AOM

FAQs

Issue 01

Date 2022-01-21

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Contents

1 User FAQs

Why Is Monitoring Data Not Displayed in Real Time on the AOM Page After Resources Are Created?

After you create resources such as hosts, applications, components, and processes, the ICAgent reports monitoring data every 10 minutes. The monitoring data is displayed on the Application Operations Management (AOM) page only after a report period ends.

Why Is the Resource Status Displayed as Normal on the AOM Page After Resources Are Deleted?

After you delete a resource such as a host or workload from a CCE cluster, the resource status is still displayed as **Normal** on the **Host Monitoring** or **Container Monitoring** page of AOM and will be automatically changed to **Deleted** 30 minutes later.

Why Is No Data Reported After the ICAgent Is Installed on a Non-HUAWEI CLOUD Host?

After the ICAgent is installed on a non-HUAWEI CLOUD host, the ICAgent needs to access the following ports to report data. If a firewall is configured on the local host, ensure that the communication in the outbound direction of the following ports is normal. Otherwise, no data can be reported and related functions are unavailable.

- Port 8149: reports metric data.
- Port 8102: reports log data.
- Port 8923: reports tracing and JVM metrics of Application Performance Management (APM).
- Port 30200: indicates the control port of the ICAgent.
- Port 30201: indicates the control port of the ICAgent.

What Can I Do If the ICAgent Fails to Be Upgraded?

In the custom cluster scenario, if the ICAgent fails to be upgraded, log in to the VM node and directly run the ICAgent installation command again.

Because the ICAgent supports overwriting installation, directly reinstall the ICAgent without uninstallation.

Can I Install the ICAgent on a New Node by Copying the Image of a Node with the ICAgent Installed?

In the non-HUAWEI CLOUD host scenario, if you install the ICAgent on a node and then copy its image to install the ICAgent on another node, you are advised to uninstall the ICAgent on the new node and then reinstall it. Otherwise, ID conflicts may occur between the two nodes. The ICAgent automatically generates a unique ID file on each node. When an image is copied to install the ICAgent on another node, the same ID file may be generated on different nodes.

What Types of Log Files Can Be Collected?

If you specify a directory, all **.log**, **.trace**, and **.out** log files in this directory are collected by default. If you specify a log file, only this file is collected. The specified file must be a text file. Other types of log files, such as binary log files, cannot be collected.

Can AOM Monitor Non-Huawei Servers?

Yes. You need to purchase a HUAWEI CLOUD Elastic Cloud Server (ECS) as a jump server to forward monitoring data, and install the ICAgent on the non-Huawei servers. For details, see **Installing the ICAgent**.

Does the ICAgent Consume Lots of Resources Such as Memory and CPU?

- AOM collects basic metrics, including CPU and memory of VMs, containers, and processes.

  Resource consumption: The resource consumption of the ICAgent is related to the number of containers and processes. In normal service traffic, the ICAgent consumes about 30 MB memory and 3% single-core CPU.

  Usage restriction: Ensure that the number of containers running on a single node is less than 1000.

  Protection mechanism:

  - The ICAgent consumes a maximum of two CPU cores.
  - When the memory consumed by the ICAgent exceeds min {4 GB, node physical memory/2}, AOM restarts the ICAgent for protection.

    NOTE

    Min {4 GB, node physical memory/2} indicates the smaller value between 4 GB and node physical memory/2.

- AOM also collects log files, including syslog, standard container output, user configuration path, and container mounting files.

  Resource consumption: The resource consumption of the ICAgent is closely related to the log volume, number of files, network bandwidth, and backend service processing capability.

How Does AOM Obtain a Custom Host IP Address on the Agent Management Page?

By default, AOM traverses all NICs on the VM and obtains the IP addresses of the Ethernet, bond, and wireless NICs based on priorities in descending order. To ensure that AOM obtains the IP address of a specific NIC, set the **IC_NET_CARD=Desired NIC name** environment variable when starting the ICAgent.

Example:

1. Add **export IC_NET_CARD=eth2** to **/etc/profile**.
2. Run the **source /etc/profile** command to make the environment variable effective in the shell.
3. Go to the **/opt/oss/servicemgr/ICAgent/bin/manual/** directory, and stop and then restart the ICAgent.

   bash mstop.sh

   bash mstart.sh
4. Check whether the environment variable is correctly transferred to the application.

   strings /proc/{icagentprocid}/envrion | grep IC_NET_CARD

NOTE

- If the IP address displayed on ICAgent is **127.0.0.1**, the ICAgent may fail to obtain the local IP address during startup. This problem may occur when a VM is powered off and then restarted. To solve the problem, you only need to restart the ICAgent.
- If the IP address of your host changes (for example, a new IP address is allocated during renewal), the original IP address may be displayed on the agent management page. To solve the problem, you only need to restart the ICAgent.

What Can I Do If the ICAgent Fails to Be Installed in the Windows Environment and the "SERVICE STOP" Message Is Displayed?

Symptom: The ICAgent fails to be installed in the Windows environment and the "SERVICE STOP" message is displayed. No ICAgent task exists in the task manager. No ICAgent service exists in the system service list. When the **sc query icagent** command is executed, a message is displayed, indicating that no ICAgent is found.

Cause: Antivirus software, such as 360 Total Security, blocks registration of the ICAgent service.

Solution:

1. Check whether antivirus software, such as 360 Total Security, is running.
2. First close the antivirus software and install the ICAgent again.

NOTE

In the Windows environment, you need to manually configure log collection paths. The ICAgent can collect **.log**, **.trace**, and **.out** files, but does not collect binary files or Windows system logs.

What Can I Do If the ICAgent Is Successfully Installed on ECS but Its Status Is Abnormal on the Agent Management Page?

The AK/SK is incorrect, or no agency is set when **Installation Mode** is set to **Create Agency**. Perform operations according to **How Do I Obtain the AK/SK by Creating an Agency?** and install the ICAgent again.

2 Consultation FAQs

2.1 What Is the Billing Policy of AOM?

See **AOM Pricing Details**.

