Application Operations Management

User Guide

Issue	01
Date	2022-08-11

Huawei Technologies Co., Ltd.

Contents

1 Introduction

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 provides flexible 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 comprehensively monitors and uniformly manages cloud 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, meeting your requirements for high efficiency and fast iteration. It provides effective IT support for your services, and protects and optimizes your IT assets, enabling you to achieve strategic goals.

2 Getting Started

2.1 Process of Using AOM

AOM is a one-stop, multi-dimensional O&M management platform for cloud applications. It monitors applications and related cloud resources in real time, analyzes application health status, and provides flexible alarm reporting and data visualization functions. It helps you detect faults in a timely manner and monitor running status of applications, services, and other resources in real time. This section describes how to get started with AOM.

1. Creating a cloud host

   Each host corresponds to a VM on the cloud, for example, an Elastic Cloud Server (ECS). A host can be directly created on the ECS console, or indirectly created on the Cloud Container Engine (CCE) console.

2. Installing the ICAgent

   ICAgent is the data collector of AOM. It collects metrics, logs, and application performance data in real time. For hosts created on the ECS console, you need to manually install the ICAgent. For hosts created on the CCE console, the ICAgent is automatically installed.

3. Configuring an alarm rule

   You can set threshold conditions for metrics by using alarm rules. If metric values meet threshold conditions, AOM generates threshold alarms. If no metric data is reported, AOM will report insufficient data events. In this way, you can identify and handle exceptions at the earliest time.

4. Viewing alarms

   AOM provides the dashboard and alarm list for you to perform routine O&M.

2.2 Installing the ICAgent

This section describes how to install an ICAgent on an ECS.

Prerequisites

- An ECS has been created.

- An EIP has been bound to the ECS.
- An AK/SK have been obtained. For details, see **4.2 Obtaining an AK/SK**.
- The browser time is the same as the ECS time.

Procedure

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

Step 2 Click **Install ICAgent**.

Step 3 Generate and copy the ICAgent installation command.

Step 4 Use a remote login tool, such as PuTTY, to log in as the **root** user to the server where the ICAgent is to be installed, run the command copied in the previous step, and enter the AK/SK as prompted to install the ICAgent.

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

----End

2.3 Adding Alarm Rules and Viewing Alarms

You can set threshold conditions for metrics by using alarm rules. If metric values meet threshold conditions, AOM will generate threshold alarms. If no metric data is reported, AOM will report insufficient data events. In this way, you can identify and handle exceptions at the earliest time.

For example, during routine O&M, a host may break down or restart due to an excessively-high CPU usage. To avoid the problem, set an alarm rule. For example, when the CPU usage of a host exceeds 85%, an alarm is reported, so that you can quickly obtain the resource running status and take measures to prevent service loss. This section describes how to add alarm rules and view alarms.

Procedure

Step 1 In the navigation pane, choose **Alarm Center** > **Alarm Rule** and click **Add Threshold**.

Step 2 Customize alarm rules.

1. Select resources: Enter a rule 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 alarm rules will be created after the creation is complete. Each resource is monitored by an alarm rule. A rule name consists of the alarm rule name you enter in the **Threshold name** text box, and a sequence number ranging from 0 to 99. The earlier a resource is selected, the smaller its sequence number.

2. Customize a threshold: Select the metric to be monitored, and set parameters such as **Threshold Condition**, **Consecutive Period (s)**, **Alarm Severity**, and **Statistic Method**.

📖 NOTE

– **Threshold Condition**: Trigger condition of a threshold alarm. A threshold condition consists of two parts: determination condition (≥, ≤, >, or <) and threshold value. For example, if **Threshold Condition** is set to **> 85** and an actual metric value exceeds 85, a threshold alarm will be generated.

– **Consecutive Period (s)**: If a metric value meets the threshold condition for a specified number of consecutive periods, a threshold alarm will be generated.

– **Statistic Method**: Method used to measure metric values.

– **Statistical Cycle**: Interval at which metric data is collected.

Step 3 Click **Submit**. As shown in the following figure, multiple alarm rules are created. Each resource is monitored by an independent rule.

For example, when a monitored component uses more than 3 CPU cores, a threshold alarm is generated on the alarm page. You can choose **Alarm Center** > **Alarm Rule** in the navigation pane to view the alarm rule.

Step 4 In the navigation pane, choose **Alarm Center** > **Alarm List**.

Step 5 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 a predefined time label, such as **Last 1 hour**, **Last 6 hours**, or **Last 1 day** in the upper right corner of the page. You can select a time range as required.

Method 2: Specify the start time and end time in the upper right corner of the page to customize a time range. You can specify up to 30 days.

2. Set filter criteria and click **Search** to view the alarms generated in the specified time range.

Step 6 Perform the operations listed in **Table 2-1** as required.

Table 2-1 Operations

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

Operation	Method	Description
Clearing alarms	In the alarm list, click 🗑 in the **Operation** column of the target alarm.	- You can clear an alarm after the corresponding problem is resolved. - You can view the cleared alarms on the **History** tab page.
Viewing alarm details	Click an alarm name to view alarm details.	-

----End

3 **User Guide**

3.1 Overview

3.1.1 O&M

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

Infrastructure Monitoring

This card mainly displays infrastructure metrics. You can select one cluster to view its information. When you select the **roma-aom2** cluster, the following information is displayed:

- Host running status, CPU usage, and physical memory usage.
- Trend graph of network traffic data in the last hour. The values of each point in the graph respectively indicate the total downlink/uplink rates of all clusters in one minute. The values displayed above the trend graph respectively indicate the total downlink/uplink rates of the cluster at the latest time point.
- Trend graph of CPU and memory usage in the last hour. The values of each point in the graph respectively indicate the average CPU and memory usage of the cluster in one minute. The values displayed above the trend graph respectively indicate the average CPU and memory usage of the cluster at the latest time point.

Application Monitoring

This card mainly displays application metrics:

1. Running status of applications, components, containers, and instances.

2. The following information is displayed when you select an application:

   – Trend graph of network traffic data in the last hour. The values of each point in the graph respectively indicate the receive rate (BPS) and send rate (BPS) of the selected application in one minute. The values above the graph respectively indicate the receive rate (BPS) and send rate (BPS) of the selected application at the latest time point.

   – Trend graph of CPU and memory usage in the last hour. The values of each point in the graph respectively indicate the CPU and memory usage of the selected application in one minute. The values above the graph respectively indicate the CPU and memory usage of the selected application at the latest time point.

Information Statistics

This card mainly displays alarms, alarm rules, and trends of alarms and hosts.

Host Monitoring (Disk)

This card mainly displays:

- The top 5 hosts with high disk read/write rate in the last minute.
- Trend graph of the disk read/write rate of the selected host in the last hour. The values of each point in the graph respectively indicate the average 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.

Cluster Monitoring (CPU and Memory)

This card mainly displays:

- The top 5 clusters with high CPU and memory usage in the last minute.
- Trend graph of the CPU and memory usage of the selected cluster in the last hour. The values of each point in the graph respectively indicate the average 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.

