

Application Operations Management

Best Practices

Issue 01
Date 2025-01-08



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 User FAQs.....	1
2 Consultation FAQs.....	4
2.1 What Are the Usage Restrictions of AOM?.....	4
2.2 What Are the Differences Between AOM and APM?.....	8
2.3 How Do I Distinguish Alarms from Events?.....	8
2.4 What Is the Relationship Between the Time Range and Statistical Cycle?.....	9
2.5 Does AOM Display Logs in Real Time?.....	10
2.6 How Can I Do If I Cannot Receive Any Email Notification After Configuring a Threshold Rule?.....	10
2.7 Why Are Connection Channels Required?.....	10
3 Usage FAQs.....	11
3.1 What Can I Do If I Do Not Have the Permission to Access SMN?.....	11
3.2 What Can I Do If Resources Are Not Running Properly?.....	11
3.3 How Do I Set the Full-Screen Online Duration?.....	13
3.4 What Can I Do If the Log Usage Reaches 90% or Is Full?.....	14
3.5 How Do I Obtain an AK/SK?.....	15
3.6 How Can I Check Whether a Service Is Available?.....	16
3.7 Why Is the Status of an Alarm Rule Displayed as "Insufficient"?.....	16
3.8 Why the Status of a Workload that Runs Normally Is Displayed as "Abnormal" on the AOM Page?...	17
3.9 How Do I Create the apm_admin_trust Agency?.....	17
3.10 What Is the Billing Policy of Logs?.....	18
3.11 Why Can't I See Any Logs on the Console?.....	18
3.12 What Can I Do If an ICAgent Is Offline?.....	19
3.13 Why Can't the Host Be Monitored After ICAgent Is Installed?.....	20
3.14 Why Is "no crontab for root" Displayed During ICAgent Installation?.....	21
3.15 Why Can't I Select an OBS Bucket When Configuring Log Dumping on AOM?.....	22
3.16 Why Can't Grafana Display Content?.....	22

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 their monitoring data every 10 minutes. Only when a report period ends, can monitoring data be displayed on the AOM page.

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 Cloud Container Engine (CCE) cluster, the resource status is still **Normal** on the **Host Monitoring** or **Container Monitoring** page of AOM. This is normal. The status of the deleted resource will be changed to **Deleted** 30 minutes later.

Why Is Data Not 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 Cloud Servers?

Yes. Purchase a Huawei Cloud Elastic Cloud Server (ECS) as a jump server to forward monitoring data, and install the ICAgent on the non-Huawei Cloud 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 $\min\{4\text{ GB, node physical memory}/2\}$, AOM restarts the ICAgent for protection.

NOTE

$\min\{4\text{ GB, node physical memory}/2\}$ indicates the smaller value between 4 GB and $\text{node physical memory}/2$.

- 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 properly 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, manually add log collection paths. The ICAgent can collect **.log**, **.trace**, and **.out** files, but does not collect binary files or Windows system logs.

2 Consultation FAQs

2.1 What Are the Usage Restrictions of AOM?

OS Usage Restrictions

AOM supports multiple operating systems (OSs). When purchasing a host, ensure that its OS 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					
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	2.5 64-bit	2.9 64-bit	2.10 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			
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	
Kylin	Kylin V10 SP1 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, learn about the restrictions in [Table 2-2](#).

Table 2-2 Resource usage restrictions

Category	Object	Usage Restrictions
Dashboard	Dashboard	A maximum of 50 dashboards can be created in a region.
	Graph 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	<ul style="list-style-type: none"> • A maximum of 100 resources across clusters can be added to a line graph. • A maximum of 12 resources can be added to a digit graph. Only one resource can be displayed. By default, the first resource is displayed. • A maximum of 10 threshold rules can be added to a threshold 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	<ul style="list-style-type: none"> • 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 30 days.
	Total number of metrics	Up to 400,000 for a single account. Up to 100,000 for a small specification.
	Metric item	After resources such as clusters, components, and hosts are deleted, their related metrics can be stored in the database for a maximum of 30 days.
	Dimension	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.