2.2 What Are the Usage Restrictions of AOM?

OS Usage Restrictions

Application Operations Management (AOM) supports multiple operating systems (OSs). When purchasing a host, ensure that it meets the requirements in **Table 2-1**. Otherwise, the host cannot be monitored by AOM.

Table 2-1 OSs and versions supported by AOM

OS Version	Version					
SUSE	SUSE Enterprise 11 SP4 64-bit	SUSE Enterprise 12 SP1 64-bit	SUSE Enterprise 12 SP2 64-bit	SUSE Enterprise 12 SP3 64-bit		
OpenSUSE	13.2 64-bit	42.2 64-bit	15.0 64-bit (Currently, syslog logs cannot be collected.)			
EulerOS	2.2 64-bit	2.3 64-bit				
CentOS	6.3 64-bit	6.5 64-bit	6.8 64-bit	6.9 64-bit	6.10 64-bit	
	7.1 64-bit	7.2 64-bit	7.3 64-bit	7.4 64-bit	7.5 64-bit	7.6 64-bit
Ubuntu	14.04 server 64-bit	16.04 server 64-bit	18.04 server 64-bit			
Fedora	24 64-bit	25 64-bit	29 64-bit			

OS Version	Version				
Debian	7.5.0 32-bit	7.5.0 64-bit	8.2.0 64-bit	8.8.0 64-bit	9.0.0 64-bit

NOTE

- For Linux x86_64 servers, AOM supports all the OSs and versions listed in the preceding table.
- For Linux Arm servers, AOM only supports CentOS 7.4 and later versions, and other OSs and versions listed in the preceding table.

Resource Usage Restrictions

When using AOM, pay attention to the restrictions in **Table 2-2**. Resource usage restrictions include quota restrictions. For details, see **Quotas**.

Table 2-2 Resource usage restrictions

Category	Object	Usage Restriction
Dashboard	Dashboard	A maximum of 50 dashboards can be created in one region, for example, CN North-Beijing1.
	Graphs in a dashboard	A maximum of 20 graphs can be added to a dashboard.
	Number of resources, threshold rules, components, or hosts in a graph	• 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 digital graph. • A maximum of 10 threshold rules can be added to a threshold-crossing status graph. • A maximum of 10 hosts can be added to a host status graph. • A maximum of 10 components can be added to a component status graph.
Metric	Metric data	• Basic edition: Metric data can be stored in the database for a maximum of 7 days. • Professional edition: Metric data can be stored in the database for a maximum of one year.
	Metric items	After resources such as clusters, components, and hosts are deleted, their related metric items can be stored in the database for a maximum of 7 days.

Category	Object	Usage Restriction
	Dimensions	A maximum of 20 dimensions can be configured for a metric.
	Metric query API	A maximum of 20 metrics can be queried at a time.
	Statistical cycle	The maximum statistical cycle is 1 hour.
	Data points returned for a single query	A maximum of 1440 data points can be returned each time.
	Custom metrics	No restrictions.
	Custom metrics to be reported	A maximum of 40 KB data can be reported each time.
	Application metrics Job metrics	• When the number of containers on a host exceeds 1000, the ICAgent stops collecting application metrics and sends the **ALM-34105 ICAgent Stopped Collecting Application Metrics** alarm. • When the number of containers on a host is less than 1000, the ICAgent resumes the collection of application metrics and the **ALM-34105 ICAgent Stopped Collecting Application Metrics** alarm is cleared. A job automatically exits after it is completed. To monitor metrics of a job, ensure that the survival time is greater than 90s so that the ICAgent can collect its metric data.
	Resources consumed by the ICAgent	When the ICAgent collects basic metrics, the resources consumed by the ICAgent are greatly affected by the number of containers and processes. On a VM without any services, the ICAgent consumes 30 MB memory and 1% CPU usage. To ensure collection reliability, ensure that the number of containers running on a single node must be less than 1000.
Threshold rules (for all regions except CN North-Beijing1 and CN East-Shanghai2)	Threshold rules	A maximum of 1000 threshold rules can be created in a project.
	Number of topics that can be selected	A maximum of five topics can be selected for each threshold rule.

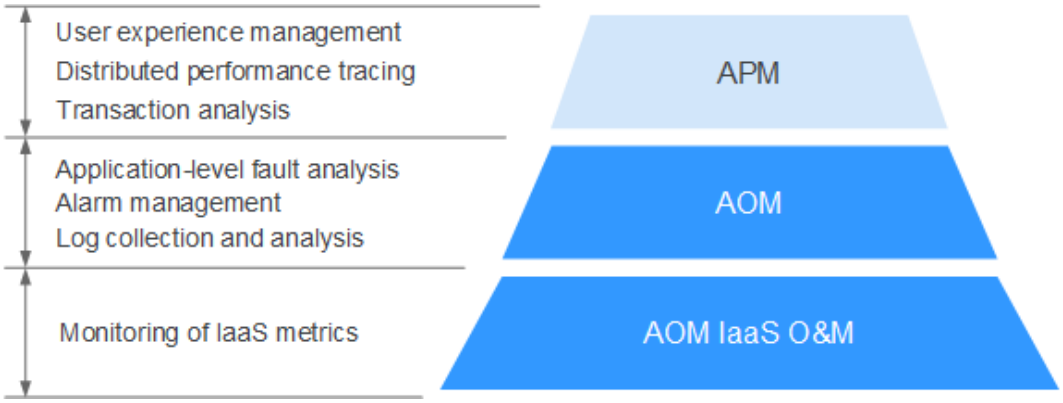
Category	Object	Usage Restriction
Threshold rules (for CN North-Beijing1 and CN East-Shanghai2)	Threshold rules	• A maximum of 1000 static threshold rules can be created. • A maximum of 10 intelligent threshold rules can be created.
	Threshold templates	• A maximum of 50 static templates can be created. • A maximum of 10 intelligent templates can be created.
	Number of topics that can be selected	A maximum of five topics can be selected for each threshold rule.
Notification rules	Number of topics that can be selected	A maximum of five topics can be selected for each notification rule.
Logs	Size of a log	The maximum size of each log is 10 KB. If a log exceeds 10 KB, the ICAgent does not collect it. In that case, the log will be discarded.
	Log traffic	A maximum of 10 MB/s is supported for each tenant in a region. If the log traffic exceeds 10 MB/s, logs may be lost. If you require more log traffic, submit a service ticket according to **Submitting a Service Ticket**.
	Historical logs	The storage duration and prices of log data vary according to editions. For details, see **AOM Pricing Details**.
	Log files	Only text log files can be collected. Other types of log files, such as binary files, cannot be collected.
		The ICAgent can collect a maximum of 20 log files from a volume mounting directory.
		The ICAgent can collect a maximum of 1000 standard container output log files. These files must be in JSON format.
	Resources consumed during log file collection	The resources consumed during log file collection are closely related to the log volume, number of files, network bandwidth, and backend service processing capability.

