Application Operation Management

FAQs

Issue   01

Date   2025-02-12

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 Dashboard

1.1 Can I Import Grafana Views to AOM Dashboards?

Symptom

Can I import Grafana views to AOM dashboards?

Solution

Obtain the Prometheus statement of a Grafana view and then create a graph in AOM by using the Prometheus statement.

Procedure:

Step 1 Log in to Grafana and obtain the Prometheus statement of a Grafana view.

Step 2 Log in to the AOM 2.0 console.

Step 3 In the navigation pane, choose **Metric Browsing**.

Step 4 Select a target Prometheus instance from the drop-down list.

Step 5 Click **Prometheus statement** and enter the Prometheus statement obtained in **Step 1**.

Step 6 Select a metric and click ⚲ in the upper right corner of the metric list.

Step 7 In the **Add to Dashboard** dialog box, select a dashboard, set a graph name, and click **Confirm**.

Then you can view the Grafana view in AOM.

For details about how to manage dashboards, see **Dashboard**.

----End

2 Alarm Management

2.1 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.

3 Log Analysis

3.1 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.

3.2 How Do I Check Which Application Generates Logs in AOM?

Symptom

A large number of logs are generated everyday. How do I check which application generates specific logs?

Solution

AOM does not show the applications to which logs belong. To view that, ingest all logs to LTS and use its resource statistics function.

Procedure:

Step 1 Create a log group and stream for your application. For details, see **Creating Log Groups and Log Streams**.

Step 2 Log in to the LTS console and view detailed resource statistics of top 100 log groups or streams using the **resource statistics** function.

----End

4 Prometheus Monitoring

4.1 How Do I Connect Prometheus Data to AOM?

To connect Prometheus data to AOM, do as follows:

Step 1 Create a Prometheus instance.

Managing Prometheus Instances

-

-

Step 2 Report native Prometheus metrics to AOM through the remote write address. For details, see **Reporting Prometheus Data to AOM**.

----End

4.2 How Do I Distinguish Basic Metrics from Custom Metrics Collected by Prometheus Monitoring?

Log in to the AOM console, go to the Prometheus instance details page, and view the types of metrics that are collected.

Procedure:

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Prometheus Monitoring** > **Instances**.

Step 3 In the instance list, click a desired Prometheus instance. The instance details page is displayed.

Step 4 In the navigation pane on the left, choose **Metric Management**. On the **Metrics** tab page, view the metric names and types of the current Prometheus instance.

----End

4.3 How Do I Obtain the Service Address of a Prometheus Instance?

You can log in to the AOM console and go to the Prometheus instance details page to obtain the service address of the Prometheus instance.

Procedure:

Step 1 Log in to the **AOM 2.0** console.

Step 2 In the navigation pane on the left, choose **Prometheus Monitoring** > **Instances**. In the instance list, click the created Prometheus instance.

Step 3 On the instance details page, choose **Settings** in the navigation pane to obtain the service address of the current instance.

The following describes how to obtain the service address of a Prometheus instance for CCE.

- Click the **Intranet** or **Public Network** tab to obtain the configuration code for Prometheus remote read and write in the intranet or public network. Click ⬜ on the right of the code to copy the code to the corresponding file.

- Obtain the configuration code for Prometheus remote read.

Figure 4-1 Configuration code for Prometheus remote read


```
Configuration Code for Prometheus Remote Read

remote_read:
  - url: 'https://aom                                              /api/v1/read'
    tls_config:
      insecure_skip_verify: true
    bearer_token: 'VV**aF'
    read_recent: true
```

Remote read address:

url: 'https://aom.{region_name}.{Site domain name suffix}/v1/{project_id}/api/v1/read'

Remote read address parameters:

  - **region_name**: domain name or IP address of the server where the REST service is deployed. The value varies depending on services and regions.
  - **Site domain name suffix**: site domain name suffix, for example, **myhuaweicloud.com**.
  - **project_id**: project ID.

- Obtain the configuration code for Prometheus remote write.

Figure 4-2 Configuration code for Prometheus remote write


```
Configuration Code for Prometheus Remote Write

remote_write:
  - url: 'https://aom-internal-access.           .        8443/v1/                    /push'
    tls_config:
      insecure_skip_verify: true
    bearer_token: 'SE**IH'
```

Remote write address in the intranet:

url: 'https://aom-internal-access.{region_name}.{Site domain name suffix}:8443/v1/{project_id}/push'

Remote write address in the public network:

url: 'https://aom-access.{region_name}.{Site domain name suffix}:8443/v1/{project_id}/push'

Remote write address parameters:

– **region_name**: domain name or IP address of the server where the REST service is deployed. The value varies depending on services and regions.

– **Site domain name suffix**: site domain name suffix, for example, **myhuaweicloud.com**.

– **project_id**: project ID.

----End

4.4 Why Can't Metrics Prefixed with aom_prom_fixed Be Discarded?

Symptom

Metrics prefixed with **aom_prom_fixed_** cannot be discarded on the **Metric Management** page. In addition, these metrics are billed when being reported to AOM.

Possible Cause

For custom metrics named after Prometheus functions (such as **count**, **max**, **min**, **avg**, **sum**, **count_values**, **stddev**, **stdvar**, **group**, **bottomk**, **topk**, or **quantile**) or operators (such as **and**, **or**, or **unless**), AOM will add the prefix **aom_prom_fixed_** to them when they are being reported to AOM to avoid PromQL query errors. For example, the original name of a custom metric is **count** and will be automatically converted to **aom_prom_fixed_count** when being reported. Due to name inconsistency, this metric fails to be discarded.

