Application Performance Management

FAQs

Date  2019-05-18
# Contents

## 1 Consultation FAQs
- 1.1 What Is the Billing Policy of APM? .......................... 1
- 1.2 What Are Apmex and an Apdex Threshold? ............. 1
- 1.3 How Do I Distinguish Between Alarms and Events? ... 3
- 1.4 Why Does the Number of GC Times in JVM Monitoring Data Contain Decimals? 3

## 2 Usage FAQs
- 2.1 How Do I Obtain the AK/SK and Project ID? .......... 4
- 2.2 How Do I Obtain the AK/SK by Creating an Agency? ... 6
- 2.3 What Do I Do If No Data Is Found or the Data Is Abnormal? 8
- 2.4 How Do I Connect APM to a Non-Web Program? .... 9
- 2.5 How Is the Time Line of the Call Chain Drawn? 10
- 2.6 How Does APM Collect Probe Data? .......................... 11
- 2.7 How Does APM Collect Mesh Data? .......................... 14
- 2.8 How Do I Calculate the Number of Used Instances? ... 16
- 2.9 How Do I Connect the JBoss Server in Standalone Mode to APM? 17
- 2.10 Why Can I Not Find Logs Using TraceID? ................. 18
- 2.11 How Do I Deploy APM Probes in CCE Containers? ... 18
- 2.12 What Can I Do If the SSH Tunnel Process Is Abnormal? 18
1 Consultation FAQs

1.1 What Is the Billing Policy of APM?

Application Performance Management (APM) usage is billed based on a pay-per-use or package basis. For details, see Product Pricing Details. When you have purchased a package and exhausted the instances of the package, pay-per-use rates will be incurred. If you use APM without purchasing any package, all instances are billed on a pay-per-use basis.

1.2 What Are Apdex and an Apdex Threshold?

Application Performance Index (Apdex) is an open standard developed by the Apdex alliance. It defines a standard method to measure application performance. The Apdex standard converts the application response time into user satisfaction with application performance in the range of 0 to 1.

**Apdex Principles**

An Apdex threshold is the optimal threshold for the application response time based on the application performance evaluation. Three kinds of performance are defined as follows according to the Apdex threshold and the actual application response time.

**Satisfied:** The application response time is less than or equal to the Apdex threshold. For example, if the Apdex threshold is 1.5 seconds and the response time is 1 second, the result is satisfied.

**Tolerating:** The application response time is greater than the Apdex threshold and less than or equal to 4 times of the Apdex threshold. For example, if the Apdex threshold is 1 second, the tolerable upper threshold for the application response time is 4 seconds (4 x 1 second).

**Frustrated:** The application response time is greater than 4 times of the Apdex threshold.
Apdex Calculation Method

In APM, Apdex threshold is the value of Configuring Thresholds, and the application response latency is the service latency. The value of Apdex ranges from 0 to 1 and is calculated as follows:

\[ \text{Apdex} = \frac{\text{Satisfactory sample} + \text{Acceptable sample} \times 0.5}{\text{Total number of samples}} \]

Apdex calculation results indicate application performance status, that is, user satisfaction with application performance. Apdex results are marked by different colors. For details, see Table 1-1.

Table 1-1 Apdex values

<table>
<thead>
<tr>
<th>Apdex Value</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.75 ≤ Apdex ≤ 1</td>
<td>Green</td>
<td>Applications, instances, or transactions respond quickly when they are called. User satisfaction: high.</td>
</tr>
<tr>
<td>0.3 ≤ Apdex &lt; 0.75</td>
<td>Yellow</td>
<td>Applications, instances, or transactions respond slowly when they are called. User satisfaction: medium.</td>
</tr>
<tr>
<td>0 ≤ Apdex &lt; 0.3</td>
<td>Red</td>
<td>Applications, instances, or transactions respond extremely slowly when they are called. User satisfaction: low.</td>
</tr>
</tbody>
</table>

Example
Configuring an Apdex Threshold

You can configure the Apdex threshold based on your service requirements. For details, see Configuring Thresholds.