Category	Object	Usage Restriction
	Log loss	ICAgent uses multiple mechanisms to ensure log collection reliability and prevent data loss. However, logs may be lost in the following scenarios: • The log rotation policy of Cloud Container Engine (CCE) is not used. • Log files are rotated at a high speed, for example, once per second. • Logs cannot be forwarded due to improper system security settings or syslog reasons. • The container running time, for example, shorter than 30s, is extremely short. • A single node generates logs at a high speed, exceeding the allowed transmit bandwidth or log collection speed. It is recommended that the log generation speed of a single node be lower than 5 MB/s.
	Log discarding	When a single log line exceeds 10,240 bytes, the line will be discarded.
	Log repetition	When the ICAgent is restarted, identical data may be collected around the restart time.
Alarm center	Alarms	You can query the alarms generated in the last 30 days.
	Events	You can query the events generated in the last 30 days.

2.3 What Are the Differences Between AOM and APM?

Application Operations Management (AOM) and Application Performance Management (APM) belong to the multi-dimensional O&M solution and share the ICAgent collector. AOM provides application-level fault analysis, alarm management, and log collection and analysis capabilities, which effectively prevent problems and help O&M personnel quickly locate faults, reducing O&M costs. **APM** provides user experience management, distributed performance tracing, and transaction analysis capabilities, which help O&M personnel quickly locate and resolve faults and performance bottlenecks in a distributed architecture, optimizing user experience. AOM provides basic O&M capabilities. APM is a supplement to AOM. The AOM console integrates with APM. You can perform unified O&M on the AOM console. APM also has its own console.

Figure 2-1 Multi-dimensional O&M solution



2.4 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 Application Orchestration Service (AOS), 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 AOS, 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 AOS, ServiceStage, CCE, or APM encounters some changes. Such changes do not necessarily cause service exceptions. Events do not need to be handled.

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

For Application Operations Management (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 query metrics in the last 1 hour, the available statistical cycles are 1 minute and 5 minutes.

Table 2-3 shows the relationship between the time range and statistical cycle.

Table 2-3 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, or 1 hour
Last 1 day	
Last 7 days	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 **NOTE** **1 day** is only for the metrics generated based on log statistical rules.
Last 30 days	
Last 3 months	
Last 6 months	
Last 9 months	
Last 12 months	

2.6 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.

2.7 Will Container Logs Be Deleted After They Are Dumped?

No.

2.8 How Can I Do If I Cannot Receive Any Email Notification After Configuring a Threshold Rule?

The notification configuration may be incorrect. You can check whether the alarm notification function is enabled, and whether a topic and an Application Performance Management (APM) policy are selected.

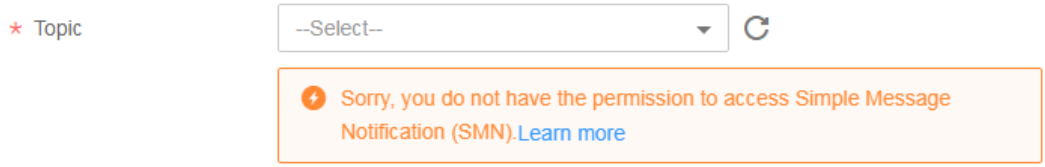
2.9 Why Are Connection Channels Required?

Different Virtual Private Clouds (VPCs) cannot communicate with each other. To solve this problem, create an application in the VPC where the data subscription application resides and set it to a VPC endpoint service. Then, create a VPC endpoint in the VPC where Distributed Message Service (DMS) resides. A connection channel can be established between the VPC endpoint and VPC endpoint service for communication.

3 Usage FAQs

3.1 What Can I Do If I Do Not Have the Permission to Access SMN?

When you log in to Application Operations Management (AOM) and create or modify a threshold rule, notification rule, intelligent threshold template, or static threshold template as an Identity and Access Management (IAM) user, 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**: You log in to AOM as an IAM user, but this user does not have the permission to access Simple Message Notification (SMN).
- **Impact**: You cannot receive notifications by email and Short Message Service (SMS) message.

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. For details, see **Adding Users to a User Group**.

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

The resource status includes **Normal**, **Warning**, **Alarm**, and **Silent**. **Warning**, **Alarm**, or **Silent** may result in resource exceptions. You can analyze and rectify exceptions based on the following suggestions.

Warning

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

Suggestion: Handle problems based on alarm details.

Alarm

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

Suggestion: Handle problems 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.**

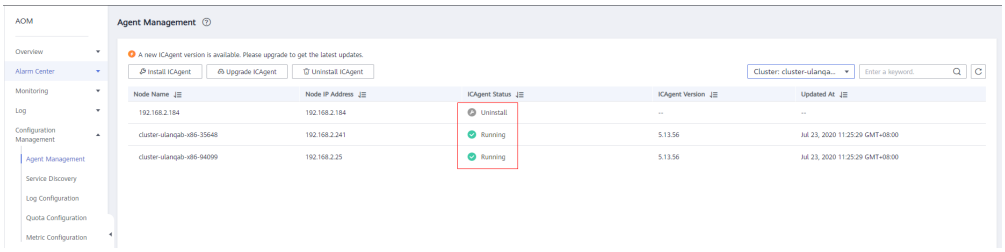
  Suggestion: In the navigation pane, choose **Configuration Management** > **Agent Management**. On the page that is displayed, check the ICAgent status, as shown in **Figure 3-1**. If the status is not **Running**, the ICAgent is uninstalled or abnormal. For details about how to solve the problem, see **Table 3-1**.