Solution

Do not use any Prometheus function (such as **count**, **max**, **min**, **avg**, **sum**, **count_values**, **stddev**, **stdvar**, **group**, **bottomk**, **topk**, or **quantile**) or operator (such as **and**, **or**, or **unless**) as metric names. Name custom metrics in the format of "xxx_xxx_xxx".

5 Infrastructure Monitoring

5.1 Why Can't AOM Detect Workloads After the Pod YAML File Is Deployed Using Helm?

Symptom

After a pod is deployed using Helm, AOM cannot find the corresponding workload.

Possible Cause

On the workload page of the CCE console, find the record of the pod deployed using Helm, and compare its YAML file with the YAML file of the pod directly deployed on the CCE console. It is found that the YAML file of the pod deployed using Helm does not contain required environment parameters.

Figure 5-1 Comparing YAML files

Solution 1

Step 1 Log in to the CCE console and click a target cluster.

Step 2 Choose **Workloads** in the navigation pane, and select the workload (pod deployed using Helm) whose metrics have not been reported to AOM.

Step 3 Choose **More** > **Edit YAML** in the **Operation** column where the target workload is located.

Step 4 In the displayed dialog box, locate **spec.template.spec.containers**.

Step 5 Add environment parameters to the end of the **image** field, as shown in **Figure 5-2**.

```
env:
    - name: PAAS_APP_NAME
      value: XXXXXXXXXXXX
    - name: PAAS_NAMESPACE
      value: XXXXXXXXXX
    - name: PAAS_PROJECT_ID
      value: 2a*********************cf
```

- **PAAS_APP_NAME**: application name, that is, the name of the workload to be deployed.

- **PAAS_NAMESPACE**: namespace of the CCE cluster where the workload to be deployed is located. To obtain the namespace, go to the namespace page on the CCE cluster details page.

- **PAAS_PROJECT_ID**: project ID of the tenant. To obtain the project ID, see **Obtaining the Project ID**.

  Replace the values of the preceding environment parameters based on site requirements.

Figure 5-2 Adding environment parameters
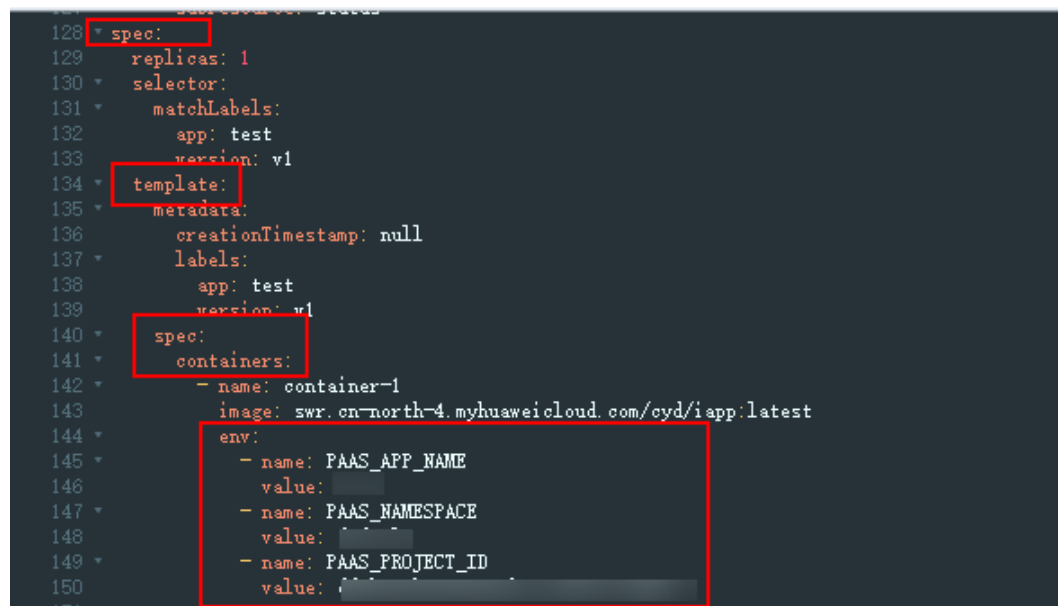
Step 6 Click **Confirm**.

