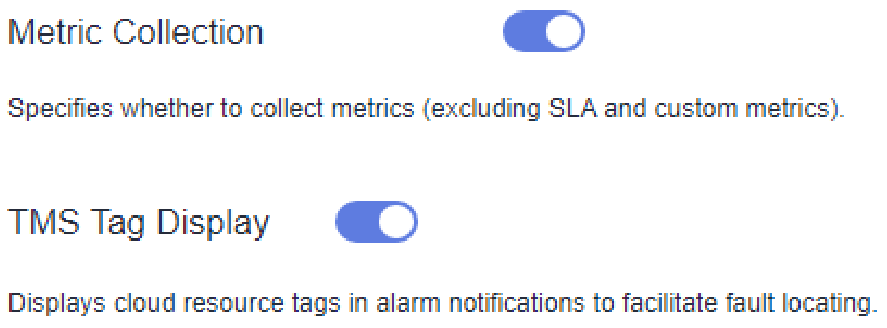
Metric Collection determines whether to collect metrics (excluding SLA and custom metrics). **TMS Tag Display** determines whether to display tags of cloud resources in alarm notifications.

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

Figure 9-17 Enabling or disabling the functions



Metric Collection

Specifies whether to collect metrics (excluding SLA and custom metrics).

TMS Tag Display

Displays cloud resource tags in alarm notifications to facilitate fault locating.

NOTE

After the metric collection function is disabled, ICAgents will stop collecting metric data and related metric data will not be updated. However, custom metrics can still be reported.

----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 need this function, **submit a service ticket**.
- A maximum of 10 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:

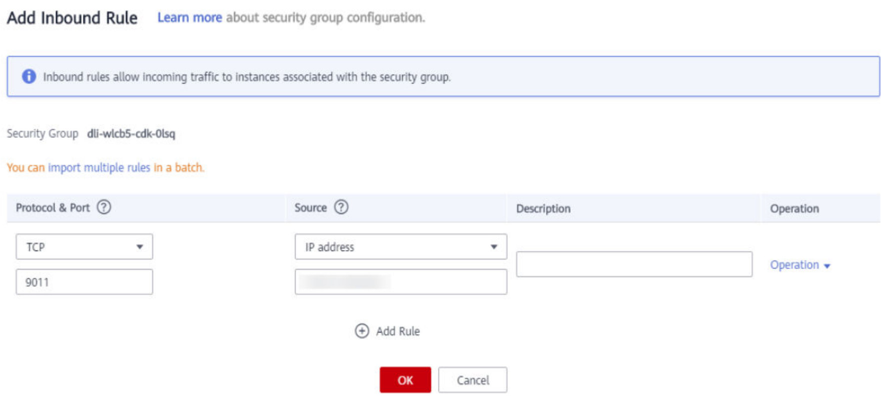
   i. Log in to the management console.

   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 9-18 Adding an inbound rule



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group dli-wlcb5-cdk-0lsq

You can import multiple rules in a batch.

Protocol & Port	Source	Description	Operation
TCP 9011	IP address		Operation

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":"test-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-9b04-33333333333333"},
{"name":"clusterName","value":"test-vss-111"},{"name":"diskDevice","value":"vda"},
{"name":"master","value":"true"}]},"values":[{"value":0,"type":"","unit":"Kilobytes/
Second","statisticvalues":"","metric_name":"diskReadRate"},{"value":30.267,"type":"","unit":"Kilobytes/
Second","statisticvalues":"","metric_name":"diskWriteRate"}],"collect_time":1597821030037}],"project_i
d":"11111111111111111111"}
```

- Alarm data format

  Example:

```
{
    "events": [{
        "id": "4346299651651991683",
        "starts_at": 1597822250194,
        "ends_at": 0,
        "arrives_at": 1597822250194,
        "timeout": 300000,
        "resource_group_id": "3123131231122222222222232131312131",
        "metadata": {
            "kind": "Pod",
            "event_severity": "Major",
            "resource_type": "service",
            "clusterId": "6add4ef5-1358-11ea-a5bf-111111111",
            "event_type": "alarm",
            "clusterName": "cce-ief-4516140c-96ca-4a5f-8d85-1111111",
            "namespace": "PAAS.NODE",
            "name": "test15769793809553052-f5557bd7f-qnfkm",
            "event_name": "FailedScheduling",
            "resource_id": "clusterName=cce-
ief-4516140c-96ca-4a5f-8d85-111111;clusterID=6add4ef5-1358-11ea-
a5bf-11111111111;kind=Pod;namespace=30d5758f166947c6b164af604a654b09;name=test157697938
09553052-f5557bd7f-qnfkm;uid=589fc746-245d-11ea-a465-fa163e5fc15d",
            "nameSpace": "30d5758f166947c6b164af604a654b09",
            "resource_provider": "CCE",
            "nodeID": "589fc746-245d-11ea-a465-fa163e5fc15d"
        },
        "annotations": {
            "alarm_probableCause_zh_cn": "FailedScheduling",
            "alarm_probableCause_en_us": "FailedScheduling",
            "message": "0/110 nodes are available: 1 node(s) had taints that the pod didn't tolerate, 109
node(s) didn't match node selector."
        },
        "attach_rule": {