Host Monitoring (CPU and Memory)

This card mainly displays:

- The top 5 hosts with high CPU and memory usage in the last minute.
- Trend graph of the CPU and memory usage of the selected host in the last hour. The values of each point in the graph respectively indicate the average 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.

Container Instance Monitoring (CPU and Memory)

This card mainly displays:

- The top 5 container instances with high CPU and memory usage in the last minute.
- Trend graph of the CPU and memory usage of the selected container instance in the last hour. The values of each point in the graph respectively indicate the average 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.
- Option , which can be selected as required.

Host Monitoring (Network)

This card mainly displays:

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

Cluster Monitoring (Disk)

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 average 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.

More Operations

You can also perform the operations described in **Table 3-1**.

Table 3-1 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.
Enlarging a 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.

3.1.2 Dashboard

With a dashboard, different graphs can be displayed on the same screen. Different graphs, such as line graphs and digit graphs can be used to display resource data, so that you can view monitoring data comprehensively.

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

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

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

- **Digit graph**: displays the latest value of a metric in real time.

  The following figure shows the average CPU usage of a component.

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

The statuses of thresholds, hosts, and components can be displayed. The statuses of one or more alarm rules, hosts, or components can be added in one graph for monitoring. Titles of health status graphs can be customized.

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

  📖 **NOTE**

  Before adding a threshold-crossing status graph, **create an alarm rule**. Otherwise, the threshold-crossing status graph cannot be added.

- **Host status graph**: monitors the health status of hosts in real time.

- **Component status graph**: monitors the health status of components in real time.

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 the top N hosts for display. If the number of resources is less than N, actual resources are displayed. The following figure lists the top 5 instances with the highest CPU usage.

☐ NOTE

- By default, the top 5 resources are displayed. To view the top 15 resources, click **Show Top15**, 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.
- 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 100 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 ten alarm rules can be added to a threshold-crossing status graph.
- A maximum of ten hosts can be added to a host status graph.
- A maximum of ten 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 dialog box, enter a dashboard name and click **OK**.

Step 3 Click **Add Metric Graph** in the upper right corner of the **Dashboard** page. Then, select **Metric Data**, **Health Status**, or **Top N Resources**.

Step 4 Add a metric graph to the dashboard.

- Under **Metric Data**, line and digit graphs can be selected.
- Under **Health Status**, threshold-crossing status graphs, host status graphs, and component status graphs can be selected.

Select a graph that is appropriate for your requirements. The following shows how to add a line graph to a dashboard:

1. On the **Dashboard** page, click **Add Metric Graph**. In the displayed **Select Which to Add** dialog box, click **Create** below **Metric Data**.

2. Select the type of the graph: In the displayed **Add Metric Graph** dialog box, select **Line graph** and then click **Next**.

3. Select the metrics and set **Statistic Method** and **Statistical Cycle**, and click **OK**.

Step 5 Click **Save** in the upper right corner of the **Dashboard** page.

📖 **NOTE**

The **Auto Refresh** (◯) option in the upper right corner of the **Dashboard** page can be enabled to automatically refresh all graphs in the dashboard.

- On (default)

    Data in the dashboard is automatically refreshed every minute.

- Off

    Data in the dashboard is not automatically refreshed.

----End

More Operations

After creating a dashboard, you can also perform the operations described in **Table 3-2**.

Table 3-2 Related operations

Operation 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 line graphs in the dashboard as CSV files to a local PC.
Graph	Add	Click **Add Metric Graph** to add a line graph, digit graph, threshold-crossing status graph, host status graph, component status graph, or top N resource graph to the dashboard.
	Edit	Choose **Edit**, **Copy**, **Delete**, or **View Larger** (support only for line graphs) from the **Operation** drop-down list. 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. **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	Hover over the lower right corner of a graph. When the cursor changes to ↘, hold down your left mouse button to resize the graph.

Operation Object	Operation	Description
	Reposition	Hover over the blank area in the upper or lower part of a graph, and drag and drop it to the desired position.

3.2 Alarm Management

3.2.1 Viewing Alarms

Alarms are the information reported when AOM or an external service such as Cloud Container Engine (CCE) is abnormal or may cause exceptions. Take measures to resolve faults. Otherwise, service exceptions may occur.

Viewing Alarms

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 a predefined time label, such as **Last 1 hour**, **Last 6 hours**, or **Last 1 day** in the upper right corner of the page. You can select a time range as required.

   Method 2: Specify the start time and end time in the upper right corner of the page to customize a time range. You can specify up to 30 days.

2. Set filter criteria and click 🔍 to view the alarms generated in the specified time range.

   You can click **x** to clear filter criteria.

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

Table 3-3 Operations

Operation	Method	Description
Viewing alarm statistics	View alarm statistics that meet filter criteria within a specific time range through a bar graph.	-
Clearing alarms	In the alarm list, click 🗑 in the **Options** column of the target alarm.	• You can clear an alarm after the corresponding problem is resolved. • You can view the cleared alarms on the **History** tab page.

Operation	Method	Description
Viewing alarm details	Click an alarm name to view alarm details.	-

----End

3.2.2 Viewing Events

Generally, events carry important information, informing you of the changes of AOM itself or an external service such as Cloud Container Engine (CCE). Such changes do not necessarily cause exceptions. Events do not need to be handled.

Viewing Events

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

Events are displayed by time. The latest event is displayed at the topmost of the 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 a predefined time label, such as **Last 1 hour**, **Last 6 hours**, or **Last 1 day** in the upper right corner of the page. You can select a time range as required.

   Method 2: Specify the start time and end time in the upper right corner of the page to customize a time range. You can specify up to 30 days.

2. Set filter criteria and click 🔍 to view the events generated in the specified time range.

   You can click **x** to clear filter criteria.

Step 3 Perform the operations listed in **Table 3-4** as required.

Table 3-4 Operations

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

----End

3.2.3 Creating Alarm Rules

You can set threshold conditions for metrics by using alarm rules. If metric values meet threshold conditions, AOM will generate threshold alarms. If no metric data is reported, AOM will report insufficient data events. In this way, you can identify and handle exceptions at the earliest time.

For example, during routine O&M, a host may break down or restart due to an excessively-high CPU usage. To avoid the problem, set an alarm rule. For example, when the CPU usage of a host exceeds 85%, an alarm is reported, so that you can quickly obtain the resource running status and take measures to prevent service loss.

Precautions

You can create a maximum of 1000 alarm rules. If the number of alarm rules reaches the upper limit, delete unnecessary rules and create new ones.

Customizing Alarm Rules

Step 1 In the navigation pane, choose **Alarm Center** > **Alarm Rule** and click **Add Threshold**.

Step 2 Customize alarm rules.

1. Select resources: Enter a threshold rule 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 alarm rules will be created after the creation is complete. Each resource is monitored by an alarm rule. A rule name consists of the alarm rule name you enter in the **Threshold name** text box, and a sequence number ranging from 0 to 99. The earlier a resource is selected, the smaller its sequence number.

