Application Performance Management

FAQs

Issue 01

Date 2024-03-05

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 General FAQs.. 1

2 Consultation FAQs.. 2

2.1 What Is the Billing Policy of APM?...2

2.2 What Are the Apdex and Apdex Threshold?..2

2.3 How Do I Distinguish Between Alarms and Events?.. 4

2.4 Why Does the Number of GC Times in JVM Monitoring Data Contain Decimals?........... 4

3 Usage FAQs.. 5

3.1 How Do I Obtain the AK/SK and Project ID?...5

3.2 How Do I Obtain the AK/SK by Creating an Agency?.. 6

3.3 What Can I Do If No Data Is Found or the Data Is Abnormal?.. 9

3.4 How Do I Connect APM to Non-Web Programs?.. 9

3.5 How Are Tracing Time Lines Drawn?.. 11

3.6 How Does APM Collect Probe Data?... 12

3.7 How Does APM Collect Mesh Data?...15

3.8 How Do I Calculate the Number of Used Instances?...17

3.9 How Do I Connect the JBoss Server in Standalone Mode to APM?..................................19

3.10 What Can I Do If I Cannot Search for Logs Based on Trace IDs?................................... 20

3.11 How Do I Deploy APM Probes in CCE Containers?..20

3.12 What Can I Do If the SSH Tunnel Process Is Abnormal?..20

3.13 How Can I Do If No Topology or Data Is Displayed After the ICAgent and Java Probes Are Installed?
....21

3.14 Why Are Tomcat Thread Metrics Not Displayed on the JVM Monitoring Page?.............22

3.15 Why Is the Allocated Memory Greater Than the Preset Maximum Memory on the JVM Monitoring Page?.. 22

3.16 How Do I Determine Whether an ICAgent Has Been Bound in CCE?............................. 23

1 General FAQs

Do APM Collection Probes Consume a Lot of Server Resources?

APM collects performance metrics, including tracing, SLA, SQL statement call, and JVM metrics.

Resource consumption: is closely related to the number of APM probes, number of inter-service call times, and sampling ratio.

Suggestion: Use a maximum of 20 APM probes on a single node.

2 Consultation FAQs

2.1 What Is the Billing Policy of APM?

APM supports both pay-per-use and package billing. For more information, see **APM Pricing Details**. The two billing modes can be used at the same time. If you use more instances than those included in a package, you will be billed on a pay-per-use basis for the excess instances used. If you use APM without purchasing any package, you will be billed on a pay-per-use basis for all instances.

2.2 What Are the Apdex and Apdex Threshold?

Application Performance Index (Apdex) is an open standard developed by the Apdex alliance to measure application performance. The application response time is converted into user satisfaction with application performance. The Apdex value ranges from 0 to 1.

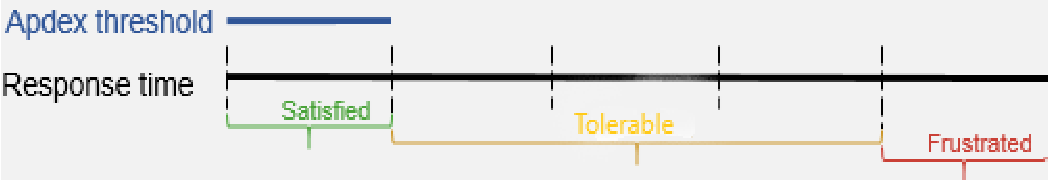
Apdex Principles

An Apdex threshold is the optimal threshold for the application response time. Based on the Apdex threshold and actual application response time, there are the following three kinds of performance:

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

Tolerable: The actual application response time is greater than the Apdex threshold, but less than or equal to 4 times of the Apdex threshold. For example, if the Apdex threshold is 1s, the tolerable upper threshold for the application response time is 4s (4 x 1s).

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



Apdex Calculation Method

In Application Performance Management (APM), the Apdex threshold is the threshold configured according to **Setting Apdex Thresholds**, and the application response latency is the service latency. The Apdex value ranges from 0 to 1 and is calculated as follows:

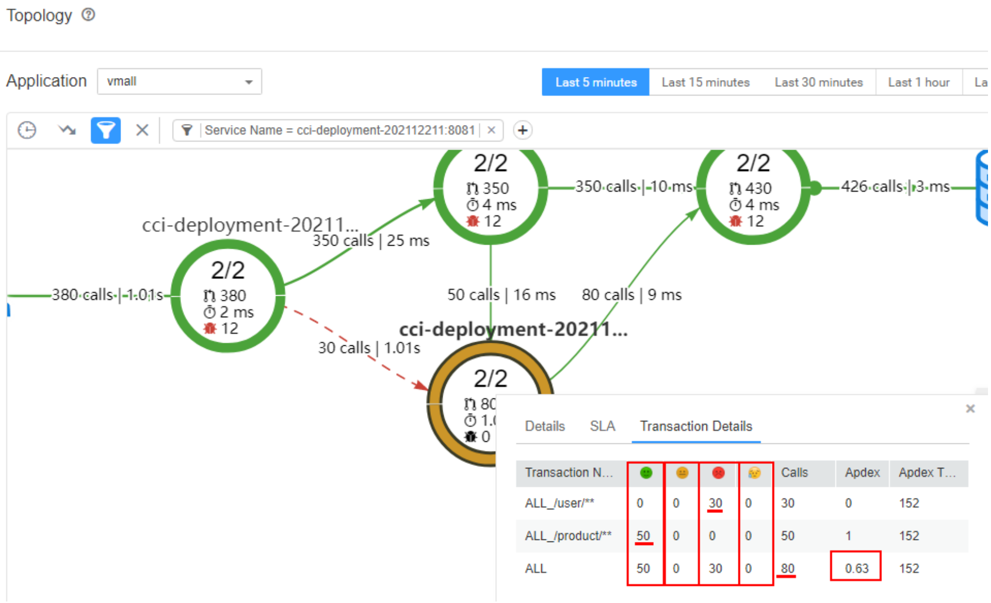
Apdex = (Satisfied samples x 1 + Tolerable samples x 0.5 + Frustrated samples x 0)/Total number of samples

Apdex calculation results indicate application performance status, that is, user satisfaction with application performance. Different colors indicate different Apdex ranges. For details, see **Table 2-1**.