  Table 3-1 ICAgent troubleshooting suggestions

Status	Suggestion
Uninstalled	Install the ICAgent according to **Installing the ICAgent (Linux)**.
Installing	Wait for 1 minute to install the ICAgent.
Installation failed	Uninstall the ICAgent according to **Uninstalling the ICAgent Through Logging In to the Server** and then install it again.
Updating	Wait for 1 minute to upgrade the ICAgent.
Upgrade failed	Uninstall the ICAgent according to **Uninstalling the ICAgent Through Logging In to the Server** and then install it again.

Status	Suggestion
Offline	Ensure that the Access Key ID/Secret Access Key (AK/SK) and Elastic Cloud Server (ECS) agency configurations are correct.
Faulty	Submit a service ticket according to **Submitting a Service Ticket**.

Figure 3-1 Checking the ICAgent status



- **Cause 2: Application Operations Management (AOM) cannot monitor the current resource.**

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

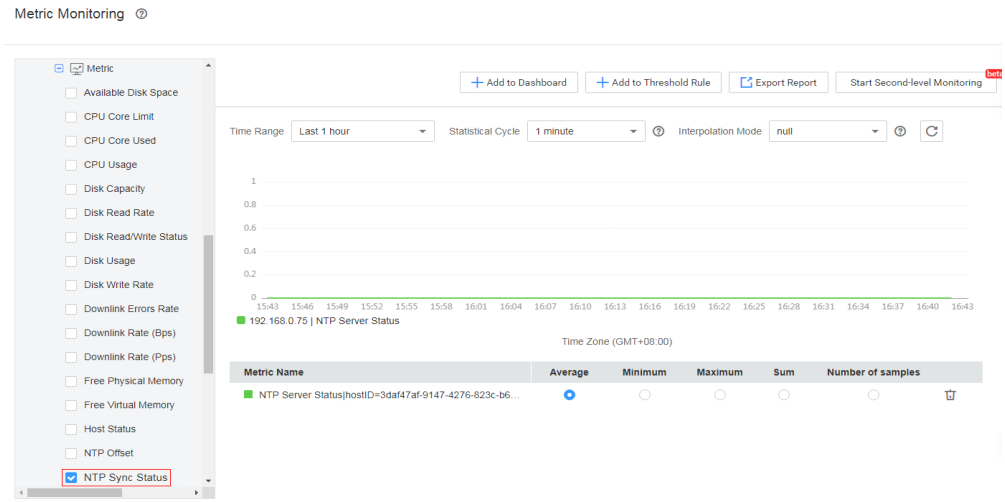
- **Cause 3: The local time of the host is not synchronized with the NTP server time.**

  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: In the navigation pane, choose **Monitoring** > **Metric Monitoring**, and check the **NTP Sync Status** metric of the host, as shown in **Figure 3-2**. If the value of **NTP Sync Status** is **1**, implement synchronization according to **Does HUAWEI CLOUD Provide the NTP Server and How Can I Install It?**

Figure 3-2 Checking the **NTP Sync Status** metric of the host

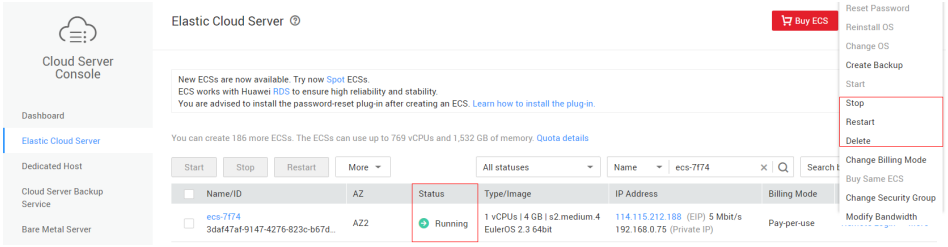


- **Cause 4: The resource is deleted or stopped.**

  Suggestion:

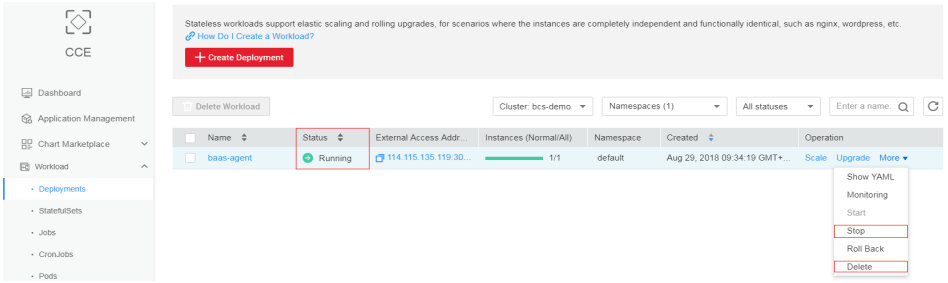
  – On the ECS page, check whether the host is restarted, stopped, or deleted, as shown in **Figure 3-3**.

  Figure 3-3 Checking whether the host is restarted, stopped, or deleted

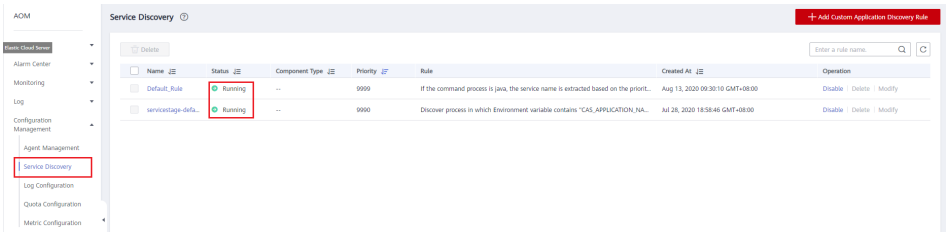
  – On the Cloud Container Engine (CCE) page, check whether the service is stopped or deleted, as shown in **Figure 3-4**.