----End

Solution 2
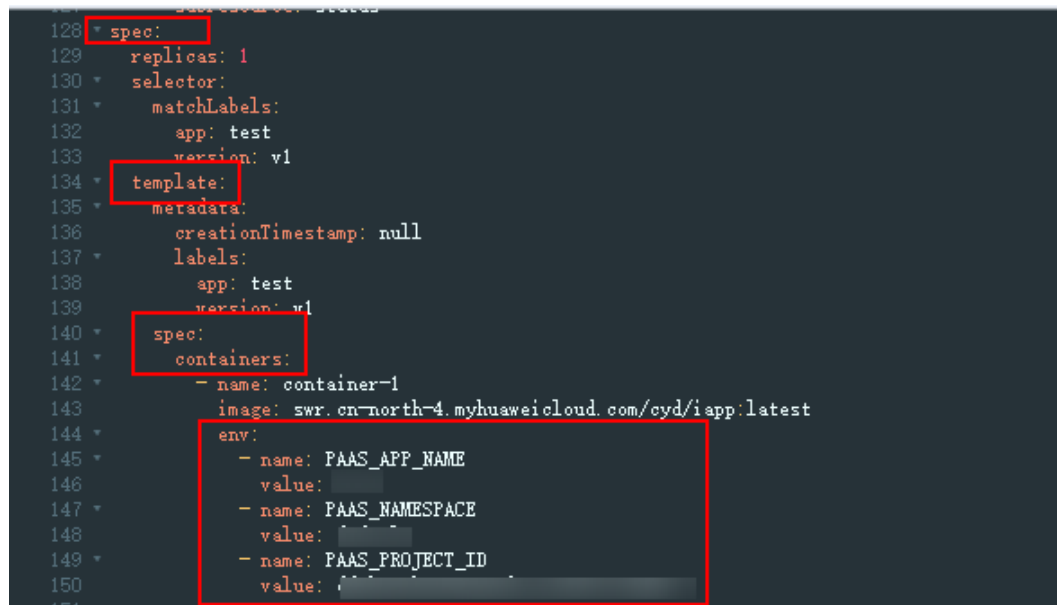
Add the following environment parameters to the YAML file for deploying the pod using Helm and then deploy the pod again.

```
env:
    - name: PAAS_APP_NAME
      value: XXXXXXXXXXXX
    - name: PAAS_NAMESPACE
      value: XXXXXXXXXX
    - name: PAAS_PROJECT_ID
      value: 2a*********************cf
```

- **PAAS_APP_NAME**: application name, that is, the name of the workload to be deployed.

- **PAAS_NAMESPACE**: namespace of the CCE cluster where the workload to be deployed is located. To obtain the namespace, go to the namespace page on the CCE cluster details page.

- **PAAS_PROJECT_ID**: project ID of the tenant. To obtain the project ID, see **Obtaining the Project ID**.

  Replace the values of the preceding environment parameters based on site requirements.

Figure 5-3 Adding environment parameters

6 Application Monitoring

6.1 What Are the Differences Between Application Monitoring Under Application Insights and that Under Process Monitoring?

The monitored objects vary depending on the navigation path.

- **Application Insights** > **Application Monitoring**:

  Resources and applications managed using CMDB. You can learn about the resource usage, status, and alarms of applications to quickly respond to requests and ensure smooth system running.

- **Process Monitoring** > **Application Monitoring**:

  Applications discovered based on application discovery rules.

7 CMDB (Unavailable Soon)

7.1 Why Are Resources Not Displayed on the Resource Management Page?

If you have purchased resources, choose **Resources** > **My Resources** on the top to check whether your resources exist. If your resources are displayed in **My Resources**, click the refresh icon on the **Resource Management** page to view them.

Figure 7-1 Viewing resources
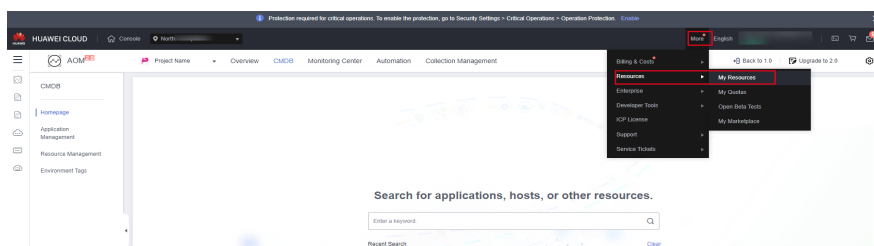
Figure 7-2 Refreshing the resource management page
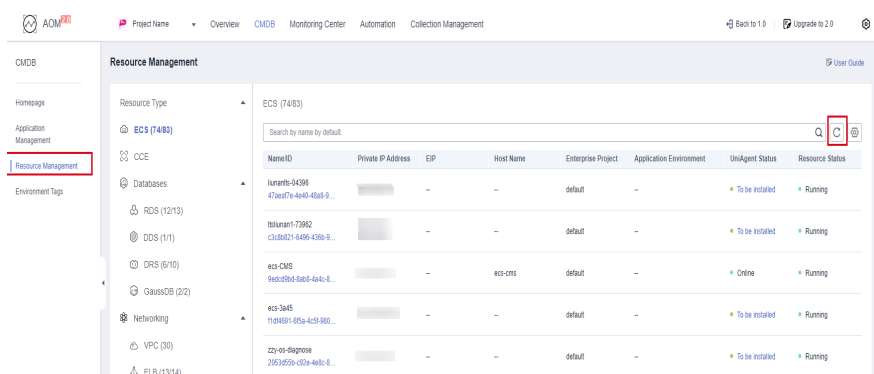
7.2 Why Are Deleted Resources Still Displayed on the Console?

For resources bound to CMDB environments, CMDB will not directly clear them when you delete them. Instead, it displays their status as **Destroyed**.

To clear such resources, manually unbind them from CMDB environments first. CMDB will then clear them in the early morning. Resources that are not bound to any CMDB environment will be cleared upon your deletion.

7.3 Why Are Resources Displayed on the CMDB Resource Management Page But Not Found When I Bind Environments?

CMDB checks whether resources are in the same enterprise project and region as environments. If they are inconsistent, resources will not be displayed.