Table 2-1 Apdex description

Apdex Value	Color	Description
0.75 ≤ Apdex ≤ 1	Green	Fast response; good user experience
0.3 ≤ Apdex < 0.75	Yellow	Slow response; fair user experience
0 ≤ Apdex < 0.3	Red	Very slow response; poor user experience
-	Gray	No application, instance, or transaction is invoked.

Example



Transaction N...	🙂	😐	☹	😢	Calls	Apdex	Apdex T...
ALL_/user/**	0	0	30	0	30	0	152
ALL_/product/**	50	0	0	0	50	1	152
ALL	50	0	30	0	80	0.63	152

As shown in the preceding figure, the number of satisfied calls is 50, the number of tolerable calls is 0, the number of frustrated calls is 30, and the number of error calls is 0. There are 80 calls in total.

According to the formula:

Apdex = (Satisfied samples x 1 + Tolerable samples x 0.5 + Frustrated samples x 0)/Total number of samples

Apdex = (50 x 1 + 0 x 0.5 + 30 x 0)/80 = 0.63

Configuring an Apdex Threshold

You can configure the Apdex threshold as required. For details, see **Setting Apdex Thresholds**.

2.3 How Do I Distinguish Between Alarms and Events?

Similarities Between Alarms and Events

For Application Performance Management (APM), both alarms and events refer to the information reported to APM when its status changes.

Differences Between Alarms and Events

- Alarms are reported when APM is abnormal or may cause errors. You need to handle alarms. Otherwise, service exceptions may occur.
- Events carry some important information, informing you of the changes of APM itself. Such changes do not necessarily cause exceptions. You do not need to handle events.

2.4 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.

3 Usage FAQs

3.1 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.

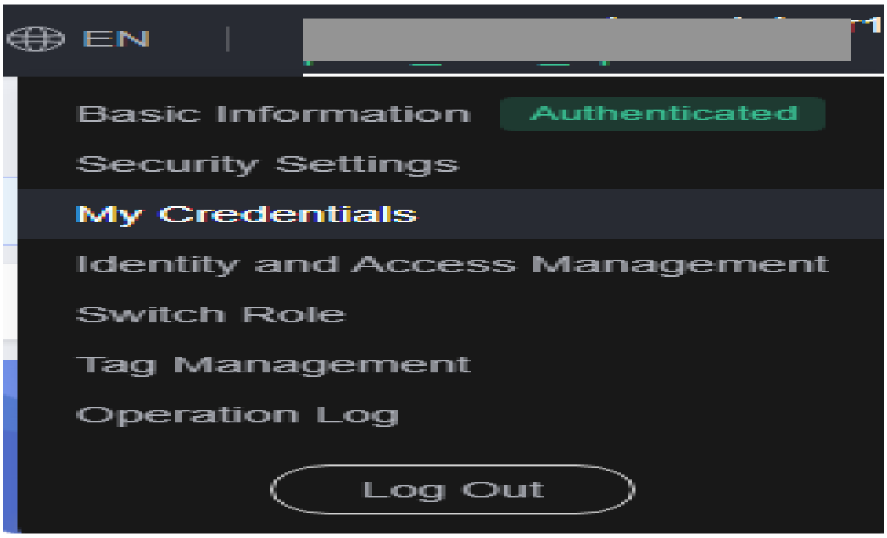
- AK: unique ID associated with the SK. It is used together with the SK to sign requests.
- SK: key used together with the AK to sign requests. The AK and SK can identify senders and prevent requests from being altered.

Procedure

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

Step 2 Click the username in the upper right corner, as shown in **Figure 3-1**. Then choose **My Credentials**.

Figure 3-1 Username

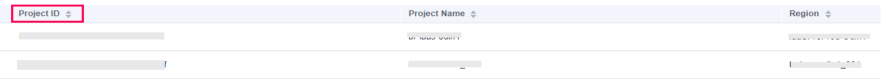


Step 3 Obtain the project ID and AK/SK.

1. Obtain the project ID.

   In the navigation pane on the left, choose **API Credentials**. On the displayed page, view the project ID in the **Project ID** column.

   Figure 3-2 Projects

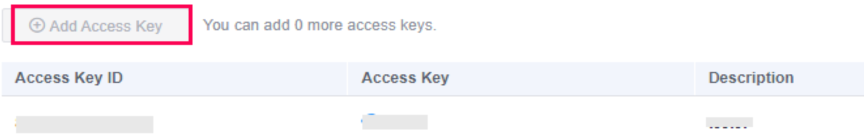
Project ID	Project Name	Region
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

2. Obtain the AK/SK.

   a. In the navigation pane on the left, choose **Access Keys**.

   b. On the displayed page, click **Add Access Key** to create an access key.

   Figure 3-3 Managing access keys

   You can add 0 more access keys.

Access Key ID	Access Key	Description
[redacted]	[redacted]	[redacted]

   c. Enter a description (optional) and click **OK**.

   NOTE

   To ensure account security, change your AK/SK pairs periodically and keep them safe.