  Figure 3-4 Checking whether the service is stopped or deleted

  – If an application discovery rule is disabled or deleted, the application discovered based on the rule will also be disabled or deleted. On the AOM page, check whether the application discovery rule is disabled or deleted, as shown in **Figure 3-5**.

  Figure 3-5 Checking whether the application discovery rule is disabled or deleted

3.3 How Do I Set the Full-Screen Online Duration?

Application Operations Management (AOM) provides an automatic logout mechanism to secure customer information. Specifically, after you access a page on the cloud but do not perform any operations within 1 hour, the system automatically logs you out.

If you set a full-screen view on the **O&M** or **Dashboard** page in the AOM console and later the system logs you out, the full-screen view will also exit. In this case,

real-time monitoring cannot be performed. AOM allows you to customize full-screen online duration, meeting various requirements.

Precautions

- For security purposes, exit the full-screen view when it is not required.
- The full-screen online duration is irrelevant to operations. If the preset duration times out, the login page is automatically displayed.
- The full-screen online duration is subject to the last setting.

  For example, if full-screen monitoring is implemented on multiple screens, the online duration is subject to the last setting.

  For another example, if the online duration is set on both the **O&M** and **Dashboard** pages, the last setting prevails.
- The full-screen online duration takes precedence over the automatic logout mechanism of the cloud.

  For example, if you log in to the cloud, set the full-screen online duration to 2 hours on AOM pages, and then open other service pages, your setting on the AOM pages also takes effect on other service pages. That is, the login page will be automatically displayed 2 hours later.
- If you leave all full-screen views, the default automatic logout mechanism is used.

  For example, if you log in to the cloud, set the full-screen online duration to 2 hours on AOM pages, open other service pages, and then leave all full-screen views of AOM, the default logout mechanism will be used. That is, if you do not perform any operations within 1 hour, the login page will be automatically displayed.

Setting the Full-Screen Online Duration on the O&M Page

Step 1 Log in to the AOM console. In the navigation pane, choose **Overview** > **O&M**.

Step 2 Click  in the upper right corner of the **O&M** page. In the dialog box that is displayed, set the full-screen online duration.

- **Custom**: The default online duration is 1 hour. You can enter 1–24 (unit: hour) in the text box.

  For example, if you enter **2** in the text box, the login page is automatically displayed 2 hours later.
- **Always online**: The full-screen online duration is not restricted. That is, you can always implement full-screen monitoring and the login page will never be displayed.

Step 3 Click **OK** to enter the full-screen mode.

----End

Setting the Full-Screen Online Duration on the Dashboard Page

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

Step 2 Click  in the upper right corner of the **Dashboard** page. In the dialog box that is displayed, set the full-screen online duration.

- **Custom**: The default online duration is 1 hour. You can enter 1–24 (unit: hour) in the text box.

  For example, if you enter **2** in the text box, the login page is automatically displayed 2 hours later.
- **Always online**: The full-screen online duration is not restricted. That is, you can always implement full-screen monitoring and the login page will never be displayed.

Step 3 Click **OK** to enter the full-screen view.

----End

3.4 What Can I Do If the Log Usage Reaches 90% or Is Full?

When the basic edition is used, a message is displayed on the **Log Files** or **Log Search** page of Application Operations Management (AOM), indicating that the log usage reaches 90% or is full.

Problem Analysis

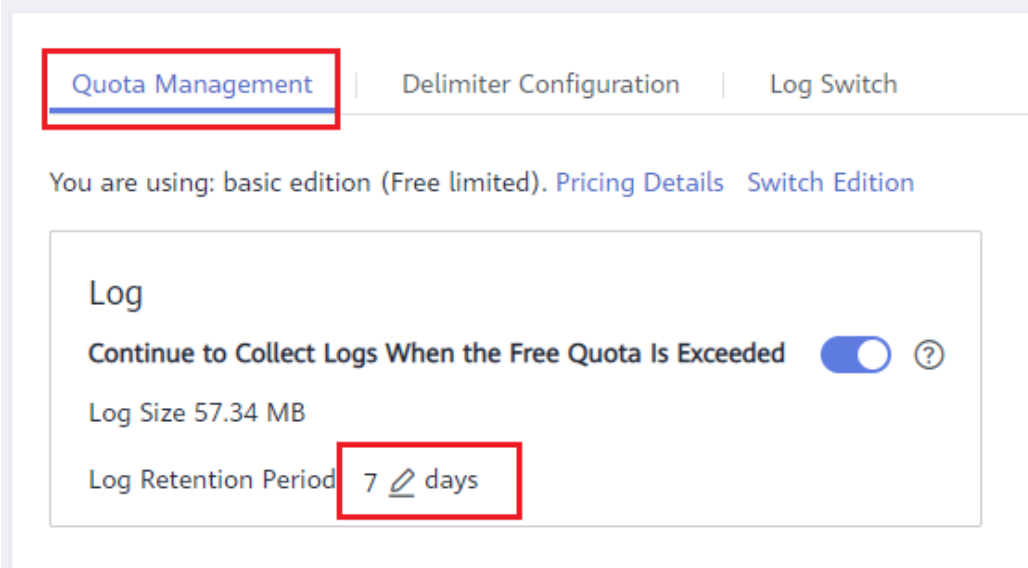
- **Cause**: For a basic edition, a maximum of 500 MB logs can be stored. When the log storage space is about to reach 500 MB or has reached 500 MB, the preceding message is displayed.
- **Impact**: When the log storage space exceeds 500 MB, the ICAgent cannot collect newly printed logs. In addition, you cannot query or analyze newly printed logs on the **Log Files** or **Log Search** page.
- **Solution**: Switch to the pay-per-use edition. Note that the basic edition is free but the pay-per-use edition is not. For details, see **AOM Pricing Details**.

Solution

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

On the **Quota Management** tab page, view the current log quota, as shown in the following figure.

Figure 3-6 Viewing the log quota



Step 2 Change the log retention period.

----End

3.5 How Do I Obtain an AK/SK?

Access Key ID/Secret Access Key (AK/SK) indicate a key pair.