1.3 How Do I Distinguish Between Alarms and Events?

Similarities Between Alarms and Events

In the APM, the alarms and events refer to the information reported to the APM after the status of the APM changes.

Differences Between Alarms and Events

- Alarms are reported when the APM is abnormal or may cause errors. In this case, you need to take measures to fix errors. Otherwise, service exceptions may occur due to abnormal functions of the APM.
- Events are used to tell you that the status of the APM changes, but may not cause service exceptions. Events are mainly used to deliver important information. You do not need to handle events.

1.4 Why Does the Number of GC Times in JVM Monitoring Data Contain Decimals?

The number of Garbage Collection (GC) times is calculated based on the average value. Therefore, decimals may be contained. The GC duration is in the unit of ms.
2 Usage FAQs

2.1 How Do I Obtain the AK/SK and Project ID?

NOTE

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: key used together with the AK to sign requests. The AK and SK can identify senders and prevent requests from being altered.

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 2-1.
**Step 3**  On the **Account Info** page, click **Manage**.

**Figure 2-2** Basic information

**Account Info**

- User Name: 
- Email Address: 
- Mobile Number: 138****8976
- Password: ********
- Authentication information: Authenticated as individual user
- Security Credentials: 

**Step 4**  Obtain the project ID and AK/SK.

1. Obtain the project ID.
   
   On the **Project List** tab page, view the project ID.

**Figure 2-3** Projects

<table>
<thead>
<tr>
<th>Region</th>
<th>Project</th>
<th>Project ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Obtain the AK/SK.

   a. On the **Access Keys** tab page, click **Add Access Key** to create an access key.
2.2 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 2-5.

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 2-1.

Table 2-1 Creating an agency

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency Name</td>
<td>Set the agency name.</td>
<td>aom_ecm_trust</td>
</tr>
<tr>
<td>Agency Type</td>
<td>Select <strong>Cloud service</strong>.</td>
<td>-</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Cloud Service</td>
<td>Select ECS BMS.</td>
<td>-</td>
</tr>
<tr>
<td>Validity Period</td>
<td>Select Permanent.</td>
<td>-</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Provide detailed information about the agency.</td>
<td>-</td>
</tr>
</tbody>
</table>

--- End

### Setting Permissions

**Step 1** In the Permissions area, click Modify in the row of the current region. The Modify Policy page is displayed.

**Step 2** For Available Policies, enter APM in the search box on the left and select APM Administrator in the search result. In this way, Application Performance Management (APM) policies are synchronized to the Selected Policies area on the right.

**Step 3** Click OK. The agency relationship is successfully created.

--- End

### Making an Agency Effective

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

**Step 2** Click the Elastic Cloud Server (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 2-6.
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 2-7. Set other parameters and click Submit.

2.3 What Do I Do If No Data Is Found or the Data Is Abnormal?

Problem Symptoms

Sometimes, when the topology and call chain of an application are queried on the GUI, the data failed to be queried or the queried data is abnormal.

Time Inconsistency

Application data is collected by ICAgent from the ECS and reported to the browser interface. If the browser time and time zone are inconsistent with the time and time zone of the ECS, the
preceding problem may occur. For example, if the browser time is 7:00 and the ECS time is 6:00, the latest data cannot be queried on the browser because the server does not have the 6:00 – 7:00 data. Similarly, for distributed applications deployed on multiple ECSs, if the time between the ECSs is inconsistent, data cannot be linked. As a result, an exception occurs during data handling by ICAgent and abnormal data is displayed during data query.

Therefore, ensure that the time between servers and between the browser and the server is consistent before installing ICAgent. **Installing ICAgent**

### 2.4 How Do I Connect APM to a Non-Web Program?

Non-web programs do not have any exposed APIs and therefore, they cannot be accessed externally. Generally, they are Java processes which are responsible for implementing scheduled tasks.