----End

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

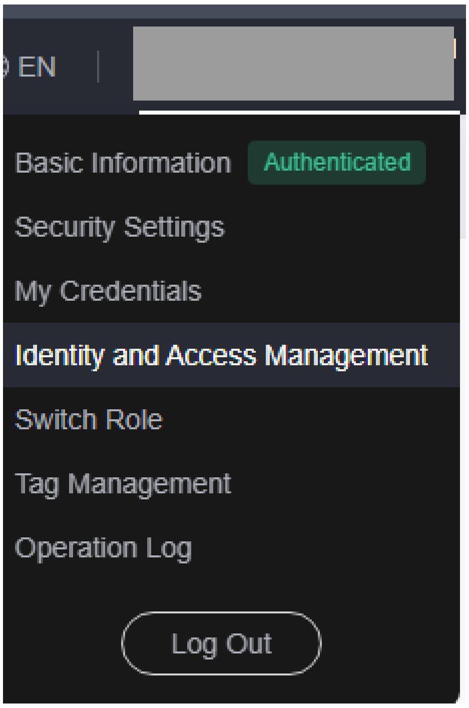
After you create an agency, the ICAgent automatically obtains the Access Key ID/ Secret Access Key (AK/SK), helping you manage application performance.

Creating an Agency

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

Step 2 Click the username in the upper right corner, as shown in **Figure 3-4**. Then choose **Identity and Access Management**.

Figure 3-4 Username



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

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

Step 5 Set parameters based on **Table 3-1**.

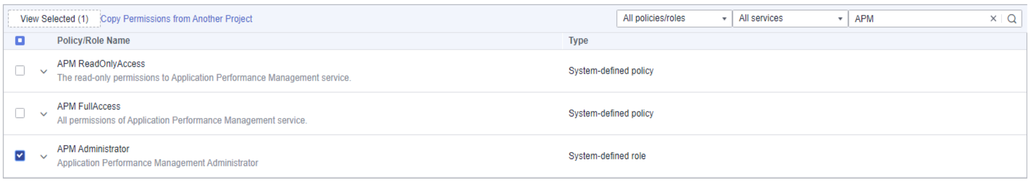
Table 3-1 Creating an agency

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

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

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

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



View Selected (1) Copy Permissions from Another Project | All policies/roles | All services | APM

■	Policy/Role Name	Type
□	APM ReadOnlyAccess The read-only permissions to Application Performance Management service.	System-defined policy
□	APM FullAccess All permissions of Application Performance Management service.	System-defined policy
☑	APM Administrator Application Performance Management Administrator	System-defined role

Step 8 Click **OK**.

----End

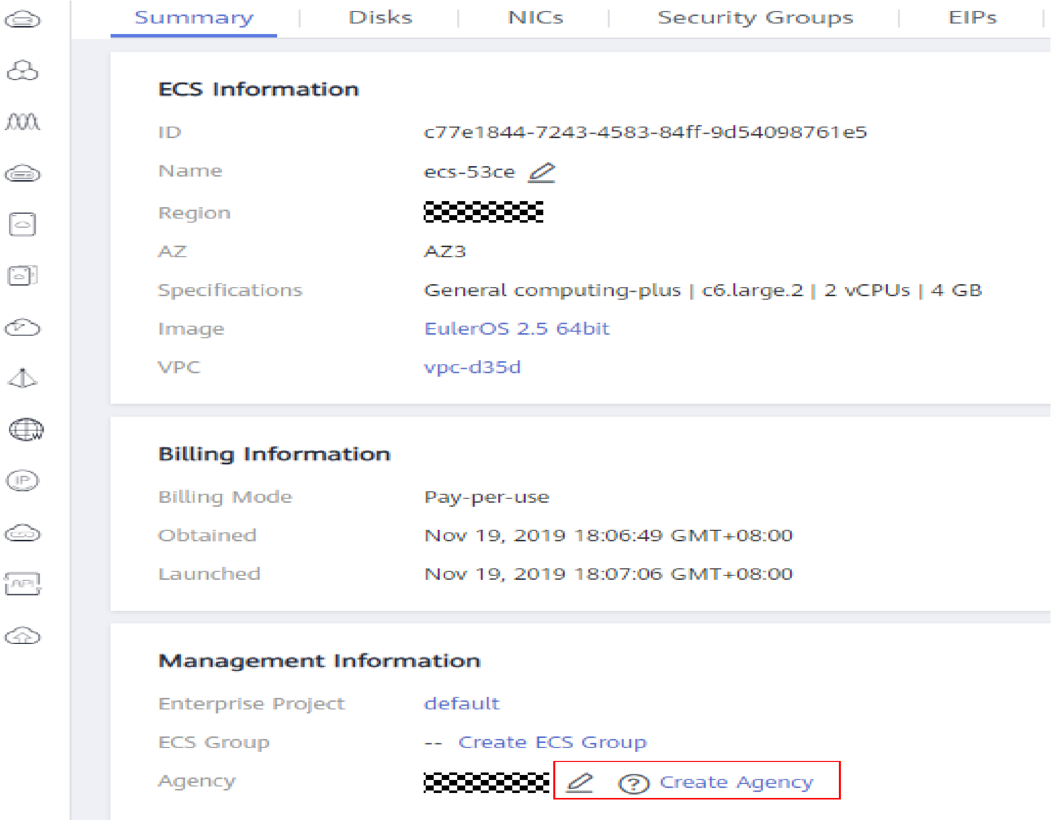
Making an Agency Effective

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

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

Step 3 Select the created agency from the **Agency** drop-down list, as shown in **Figure 3-5**.