If the preceding conditions are met but the corresponding resource is still not displayed, the resource has been bound to the environment and will not be displayed on the resource association page by default. You can set **Status** to **Bound** to view the resources that have been bound.

A resource can be bound to multiple environments by **transferring resources**. Repeated binding is not supported on the resource binding page.

7.4 Why Is "AOM.11007006: get policy list failed." Displayed?

Symptom

The system displays "AOM.11007006: get policy list failed" during resource search on the CMDB homepage.

Possible Causes

Your account is in arrears or frozen.

Solution

- If your account is in arrears, top it up by referring to **Top-Up and Repayment**.
- If your account is frozen or suspended but is still in the retention period, renew or top up your account by referring to **Can Frozen Resources Be Unsubscribed from, Released, or Deleted?**

8 O&M Management (Unavailable Soon)

8.1 How Can I Obtain the OBS Permission for Installing Packages?

Symptom

The user does not have the OBS permission when installing packages.

Possible Causes

To obtain packages from OBS, obtain an access credential first.

Solution

Go to the Automation (Retiring) console, choose **Settings** > **Access Credentials**, and check whether there is an access credential. If no access credential is available, create one.

8.2 Why Can't Scheduled Tasks Be Triggered?

Symptom

After scheduled tasks are created, operations (such as script execution and file/scenario/job management) cannot be triggered at a specified time or periodically.

Possible Causes

Your account may be in arrears, frozen, or suspended.

Solution

- If your account is in arrears, top it up by referring to **Top-Up and Repayment**.
- If your account is frozen or suspended but is still in the retention period, renew or top up your account by referring to **Can Frozen Resources Be Unsubscribed from, Released, or Deleted?**

After your account is restored, the scheduled tasks can be triggered.

8.3 Can I Specify Script Parameters and Hosts During Job Execution?

Yes. You can set global parameters and reference them in job steps.

Procedure

Step 1 Log in to the AOM 2.0 console. In the navigation pane, choose **Automation (Retiring)**.

Step 2 In the navigation pane, choose **Jobs** and click **Create Job** in the upper right corner.

Step 3 On the displayed page, click **Add Global Parameter**, add **param1** whose parameter type is **String** and **param2** whose parameter type is **Host**, and save the settings.

Step 4 Add a job step. For **Script Parameters**, use **${param1}** to reference the string parameter. For **Target Instances**, select **Global Parameter** and then select **param2** from the drop-down list. Next, save the settings.

Step 5 When executing a job plan, specify **param1** and **param2** (instances to be executed) as required.

----End

8.4 Why Is a Parameter Error Displayed When I Create a Scheduled Task Using a Cron Expression?

Symptom

When a scheduled O&M task is created using a cron expression, the system shows that there is a parameter error.

Possible Causes

- The cron expression does not comply with the Spring cron syntax.
- The interval for triggering a scheduled task is less than 30 minutes.

Procedure

Step 1 Ensure that the cron expression complies with the Spring cron syntax.

Step 2 Ensure that the interval for triggering a scheduled task is greater than or equal to 30 minutes.

----End

8.5 How Can I Set a Review for an Execution Plan?

No review can be set for an execution plan. However, the plan can inherit the job's review settings.

Solution

When you create a job, enable **Review**. By default, this option is disabled. If it is enabled, the job's execution plan will need to be reviewed before being executed. For details about how to create a job, see **Jobs**.

8.6 Why Is "delete success:{}" Displayed (Files Cannot Be Deleted) During Disk Clearance?

Symptom

During disk clearance, message "delete success:{}" is displayed, indicating that the files in the specified directory cannot be deleted.

Possible Causes

- The directory or file to be cleared does not exist.
- The result of the current time minus the last modification time of the target file or directory is less than the file retention time specified in the clearing rule.

Solution

Check whether the directory or file to be cleared exists. If they exist, ensure that the result of the current time minus the last modification time of the file or directory is greater than the file retention time specified in the clearing rule.

Example: To delete files generated one day ago, ensure that the result of the current time minus the last modification time of the file or directory is greater than 24 hours.

8.7 What Can I Do If the Execution Plan Is Not Updated After I Modify the Job?

After a job is modified, its execution plan is not automatically updated.

Solution

Create an execution plan for the job again. For details about how to create an execution plan, see **Jobs**.

8.8 What Can I Do If "agent not found" Is Displayed?

Symptom

Message "agent not found" is displayed when I execute a script on an ECS.

Possible Causes

- The UniAgent is not properly installed.
- The UniAgent is not in the **Running** state.

Solution

Check the UniAgent status and perform operations by following the instructions below:

- **Error**: The UniAgent is not working. Contact technical support.
- **Installing**: The UniAgent is being installed. The installation takes about 1 minute to complete.
- **Installation failed**: The UniAgent fails to be installed. Install it again.
- **Not installed**: The UniAgent has not been installed. Install it by referring to **Installing a UniAgent**.

After the UniAgent status changes to **Running**, execute the script on the ECS again.

8.9 Why Are the Hosts Listed in Execution Logs Inconsistent with Those I Configured for a Task?

Possible Causes

If the hosts configured in the task have been deleted or you do not have permission to use them, these hosts will be ignored and will not be displayed in the execution logs.

Solution

Ensure that all hosts configured in the task are valid.