2. Customize a threshold: Select the metric to be monitored, and set parameters such as **Threshold Condition**, **Consecutive Period (s)**, **Alarm Severity**, and **Statistic Method**.

   📖 NOTE

   – **Threshold Condition**: Trigger condition of a threshold alarm. A threshold condition consists of two parts: determination condition (≥, ≤, >, or <) and threshold value. For example, if **Threshold Condition** is set to **> 85** and an actual metric value exceeds 85, a threshold alarm will be generated.

   – **Consecutive Period (s)**: If a metric value meets the threshold condition for a specified number of consecutive periods, a threshold alarm will be generated.

   – **Alarm Severity**: **Critical**, **Major**, **Minor**, or **Warning**.

   – **Send Notification**: Alarm notifications sent by SMN will be billed according to the standard pricing of SMN. If you select **Yes**, select a topic and trigger condition.

     ■ **Topic**: If the topic you want to select does not exist, create one on the SMN console.

     ■ **Trigger Condition**: The condition can be **Threshold crossing**, **Normal**, or **Insufficient data**.

   – **Statistic Method**: Method used to measure metric values.

   – **Statistical Cycle**: Interval at which metric data is collected.

Step 3 Click **Submit**. As shown in the following figure, multiple alarm rules are created. Each resource is monitored by an independent rule.

For example, when a monitored component uses more than 3 CPU cores, a threshold alarm is generated on the alarm page. You can choose **Alarm Center** > **Alarm Rule** in the navigation pane to view the alarm rule.

----End

More Operations

After creating an alarm rule, you can also perform the operations described in **Table 3-5**.

Table 3-5 Related operations

Operation	Description
Modifying an alarm rule	Click **Modify** in the **Operation** column.
Deleting an alarm rule	• To delete an alarm rule, click **Delete** in the **Operation** column. • To delete one or more alarm rules, select them and click **Delete** above the rule list.
Searching for an alarm rule	Enter the rule name or description in the search box in the upper right corner and click Q to search.
Viewing an alarm rule	Click ⌄ next to an alarm rule to view its details.
Viewing an alarm	If the metric value of a resource meets a threshold condition in the specified number of consecutive periods, a threshold alarm will be sent. In the navigation pane, choose **Alarm Center** > **Alarm List** to view the alarm.
Viewing an event	During the configured consecutive periods, if no metric data of a resource is reported, an insufficient data event will be sent. In the navigation pane, choose **Alarm Center** > **Event List** to view the event.

3.2.4 Creating Notification Rules

Application Operations Management (AOM) supports alarm notification. You can use this function by creating notification rules. When alarms are reported due to an exception in AOM or an external service, alarm information can be sent to specified personnel by email or Short Message Service (SMS) message. In this way, these personnel can rectify faults in time to avoid service loss.

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

Procedure

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

For example, to ensure that O&M personnel can receive notifications by email when the ICAgent on HostA, HostB, HostC, or HostD in Cluster1 is abnormal or fails to be installed, upgraded, or uninstalled, perform the following operations:

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 configured a notification policy, skip this step.

1. Create a topic according to "Creating a Topic" in the *SMN User Guide*.

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

2. Set a topic policy according to "Creating a Topic" in the *SMN User Guide*.

   Select **apm** for **Services that can publish messages to this topic**. Otherwise, notifications cannot be sent.

3. Add a subscriber, that is, the email or SMS message recipient, for the topic according to "Adding a Subscription" in the *SMN User Guide*. In this way, SMN can notify subscribers of alarm information in real time.

   For example, enter O&M personnel's email addresses.

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 rule description, and click **Confirm**.

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

----End

More Operations

After creating a notification rule, you can also perform the operations described in **Table 3-6**.

Table 3-6 Related operations

Operation	Description
Modifying a notification rule	Click **Modify** in the **Operation** column.
Deleting a notification rule	• To delete a notification rule, click **Delete** in the **Operation** column. • To delete one or more notification rules, select them and click **Delete** above the rule list.

Operation	Description
Searching for a notification rule	Enter a keyword of the notification rule name in the search box in the upper right corner and click 🔍.

3.3 Resource Monitoring

3.3.1 Application Monitoring

An application is a group of identical or similar components divided based on business requirements. Applications are classified into system applications and custom applications. System applications are discovered based on built-in discovery rules, and custom applications are discovered based on custom rules.

After application discovery rules are set, Application Operations Management (AOM) automatically discovers applications that meet the rules and monitors related metrics. For details, see **3.5.2 Configuring Application Discovery**.

Procedure

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

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

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

Step 3 On the application details page, click the **View Monitor Graphs** tab and monitor application metrics.

You can also perform the following operations:

- **Adding an application**

  For the same or similar components that are discovered by default discovery rules or that are not installed with 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** to add a custom application discovery rule. For details, see **3.5.2 Configuring Application Discovery**. After the rule is added, you can monitor the application. AOM can display O&M information by component. For details, see **3.3.2 Component Monitoring**.

- **Creating a view template**

  AOM provides the default view template (**Application Template**) that you can modify. You can also click the plus sign (+) in
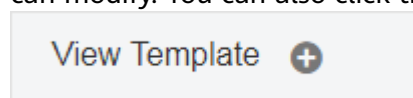
  View Template ⊕

  to add you own template.

- **Adding a metric graph**

You can click to add a line graph or to add a digit graph to the view template. You can also delete, move, and copy metric graphs in the view template according to **3.1.2 Dashboard**.

- **Adding a view template to a dashboard**

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

  ----End

3.3.2 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 information such as type, CPU usage, and memory usage of each component. 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. You can implement multi-dimensional monitoring.

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

- The component list displays information such as **Component Name**, **Status**, **Application**, and **Deployment Mode**.

- Click ![icon] in the upper right corner and select **Hide system component**.

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.

- **Adding a tag**

  Tags are used to identify components. You can distinguish system components from non-system ones by using 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 ![icon] in the upper right corner and select or deselect **Hide system component**. You can also customize tags to facilitate component management.

  In the component list, click **Add tags** in the **Operation** column of the row that contains the target component, click , enter a tag, and click ✓ and **OK**.

> **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 them.

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

> **NOTE**
>
> Components cannot be searched by alias.

Step 4 Click the component name to go to the **Component Details** page.

- Click **View Log** next to the component name to go to the log search page and view the logs of the component. Logs of ServiceStage components cannot be viewed on the **Component Details** page.

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

  > **NOTE**
  >
  > Click an instance name to monitor the resource usage and health status of service processes or instances.

- 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.

----End

3.3.3 Host Monitoring

Hosts include Elastic Cloud Servers (ECSs). AOM monitors the hosts created during Cloud Container Engine (CCE) or ServiceStage cluster creation and the hosts that are directly created. Ensure that the directly created hosts meet operating system (OS) and version requirements and install the ICAgent on these hosts according to **3.5.1.1 Installing the ICAgent**. Otherwise, these hosts cannot be monitored by AOM. In addition, the hosts support both IPv4 and IPv6 addresses.