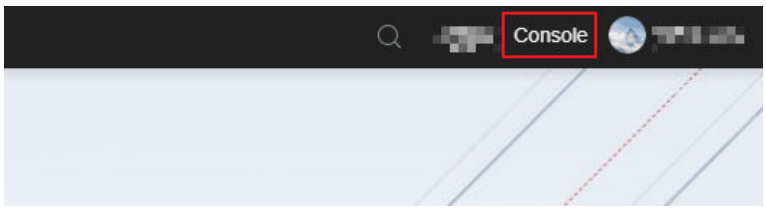
- AK: access key ID, which is a unique identifier associated with a secret access key and is used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents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

NOTE

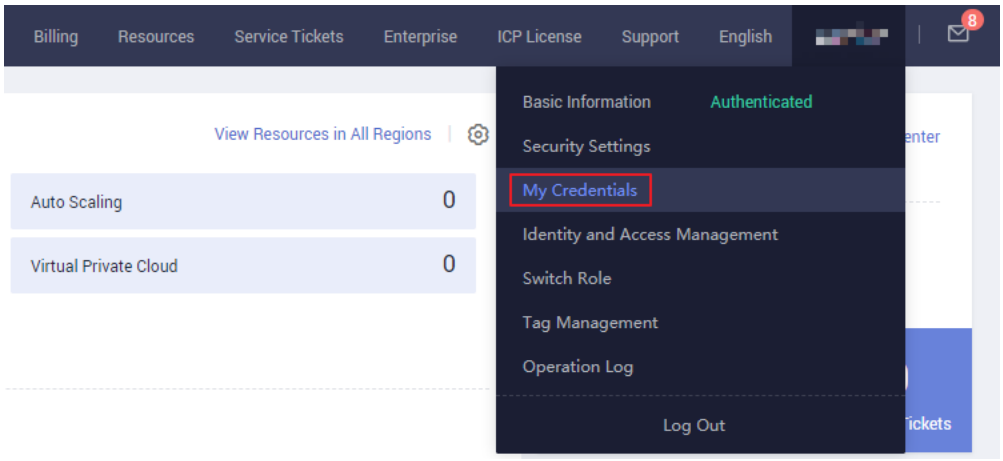
Each user can create a maximum of two AK/SK pairs. Once they are generated, they are permanently valid. For details, see **Creating an Access Key**.

Creating an Access Key

Step 1 Log in to HUAWEI CLOUD and click **Console** in the upper right corner.

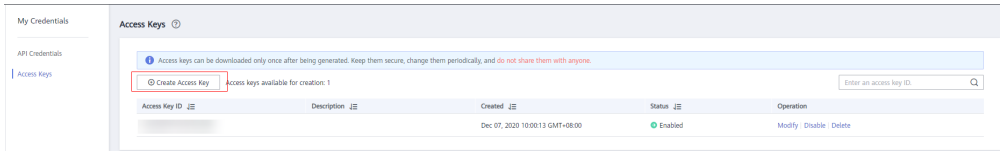


Step 2 On the management console, hover over the username in the upper right corner and choose **My Credentials** from the drop-down list.



Step 3 Choose **Access Keys** from the navigation pane.

Step 4 Click **Create Access Key**, and enter the verification code or password.



NOTE

- You can create a maximum of **two** access keys. The quota cannot be increased. If you already have two access keys, you can only delete an access key and create a new one.
- To change an access key, delete it and create a new one.

Step 5 Click **OK** to generate an access key and download it.

After the access key is created, view the AK in the access key list and view the SK in the downloaded CSV file.

NOTE

- Download the access key file and keep it properly. If the download page is closed, you will not be able to download the access key. However, you can create a new one.
- Open the CSV file in the lower left corner, or choose **Downloads** in the upper right corner of the browser and open the CSV file.
- Keep your access keys secure and change them periodically for security purposes. To change an access key, delete it and create a new one.

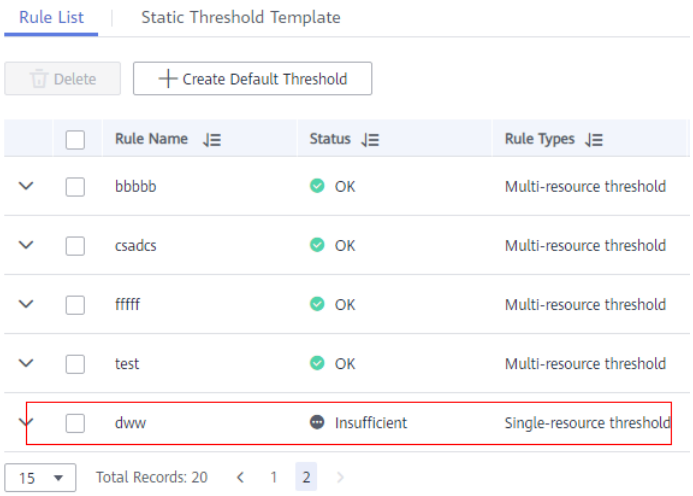
----End

3.6 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.

3.7 Why Is the Status of a Threshold Rule Displayed as "Insufficient"?

When you create a threshold rule for a resource, its data reported to AOM may be insufficient, as shown in the following figure.



Possible causes:

1. The data reporting latency is too large. That is, the difference between the latest data reporting time of the line graph and the current time is greater than one threshold reporting period, which can be set to 1 or 5 minutes. If no data is obtained within such a period, a message indicating insufficient data is displayed.
2. If a metric is deleted or the host to which the metric belongs does not exist, but the threshold rule still exists, a message indicating insufficient data is displayed.

3.8 Why the Status of a Workload that Runs Normally Is Abnormal on the AOM Page?

1. A workload runs normally on Cloud Container Engine (CCE), but its status is **Abnormal** on the Application Operations Management (AOM) page.

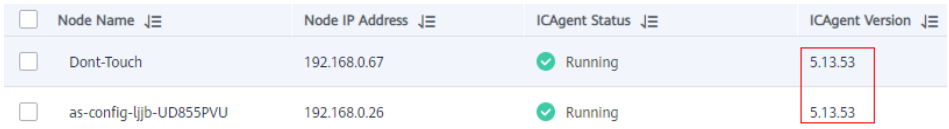
Workload	Status	Cluster	Namespace
coredns	Abnormal	cluster-factory	kube-system
storage-driver	Abnormal	cluster-factory	kube-system

Possible causes:

a. The ICAgent version is too early.