8.10 Why Did a Task Fail to Execute?

Symptom

When a resource is selected from CMDB to execute a task, message "Access denied, The *{ECS Instance/RDS Instance/Workload}* does not belong to the current project, *{ECS Instance/RDS Instance/Workload}* ID is *{Instance ID}*" is displayed.

Possible Causes

The system will check whether the resource to be operated is under the selected sub-project. If it is not under the sub-project, operations will not be performed on it.

Solution

Ensure that the resource to be operated is under the selected sub-project. If it is not under the sub-project, add it to the current sub-project or select another sub-project. For details about how to view resource information, see **Resource Management**.

9 Collection Management

9.1 Are ICAgent and UniAgent the Same?

ICAgent is a plug-in, but UniAgent is not.

- UniAgent is an Agent for unified data collection and serves as the base of the cloud service O&M system. It delivers instructions, such as script delivery and execution, and integrates plug-ins (such as ICAgent, Cloud Eye, and Telescope) and maintains their status. UniAgent provides middleware and custom metric collection capabilities.

  ☐ NOTE

    UniAgent does not collect O&M data; instead, collection plug-ins do that.

- ICAgent collects metrics and logs for AOM and LTS.

Figure 9-1 ICAgent and UniAgent
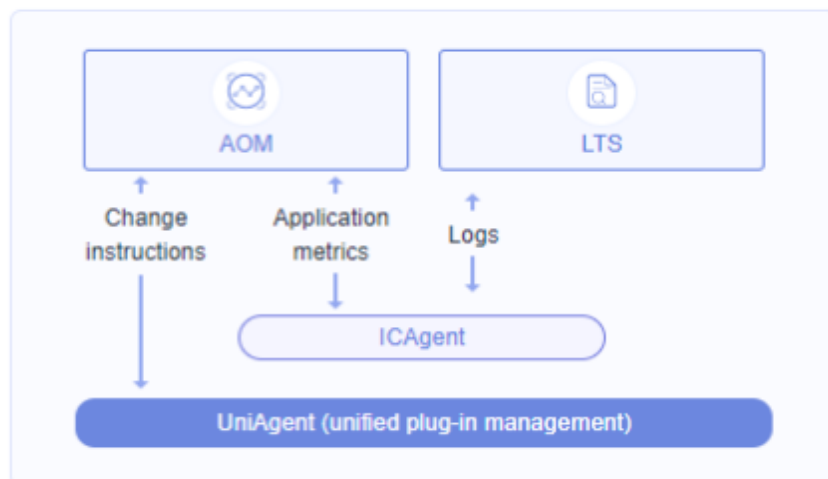
9.2 What Can I Do If an ICAgent Is Offline?

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

9.3 Why Is an Installed ICAgent Displayed as "Abnormal" on the UniAgent Installation and Configuration Page?

Symptom

An installed ICAgent is displayed as "Abnormal" on the UniAgent Installation and Configuration page.

Possible Causes

The AK/SK are incorrect, or no agency is set.

Solution

Obtain an AK/SK by creating an agency and then reinstall the ICAgent.

9.4 Why Can't I View the ICAgent Status After It Is Installed?

Symptom

After the ICAgent is installed, its status cannot be viewed on the console.

Possible Cause

The virtual NIC is used on the user side. To obtain the ICAgent status, modify the script according to the following procedure.

Solution

Step 1 Log in to a host where the ICAgent has been installed as the **root** user.

Step 2 Check the host IP address in use, as shown in **Figure 9-2**:

netstat -nap | grep establish -i

Figure 9-2 Checking the host IP address

Step 3 Check the NIC corresponding to the IP address, as shown in **Figure 9-3**:

ifconfig | grep *IP address* -B1

Figure 9-3 Checking the NIC corresponding to the IP address

Step 4 Go to the **/sys/devices/virtual/net/** directory and check whether the NIC name exists.

- If it exists, it is a virtual NIC. Then go to **Step 5**.
- If it does not exist, it is not a virtual NIC. Then contact technical support.

Step 5 Modify the ICAgent startup script:

1. Open the **icagent_mgr.sh** file (command varies depending on the ICAgent version):

   vi /opt/oss/servicemgr/ICAgent/bin/manual/icagent_mgr.sh

   Or

   vi /var/opt/oss/servicemgr/ICAgent/bin/manual/icagent_mgr.sh

2. Modify the script file:

Add **export IC_NET_CARD=**_NIC name_ to the file, as shown in **Figure 9-4**.

Figure 9-4 Modifying the script

```
ICAGENT_CURRENT_PATH=$(cd $(dirname $BASH_SOURCE) && pwd)
APP_ROOT=$ICAGENT_CURRENT_PATH/../..
export APP_ROOT
export ConfFilePath="/opt/oss/servicemgr/ICAgent/envs"
export GODEBUG=netdns=go
export IC_NET_CARD="et   1"
```

Step 6 Restart the ICAgent (commands vary depending on the ICAgent version):

sh /opt/oss/servicemgr/ICAgent/bin/manual/mstop.sh
sh /opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh

Or

sh /opt/oss/servicemgr/ICAgent/bin/manual/mstop.sh
sh /var/opt/oss/servicemgr/ICAgent/bin/manual/mstop.sh

Step 7 Log in to the AOM console, choose **Collection Management**, and check whether the ICAgent status is displayed.

- If the ICAgent status is displayed, no further action is required.
- If the ICAgent status is still not displayed, contact technical support.