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

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 when the host generates a threshold alarm. For more information, see **4.4 What Can I Do If Resources Are Not Running Properly?**.

Procedure

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

Click [icon] in the upper right corner and select **Hide master host**.

Step 2 Perform the following operations as required:

- **Adding an alias**

  If a host name is too complex to identify, you can add an alias, which makes it easy to identify a host as required.

  Click **Add alias** in the **Operations** column of the target host.

- **Adding a tag**

  Tags are identifiers of hosts. You can manage hosts using tags. After a tag is added, you can quickly identify and select a host.

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

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 the instances running on the host. Click the **View Monitor Graphs** tab to monitor all the metrics of the host.

Step 5 Monitor common system devices such as GPUs and NICs 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 GPUs 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 NICs 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 disks 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.

----End

3.3.4 Container Monitoring

The difference between container and component monitoring is that their monitored objects are different. For component monitoring, workloads deployed by using Cloud Container Engine (CCE), applications created by using

ServiceStage, and components deployed on Elastic Cloud Server (ECS) are monitored. For container monitoring, only workloads deployed by using CCE and applications created by using ServiceStage are monitored. For details, see **3.3.2 Component Monitoring**.

3.3.5 Metric Monitoring

Metric monitoring displays metric data of each resource. You can monitor metric values and trends in real time, add desired metrics to a dashboard, create alarm rules, and export monitoring reports. 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 up to 12 metrics to be monitored.

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

Table 3-7 Metric parameters

Parameter	Description
Time Range	Time period when metrics are monitored.
Statistical Cycle	Interval at which metric data is collected.
Statistic Method	Method used to measure metrics.

📖 **NOTE**

The number of samples equals to the count of data points.

----End

More Operations

You can also perform the operations described in **Table 3-8**.

Table 3-8 Related operations

Operation	Description
Adding a metric graph to a dashboard	Click **Add to Dashboard** to add your desired metric graph to a dashboard.

Operation	Description
Adding a threshold rule for a metric	After selecting a metric, click **Add to Threshold Rule** to create a threshold rule for the metric.
Exporting a monitoring report	Click **Export Report** to export a metric graph as a CSV file to a local PC.

Operation	Description
Setting an interpolation mode	By default, AOM uses **null** to represent breakpoints in a metric graph. However, a metric graph with breakpoints is not suitable for reports or presentation. You can replace the missing metric data and avoid breakpoints by setting the value of **Interpolation Mode** to **0** or **average**. The value of **Interpolation Mode** can be **null**, **0**, or **average**. ● **null**: Breakpoints are represented by **null** by default. ● **0**: Breakpoints are represented by **0**. ● **average**: Breakpoints are represented by average values. **NOTE** If the value of **Interpolation Mode** is set to **average**, breakpoints will be represented by average values. The following describes how to calculate average values. A metric graph may have multiple breakpoints. When multiple breakpoints exist, values will be interpolated for these breakpoints from left to right. The following uses the first breakpoint in a graph as an example to describe the method of calculating the average value. This method can also be applied to other breakpoints. ● If the first breakpoint is at the start of a metric graph, the value of the breakpoint is the first valid data from its next point to the right. For example, if a metric graph has points a, b, c, d, and e, where a = Null, b = Null, c = Null, d = Null, and e = 5, the value of the first breakpoint (that is, point a) is **5**. ● If the first breakpoint is in the middle of a metric graph, there are the following two scenarios: Scenario 1: If the values of the previous and next points of the breakpoint are valid, the value of the breakpoint is the average value of these two points. For example, if a metric graph has points a, b, c, d, and e, where a = 1, b = Null, c = 3, d = Null, and e = 5, the value of the first breakpoint (that is, point b) is (a + c)/2 = (1 + 3)/2 = 2. Scenario 2: If the value of the previous point of the breakpoint is valid and the value of its next point is null, the value of the breakpoint is the average value of its previous point and the first valid data from its next point to the right. For example, if a metric graph has points a, b, c, d, and e, where a = 1, b = Null, c = Null, d = Null, and e = 5, the value of the first breakpoint (that is, point b) is (a + e)/2= (1 + 5)/2 = 3. Because values are interpolated for breakpoints from left to right, the value of the second breakpoint (that is, point c) is (b + e)/2 = (3 + 5)/2 = 4, the value of the third breakpoint (that is, point d) is (c + e)/2 = (4 + 5)/2 = 4.5. ● If the first breakpoint is at the end of a metric graph, the value of the breakpoint is the value of the previous point. For example, if a metric graph has points a, b, c, d, and e, where a = 1, b = 2, c = 3, d = 4, and e = Null, the value of the first breakpoint (that is, point e) is **4**. ● If all points in a metric graph are breakpoints, the values of all these points are still **null**, even though you set the value of **Interpolation Mode** to **average**. For example, if a metric graph has points a, b, c, d, and e, where a = Null, b = Null, c = Null, d = Null, and e = Null, the values of all breakpoints are **null**.

3.4 Log Management

3.4.1 Searching for Logs

AOM enables you to quickly query logs, and use log source information and context to locate faults.

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 case-sensitive keyword.

   - Enter a keyword for exact search. A keyword refers to a word between two adjacent delimiters.

   - Enter a keyword containing an asterisk (*) or a question mark (?) for fuzzy search. For example, enter **ER?OR**, ***ROR**, or **ER*R**.

   - Enter a phrase for exact search. For example, enter **Start to refresh** or **Start-to-refresh**. Note that hyphens (-) are **delimiters**.

   - Enter a keyword containing AND (&&) or OR (||) for search. For example, enter **query logs&&error*** or **query logs||error**.

   - If no log is found, you are advised to narrow down the search scope and add an asterisk (*) before and after the keyword for fuzzy match.

Step 3 View the search results of logs.

The search results are sorted based on the log collection time. The keywords in the search results are highlighted. You can click ⌗ in the **Time** column to change the 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 surrounding 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 more than or equal to 100 logs printed prior to a log and more than or equal to 99 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 [icon] on the right of the **Log Search** page, select an export format, and export the search result to a local PC.

Logs are sorted according to the order set in **Step 3** and a maximum of 5000 logs can be exported. For example, when 6000 logs in the search result are sorted in the descending order, only the first 5000 logs can be exported.

Logs can be exported in CSV or TXT format. You can select a format as required. If you select the CSV format, detailed information (such as the log content, host IP address, and source) can be exported, as shown in . If the TXT format is selected, only the log content can be exported, as shown in . Each row represents a log. If a log contains a large amount of content, you are advised to view logs using tools such as Notepad++.

----End

3.4.2 Viewing Log Files

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

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

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

Step 3 Click **View** in the **Operation** column of the desired instance. **Table 3-9** shows how to view log file details.