Figure 3-5 Setting an agency



ECS Information

ID c77e1844-7243-4583-84ff-9d54098761e5
Name ecs-53ce
Region [redacted]
AZ AZ3
Specifications General computing-plus | c6.large.2 | 2 vCPUs | 4 GB
Image EulerOS 2.5 64bit
VPC vpc-d35d

Billing Information

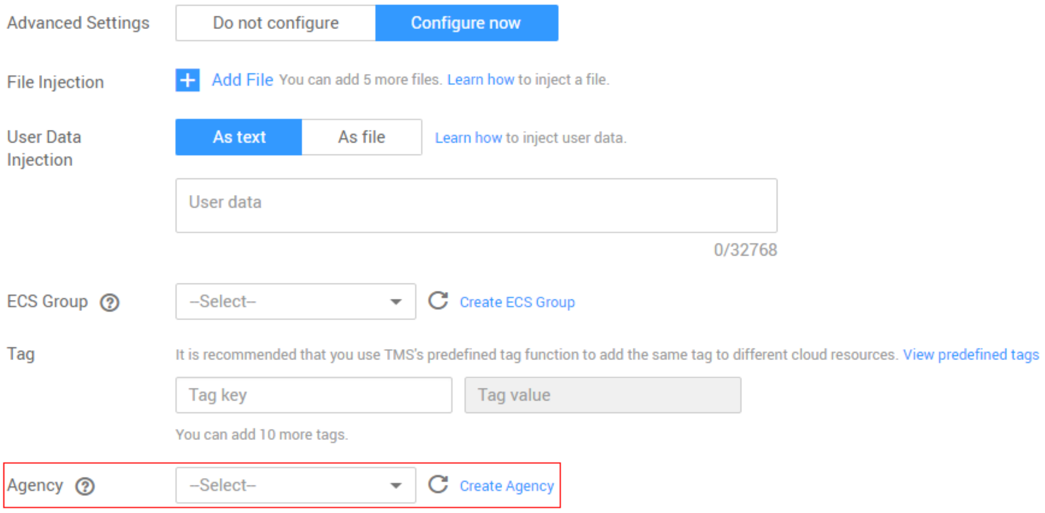
Billing Mode Pay-per-use
Obtained Nov 19, 2019 18:06:49 GMT+08:00
Launched Nov 19, 2019 18:07:06 GMT+08:00

Management Information

Enterprise Project default
ECS Group -- Create ECS Group
Agency [redacted] Create Agency

Step 4 (Optional) To set an agency for a newly purchased ECS, do as follows: On the **Buy ECS** page, set the value of **Advanced Settings** to **Configure now** and select the created agency from the **Agency** drop-down list, as shown in **Figure 3-6**. Set other parameters and click **Submit**.

Figure 3-6 Setting an agency



Advanced Settings: Do not configure | **Configure now**

File Injection: ＋ Add File You can add 5 more files. Learn how to inject a file.

User Data Injection: **As text** | As file Learn how to inject user data.

User data

0/32768

ECS Group ⓘ: --Select-- Create ECS Group

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

Tag key | Tag value

You can add 10 more tags.

Agency ⓘ: --Select-- Create Agency

----End

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

Symptom

When you query the topology and tracing data of an application on the Application Performance Management (APM) console, no data can be found or the data is abnormal. The cause may be as follows:

Cause: Time Inconsistency

Application data is collected by the ICAgent from the Elastic Cloud Server (ECS) and reported to the browser interface. If the time and time zone of the local browser are inconsistent with those 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 ECSs is inconsistent, data cannot be linked. As a result, an exception occurs during data handling by the ICAgent and abnormal data is displayed during data query.

Therefore, ensure that the time of the browser and ECSs is consistent before installing the ICAgent. For how to install the ICAgent, see **Installing the ICAgent (Linux)**.

3.4 How Do I Connect APM to Non-Web Programs?

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

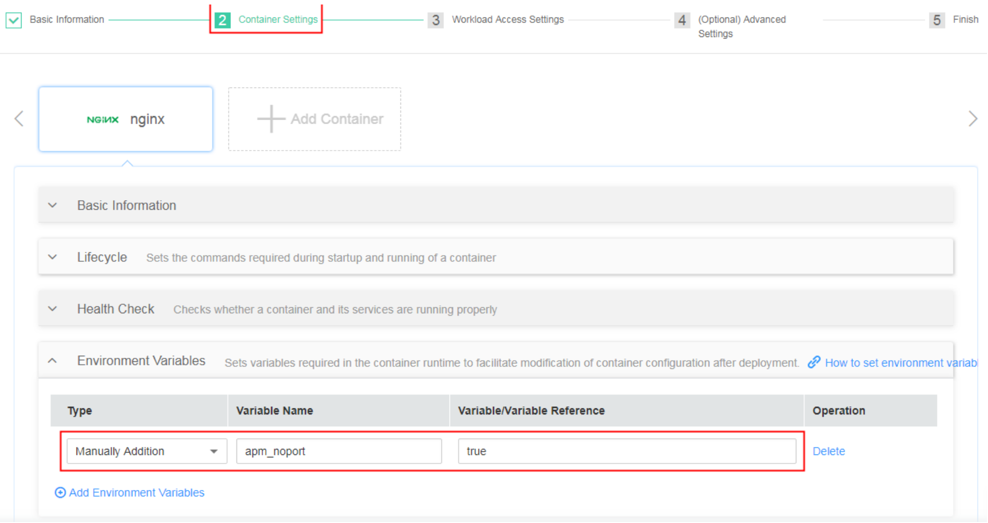
Application Performance Management (APM) can connect to non-web programs, and collect and display their data. To connect APM to non-web programs, do as follows:

- For non-web programs deployed through Cloud Container Engine (CCE), see **CCE Mode**.
- For non-web programs deployed on Elastic Cloud Server (ECS) or Bare Metal Server (BMS), see **VM Mode**.

CCE Mode

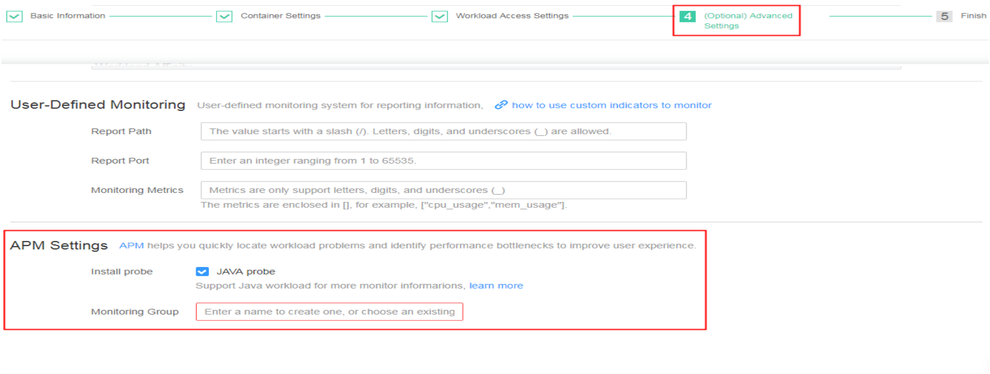
CCE provides containerized application management. When you create or upgrade a non-web program, set environment variables and select the probe according to the following figures so that it can be installed in the non-web program. Three minutes after you start the program, log in to the APM console to view the program status on the **Topology** and **Transactions** pages.