Category	Object	Usage Restrictions
	Statistical period	The maximum statistical period is 1 hour.
	Data points returned for a single query	A maximum of 1440 data points can be returned each time.
	Custom metric	Unlimited.
	Custom metric to be reported	A single request cannot exceed 40 KB. The timestamp of a reported metric cannot 10 minutes later than the standard UTC time. In addition, out-of-order metrics are not received. That is, if a metric is reported at a certain time point, the metrics of earlier time points cannot be reported.
	Application metric	<ul style="list-style-type: none"> When the number of containers on a host exceeds 1000, the ICAgent stops collecting application metrics and sends the ICAgent Stopped Collecting Application Metrics alarm (ID: 34105). When the number of containers on a host is less than 1000, the ICAgent resumes the collection of application metrics and the ICAgent Stopped Collecting Application Metrics alarm is cleared.
	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 records 1% CPU usage. To ensure collection reliability, ensure that the number of containers running on a single node must be less than 1000.
Threshold rule	Threshold rule	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.
Alarm rule	Alarm rule	A maximum of 1000 alarm rules (including threshold rules and event alarm rules) can be created.
	Static threshold template	A maximum of 50 static threshold templates can be created.

Category	Object	Usage Restrictions
Notification rule	Number of topics that can be selected	A maximum of five topics can be selected for each notification rule.
Log	Size of a log	The maximum size of each log is 10 KB. If a log is greater than that, the ICAgent will 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.
	Log file	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.
	Log loss	ICAgent uses multiple mechanisms to ensure log collection reliability and prevent data loss. However, logs may be lost in the following scenarios: <ul style="list-style-type: none"> • 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 itself. • 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. Ensure that the log generation speed of a single node is lower than 5 MB/s.
Log loss	When a single log line exceeds 1024 bytes, this line will be discarded.	
Log repetition	When the ICAgent is restarted, identical data may be collected around the restart time.	

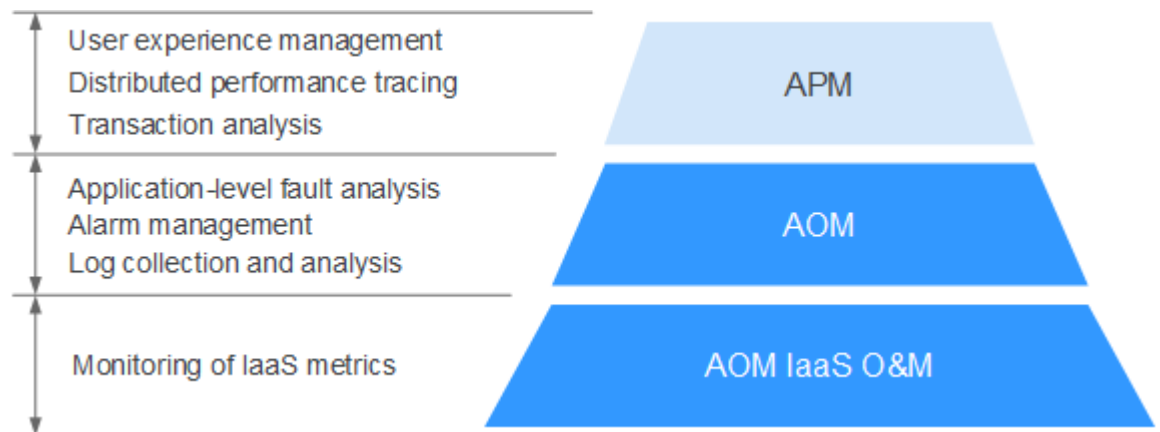
Category	Object	Usage Restrictions
Alarm	Alarm	You can query the alarms generated in the last 31 days.
	Event	You can query the events generated in the last 31 days.
-	Application discovery rule	You can create a maximum of 100 application discovery rules.