Table 3-9 Operations

Operation	Setup	Description
Setting a time range	Date and time	Click to select the date and time.
	Time range	Select a specific time range on the time axis to view logs. You can select only one range (5 minutes) each time.
Viewing log files	Clear	Click **Clear** to clear the logs displayed on the screen. This operation clears only the logs displayed on the screen but does not delete them.
	Viewing real-time logs	The function of real-time monitoring is disabled by default. To enable it, click **Enable Real-Time Viewing**. 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.
Viewing log files	Maximized display	Click to maximize a page. Components like the time axis are invisible on the screen. Click again to cancel the maximized display.

----End

3.4.3 Configuring VM Log Collection Paths

AOM can collect and display VM logs. VM refers to an Elastic Cloud Server (ECS) running Linux. Before collecting logs, configure a log collection path according to the following procedure.

Prerequisites

You have installed the ICAgent on a VM according to **3.5.1.1 Installing the ICAgent**. About five minutes after the ICAgent is installed, you can view your VM in the VM list on the **Path Configuration** page.

Precautions

- The ICAgent collects ***.log**, ***.trace**, and ***.out** log files only. For example, **/opt/yilu/work/xig/debug_cpu.log**.

- Ensure that an absolute path of the log directory or file is configured and the path exists. For example, **/opt/yilu/work/xig** or **/opt/yilu/work/xig/debug_cpu.log**.

- The ICAgent does not collect log files from subdirectories. For example, the ICAgent does not collect log files from the **/opt/yilu/work/xig/debug** subdirectory of **/opt/yilu/work/xig**.

- A maximum of 20 log collection paths can be configured for a VM.

- For ECSs in the same resource set, only the latest log collection configuration in the system will be used. AOM and LTS log collection configurations cannot take effect at the same time. For example, if you configure log collection paths in AOM for ECSs, the previous LTS collection configurations of all ECSs under the resource set become invalid.

Configuring Log Collection Paths for a Single VM on the Console

Step 1 Log in to the AOM console. In the navigation pane, choose **Log** > **Path Configuration** and click the **Host Log** tab.

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 files that have file handles and are suffixed with **.log**, **.trace**, or **.out** 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.

- **Manually configuring log collection paths**

  If the paths automatically identified by the ICAgent cannot meet your requirements, enter a log directory or file (for example, **/opt/yilu/work/xig/debug_cpu.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.

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 component is deployed on multiple VMs, configuring log collection paths in batches helps you greatly reduce workload.

Step 1 Log in to the AOM console. In the navigation pane, choose **Log** > **Path Configuration** and click the **Host Log** tab.

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**.

◻ 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 a log collection path is configured, the ICAgent collects log files from the configured path. The collection takes about 1 minute. After the collection is complete, 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 **3.4.2 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 **3.4.1 Searching for Logs**.

3.5 Configuration Management

3.5.1 Agent Management

3.5.1.1 Installing the ICAgent

The following table describes the ICAgent status.

Table 3-10 ICAgent status

Status	Description
Running	The ICAgent is running properly.
Uninstalled	The ICAgent is not installed. For details about how to install the ICAgent, see **3.5.1.1 Installing the ICAgent**.
Installing	The ICAgent is being installed. This operation takes about 1 minute to complete.

Status	Description
Installation failed	Failed to install the ICAgent. Uninstall the ICAgent according to **Uninstalling the ICAgent Through Logging In to the Server** and then install it again.
Upgrading	The ICAgent is being upgraded. This operation takes about 1 minute to complete.
Upgrade failed	Failed to upgrade the ICAgent. Uninstall the ICAgent according to **Uninstalling the ICAgent Through Logging In to the Server** and then install it again.
Offline	The Access Key ID/Secret Access Key (AK/SK) are incorrect. Obtain the correct AK/SK and install the ICAgent again.
Abnormal	The ICAgent is abnormal. Contact technical support.
Restricted	The AOM license is restricted. Check the license and update it in a timely manner.

Prerequisites

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

Installation Methods

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

For details, see **Table 3-11**.

Table 3-11 Installation methods

Method	Application Scenario
Initial installation	This method is used when the following conditions are met: 1. An elastic IP address (EIP) has been bound to the server. 2. The ICAgent has never been installed on the server.
Inherited installation	This method is used when the following conditions are met: You have multiple servers on which the ICAgent is to be installed. One server is bound to an EIP, but others are not bound to an EIP. You can use this method to install the ICAgent on the servers that are not bound to an EIP.

Initial Installation

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

Step 1 Obtain an AK/SK.

- If you have obtained the AK/SK, skip this step.

- If you do not have an AK/SK, **obtain them** first.

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

Step 3 Click **Install ICAgent**.

Step 4 Generate and copy the ICAgent installation command.

1. Enter the obtained AK/SK in the text box to generate the ICAgent installation command.

   📖 **NOTE**

   Ensure that the AK/SK are correct. Otherwise, the ICAgent cannot be installed.

2. Click **Copy Command**.

Step 5 Use a remote login tool, such as PuTTY, to log in as user **root** to the server where the ICAgent is to be installed, and run the command copied in the previous step to install the ICAgent.

Step 6 Run the command copied in **Step 4** and enter the obtained AK/SK as prompted to install the ICAgent.

----End

📖 **NOTE**

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

- If the ICAgent fails to be installed, uninstall it according to **Uninstalling the ICAgent Through Logging In to the Server** and then install it again. If the problem persists, contact technical support.

Inherited Installation

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

> **NOTICE**
>
> After the ICAgent is upgraded, the **/opt/ICAgent/** directory and the files stored in it will be deleted. Therefore, reinstall the ICAgent and then perform inherited installation.

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

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

Step 2 Enter the password of the **root** user of the server where the ICAgent is to be installed as prompted.

◻ NOTE

- If both the Expect tool and the ICAgent have been installed on the server, the ICAgent will be installed on the remote server after the preceding command is executed. If the ICAgent has been installed on the server, but the Expect tool has not, enter the information as prompted.

- Ensure that the **root** user can run the **SSH** or **SCP** command on the server where the ICAgent has been installed to remotely communicate with the server where the ICAgent is to be installed.

- Ensure that the **ICProbeAgent.tar.gz** installation package is transmitted to the server to be installed.

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

- If the ICAgent fails to be installed, uninstall it according to **Uninstalling the ICAgent Through Logging In to the Server** and then install it again. If the problem persists, contact technical support.

----End

Inherited Batch Installation

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

> **NOTICE**
>
> 1. Ensure that you can run the **SSH** and **SCP** commands on the ECS server where the ICAgent has been installed to communicate with the remote ECS servers where the ICAgent is to be installed.
>
> 2. If you have installed the ICAgent in a server through an agency, you also need to set an agency for other servers where the ICAgent is to be installed.
>
> 3. Batch installation scripts depend on Python versions. You are advised to implement batch installation on hosts running Python 2.x. Python 3.x does not support batch installation.
>
> 4. You need to press **Enter** at the end of each line in the **iplist.cfg** file.
>
> 5. After the ICAgent is upgraded, the **/opt/ICAgent/** directory and the files stored in it will be deleted. Therefore, reinstall the ICAgent and then perform inherited batch installation.