Figure 3-7 Setting environment variables


Basic Information
2 Container Settings
3 Workload Access Settings
4 (Optional) Advanced Settings
5 Finish
NGINX nginx
Add Container
Basic Information
Lifecycle Sets the commands required during startup and running of a container
Health Check Checks whether a container and its services are running properly
Environment Variables Sets variables required in the container runtime to facilitate modification of container configuration after deployment.
How to set environment variab
Add Environment Variables

Type	Variable Name	Variable/Variable Reference	Operation
Manually Addition	apm_noport	true	Delete

Figure 3-8 Selecting the probe


Basic Information
Container Settings
Workload Access Settings
4 (Optional) Advanced Settings
5 Finish
User-Defined Monitoring
User-defined monitoring system for reporting information,
how to use custom indicators to monitor
APM Settings

Report Path: The value starts with a slash (/). Letters, digits, and underscores (_) are allowed.

Report Port: Enter an integer ranging from 1 to 65535.

Monitoring Metrics: Metrics are only support letters, digits, and underscores (_)
The metrics are enclosed in [], for example, ["cpu_usage","mem_usage"].

APM helps you quickly locate workload problems and identify performance bottlenecks to improve user experience.

Install probe: ☑ JAVA probe
Support Java workload for more monitor informarions, learn more

Monitoring Group: Enter a name to create one, or choose an existing

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

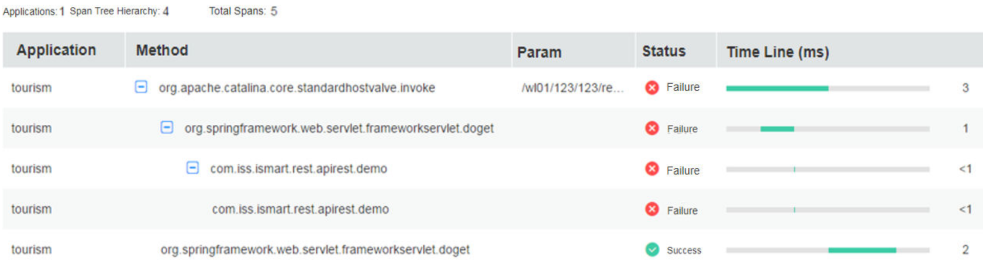
If the application name is **vmall** and the service name is **vmall-product-service**, the modified startup script will be as follows:

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

3.5 How Are Tracing Time Lines Drawn?

Symptom

If the following tracing time lines are displayed and you cannot determine whether they are correct, see the following description.

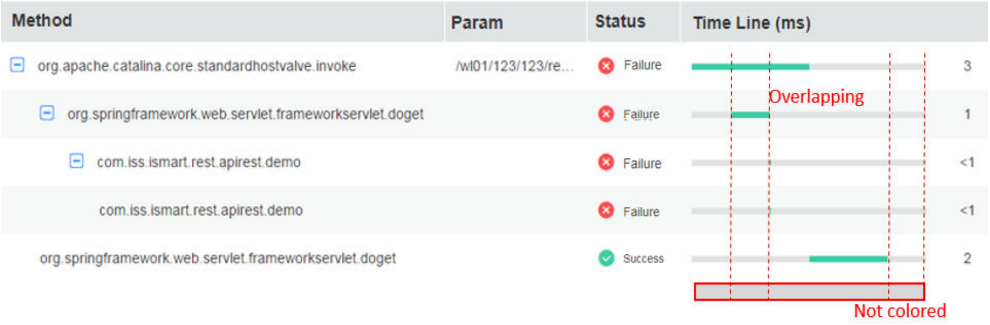


Applications: 1 Span Tree Hierarchy: 4 Total Spans: 5

Application	Method	Param	Status	Time Line (ms)
tourism	⊟ org.apache.catalina.core.standardhostvalve.invoke	/wl01/123/123/re...	✕ Failure	3
tourism	⊟ org.springframework.web.servlet.frameworkservlet.doget		✕ Failure	1
tourism	⊟ com.iss.ismart.rest.apirest.demo		✕ Failure	<1
tourism	com.iss.ismart.rest.apirest.demo		✕ Failure	<1
tourism	org.springframework.web.servlet.frameworkservlet.doget		✓ Success	2

Answer

The time line of each method indicates the start position and total duration of the method. On the tracing page, method lines are gray, and the time duration of each method is filled with green. The part filled with green indicates the total duration. 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.

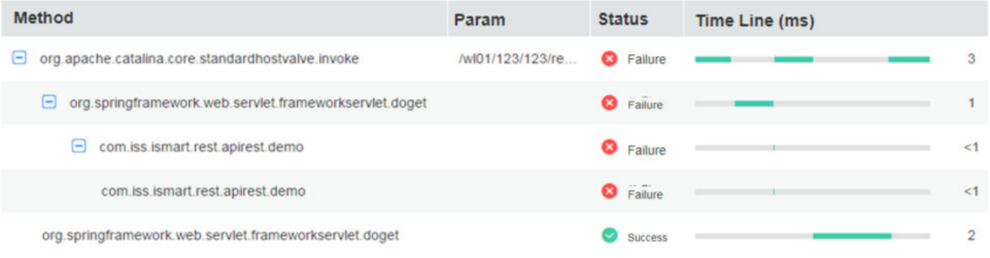


Method	Param	Status	Time Line (ms)	
⊟ org.apache.catalina.core.standardhostvalve.invoke	/wl01/123/123/re...	✕ Failure		3
⊟ org.springframework.web.servlet.frameworkservlet.doget		✕ Failure		1
⊟ com.iss.ismart.rest.apirest.demo		✕ Failure		<1
com.iss.ismart.rest.apirest.demo		✕ Failure		<1
org.springframework.web.servlet.frameworkservlet.doget		✓ Success		2

Overlapping

Not colored

The time lines are correct. Usually, they should be drawn as shown in the following figure. However, in Application Performance Management (APM), the time line of each method indicates the start position and total duration of the method. Therefore, the time lines are drawn as shown in the preceding figure.