2.2 What Are the Differences Between AOM and APM?

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. AOM integrates with some APM functions for unified O&M. You can also use these functions on the APM console.

Figure 2-1 Multi-dimensional O&M solution



2.3 How Do I Distinguish Alarms from Events?

Similarities Between Alarms and Events

Both alarms and events are the information reported to AOM when the status of AOM or an external service (such as ServiceStage or CCE) changes.

Differences Between Alarms and Events

- Alarms are reported when AOM or an external service (such as ServiceStage or CCE) is abnormal or may cause exceptions. Alarms must 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 or CCE) has some changes. Such changes do not necessarily cause service exceptions. Events do not need to be handled.

2.4 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	

2.5 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.

2.6 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.

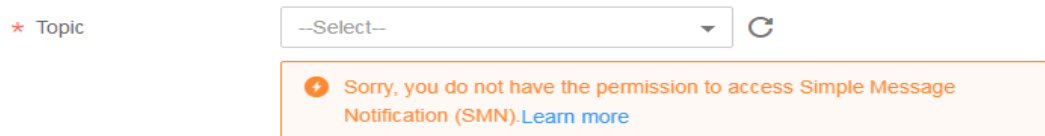
2.7 Why Are Connection Channels Required?

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 AOM and create or modify a threshold rule, notification rule, or static threshold template as an 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 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 or Removing Users from 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. If the status is not **Running**, the ICAgent is not installed or abnormal. For details about how to solve the problem, see [Table 3-1](#).

Table 3-1 ICAgent troubleshooting suggestions

Status	Suggestion
Uninstalled	Install an ICAgent .
Installing	Wait for 1 minute to install the ICAgent.
Installation failed	Uninstall the ICAgent by logging in to the server and then install it again.
Upgrading	Wait for 1 minute to upgrade the ICAgent.
Upgrade failed	Uninstall the ICAgent by logging in to the server and then install it again.
Offline	The AK/SK is incorrect or port 30200 or 30201 is disconnected. Solve the issue according to What Can I Do If an ICAgent Is Offline .
Faulty	The ICAgent is abnormal. Contact technical support.

- **Cause 2: 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 resource is deleted or stopped.**

Suggestion:

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

- On the CCE page, check 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. Check whether the application discovery rule is disabled or deleted on AOM.

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

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


If you set a full-screen view 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 console, set the full-screen online duration to 2 hours on AOM pages, and then open other pages, your setting on the AOM pages also takes effect on other pages. That is, the login page will be automatically displayed 2 hours later.
- If you leave all full-screen views, the default automatic logout mechanism is used.
For example, if you log in to the console, set the full-screen online duration to 2 hours on AOM pages, open other pages, and then leave all full-screen views of AOM, the default logout mechanism will be used. That is, if you do not perform any operations within 1 hour, the login page will be automatically displayed.