Prerequisites

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

192.168.0.109 password (Set the password as required.)

192.168.0.39 password (Set the password as required.)

◻ NOTE

- Because the **iplist.cfg** file contains sensitive information, you are advised to clear the information after use.

- If the passwords of all servers are the same, only list IP addresses in the **iplist.cfg** file and enter the password once during execution. If the password of an IP address is different from those of the other ones, list both passwords and IP addresses in the **iplist.cfg** file.

- The batch installation function depends on Python 2.7.*. If the system displays a message indicating that Python cannot be found during the installation, install Python 2.7.* and try again.

Procedure

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

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

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

```
batch install begin
start to install python pexpect module
use local pyexpect package
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 is successfully installed on all the hosts listed in the configuration file.

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

----End

3.5.1.2 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:

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

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

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

Step 4 Wait for about 1 minute to complete the upgrade. When the ICAgent status changes from **Updating** to **Running**, the ICAgent is successfully upgraded.

📖 NOTE

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

----End

3.5.1.3 Uninstalling the ICAgent

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

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

- **Uninstalling the ICAgent Through the AOM Console**: Applies to the scenario where the ICAgent has been successfully installed and needs to be uninstalled.

- **Uninstalling the ICAgent Through Logging In to the Server**: Applies to the scenario where the ICAgent fails to be installed and needs to be uninstalled for reinstallation.

- **Remotely Uninstalling the ICAgent**: Applies to the scenario where the ICAgent has been successfully installed and needs to be remotely uninstalled.

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

Uninstalling the ICAgent Through the AOM Console

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

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

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

The ICAgent begins to be uninstalled. This operation takes about 1 minute to complete. If the involved server is removed from the node list, the ICAgent is successfully uninstalled.

----End

Uninstalling the ICAgent Through Logging In to the Server

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

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 is successfully uninstalled.

----End

Remotely Uninstalling 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 of the server where the ICAgent is to be uninstalled 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.
- 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 is successfully uninstalled. After the ICAgent is successfully 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 after use.
- If the passwords of all servers are the same, only list IP addresses in the **iplist.cfg** file and enter the password once during execution. If the password of an IP address is different from those of the other ones, list both passwords and IP addresses in the **iplist.cfg** file.
- 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 is successfully uninstalled from all the hosts listed in the configuration file.

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

----End

3.5.2 Configuring Application Discovery

AOM can discover applications and collect their metrics based on configured rules. Application discovery supports both automatic and manual configuration. This section focuses on manual configuration.

- **Automatic configuration**

  After you install the ICAgent on a host according to **3.5.1.1 Installing the ICAgent**, the ICAgent automatically discovers applications on the host based

on **Built-in Service Discovery Rules** and displays them on the **Application Monitoring** page.

- **Manual configuration**

  After you add a custom application discovery rule on the application discovery page and apply it to the host where the ICAgent is installed (for details, see **3.5.1.1 Installing the ICAgent**), the ICAgent discovers applications on the host based on the configured service discovery rule and displays them on the **Application Monitoring** page.

Filtering Rules

The ICAgent will periodically detect processes on the target host. The effect is similar to that of running the **ps -e -o pid,comm,lstart,cmd | grep -v defunct** command. Then, the ICAgent checks whether processes match the filtering rules in **Table 3-12**. If a process meets a filtering rule, the process is filtered out and is not discovered by AOM. If a process does not meet any filtering rules, the process is not filtered and is discovered by AOM.

ICAgent detection results may as follows:

```
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 3-12 Filtering rules

Filtering Rule	Example
If the **COMMAND** value of a process is **docker-containe**, **vi**, **vim**, **pause**, **sshd**, **ps**, **sleep**, **grep**, **tailf**, **tail**, or **systemd-udevd**, and the process is not running in the container, the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose **PID** is **1154** is not discovered by AOM because its **COMMAND** value is **docker-containe**.
If the **CMD** value of a process starts with **[** and ends with **]**, the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose **PID** is **2** is not discovered by AOM because its **CMD** value is **[kthreadd]**.
If the **CMD** value of a process starts with **(** and ends with **)**, the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose **PID** is **3** is not discovered by AOM because its **CMD** value is **(ksoftirqd/0)**.

Filtering Rule	Example
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 Service Discovery Rules

AOM provides **Default_Rule**, ServiceStage provides **servicestage-default-rule**, and ICAgent has the built-in **Sys_Rule**. These rules are executed on all hosts, including those added later. The priorities of the three built-in discovery rules are as follows: **Sys_Rule** > **servicestage-default-rule** > **Default_Rule**. Rule details are as follows:

Sys_Rule (cannot be disabled)

- For the component name, obtain the value of **-Dapm_tier** in the command, the value of the environment variable **PAAS_APP_NAME**, and the value of **-Dapm_tier** of the environment variable **JAVA_TOOL_OPTIONS** based on the priorities in descending order.

- For the application name, obtain the value of **-Dapm_application** in the command, the value of environment variable **PAAS_MONITORING_GROUP**, and the value of **-Dapm_application** in the environment variable **JAVA_TOOL_OPTIONS** based on the priorities in descending order.