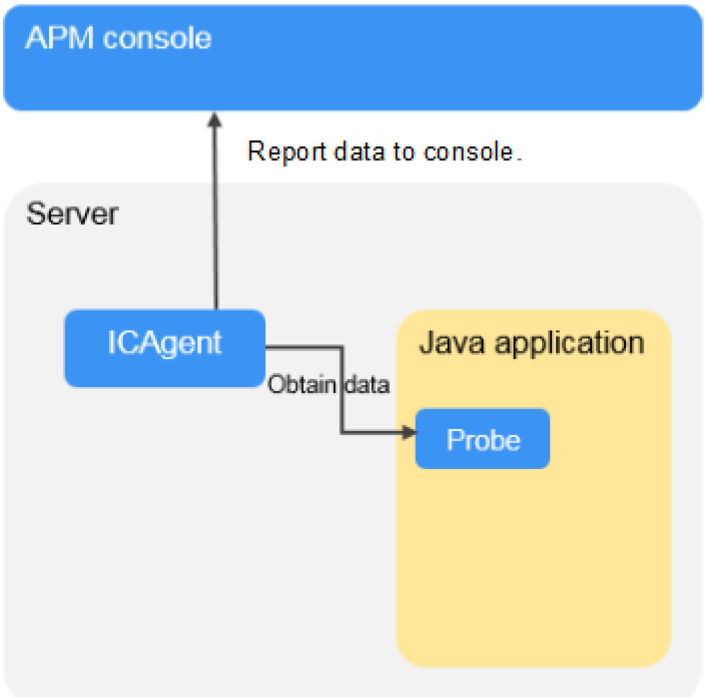


Method	Param	Status	Time Line (ms)	
⊟ org.apache.catalina.core.standardhostvalve.invoke	/wl01/123/123/re...	✕ Failure		3
⊟ org.springframework.web.servlet.frameworkservlet.doget		✕ Failure		1
⊟ com.iss.ismart.rest.apirest.demo		✕ Failure		<1
com.iss.ismart.rest.apirest.demo		✕ Failure		<1
org.springframework.web.servlet.frameworkservlet.doget		✓ Success		2

3.6 How Does APM Collect Probe Data?

Collecting Data

Application Performance Management (APM) collects application data through probes. Probes use the bytecode enhancement technology to trace resources and generate call data. The ICAgent obtains and processes the call data. Then, all 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 monitoring information, and call request KPI data, but does not collect your personal data. The collected data is used only for APM performance analysis and fault diagnosis, and is not used for any commercial purposes. The following table lists the details.

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

Call request KPI data	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 KPI metrics, such as 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 monitoring data	Memory usage, used memory, maximum memory, remaining memory, memory threshold-crossing time, and memory monitoring 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.

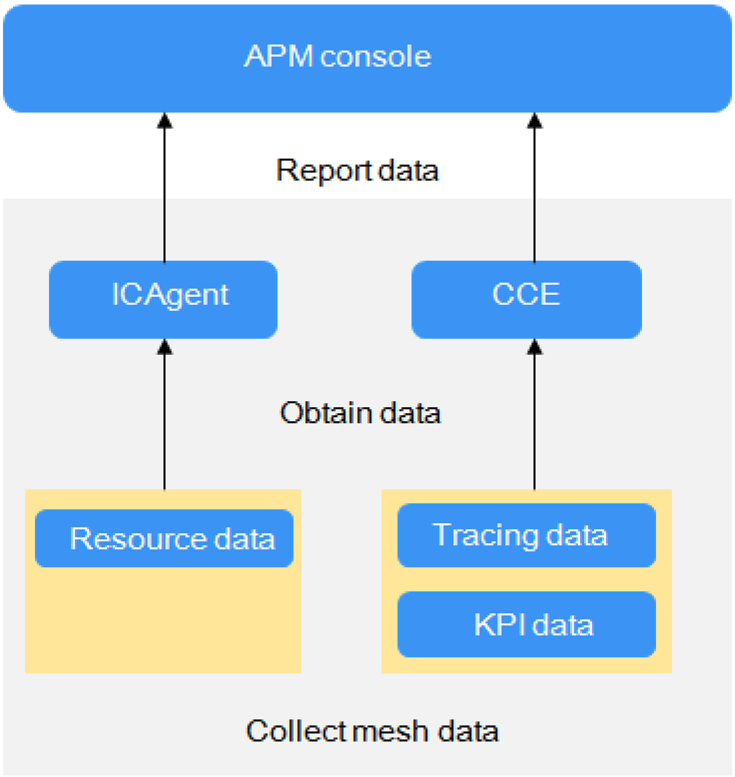
APM Resource Overhead

The CPU usage of each probe is **less than 5%** and used memory is about **250 MB**.