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

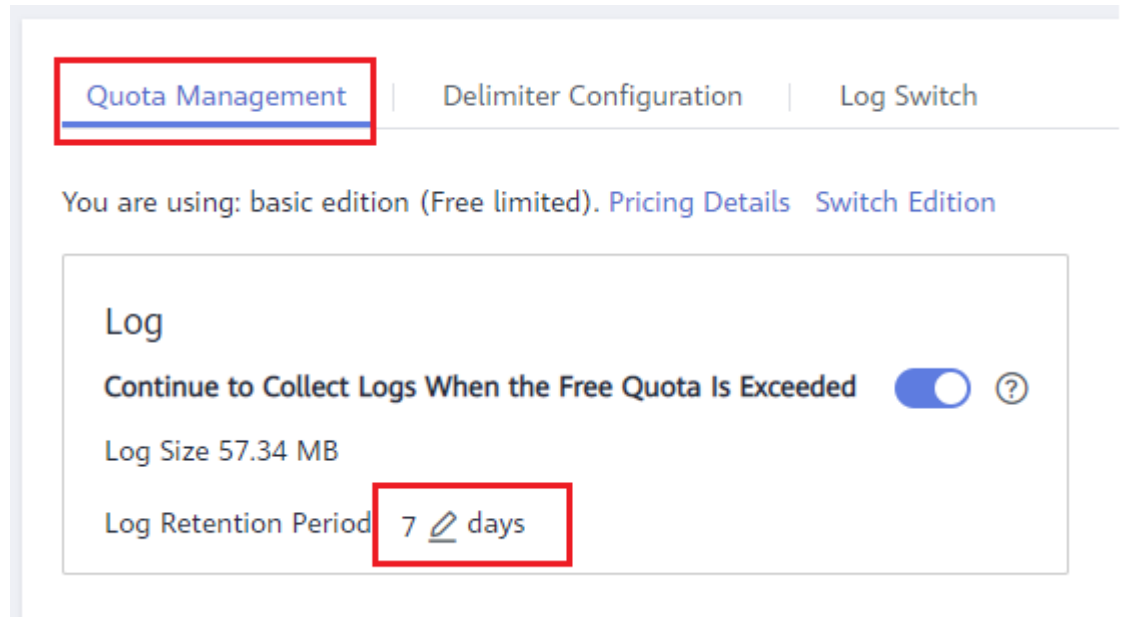
- **Cause:** For a basic edition, a maximum of 500 MB logs can be stored. When the log storage space is about to reach 500 MB or has reached 500 MB, the preceding message is displayed.
- **Impact:** When the log storage space exceeds 500 MB, the ICAgent cannot collect newly printed logs. In addition, 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.

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 3-1 Viewing the log quota



Step 2 Change the log retention period.

----End

3.5 How Do I Obtain an AK/SK?

Each user can create a maximum of two Access Key ID/Secret Access Key (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** above the list and enter the verification code or password.
4. Click **OK** to download the generated AK/SK.
You can obtain the AK from the access key list and SK from the downloaded CSV file.

 NOTE

- Keep the CSV file properly. You can only download the file right after the access key is created. If you cannot find the file, you can create an access key again.
- 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.

3.6 How Can I Check Whether a Service Is Available?

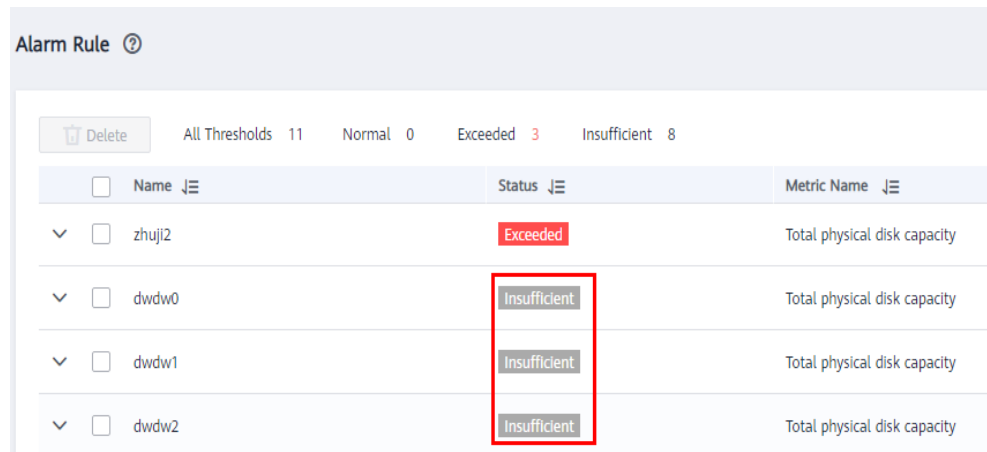
Log in to the Application Operations Management (AOM) console, choose **Container Monitoring** in the navigation pane, and check the service status value at each time point in the workload monitoring view.





If the value is **0**, the service is normal. Otherwise, the service is abnormal.