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
```

📖 **NOTE**

> **sys_rule** (built-in application discovery rule) is used to discover CCE workloads in the CCE scenario (except the APM scenario).

servicestage-default-rule (can be disabled)

Detect the processes whose environment variables contain **CAS_APPLICATION_NAME**, **CAS_COMPONENT_NAME**, and **CAS_ENVIRONMENT_NAME**.

Obtain the value of the environment variable **CAS_COMPONENT_NAME** and combine it as the component name.

Obtain the value of the environment variable **CAS_APPLICATION_NAME** and combine it as the application name.

> **NOTE**
>
> Nginx of a version earlier than 1.19 does not support manual configuration of environment variables. Therefore, the data source of the Nginx component configured on ServiceStage may be displayed as **CCE** on the **Component Monitoring** page of AOM. To solve this problem, use Nginx of 1.19 or a later version, manually configure environment variables such as **CAS_COMPONENT_NAME** and **CAS_COMPONENT_ID**.

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

The priorities of discovery rules are as follows: Sys_Rule > Custom discovery rules > Default_Rule. **servicestage-default-rule** is also a custom discovery rule.

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

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

Step 3 Select a host for pre-detection.

1. Customize a rule name, for example, **ruletest**.

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

Step 4 Set an application discovery rule.

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

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

   > **NOTE**
   >
   > – To precisely detect processes, you are advised to add check items about unique features of the processes.
   >
   > – You need to add one check item at least and can add five check items at most. 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, go to the next step.

Step 5 Set a component name.

1. Set an application name.

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

   📖 **NOTE**

   – If you do not set an application name, **unknownapplicationname** is used by default.

   – When you add multiple naming rules, all the naming rules are combined as the application name of the process. Metrics with the same application name are aggregated.

2. Set a component name.

   In the **Component Name Settings** area, click **Add Naming Rule** to set a component name for the discovered process.

   📖 **NOTE**

   – The component name cannot be left blank.

   – When you add multiple naming rules, all the naming rules are combined as the component name of the process. Metrics with the same component name are aggregated.

3. Preview the component name.

   If the application or component name does not meet your requirements, click

   🖉 in the **Preview Component Name** table for renaming.

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.

   📖 **NOTE**

   Do not use multiple custom discovery rules with the same priority for the same process.

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 those added later.

Step 7 Click **Add** to complete the configuration. AOM collects metrics of the process.

Step 8 Wait for about two minutes, choose **Monitoring** > **Component Monitoring** in the navigation pane, select the **hhhhhh-27465** host from the cluster drop-down list, and find out the **/openvswitch/** component that has been monitored.

----End

📖 **NOTE**

Custom discovery rules cannot be used to discover workload processes in the CCE scenario. You are advised to use custom discovery rules to discover non-workload processes in the CCE scenario or processes in the VM scenario.

More Operations

After creating an application discovery rule, you can also perform the operations described in **Table 3-13**.

Table 3-13 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 process metrics.
Deleting a rule	To delete a discovery rule, click **Delete** in the **Operation** column. **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.

3.5.3 Log Configuration

3.5.3.1 Viewing 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** tab page, view the log size and log retention period.

The default log retention period is 7 days and cannot be changed.

----End

3.5.3.2 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 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.

- Custom delimiters: Click ✎, enter a delimiter in the text box, and click ✔.
- Use ASCII code: 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 preview in the text box and click **Preview**.

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 3-14 ASCII comparison table

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

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

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

3.5.4 Data Subscription

AOM allows you to subscribe to metrics or alarms. After the subscription, data can be forwarded to configured Kafka topics for you to retrieve.

Procedure

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

Step 2 Click **Create Subscription Rule** in the upper right corner of the page. Then, set parameters according to **Table 3-15** and click **OK**.

Table 3-15 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	Custom Kafka, which cannot be changed.	-
Subscription Target Address	Kafka address, which needs to be connected to Internet. If there are multiple addresses in the format of "IPv4 address:port", separate them by commas (,). Example: **192.168.0.1:9092,192.168.0.2:9092**	Set this parameter as required.

Step 3 On the **Rule Details** page, click **Verify and Save Custom Kafka Configuration** to verify the connectivity of the custom Kafka instance.

Step 4 Select the Kafka topic to which the data is to be sent. 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":"xx-region-1-vss-cop-master-1"},{"name":"nodeIP","value":"1.1.1.1"},
{"name":"hostID","value":"75d97111-4734-4c6c-ae9e-f6111111111"},
{"name":"nameSpace","value":"default"},
{"name":"clusterId","value":"46a7bc0d-1d8b-11ea-9b04-333333333333333"},
{"name":"clusterName","value":"xx-region-1-vss-111"},{"name":"diskDevice","value":"vda"},
{"name":"master","value":"true"}]},"values":[{"value":0,"type":"","unit":"Kilobytes/
Second","statisticvalues":"","metric_name":"diskReadRate"},{"value":30.267,"type":"","unit":"Kilobytes/
Second","statisticvalues":"","metric_name":"diskWriteRate"}],"collect_time":
1597821030037}],"project_id":"111111111111111111111"}
```