Currently, the ICAgent needs to be upgraded by users. However, if the ICAgent version is too early, the workload status may fail to be reported in time.

If the displayed workload status is incorrect, first check whether the ICAgent is in the latest version on the **Agent Management** page.



b. The node time is not synchronized with the actual time.

If the difference between the node time and the actual time is too large, the ICAgent fails to report metrics in time.

If the displayed workload status is incorrect, check whether the node time is different from the actual time or check the NTP offset on the AOM page.

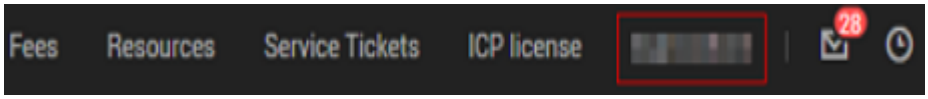
3.9 How Do I Create the apm_admin_trust Agency?

Procedure

Step 1 Log in to the **management console**.

Step 2 Click the username in the upper right corner to access the account center, as shown in **Figure 3-7**.

Figure 3-7 Username



Step 3 Click **Identity and Access Management** to go to the IAM page.

Step 4 In the navigation pane, choose **Agencies**.

Step 5 On the page that is displayed, click **Create Agency** in the upper right corner. The **Create Agency** page is displayed.

Step 6 Set parameters based on **Table 3-2**.

Table 3-2 Parameters for creating an agency

Parameter	Description	Example
Agency Name	Set an agency name. **NOTE** The agency name must be **apm_admin_trust**.	**apm_admin_trust**
Agency Type	Select **Account**.	Common account
Delegated Account	Specify a HUAWEI CLOUD account to delegate.	-

Parameter	Description	Example
Validity Period	Select **Unlimited**.	**Unlimited**
Description	(Optional) Provide details about the agency.	-

Step 7 On the **Permissions** area, click **Assign Permissions**.

Step 8 Configure the following permissions: **DMS User** (or **DMS UserAccess**), **CCE Administrator**, **CCI Administrator**, and **ECS User** (or **ECS CommonOperations**), and select a region in **Project [Region]**.

Step 9 Click **OK**.

----End

3.10 How Do I Obtain the AK/SK by Creating an Agency?

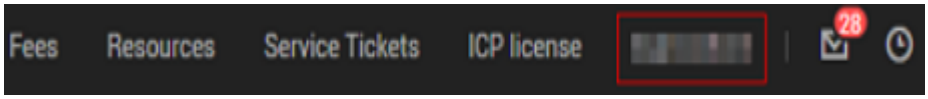
After you create an agency, the ICAgent automatically obtains the Access Key ID/Secret Access Key (AK/SK), helping you manage application performance.

Creating an Agency

Step 1 Log in to the **management console**.

Step 2 Click the username in the upper right corner to access the account center, as shown in **Figure 3-8**.

Figure 3-8 Username



Step 3 On the **Identity and Access Management** page, choose **Agencies**. The **Agencies** page is displayed.

Step 4 Click **Create Agency** in the upper right corner. The **Create Agency** page is displayed.

Step 5 Set parameters based on **Table 3-3**.

Table 3-3 Creating an agency

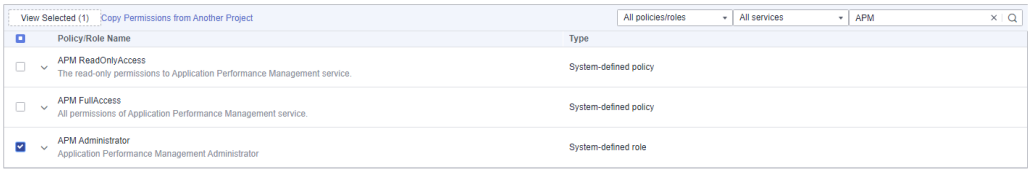
Parameter	Description	Example
Agency Name	Set an agency name.	aom_ecm_trust

Parameter	Description	Example
Agency Type	Select **Cloud service**.	-
Cloud Service	Select **Elastic Cloud Server (ECS) and Bare Metal Server (BMS)** from the drop-down list.	-
Validity Period	Select **Unlimited**.	-
Description	(Optional) Provide detailed information about the agency.	-

Step 6 Click **Next** to authorize the agency.

Step 7 Set **Scope** to **Region-specific projects** and select required projects.

In the **Permissions** area, enter **APM** in the search box and select **APM Administrator** from the search result.



Step 8 Click **OK**.