        }
    }],
    "project_id": "31231312311222222222232131312131"
}
```

Parameter description:

Table 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.
arrives_at	Long	Time when an event or alarm reaches AOM. The value is a CST timestamp precise down to the millisecond.

Parameter	Type	Description
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 Resource Groups

AOM supports resource management by enterprise project and resource granularity, helping you quickly manage and use resources.

NOTICE

You can create a maximum of 100 resource groups.

Creating Resource Groups

Step 1 In the navigation pane, choose **Resource Groups** to view information.

Step 2 Click **Create Resource Group** in the upper right corner.

Step 3 Set parameters based on **Table 10-1**.

Table 10-1 Configuration parameters

Parameter	Description	Example
Group Name	Enter a group name.	AOM
Enterprise Project	Select an enterprise project. If no enterprise project is available, click **Create Enterprise Project** to create one.	default
Description	Enter a description.	-
Group Tag	Enter a tag key and value. **NOTE** A maximum of 10 group tags can be added.	-
Resource List		
Add Resource	To add resources, click **Add Resource**.	-

Parameter	Description	Example
To-Be-Added Resource	Select **Dynamic resource** or **Specified resource** as required. To delete all added resources, click 🗑.	Dynamic resource
Resource Match Rule	Select a resource match rule as required. ● To add more rules, click **Add Rule**. ● To delete a resource match rule, click 🗑. **NOTE** ● **Resource Match Rule** is displayed only when **To-Be-Added Resource** is set to **Dynamic resource**. ● You can add a maximum of 100 resource match rules.	-
Resource Type	Select a resource type based on site requirements. The options are: **Cluster**, **Host**, **Application**, **Component**, **Instance**, **Process**, and **Container**. **NOTE** **Resource Type** is displayed only when **To-Be-Added Resource** is set to **Specified resource**.	Select **Cluster** from the **Resource Type** drop-down list.
Resource Name	The selected resource name is displayed. **NOTE** **Resource Name** is displayed only when **To-Be-Added Resource** is set to **Specified resource**.	arm-test-77169
Resource List	Select a required resource. **NOTE** **Resource List** is displayed only when **To-Be-Added Resource** is set to **Specified resource**.	arm-test-77169

Step 4 After setting the parameters, click **OK**.

----End

Viewing Resource Groups

Step 1 In the navigation pane, choose **Resource Groups** to view information.

You can enter a keyword in the search box on the right to search for a resource group.

----End

Modifying Resource Groups

Step 1 In the navigation pane, choose **Resource Groups** to view information.

Step 2 Click **Modify** in the **Operation** column of the target resource group.

Step 3 In the dialog box that is displayed, modify the resource information and click **OK**.

----End

Deleting Resource Groups

Step 1 In the navigation pane, choose **Resource Groups** to view information.

Step 2 Click **Delete** in the **Operation** column of the target resource group.

----End

11 Auditing

11.1 Operations Logged by CTS

AOM is a one-stop O&M platform that monitors applications and resources in real time. By analyzing dozens of metrics and correlation between alarms and logs, AOM helps O&M personnel quickly locate faults.

You can use AOM to comprehensively monitor and uniformly manage servers, storage, networks, web containers, and applications hosted in Docker and Kubernetes. This effectively prevents problems and helps O&M personnel locate faults in minutes, reducing O&M costs. Also, AOM provides unified APIs to interconnect in-house monitoring systems or report systems. 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 and maximize value. With CTS, you can record operations associated with AOM for future query, audit, and backtracking.

NOTE

pe traces actually record AOM operations, but these operations are performed through CCE or ServiceStage.

Table 11-1 Operations logged by CTS

Operation	Resource Type	Event Name
Creating a dashboard	ams	add-view-action
Modifying a dashboard	ams	update-view-action
Deleting a dashboard	ams	deleteDashboard
Creating a threshold	ams	addThreshold
Modifying a threshold	ams	updateThreshold
Deleting a threshold	ams	deleteThreshold

Operation	Resource Type	Event Name
Deleting a subscription rule	apminventory	deleteSubscribeRule
Modifying a subscription rule name	apminventory	updateSubscribeName
Creating a subscription rule	apminventory	createSubscribeRule
Enabling the pay-per-use edition	OpenOrCloseProService	openProBillingService
Disabling the pay-per-use edition	OpenOrCloseProService	closeProBillingService
Deleting a threshold rule	threshold_rules_v2	deleteOneAlarmById
Deleting threshold rules in batches	threshold_rules_v2	deleteAlarmRules
Modifying a threshold rule	threshold_rules_v2	updateAlarm
Creating a threshold rule	threshold_rules_v2	addAlarmForDT
Modifying an event alarm rule	event2alarm_rule	updateEvent2AlarmRule
Creating an event alarm rule	event2alarm_rule	addEvent2AlarmRule
Deleting an event alarm rule	event2alarm_rule	deleteEvent2AlarmRule
Installing a collector	icmgr	icagentInstall
Upgrading a collector	icmgr	icagentUpgrade
Upgrading a probe	icmgr	pinPointUpgrade
Uninstalling a collector	icmgr	IcagentUninstall
Setting metric and log collection	icmgr	metricAndLogSwitches
Creating an access code	icmgr	icmgrAddAccessCode
Deleting an access code	icmgr	icmgrDelAccessCode
Delivering configuration	icmgr	webIcAgentEvent
Clearing an alarm	pushEvents	clearEvents

Operation	Resource Type	Event Name
Creating an alarm action rule	actionRule	addActionRule
Modifying an alarm action rule	actionRule	updateActionRule
Deleting an alarm action rule	actionRule	delActionRule
Creating a message template	notificationTemplate	addNotificationTemplate
Modifying a message template	notificationTemplate	updateTemplate
Deleting a message template	notificationTemplate	delTemplate
Creating a grouping rule	groupRule	addGroupRule
Modifying a grouping rule	groupRule	updateGroupRule
Deleting a grouping rule	groupRule	delGroupRule
Creating a suppression rule	inhibitRule	addInhibitRule
Modifying a suppression rule	inhibitRule	updateInhibitRule
Deleting a suppression rule	inhibitRule	delInhibitRule
Creating a silence rule	muteRule	addMuteRule
Modifying a silence rule	muteRule	updateMuteRule
Deleting a silence rule	muteRule	delMuteRule
Creating or modifying an application discovery rule	apminventory	addOrUpdateAppRules
Deleting an application discovery rule	apminventory	deleteAppRules
Modifying the alias or tag of an application, host, or component	apminventory	updateInventoryTag
Creating a policy group	pe	createPolicyGroup

Operation	Resource Type	Event Name
Deleting a policy group	pe	deletePolicyGroup
Updating a policy group	pe	updatePolicyGroup
Enabling a policy group	pe	enablePolicyGroup
Disabling a policy group	pe	disablePolicyGroup
Creating a policy	pe	createPolicy
Deleting a policy	pe	deletePolicy
Updating a policy	pe	updatePolicy
Enabling a policy	pe	enablePolicy
Disabling a policy	pe	disablePolicy
Updating the aging period	als	updateLogStorgeSetting

11.2 Viewing Audit Logs

For details, see **Querying Real-Time Traces**.