**Operation**

Application Performance Management (APM) can connect to non-web programs, and collect and display their data. To connect APM to non-web programs, do as follows:

- For the non-web programs that are deployed through Cloud Container Engine (CCE), see **CCE Mode**.
- For the non-web programs that are deployed on Elastic Cloud Server (ECS) or Bare Metal Server (BMS) but not through CCE, see **VM Mode**.

**CCE Mode**

**CCE** provides container application management services. When you create or upgrade a non-web program, set environment variables and select the probe according to the following figures. In this way, the APM probe is installed in the non-web program. After starting the program for about 3 minutes, log in to the APM console to view the program status on the **Topology** and **Transactions** pages.

**Figure 2-8 Setting environment variables**

![Figure 2-8 Setting environment variables]

<table>
<thead>
<tr>
<th>Type</th>
<th>Variable Name</th>
<th>Variable/Variable Reference</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually Add</td>
<td>apm_export</td>
<td>test</td>
<td>Write</td>
</tr>
</tbody>
</table>

2019-05-18
VM Mode

To connect APM to non-web programs deployed on ECS or BMS, add the following configurations to the startup script:

```
-javaagent:/opt/oss/servicemgr/ICAgent/pinpoint/pinpoint-bootstrap.jar -
Dapm_application=Application name -Dapm_tier=Service name -Dapm_noport=true
```

After the configurations are added, start the program and then view the program data on the APM console.

For example, assume that the original startup script is as follows:

```
java -jar app.jar
```

If the application name is `vmall` and the service name is `vmall-product-service`, the modified startup script will be as follows:

```
java -javaagent:/opt/oss/servicemgr/ICAgent/pinpoint/pinpoint-bootstrap.jar -
Dapm_application=vmall -Dapm_tier=vmall-product-service -Dapm_noport=true -jar app.jar
```

2.5 How Is the Time Line of the Call Chain Drawn?

Problem Symptoms

How is the time line of the call chain drawn? When the time lines of the call chain are drawn as shown in the following figure, are they drawn incorrectly?

Problem Resolving

The time line of each method indicates the start position and total duration of the method. On the call chain page, a time line is drawn in gray, and the part of the duration of each method is
filled with green. The part filled with green indicates the total duration. You may be confused about the call chain shown in the preceding figure. The time lines of methods 1 and 2 partially overlap, and the last part of each time line is not green.

Actually, the time lines are drawn correctly. Normally, they should be drawn as shown in the following figure. However, for the call chain in APM, the time line of each method indicates the start position and total duration of the method. Therefore, the time lines are drawn as described in the problem symptoms.

2.6 How Does APM Collect Probe Data?

Collecting Data

Application Performance Management (APM) collects application data through probes. Probes use the bytecode enhancement technology to track resources and generate call data. The ICAgent obtains and processes the call data. Then, the data is reported to and displayed on APM. The procedure is as follows:
Collected Data

APM collects service tracing data, resource information, resource attributes, memory detection information, and call request metrics, but does not collect your personal data. The collected data is used only for performance analysis and fault diagnosis. It is not used for commercial purposes. The following table lists the details.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Collected Data</th>
<th>Transmission Mode</th>
<th>Storage Mode</th>
<th>Data Purpose</th>
<th>Storage Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracing</td>
<td>Tracing span data</td>
<td>Transmission through HTTPS encryption and Access Key ID/Secret Access Key (AK/SK)</td>
<td>Project-based isolated storage</td>
<td>Query and display at the tracing frontend</td>
<td>Configurable (7 days at most). The data will be deleted upon expiration.</td>
</tr>
</tbody>
</table>

Server

APM console

Report data to console.