3.7 Why Is the Status of an Alarm Rule Displayed as "Insufficient"?

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

Figure 3-2 Checking the rule status



Alarm Rule ?		
 Delete	All Thresholds 11	Normal 0 Exceeded 3 Insufficient 8
<input type="checkbox"/> Name 	Status 	Metric Name 
<input type="checkbox"/> zhujj2	Exceeded	Total physical disk capacity
<input type="checkbox"/> dwdw0	Insufficient	Total physical disk capacity
<input type="checkbox"/> dwdw1	Insufficient	Total physical disk capacity
<input type="checkbox"/> dwdw2	Insufficient	Total physical disk capacity

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 minute 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 Displayed as "Abnormal" on the AOM Page?

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

Figure 3-3 Checking the workload status

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

Possible causes:

- The ICAgent version is too old.
ICAgent needs to be upgraded manually. If the ICAgent version is too old, 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.

Figure 3-4 Checking the ICAgent version

Node Name	Node IP Address	ICAgent Status	ICAgent Version
<input type="checkbox"/> Dont-Touch	192.168.0.67	✔ Running	5.13.53
<input type="checkbox"/> as-config-ljib-UD855PVU	192.168.0.26	✔ Running	5.13.53

- 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 IAM console.
- Step 2** In the navigation pane, choose **Agencies**.
- Step 3** On the page that is displayed, click **Create Agency** in the upper right corner. The **Create Agency** page is displayed.
- Step 4** Set parameters by referring to [Table 3-2](#).

Table 3-2 Parameters for creating an agency

Parameter	Description	Example
Agency Name	Set an agency name. NOTICE The agency name must be apm_admin_trust .	-
Agency Type	Select Cloud service .	Cloud service
Cloud Service	Select Application Operations Management (AOM) .	-
Validity Period	Select Unlimited .	Unlimited
Description	(Optional) Provide details about the agency.	-

Step 5 Click **Next**. The **Authorize Agency** page is displayed.

Step 6 On the **Select Policy/Role** tab page, select **DMS UserAccess** and click **Next**.

DMS UserAccess: Common user permissions for DMS, excluding permissions for creating, modifying, deleting, scaling up instances and dumping.

Step 7 On the **Select Scope** tab page, set **Scope** to **Region-specific Projects** and select target projects under **Project [Region]**.

Step 8 Click **OK**.

----End

3.10 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.

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

Symptom

No logs are displayed on the AOM console.

Possible Causes

- No ICAgent has been installed.
- The log collection path is incorrect.
- Log collection has not been enabled on the AOM console.
- The **Continue to Collect Logs When the Free Quota Is Exceeded** option has not been enabled on the AOM console.
- Your account is in arrears.
- The rate of writing logs into log streams or the length of single-line logs exceeds the upper limit.

Solution

- To install an ICAgent, do as follows:
 - a. In the navigation pane, choose **Configuration Management > Agent Management**.
 - b. Select a cluster and click **Install ICAgent**. In the dialog box that is displayed, click **OK**.

Wait until the ICAgent status changes to **Running**, indicating that the ICAgent is successfully installed.
- 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 a text file name, the corresponding file is directly collected. For more details, see [Configuring Log Collection Paths](#).
- Log in to the AOM console. In the navigation pane, choose **Configuration Management > Log Configuration**. On the **Log Switch** tab page, enable log collection.
- You are billed based on log usage, including log read/write, log indexing, and log retention. If **Continue to Collect Logs When the Free Quota Is Exceeded** is disabled, log collection will be stopped when the free quota is used up. Log read/write and indexing will no longer be available. No fees will be incurred for log read/write and indexing. If necessary, enable **Continue to Collect Logs When the Free Quota Is Exceeded**. The procedure is as follows:

Log in to the AOM console. In the navigation pane, choose **Configuration Management > Log Configuration**. On the **Quota Management** tab page, enable **Continue to Collect Logs When the Free Quota Is Exceeded**.
- Top up your account if your account is in arrears.
- Use the Chrome or Firefox browser to query logs.
- If the issue persists after you have tried the methods above, [submit a service ticket](#).