----End

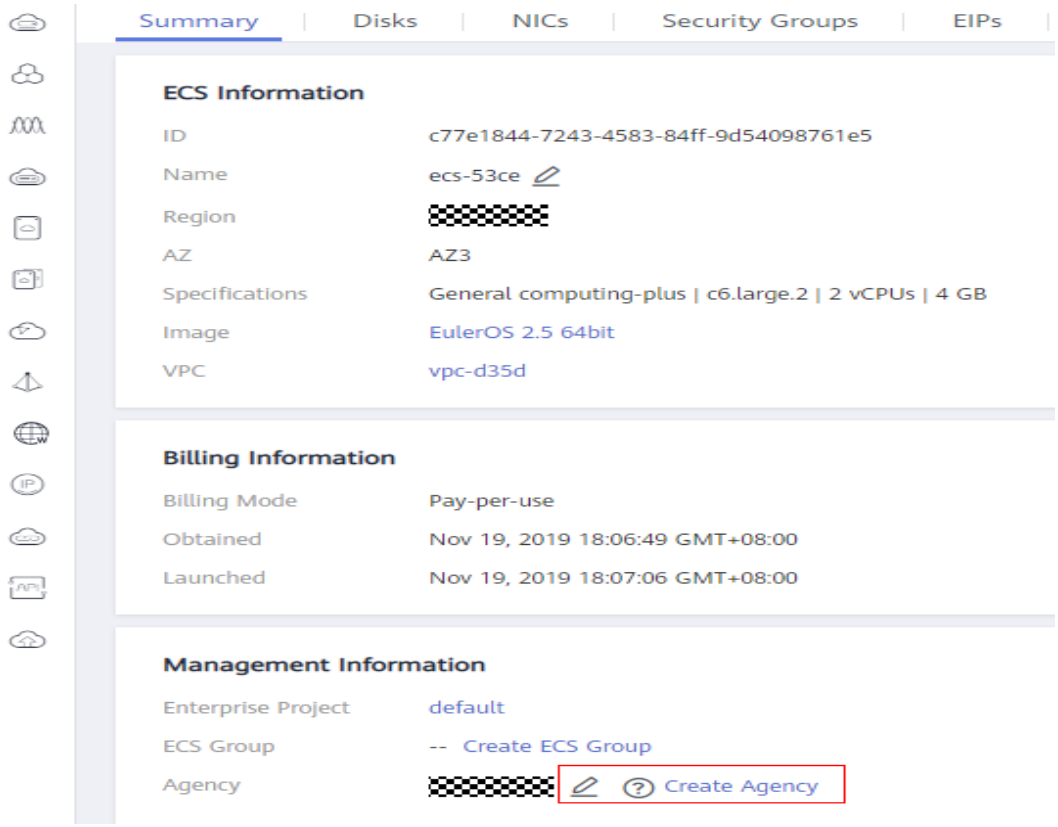
Making an Agency Effective

Step 1 Choose **Service List** > **Computing** > **Elastic Cloud Server**.

Step 2 Click the ECS where the ICAgent is installed. The ECS details page is displayed.

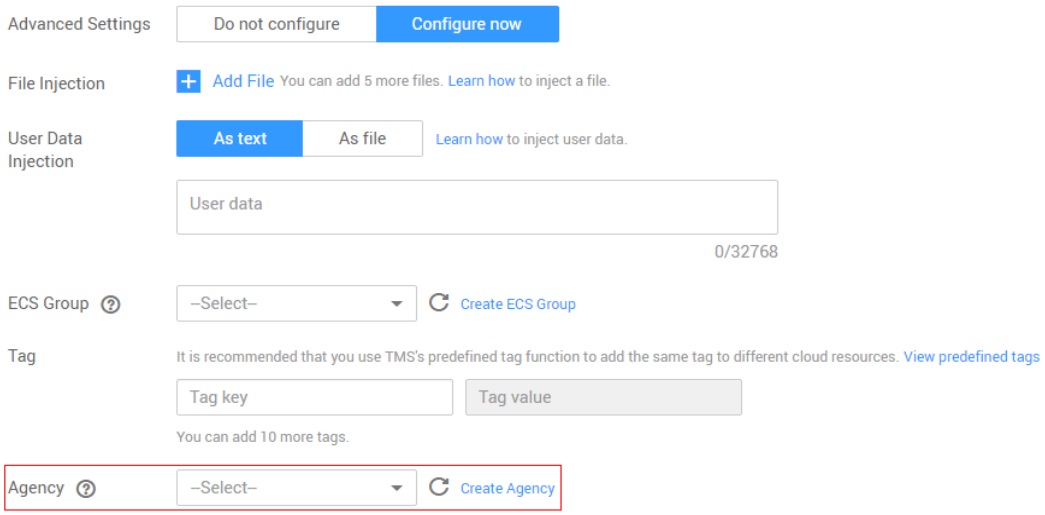
Step 3 Select the created agency from the **Agency** drop-down list, as shown in **Figure 3-9**.

Figure 3-9 Setting an agency



Step 4 (Optional) To set an agency for a newly purchased ECS, do as follows: On the **Buy ECS** page, set the value of **Advanced Settings** to **Configure now** and select the created agency from the **Agency** drop-down list, as shown in **Figure 3-10**. Set other parameters and click **Submit**.

Figure 3-10 Setting an agency



----End

3.11 What Is the Billing Policy of Logs?

When using AOM for the first time, you are provided with the basic edition by default. You can enjoy a free tier, for example, 500 MB log read and write traffic. If the resource quota included in the package is used up, you will be billed on a pay-per-use basis.

AOM uses some log functions of **Log Tank Service (LTS)**, but will not charge you for using these functions. Instead, LTS reports service detail records (SDRs) and charges you for them. To stop log billing, see:

How Can I Stop Log Collection When My Free Quota Is Used Up to Avoid Extra Expenses?

For more information, see **AOM Pricing Details**.

3.12 Why Can't I See Any Logs on the Console?

Symptom

No logs are displayed on the AOM console.

Possible Causes

- ICAgent has not been installed.
- The collection path is incorrectly configured.
- You set the log collection to be stopped when the free quota is used up on the Application Operations Management (AOM) console.
- You set the log collection to be stopped when the free quota is used up on the LTS console.
- Log collection was stopped because your account is in arrears.
- The rate of writing logs into log streams or length of single-line logs exceeds what is supported.
- The browser has slowed down because of the amount of log data.

Solution

- Install ICAgent. For details, see **Installing ICAgent**.
- If the collection path is set to a directory, for example, **/var/logs/**, only .log, .trace, and .out files in the directory are collected. If the collection path is set to name of a file, ensure that the file is a text file. For details about log collection paths, see **Configuring Log Collection Rules**.
- Log in to the AOM console and choose **Configuration Management** > **Log Configuration**. On the **Quota Management** tab, enable **Continue to Collect Logs When the Free Quota Is Exceeded**.
- Log usage, including log read/write, log indexing, and log retention, is billed in LTS. If you have disabled **Continue to Collect Logs When the Free Quota Is Exceeded** on the LTS console, log collection will be stopped when the free quota is used up. Logs will not be able to be read, written, or indexed. No fees

will be incurred for log read/write and indexing. To resume log collection, enable **Continue to Collect Logs When the Free Quota Is Exceeded** on the LTS console. For details, see **Configuration Center**.

- Top up your account if your account is in arrears. For details, see **Repaying Outstanding Amount**.
- For details about log usage restrictions, see **Usage Restrictions**.
- Use Google Chrome or Mozilla Firefox to query logs.
- If the issue persists after you have tried the methods above, **submit a service ticket**.