3.7 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:



Collected Data

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

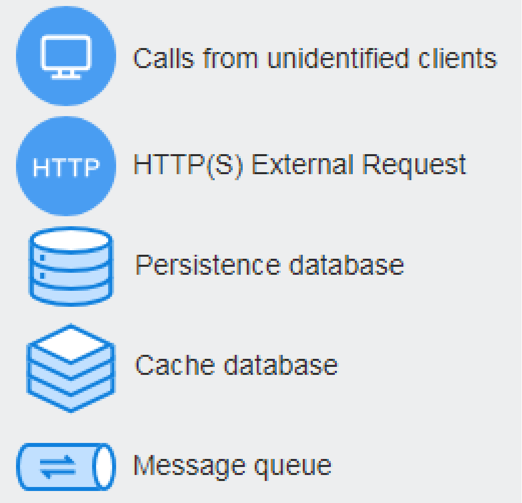
Data Type	Collected Data	Transmission Mode	Storage Mode	Data Purpose	Storage Period

Tracing data	Tracing span data	Transmission through HTTPS encryption and Access Key ID/Secret Access Key (AK/SK) authentication	Project-based isolated storage	Query and display at the tracing frontend	Configurable (7 days at most). The data will be deleted upon expiration.
Call request KPI data	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 KPI metrics, such as 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.

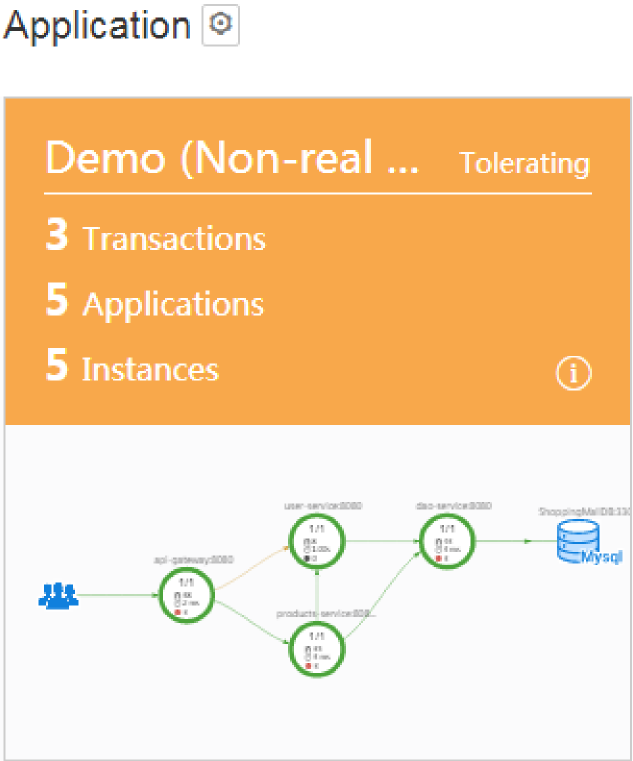
3.8 How Do I Calculate the Number of Used Instances?

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 3-9** 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 3-9 Instances that do not use probes



Example of calculating the number of used instances


Application

Demo (Non-real ... Tolerating

3 Transactions

5 Applications

5 Instances

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

3.9 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:

   ```
   JBOSS_MODULES_SYSTEM_PKGS="org.jboss.byteman,com.manageengine,org.jboss.logmanager,com.navercorp.pinpoint.bootstrap,com.navercorp.pinpoint.common,com.navercorp.pinpoint.exception"
   JAVA_OPTS="$JAVA_OPTS -Djava.util.logging.manager=org.jboss.logmanager.LogManager"
   JAVA_OPTS="$JAVA_OPTS -javaagent:/paas-apm/collectors/pinpoint/pinpoint-bootstrap.jar"
   JAVA_OPTS="$JAVA_OPTS -Xbootclasspath/p:$JBOSS_HOME/modules/system/layers/base/org/jboss/logmanager/main/jboss-logmanager-1.5.1.Final-redhat-1.jar"
   JAVA_OPTS="$JAVA_OPTS -Djboss.modules.system.pkgs=$JBOSS_MODULES_SYSTEM_PKGS -Djava.awt.headless=true"
   JAVA_OPTS="$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="$JAVA_OPTS -Xbootclasspath/p:$JBOSS_HOME/modules/system/layers/base/org/jboss/log4j/logmanager/main/slf4j-api-1.7.2.jbossorg-1.jar"
   JAVA_OPTS="$JAVA_OPTS -Xbootclasspath/p:$JBOSS_HOME/modules/system/layers/base/org/slf4j/main/slf4j-api-1.7.22.jbossorg-1.jar"
   JAVA_OPTS="$JAVA_OPTS -Xbootclasspath/p:$JBOSS_HOME/modules/system/layers/base/org/jboss/logmanager/main/jboss-logmanager-1.5.2.Final.jar"
   JAVA_OPTS="$JAVA_OPTS -Djava.util.logging.manager=org.jboss.logmanager.LogManager"
   JAVA_OPTS="$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,$JBOSS_MODULES_SYSTEM_PKGS"
   JAVA_OPTS="$JAVA_OPTS -Xbootclasspath/p:$JBOSS_HOME/modules/system/layers/base/org/jboss/log4j/logmanager/main/log4j-jboss-logmanager-1.1.4.Final.jar"
   JAVA_OPTS="$JAVA_OPTS -Xbootclasspath/p:$JBOSS_HOME/modules/system/layers/base/org/slf4j/main/slf4j-api-1.7.22.jbossorg-1.jar"
   JAVA_OPTS="$JAVA_OPTS -Xbootclasspath/p:$JBOSS_HOME/modules/system/layers/base/org/jboss/logmanager/main/jboss-logmanager-2.0.9.Final.jar"
   JAVA_OPTS="$JAVA_OPTS -Djava.util.logging.manager=org.jboss.logmanager.LogManager"
   JAVA_OPTS="$JAVA_OPTS -Djboss.modules.system.pkgs=$JBOSS_MODULES_SYSTEM_PKGS -Djava.awt.headless=true"
   ```