3.12 What Can I Do If an ICAgent Is Offline?

After an ICAgent is installed, its status is offline.

Problem Analysis

- **Cause:** The AK/SK are incorrect or ports 30200 and 30201 are disconnected.

- **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 a command output is displayed, the AK/SK configuration is correct. Go to [Step 4](#).

Step 3 After configuring the AK/SK, reinstall 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 the connectivity of ports 30200 and 30201:

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

```
curl -k https://ACCESS_IP:30201
```

- 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 the ICAgent. If the installation still fails, contact technical support.

----End

3.13 Why Can't the Host Be Monitored After ICAgent Is Installed?

Symptom

An ICAgent has been installed and is working. However, the host cannot be monitored.

Possible Causes

Generally, the possible causes are as follows:

- The ICAgent fails to be installed.
- The ICAgent is successfully installed but incorrectly configured.
- The ICAgent is successfully installed but fails to collect data.

Solution

Step 1 If the ICAgent fails to be installed, [reinstall it](#).

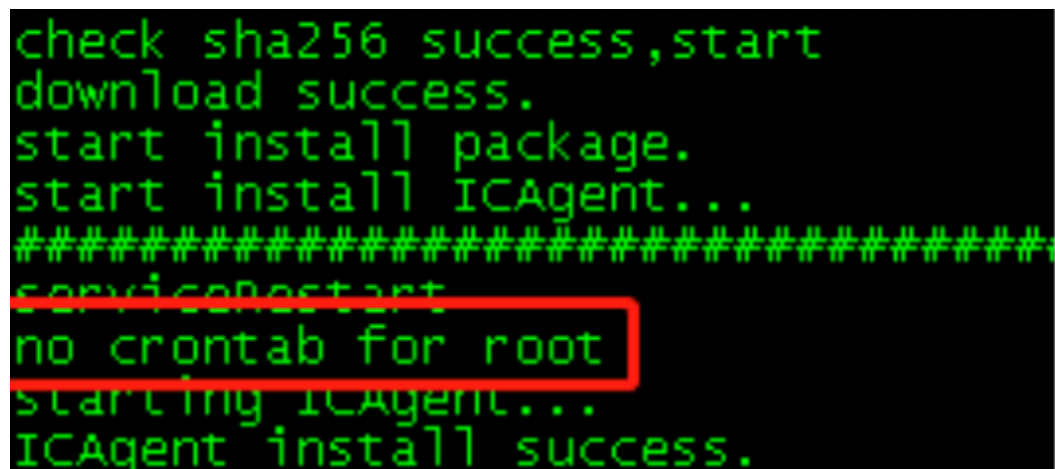
- Step 2** If the ICAgent is successfully installed but the host cannot be monitored, do as follows:
- Check whether the configuration (region name and PodLB address) is correct.
 - Check data collection (whether the OpenStack API is successfully called and the host ID has been specified).
- Step 3** View ICAgent logs, check the configuration, and determine the cause based on logs.
- End

3.14 Why Is "no crontab for root" Displayed During ICAgent Installation?

Symptom

During ICAgent installation, the system displays the message "no crontab for root".

Figure 3-5 Installing an ICAgent



```
check sha256 success,start
download success.
start install package.
start install ICAgent...
#####
service restart
no crontab for root
starting ICAgent...
ICAgent install success.
```

Possible Causes

When you execute the script for installing an ICAgent, crontab scheduled tasks will also be installed. The message "no crontab for root" indicates that there is no scheduled task of the **root** user.

Solution

No measure needs to be taken.

If the command output contains "ICAgent install success", the ICAgent is successfully installed and O&M data can be collected.