----End

9.5 Why Can't AOM Monitor CPU and Memory Usage After ICAgent Is Installed?

Symptom

AOM cannot monitor information (such as CPU and memory usage) after the ICAgent is installed.

Possible Cause

- Port 8149 is not connected.
- The node time on the user side is inconsistent with the time of the current time zone.

Solution

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

Step 2 Check whether the ICAgent can report metrics:

cat /var/ICAgent/oss.icAgent.trace | grep httpsend | grep MONITOR

- If the command output contains **failed**, the ICAgent cannot report metrics. In this case, go to **3**.
- If the command output does not contain **failed**, the ICAgent can report metrics. In this case, go to **4**.

Step 3 Check whether the port is connected.

1. Obtain the access IP address:
   ```
   cat /opt/oss/servicemgr/ICAgent/envs/ICProbeAgent.properties | grep ACCESS_IP
   ```

2. Check the connectivity of port 8149:
   ```
   curl -k https://ACCESS_IP:8149
   ```
   - If **404** is returned, the port is connected. In this case, contact technical support.

   - If **404** is not returned, the port is not connected. In this case, contact the network administrator to open the port and reinstall the ICAgent. If the installation still fails, contact technical support.

Step 4 Check the node time on the user side:
```
date
```
- If the queried time is the same as the time of the current time zone, contact technical support.

- If they are different, go to **5**.

Step 5 Reconfigure the node time on the user side:
date -s *Time of the current time zone* (for example, **12:34:56**)

----End

9.6 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.

9.7 FAQs About UniAgent and ICAgent Installation

1. What Can I Do If the Network Between the UniAgent Installation Host and Target Host Is Disconnected ("[warn] ssh connect failed, 1.2.1.2:22")?

   Check network connectivity before installing an Agent, and select an installation host that is accessible from the Internet.

2. What Can I Do If the Heartbeat Detection and Registration Fail and the Network Is Disconnected After I Install a UniAgent?

   Run the **telnet** *proxy IP address* command on the target host to check whether the network between the proxy and target host is normal.

3. Ports 8149, 8102, 8923, 30200, 30201, and 80 need to be enabled during ICAgent installation. Can port 80 be disabled after ICAgent is installed?

   Port 80 is used only for pulling Kubernetes software packages. You can disable it after installing the ICAgent.

4. Will the ICAgent installed in a Kubernetes cluster be affected after the cluster version is upgraded?

   After the cluster version is upgraded, the system will restart the ICAgent and upgrade it to the latest version.

9.8 How Do I Enable the Nginx stub_status Module?

Nginx Prometheus Exporter monitors the Nginx service using the stub_status module. Ensure that this module is enabled. Perform the following operations:

1. Log in to the node where the Nginx service is deployed and run the following command (generally in the **/usr/local/nginx/sbin/nginx** directory) as the **root** user to check whether the stub_status module is enabled:
   ```
   nginx -V 2>&1 | grep -o with-http_stub_status_module
   ```
   - If **with-http_stub_status_module** is returned, the stub_status module is enabled.
   - If no result is returned, enable the stub_status module by setting **--with-http_stub_status_module** in the configuration file. Example:
     ```
     ./configure \
     ## Add the --with-http_stub_status_module parameter.
     --with-http_stub_status_module
     make
     sudo make install
     ```

2. After the stub_status module is enabled, add the following content to the **nginx.conf** file (which is generally in the **/usr/local/nginx/conf** directory): Example:

   a. Open the **nginx.conf** file using the vi editor:
   ```
   vi /usr/local/nginx/conf/nginx.conf
   ```

      b.   Press **i** to enter the editing mode and add the following configuration information:

```
server {
 listen 8080;  # Listening port. Set this parameter based on service requirements.
 listen [::]:8080; # IPv6 listening port. Set this parameter based on service requirements.
 server_name localhost; # Set this parameter based on service requirements.
 location = /stub_status { # Path. Set this parameter based on service requirements.
    stub_status on;
    access_log off;
    allow 127.0.0.1;
 }
}
```

      c.   Press **Esc** and enter **:wq** to save the settings and exit.

  3.   Restart the Nginx service.
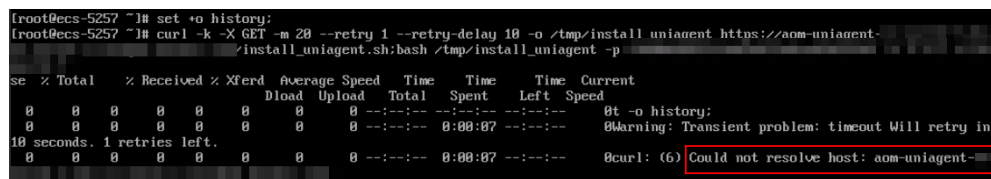
9.9 Why Does APM Metric Collection Fail?

1. You can check metric data several minutes after you connect APM Agents.

2. If data collection stops, check the following:

   – Instance level: Agents are stopped on the **Instance** tab page.

   – Monitoring item level: Monitoring items are manually disabled on the **Monitoring Item** tab page.

   – Global level: The **Stop Collecting Data Through Bytecode Instrumentation** option is enabled on the **General Configuration** page of APM.

3. If no data is collected for a long time, check the following:

   – Java 9 prompts that the **sql.time** class cannot be found.

     Cause analysis: Agents are developed using JDK 1.7. However, after Java 9 modularization, no SQL package is provided by default.