ICA\textit{g}ent

Obtain data

Java application

Probe

APM collects service tracing data, resource information, resource attributes, memory detection information, and call request metrics, but does not collect your personal data. The collected data is used only for performance analysis and fault diagnosis. It is not used for commercial purposes. The following table lists the details.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Collected Data</th>
<th>Transmission Mode</th>
<th>Storage Mode</th>
<th>Data Purpose</th>
<th>Storage Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracing</td>
<td>Tracing span data</td>
<td>Transmission through HTTPS encryption and Access Key ID/Secret Access Key (AK/SK)</td>
<td>Project-based isolated storage</td>
<td>Query and display at the tracing frontend</td>
<td>Configurable (7 days at most). The data will be deleted upon expiration.</td>
</tr>
</tbody>
</table>
### Call request metrics
- Call initiator address, receiver address, API, duration, and status
- Transmission through HTTPS encryption and AK/SK authentication
- Project-based isolated storage
- Calculation of transaction call metrics, such as the throughput, TP99 latency, average latency, and error calls, drawing of application topologies, and display at the frontend
- 7 days. The data will be deleted upon expiration.

### Resource data
- Service type, service name, creation time, deletion time, node address, and service release API
- Transmission through HTTPS encryption and AK/SK authentication
- Project-based isolated storage
- Query and display at the resource library frontend
- 7 days. The data will be deleted upon expiration.

### Resource attributes
- System type, system startup event, number of CPUs, service executor, service process ID, service pod ID, CPU label, system version, web framework, JVM version, time zone, system name, collector version, and LastMail URL
- Transmission through HTTPS encryption and AK/SK authentication
- Project-based isolated storage
- Query and display at the resource library frontend
- 7 days. The data will be deleted upon expiration.

### Memory detection data
- Memory usage, used memory, maximum memory, remaining memory, memory threshold-crossing time, and memory detection configurations
- Transmission through HTTPS encryption and AK/SK authentication
- Project-based isolated storage
- Query and display at the resource library frontend
- 7 days. The data will be deleted upon expiration.

---

**APM Resource Overhead**

For each probe, the CPU usage is **less than 5%** and used memory is **less than 50 MB**.
2.7 How Does APM Collect Mesh Data?

**Collecting Data**

Application Performance Management (APM) collects application data through the Istio mesh. The Istio mesh obtains input and output data of applications in non-intrusive mode. Specifically, the Istio mixer of Cloud Container Engine (CCE) obtains and processes service tracing data and call request KPI data while the ICAgent obtains and processes resource data. Then, all the data is reported to and displayed on APM. The procedure is as follows:

![Diagram of APM data collection](image)

**Collected Data**

APM collects the service tracing data, resource data, and call request KPI data, but does not collect any privacy data. The collected data is used only for APM performance analysis and fault diagnosis, and is not used for any commercial purposes. The data collection scopes and purposes are as follows:

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Collected Data</th>
<th>Transmission Mode</th>
<th>Storage Mode</th>
<th>Data Purpose</th>
<th>Storage Period</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Diagram Image*

*Diagram Image Description*
<table>
<thead>
<tr>
<th>Tracing data</th>
<th>Tracing span data</th>
<th>HTTPS encryption and Access Key ID/Secret Access Key (AK/SK) authentication for transmission</th>
<th>Project-based isolated storage</th>
<th>Query and display in the tracing foreground</th>
<th>Configurable. The maximum storage period is 7 days. When this period expires, the data is permanently deleted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call request KPI data</td>
<td>Call initiator address, call receiver address, call API, call duration, and call status</td>
<td>HTTPS encryption and AK/SK authentication for transmission</td>
<td>Project-based isolated storage</td>
<td>Calculation of transaction call KPI metrics, such as the throughput, TP99 latency, average latency, or number of call failures; drawing of application topologies; display in the foreground</td>
<td>7 days. When this period expires, the data is permanently deleted.</td>
</tr>
<tr>
<td>Resource data</td>
<td>Service type, service name, creation time, deletion time, node address, and service release API</td>
<td>HTTPS encryption and AK/SK authentication for transmission</td>
<td>Project-based isolated storage</td>
<td>Query and display in the resource library foreground</td>
<td>7 days. When this period expires, the data is permanently deleted.</td>
</tr>
</tbody>
</table>
2.8 How Do I Calculate the Number of Used Instances?