3.15 Why Can't I Select an OBS Bucket When Configuring Log Dumping on AOM?

Symptom

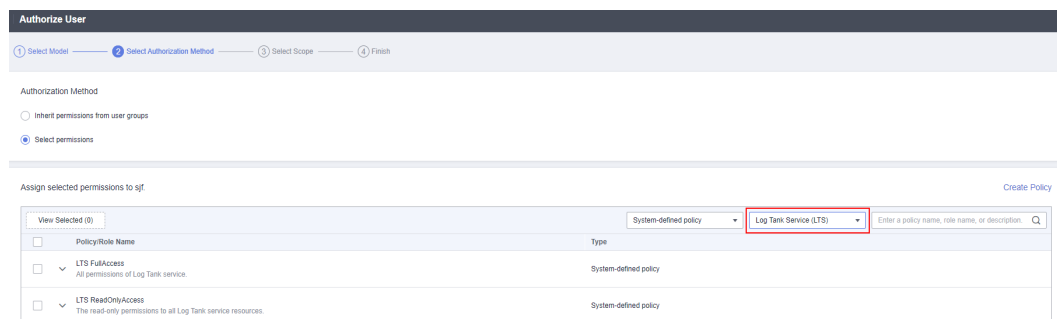
The account has permission for OBS, but cannot view the OBS bucket list during log dumping. Error code LTS.0203 is reported.

Possible Causes

The account does not have the LTS permission.

Solution

- Step 1** Log in to the IAM console as an administrator.
- Step 2** On the **Users** page, locate the target username and click **Authorize** in the **Operation** column.
- Step 3** Select the **RBAC** authorization model and click **Next**.
- Step 4** Specify **Select permissions** for **Authorization Method**, and enter **LTS** to search, select **LTS FullAccess** or **LTS ReadOnlyAccess**, and click **Next**.



- Step 5** Select target region-specific projects and click **OK**.

----End

3.16 Why Can't Grafana Display Content?

Symptom

After the Prometheus add-on is installed on the CCE add-on page, Grafana cannot display monitoring data.

Possible Causes

Grafana parameters are incorrect.

Solution

Step 1 Log in to the CCE console (old version).

Step 2 In the navigation pane on the left, choose **Resource Management > Network**. On the **Services** tab page, obtain the access address and port number of the Grafana service and the access domain name and port number of the Prometheus service.

Service Name	Internal Domain Name	Workload	Access Address	Access Type	Access Port -> Container Port / Protocol	Operation
<input type="checkbox"/> prometheus		N/A		NodePort	80 -> / TCP	Update Edit YAML Delete
<input type="checkbox"/> grafana-test		N/A		NodePort	80 -> / TCP	Update Edit YAML Delete

Step 3 In the navigation pane on the left, choose **Configuration Center > ConfigMaps**. On the displayed page, locate **grafana-conf**, click **Edit YAML** in the **Operation** column, and change **root_url** to the Grafana access address.

```

72  # Redirect to correct domain if host header does not match domain
73  # Prevents DNS rebinding attacks
74  enforce_domain = false
75
76  # The full public facing url
77  root_url = %(protocol)s://%(domain)s:%(http_port)s/grafana/
78
79  # Log web requests
80  router_logging = false
81
82  # the path relative working path
83  static_root_path = public
84
85  # enable gzip
86  enable_gzip = false
87

```

Change it to the target Grafana access address.

Step 4 On the **ConfigMaps** page, locate **grafana-datasources**, click **Edit YAML** in the **Operation** column, and change **url** to the Prometheus domain name.

```

28 data:
29   prometheus.yaml: |-
30     {
31       "apiVersion": 1,
32       "datasources": [
33         {
34           "access": "proxy",
35           "editable": false,
36           "name": "prometheus",
37           "orgId": 1,
38           "type": "prometheus",
39           "url": "http://cceaddon-prometheus-server.cce-monitor.svc:80",
40           "version": 1
41         }
42       ]
43     }

```

Change it to the Prometheus domain name.

Step 5 Restart the Grafana pod to view monitoring data.

----End