     Occurrence: This problem occurs under certain conditions.

     Workaround: Ensure that the component can proactively import **java.sql** to **module-info.java**.

   – Java 11 prompts that "Caused by: java.lang.NoClassDefFoundError: sun/misc/Unsafe class cannot be found."

     Cause analysis: Agents are developed using JDK 1.7, but the Java 11 Unsafe class is categorized to a different package.

     Occurrence: This problem occurs inevitably.

     Workaround: Ensure that the application can proactively import **jdk.unsupported** to **module-info.java**.

   – Java 9 reports an illegal reflective access alarm. (This problem will be solved in versions later than Java 9.)

     Workaround: Set **--illegal-access** to **warn** or delete this option.

9.10 Why Cannot the Installation Script Be Downloaded When I Try to Install UniAgent on an ECS?

Symptom

During UniAgent installation on an ECS, the installation script cannot be downloaded. Message "Cloud not resolve host: aom-uniagent-*xxxxxxxxxxxxxxxxxxxxxxxxxxx*" is displayed.

Figure 9-5 Error information

Possible Cause

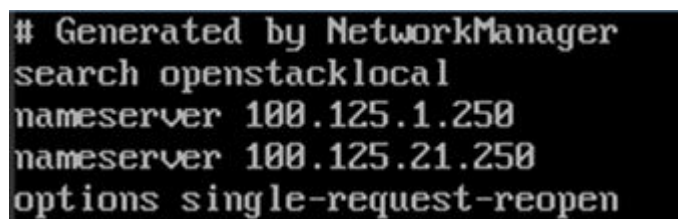The host cannot resolve the Object Storage Service (OBS) domain name.

Solution

Add Domain Name Service (DNS) server addresses for the ECS running Linux and then add a security group.

You can add DNS server addresses for the ECS by running commands or through the management console.

- To add DNS server addresses by running commands, perform the following steps:

  a. Log in to the ECS as user **root**.

  b. Run the **vi /etc/resolv.conf** command to open the file.

  c. Add **nameserver** *xx.xx.xx* to the file.

     xx.xx.xx indicates private DNS server addresses. Take the **CN North-Beijing1** region as an example. The private DNS server addresses are **100.125.1.250** and **100.125.21.250**.

   **Figure 9-6** Adding DNS server addresses (Linux)

☐ **NOTE**

Private DNS server addresses vary depending on regions. For details, see **What Are Huawei Cloud Private DNS Server Addresses?**

d. Enter **:wq** and press **Enter** to save the settings and exit.

- To add DNS server addresses for the ECS through the management console, perform the following steps:

    a. In the upper left corner of the management console, select a target region and project.

    b. Click **Service List** in the upper left corner. Under **Compute**, select **Elastic Cloud Server**.

    c. In the ECS list, click the ECS name to go to the ECS details page.

    d. In the **Summary** tab page, click the VPC name, as shown in **Figure 9-7**.

        The **Virtual Private Cloud** page is displayed.
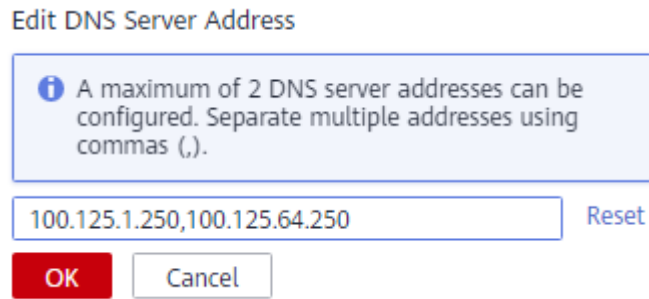
Figure 9-7 VPC
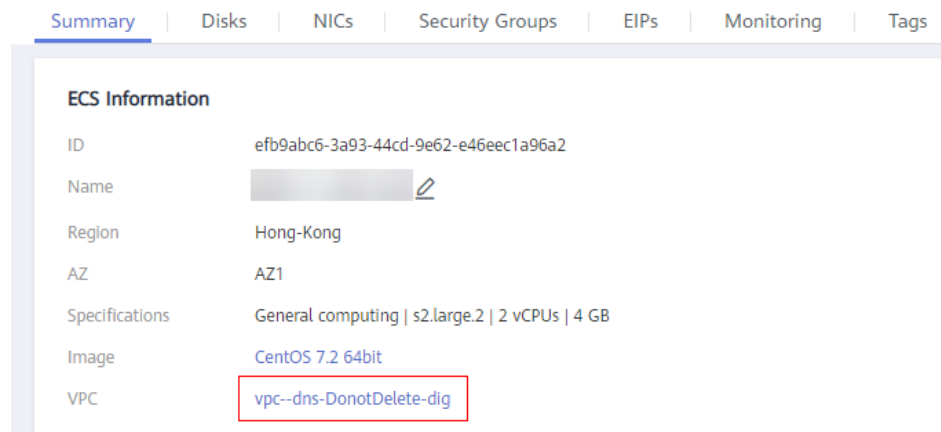
    e. In the VPC list, locate the target VPC and click its name.

    f. In the **Networking Components** area, click the number following **Subnets**.

        The **Subnets** page is displayed.

    g. In the subnet list, locate the target subnet and click its name.

    h. In the **Gateway and DNS Information** area, click [pencil icon] following **DNS Server Address**.