- Alarm data format

    Example:

```
{
    "events": [{
        "id": "4346299651651991683",
        "starts_at": 1597822250194,
        "ends_at": 0,
        "arrives_at": 1597822250194,
        "timeout": 300000,
        "resource_group_id": "31231312311222222222232131312131",
        "metadata": {
            "kind": "Pod",
            "event_severity": "Major",
            "resource_type": "service",
            "clusterId": "6add4ef5-1358-11ea-a5bf-111111111",
            "event_type": "alarm",
            "clusterName": "cce-ief-4516140c-96ca-4a5f-8d85-1111111",
            "namespace": "PAAS.NODE",
            "name": "test15769793809553052-f5557bd7f-qnfkm",
            "event_name": "FailedScheduling",
            "resource_id": "clusterName=cce-
ief-4516140c-96ca-4a5f-8d85-111111;clusterID=6add4ef5-1358-11ea-
a5bf-11111111111;kind=Pod;namespace=30d5758f166947c6b164af604a654b09;name=test157697938
09553052-f5557bd7f-qnfkm;uid=589fc746-245d-11ea-a465-fa163e5fc15d",
            "nameSpace": "30d5758f166947c6b164af604a654b09",
            "resource_provider": "CCE",
            "nodeID": "589fc746-245d-11ea-a465-fa163e5fc15d"
        },
        "annotations": {
            "alarm_probableCause_zh_cn": "FailedScheduling",
            "alarm_probableCause_en_us": "FailedScheduling",
            "message": "0/110 nodes are available: 1 node(s) had taints that the pod didn't tolerate, 109
node(s) didn't match node selector."
        },
        "attach_rule": {

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

The following table describes the parameters.

Table 3-16 Alarm parameters

Parameter	Type	Description
events	Array of objects. For details, see **Table 3-17**.	Event or alarm details.
project_id	String	Project ID obtained from Identity and Access Management (IAM). Generally, a project ID contains 32 characters.

Table 3-17 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 (CST timestamp precise down to the millisecond).
ends_at	Long	Time when an event or alarm is cleared. The value is a CST timestamp precise down to the millisecond. If the value is **0**, the event or alarm is not deleted.
arrives_at	Long	Time when an event or alarm reaches AOM. The value is a CST timestamp precise down to the millisecond.
timeout	Long	Duration (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**.

Parameter	Type	Description
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 string elements. Options: **Critical**, **Major**, **Minor**, and **Info**. ● **event_type**: event type, which is an enumerated value with string elements. 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 configured Kafka topic so that you can retrieve the subscribed metrics or alarms.

Copyright © Huawei Technologies Co., Ltd.

4 FAQs

4.1 What Can I Do If an ICAgent Is Offline?

After an ICAgent is installed, its status is offline.

Problem Analysis

- **Cause:** The AK/SK configuration is incorrect or ports 30200, 30201, 8149, 8923, and 8102 are not connected.

- **Impact:** The ICAgent cannot work.

Solution

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

Step 2 Run the following command to check whether the AK/SK configuration is correct:

`cat /var/ICAgent/oss.icAgent.trace | grep proxyworkflow.go`

- If no command output is displayed, the AK/SK configuration is incorrect. Go to **Step 3**.

- If the command output is displayed, the AK/SK configuration is correct. Go to **Step 4**.

Step 3 After configuring the AK/SK, reinstall the ICAgent. For details, see **3.5.1.1 Installing the ICAgent**. If the installation still fails, go to **Step 4**.

Step 4 Check port connectivity.

1. Run the following command to obtain the access IP address:

   `cat /opt/oss/servicemgr/ICAgent/envs/ICProbeAgent.properties | grep ACCESS_IP`

2. Run the following command to respectively check whether ports 30200, 30201, 8149, 8923, and 8102 are connected:

   `curl -k https://ACCESS_IP:30200`

   – If **404** is displayed, the port is connected. In this case, contact technical support.

–　　If the command output is not **404**, the port is not connected. Contact the network administrator to open the port and reinstall ICAgent. If the installation still fails, contact technical support.

----End

4.2 Obtaining an AK/SK

📖 **NOTE**

Each user can create a maximum of two AK/SK pairs. Once they are generated, they are permanently valid.

- AK: unique ID associated with the SK. It is used together with the SK to sign requests.
- SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

Procedure

1. Log in to the management console, hover the mouse pointer over the username in the upper right corner, and select **My Credentials** from the drop-down list.

2. On the **My Credentials** page, click the **Access Keys** tab.

3. Click **Create Access Key**. In the dialog box that is displayed, enter the login password and verification code sent to your email or mobile phone.

4. Click **OK** and download the generated AK/SK pair.

   📖 **NOTE**

   Keep the AK/SK secure.

4.3 What Is the Relationship Between the Time Range and Statistical Cycle?

In AOM, a maximum of 1440 data points can be returned for a single metric query. The relationship between the time range and statistical cycle is as follows:

Maximum time range = Statistical cycle x 1440

If you select a time range shorter than or equal to the maximum time range, all the statistical cycles that meet the preceding formula can be selected. For example, if you want to query metrics in the last hour, the available statistical cycles are 1 minute and 5 minutes.

For a **dashboard**, the relationship between the time range and statistical cycle is shown in the following table.

Table 4-1 Relationship between the time range and statistical cycle

Time Range	Statistical Cycle
Last 1 hour	1 minute or 5 minutes
Last 6 hours	1 minute, 5 minutes, 15 minutes, or 1 hour
Last 1 day	
Last 1 week	15 minutes, 1 hour, or 1 day **NOTE** 　**1 day** is only for the metrics generated based on log statistical rules.
Last 15 days	1 hour or 1 day
Last 30 days	**NOTE** 　**1 day** is only for the metrics generated based on log statistical rules.

4.4 What Can I Do If Resources Are Not Running Properly?

Resource statuses include **Normal**, **Warning**, **Abnormal**, **Deleted**, and **Silent**. **Warning**, **Abnormal**, and **Silent** indicate improper resource running. Analyze and rectify faults according to the following instructions.

Warning

If a minor alarm or warning exists, the resource status is **Warning**.

Suggestion: Handle the alarm based on alarm details.

Abnormal

If a critical or major alarm exists, the resource status is **Abnormal**.

Suggestion: Handle the alarm based on alarm details.

Silent

If the ICAgent fails to collect resource metrics, the resource status is **Silent**. The causes include but are not limited to:

- **Cause 1: The ICAgent is abnormal.**

  Suggestion: In the navigation pane, choose **Configuration Management** > **Agent Management**. On the page that is displayed, check the ICAgent status. If the status is not **Running**, the ICAgent has been uninstalled or is abnormal. For details on how to solve the problem, see **Table 4-2**.

Table 4-2 ICAgent troubleshooting suggestions

Status	Suggestion
Uninstalled	Install the ICAgent according to **3.5.1.1 Installing the ICAgent**.
Installing	Wait for about 1 minute to complete the ICAgent installation.
Installation failed	Uninstall the ICAgent according to **Uninstalling the ICAgent Through Logging In to the Server**. Install the ICAgent again.
Upgrading	Wait for about 1 minute to complete the ICAgent upgrade.
Upgrade failed	**Log in to the server to uninstall the ICAgent**. Install the ICAgent again.
Offline	Ensure that the Access Key ID/Secret Access Key (AK/SK) or Elastic Cloud Server (ECS) agency configuration is correct.
Faulty	Contact technical support.

- **Cause 2: AOM cannot monitor the current resource.**

  Suggestion: Check whether your resources can be monitored by AOM. AOM can monitor hosts, Kubernetes containers, and user processes, but does not monitor system processes.

- **Cause 3: The local time of the host is not synchronized with the NTP server time.**

  ◯ **NOTE**

  NTP Sync Status: indicates whether the local time of the host is synchronized with the NTP server time. The value can be **0** or **1**. **0** indicates the synchronized status while **1** indicates the asynchronized status.

  Suggestion: Choose **Monitoring** > **Metric Monitoring** and check the **NTP Sync Status** metric of the host. If the value of **NTP Sync Status** is **1**, the local time of the host is not synchronized with that of the NTP server. To solve the problem, perform synchronization.

- **Cause 4: The resource is deleted or stopped.**

  Suggestions:

  – On the ECS page, check whether the host is restarted, stopped, or deleted.

  – On the Cloud Container Engine (CCE) page, check whether the component is stopped or deleted.

  – If a discovery rule is stopped or deleted, the component discovered based on the rule will also be stopped or deleted. On the AOM page, check whether the discovery rule is stopped or deleted.

4.5 How Can I Do If I Do Not Have the Permission to Access SMN?

When you log in to Application Operations Management (AOM) as an Identity and Access Management (IAM) user and create or modify a threshold rule, notification rule, or static threshold template, the message "Sorry, you do not have the permission to access Simple Message Notification (SMN)" is displayed below **Topic**, as shown in the following figure.

Problem Analysis

- **Cause**: The IAM user does not have the permission to access Simple Message Notification (SMN).

- **Impact**: Email or message notifications cannot be received.

Solution

Contact the administrator (account to which the IAM user belongs) to add the SMN access permission. To add the permission, do as follows:

Log in to IAM as the administrator, and add the SMN access permission to the IAM user.

4.6 How Do I Distinguish Alarms and Events?

Similarities Between Alarms and Events

Alarms and events refer to the information reported to Application Operation Management (AOM) when the status of AOM or an external service, such as ServiceStage, Cloud Container Engine (CCE), or Application Performance Management (APM) changes.

Differences Between Alarms and Events

- Alarms are reported when AOM or an external service, such as ServiceStage, CCE, or APM is abnormal or may cause exceptions. Alarms need to be handled. Otherwise, service exceptions may occur.

- Events generally carry some important information. They are reported when AOM or an external service, such as ServiceStage, CCE, or APM encounters some changes. Such changes do not necessarily cause service exceptions. Events do not need to be handled.

4.7 Does AOM Display Logs in Real Time?

The logs displayed on Application Operations Management (AOM) are near real-time logs, of which the latency is in seconds.

There is a time interval between log collection and processing. If the number of logs is small, the latency is about 10s. If the number of logs is large, the latency is much longer.

4.8 How Can I Check Whether a Service Is Available?

Log in to the Application Operations Management (AOM) console, choose **Container Monitoring** in the navigation pane, and check the service status value at each time point in the workload monitoring view. If the value is **0**, the service is normal. Otherwise, the service is abnormal.