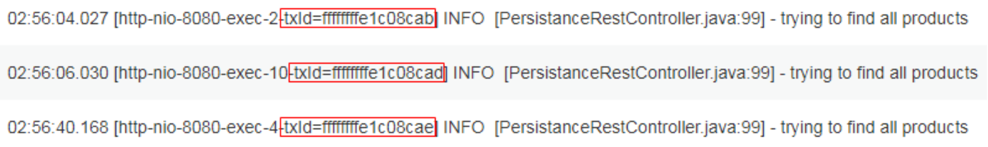
   JBoss uses the undertow as the application service. Therefore, the management parameter in the **wildfly-12.0.0.Final/bin/standalone.sh -bmanagement 127.0.0.1** command cannot be set to **0.0.0.0**. Otherwise, an exception occurs. The error information is as follows:

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

3.10 What Can I Do If I Cannot Search for Logs Based on Trace IDs?

Trace IDs are unique identifiers of tracings. When you enable the function of adding trace IDs to logs, you can search for logs based on trace IDs. If you cannot search for logs based on trace IDs, do as follows:

Check whether the log component uses log4j. For details, see **log4j**. In addition, check whether output logs contain trace names, as shown in the following figure.



```
02:56:04.027 [http-nio-8080-exec-2-txId=fffffffe1c08cab] INFO  [PersistanceRestController.java:99] - trying to find all products
02:56:06.030 [http-nio-8080-exec-10-txId=fffffffe1c08cad] INFO  [PersistanceRestController.java:99] - trying to find all products
02:56:40.168 [http-nio-8080-exec-4-txId=fffffffe1c08cae] INFO  [PersistanceRestController.java:99] - trying to find all products
```

3.11 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.

3.12 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 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.

   Download address: https://icagent-{*region*}.obs.{*region*}.myhuaweicloud.com/ICAgent_linux/checkSsh.sh

   The download address varies according to region. Replace *{region}* in the download address with the actual region.

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}
crond 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

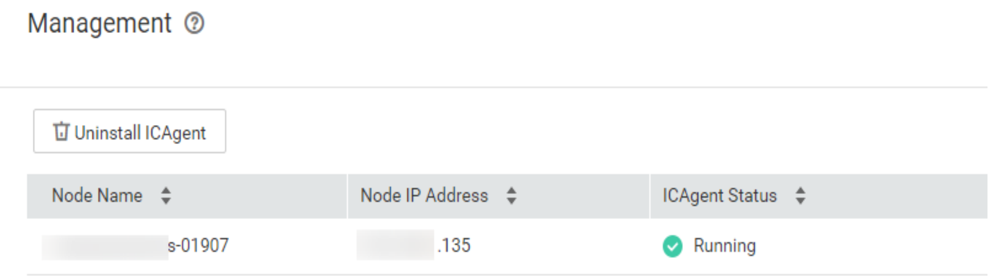
3.13 How Can I Do If No Topology or Data Is Displayed After the ICAgent and Java Probes Are Installed?

Symptom

After the ICAgent and Java probes are installed, no topology or data is displayed on Application Performance Management (APM).

Troubleshooting

1. If only the gray circle is displayed in the topology, check whether you are using the basic edition of APM. If yes, switch to the enterprise or professional edition, or click **Experience for Free**.
2. Check whether there are calls in the specified time range. Call relationships are generated only when there are calls in the specified time range. Data will be collected two or three minutes after calls are performed. In addition, check whether the time of the browser (Windows) is the same as that of the target Elastic Cloud Server (ECS).
3. Check whether applications (including the OS and Java type) meet **usage restrictions**.
4. Check whether the ICAgent on the host where services reside is normal.



Management

Node Name	Node IP Address	ICAgent Status
[redacted]s-01907	[redacted].135	Running

5. Check whether applications are correctly connected to APM.
   - **Connecting an ECS Application to APM**
   - **Connecting a HUAWEI CLOUD Containerized Application to APM**
6. If you connect an ECS application to APM and start the program as a non-root user, check whether the following commands have been run to modify the permissions on the probe file and output directory before enabling application monitoring:
   - If the commands have not been run, run them.
     ```
     chmod -R 777 /opt/oss/servicemgr/ICAgent/pinpoint/
     mkdir -p /paas-apm/collectors/pinpoint
     chmod -R 777 /paas-apm
     ```
   - If the commands have been run, continue to check other items.
7. If you connect an ECS application to APM, check whether Dapm_application (application name) and Dapm_tier (service name) comply with the following naming rule:

   Each name must be 1 to 64 characters starting with a letter or an underscore (_). Only lowercase letters, digits, hyphens (-), and underscores are allowed.
8. In the navigation pane of the APM console, choose **Agent** > **Configuration** and check whether data collection is enabled. If it is disabled, enable it.

3.14 Why Are Tomcat Thread Metrics Not Displayed on the JVM Monitoring Page?

For Spring Boot 2.1.x or later, set **server.tomcat.mbeanregistry.enabled** to **true** in the configuration file to enable the MBean registry of Tomcat. In this way, APM probes can collect Tomcat metrics.

3.15 Why Is the Allocated Memory Greater Than the Preset Maximum Memory on the JVM Monitoring Page?

JVM uses the dynamic memory allocation mechanism. The amount of memory to be allocated must be a multiple of 2. Even if the minimum memory, **-Xms** is configured, JVM may not allocate the minimum amount of memory at the beginning. In some cases, the allocated memory may slightly exceed the maximum memory, **-Xmx**. To solve the problem, configure **-XX:+AlwaysPretouch** to prevent dynamic heap memory allocation.

3.16 How Do I Determine Whether an ICAgent Has Been Bound in CCE?

To check whether an ICAgent has been bound in CCE, do as follows:

Step 1 Log in to the CCE console.

Step 2 Choose **Clusters** in the navigation pane and click your desire cluster.

Step 3 On the displayed page, choose **Workloads** in the navigation pane. Then, select **kube-system** from the **Namespace** drop-down list, and click the **DaemonSets** tab.

Step 4 If **ICAgent** is displayed in the **Workload Name** column, the ICAgent has been bound. If **ICAgent** is not displayed, no ICAgent has been bound.

----End