        ☐ **NOTE**

        Set the DNS server address to the value of **nameserver** in **3**.

Figure 9-8 Modifying the DNS server address

Edit DNS Server Address

ℹ️ A maximum of 2 DNS server addresses can be configured. Separate multiple addresses using commas (,).

```
100.125.1.250,100.125.64.250
```
Reset

OK   Cancel

    i.   Click **OK**.

    📖 NOTE

        The new DNS server address takes effect after the ECS is restarted.

- To add a security group through the management console, perform the following steps:

    a.   In the upper left corner of the management console, select a target region and project.

    b.   Click **Service List** in the upper left corner. Under **Compute**, select **Elastic Cloud Server**.

    c.   In the ECS list, click the ECS name to go to the ECS details page.

    d.   On the **Security Groups** tab page, click a security group name. The security group details page is displayed.

    e.   Go to the **Outbound Rules** tab page and then click **Add Rule**.

        Add a rule by referring to **Table 9-1**.

Table 9-1 Parameters for adding a security group rule

Priority	Action	Type	Protocol & Port		Destination	Description
1	Allow	IPv4	TCP	80	100.125.0.0/16	Used to download the UniAgent installation package from the OBS bucket to the ECS and obtain the metadata and authentication information of the ECS.

Priority	Action	Type	Protocol & Port		Destination	Description
1	Allow	IPv4	TCP and UDP	53	100.125.0.0 /16	Used by DNS to resolve domain names, for example, resolve the OBS domain name when you download the UniAgent installation package, and resolve the UniAgent address.
1	Allow	IPv4	TCP	443	100.125.0.0 /16	Used to collect monitoring data and report them to AOM.

10 Other FAQs

10.1 Comparison Between AOM 1.0 and AOM 2.0

Do I Need to Be Authorized to Use AOM 2.0 While I Already Have AOM 1.0 Permissions?

AOM 2.0 billing is different from that of AOM 1.0. If you switch from AOM 1.0 to AOM 2.0 for the first time, apply for the permission to use AOM 2.0 by referring to **Subscribing to AOM 2.0**.

What Are the Function Differences Between AOM 2.0 and AOM 1.0?

Based on AOM 1.0 functions and common application monitoring, AOM 2.0 collects and monitors more metrics and log data, and displays monitoring results in a visualized manner. In addition, the Automation service makes routine O&M operations servitized and automated, reducing repeated operations. For details, see **Comparison Between AOM 1.0 and AOM 2.0**.

As AOM 1.0 functions are gradually replaced by AOM 2.0, AOM 1.0 will be brought offline soon. You are advised to upgrade AOM 1.0 to AOM 2.0. For details, see **Upgrading to AOM 2.0**.

10.2 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 10-1 Multi-dimensional O&M solution
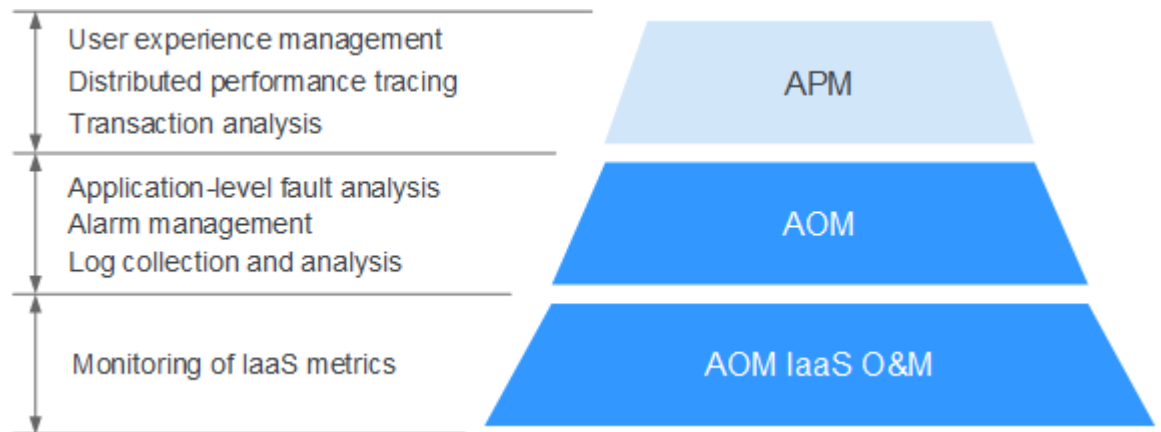
10.3 What Are the Differences Between the Log Functions of AOM and LTS?

Log Tank Service (LTS) can collect, analyze, and store log data. You can use LTS for efficient device O&M, service trend analysis, security audits, and monitoring.

AOM is a one-stop platform for Huawei Cloud service observability analysis. It integrates the log functions of **Log Tank Service (LTS)**. Charging data records (CDRs) are reported by LTS instead of AOM. You will not be billed twice. AOM incorporates LTS functions for unified O&M. LTS also has its own independent console and can be used separately. To stop billing, see **How Do I Stop Billing on the LTS Page?**

10.4 How Do I Create the apm_admin_trust Agency?

Creating the apm_admin_trust Agency

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 10-1**.

Table 10-1 Parameters for creating an agency

Parameter	Description	Example
Agency Name	Set an agency name. The agency name must be **apm_admin_trust**.	-
Agency Type	Select **Cloud service**.	Cloud service

Parameter	Description	Example
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