In Application Performance Management (APM), the number of used instances is calculated based on the number of probes. One probe corresponds to one service instance. You can obtain the number of used instances by calculating the number of probes. Note that the instances listed in Figure 2-10 do not use probes to report data and need to be excluded. The formula is as follows:

Number of used instances (equals to that of probes) = Total number of instances on the application topology page – Number of instances that do not use probes

**Figure 2-10** Instances that do not use probes

Example of calculating the number of used instances

<table>
<thead>
<tr>
<th>Demo (Non-real ...</th>
<th>Tolerating</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 Transactions</td>
<td></td>
</tr>
<tr>
<td>5 Applications</td>
<td></td>
</tr>
<tr>
<td>5 Instances</td>
<td></td>
</tr>
</tbody>
</table>
In the preceding figure, there are five instances, one of which is the MySQL database. 
Number of used instances (equals to that of probes) = 5 - 1 = 4

2.9 How Do I Connect the JBoss Server in Standalone Mode to APM?

Application Performance Management (APM) supports JBoss servers. When using JAVA probes on JBoss servers, you need to make some special configurations.

The following describes how to connect JBoss 6.2.0, JBoss 8.1.0, and JBoss 12.0.0 in standalone mode to APM. For other JBoss versions, the connection process is similar.

1. JBoss 6.2.0:
   Modify the eap-6.2.0.Final/bin/standalone.conf file of the JBoss server in standalone mode as follows:
   
   JAVA_OPTS=-Djava.util.logging.manager=org.jboss.logmanager.LogManager
   JAVA_OPTS=-javaagent:/paas-apm/collectors/pinpoint/pinpoint-bootstrap.jar
   JAVA_OPTS=-Djboss.modules.system.pkgs=$JBOSS_MODULES_SYSTEM_PKGS -Djava.awt.headless=true
   JAVA_OPTS=-Djava.net.preferIPv4Stack=true

2. JBoss 8.1.0:
   Modify the wildfly-8.1.0.Final/bin/standalone.conf file of the JBoss server in standalone mode as follows:

   JBOSS_MODULES_SYSTEM_PKGS="org.jboss.byteman,org.jboss.logmanager,com.navercorp.pinpoint.bootstrap,com.navercorp.pinpoint.common,com.navercorp.pinpoint.exception"
   JAVA_OPTS=-Xbootclasspath/p:$JBOSS_HOME/modules/system/layers/base/org/jboss/log4j/logmanager/main/slf4j-api-1.7.2.jbossorg-1.jar
   JAVA_OPTS=-Xbootclasspath/p:$JBOSS_HOME/modules/system/layers/base/org/slf4j/main/slf4j-api-1.7.22.jbossorg-1.jar
   JAVA_OPTS=-Xbootclasspath/p:$JBOSS_HOME/modules/system/layers/base/org/jboss/logmanager/main/jboss-logmanager-1.5.2.Final.jar
   JAVA_OPTS=-Djava.util.logging.manager=org.jboss.logmanager.LogManager
   JAVA_OPTS=-Djboss.modules.system.pkgs=$JBOSS_MODULES_SYSTEM_PKGS -Djava.awt.headless=true

3. JBoss 12.0.0:
   Modify the wildfly-12.0.0.Final/bin/standalone.conf file of the JBoss server in standalone mode as follows:

   JBOSS_MODULES_SYSTEM_PKGS="org.jboss.byteman,org.jboss.logmanager,com.navercorp.pinpoint.bootstrap,com.navercorp.pinpoint.common,com.navercorp.pinpoint.exception,$JBOSS_MODULES_SYSTEM_PKGS"
   JAVA_OPTS=-Djava.util.logging.manager=org.jboss.logmanager.LogManager
   JAVA_OPTS=-Djboss.modules.system.pkgs=$JBOSS_MODULES_SYSTEM_PKGS -Djava.awt.headless=true
JBoss uses the undertow as the application service. Therefore, the management parameter in the `wildfly-12.0.0.Final/bin/standalone.sh -bmanagement 127.0.0.1` command cannot be set to `0.0.0.0`. Otherwise, an exception occurs. The error information is as follows:

```
java.net.SocketException: Protocol family unavailable
```

### 2.10 Why Can I Not Find Logs Using TraceID?

TraceID is used to uniquely identify a tracing. After this identification, the system adds TraceID to your log files. You can use TraceID to accurately search for tracing logs. TraceID is enabled when configuring ICAgent. Why can I not find logs using TraceID on the search log page?

Check whether the log component uses log4j. For details, see [log4j](#). Check whether the output log contains a trace name, as shown in the following figure.

### 2.11 How Do I Deploy APM Probes in CCE Containers?

You can deploy Application Performance Management (APM) probes in Cloud Container Engine (CCE) containers as follows:

- If you have not created workloads, select Java probes when creating workloads.
- If you have created workloads, select Java probes and restart instances on the Workload O&M page of CCE.

### 2.12 What Can I Do If the SSH Tunnel Process Is Abnormal?

In the hybrid cloud scenario, the Secure Shell (SSH) tunnel process becomes abnormal when monitoring data is forwarded to Application Performance Management (APM) through a jump server. To solve the problem, do as follows:

**Step 1** Log in to the jump server using a remote login tool.

**Step 2** Run the following command to configure interaction-free login:

```
ssh-keygen
cd /root/.ssh/
cat id_rsa.pub > authorized_keys
vi /etc/ssh/sshd_config
```

Set the value of **PubkeyAuthentication** to **yes**.

```
service sshd restart
```

**Step 3** Obtain the `checkSsh.sh` script, modify the configuration, and set the permission.

1. Obtain the script.

   Click [Download](#) to obtain the `checkSsh.sh` script, or contact technical support.
2. Set the permission.
   chmod +x checkSsh.sh

3. Execute the `checkSsh.sh` script.
   
   **NOTE**
   - In the following commands, replace `{Jump server IP address}`, `{ELB IP address}`, and `{region}` with the actual values.
   - If the jump server runs Ubuntu or Debian, run the `sudo dpkg-reconfigure dash` command and select NO before running the `checkSsh.sh` script.
   ```
   sh checkSsh.sh "ssh -f -N -L {Jump server IP address}:8149:{ELB IP address}:8149 -L {Jump server IP address}:8102:{ELB IP address}:8102 -L {Jump server IP address}:8923:{ELB IP address}:8923 -L {Jump server IP address}:30200:{ELB IP address}:30200 -L {Jump server IP address}:30201:{ELB IP address}:30201 -L {Jump server IP address}:80:icagent-{region}.obs.{region}.myhuaweicloud.com:80 {Jump server IP address}"
   ```

Step 4  Configure the `crontab` command and run it periodically.

   ```
crontab -e
*/10 * * * * /home/tools/checkSsh.sh ssh -f -N -L {Jump server IP address}:8149:{ELB IP address}:8149 -L {Jump server IP address}:8102:{ELB IP address}:8102 -L {Jump server IP address}:8923:{ELB IP address}:8923 -L {Jump server IP address}:30200:{ELB IP address}:30200 -L {Jump server IP address}:30201:{ELB IP address}:30201 -L {Jump server IP address}:80:icagent-{region}.obs.{region}.myhuaweicloud.com:80 {Jump server IP address}
cron restart
```

**NOTE**
- In the preceding command, the `/home/tools/checkSsh.sh` directory is used as an example. Replace it with an actual directory.
- 10 indicates that the command is run every 10 minutes. You can change the value as required.

----End