APM

User Guide

Issue	01
Date	2022-06-02

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.

Contents

1 Before You Start

This document describes how to use Application Performance Management (APM).

Topology	The call and dependency relationships between applications are displayed, and abnormal instances can be automatically discovered.
Call Chain	Information such as the call status, duration, and API is displayed, helping you further locate fault causes.
Transactions	Key metrics of transactions are displayed and Application Performance Index (Apdex) values intuitively reflect users' satisfaction with applications. ● When a transaction is abnormal, an **alarm** is reported. ● For transactions with poor user experience, faults can be located based on **topology** and **tracing**.
Method Tracing	Developers are able to locate method-level performance problems online.
SQL Analysis	Abnormal SQL statements are analyzed to solve database performance problems. The **topology** displays the key metrics of databases and SQL statements.
JVM Monitoring	The memory and thread metrics of the JVM running environment are monitored in real time, enabling you to quickly detect problems such as memory leakage and thread exceptions. ● The **topology** displays the JVM metrics of instances. ● When a JVM metric is abnormal, an **alarm** is reported.

2 Permissions Management

2.1 Creating a User and Granting Permissions

This section describes the fine-grained permissions management provided by Identity and Access Management (IAM) for your APM. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to APM resources.
- Grant only the permissions required for users to perform a task.
- Entrust a cloud account or service to perform professional and efficient O&M on your APM resources.

If your account does not need individual IAM users, then you may skip over this chapter.

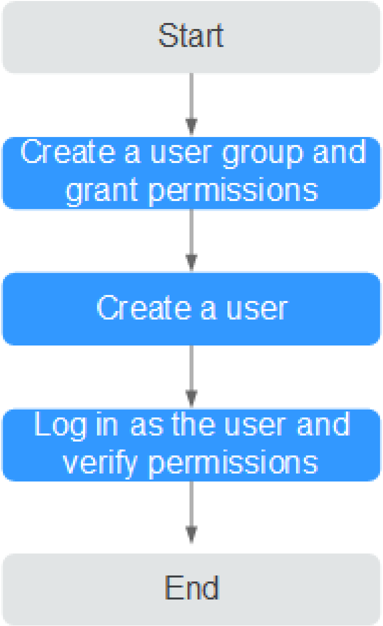
This section describes the procedure for granting permissions (see **Figure 2-1**).

Prerequisites

Learn about the permissions supported by APM (see **Permissions Management**) and choose policies or roles based on your requirements. For the permissions of other services, see **System Permissions**.

Process

Figure 2-1 Granting APM permissions


Start
Create a user group and grant permissions
Create a user
Log in as the user and verify permissions
End

1. **Create a user group and assign permissions** to it.

   Create a user group on the IAM console, and assign the **APM ReadOnlyAccess** policy to the group.

2. **Create a user and add it to a user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Logging In Using an IAM User** and Verifying Permissions

   Log in to the APM console as the created user, and verify that it has only the read permissions for APM.

2.2 Creating a Custom Policy

Custom policies can be created as a supplement to the system policies of APM. For the actions that can be added to custom policies, see **Permissions Policies and Supported Actions**.

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions without the need to know policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details about how to create a custom policy, see **Creating a Custom Policy**. The following section contains examples of common APM custom policies.

Example Custom Policies

- Example 1: Allowing a user to install the ICAgent

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "apm:icmgr:create"
            ]
        }
    ]
}
```

- Example 2: Denying collection component uninstallation

  A deny policy must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

  To grant a user the **APM FullAccess** system policy but forbid the user to uninstall collection components, create a custom policy that denies the uninstallation of collection components and grant both the **APM FullAccess** and deny policies to the user. Because the Deny action takes precedence, the user can perform all operations except uninstalling collection components. The following is an example deny policy:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "apm:icmgr:delete"
            ]
        }
    ]
}
```

- Example 3: Defining permissions for multiple services in a policy

  A custom policy can contain actions of multiple services that are all of the project-level type. The following is an example policy containing actions of multiple services:

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "aom:*:list",
                                "aom:*:get",
                                "apm:*:list",
                                "apm:*:get"
                        ]
                },
                {
                         "Effect": "Allow",
                         "Action": [
                                 "cce:cluster:get",
                                 "cce:cluster:list",
                                 "cce:node:get",
                                 "cce:node:list"
                        ]
                }
        ]
}
```

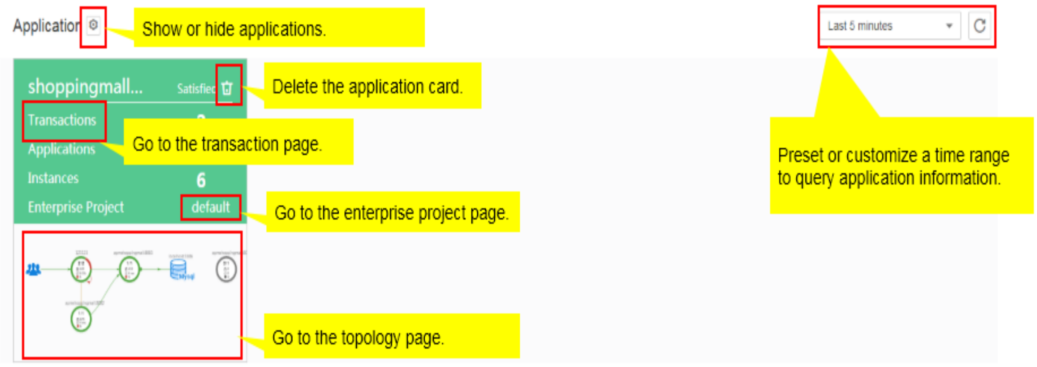
3 Application Overview

3.1 Dashboard

An application is a logical group of the same or similar services categorized based on service requirements. You can put services that fulfill the same function into one application for performance management. For example, you can put accounts, products, and payment services into the **Mall** application.

You can quickly obtain the health status of applications through the dashboard. On the **Dashboard** page, you can perform the following operations:

Figure 3-1 Dashboard page


Application
Show or hide applications.
Last 5 minutes
shoppingmall...
Satisfied
Delete the application card.
Transactions
Applications
Instances
6
Enterprise Project
default
Go to the transaction page.
Preset or customize a time range to query application information.
Go to the enterprise project page.
Go to the topology page.

NOTE

The **Enterprise Project** option is displayed only when you have enabled the enterprise project function. After this function is enabled, both historical and new probe applications are added to the **default** enterprise project by default. To change the enterprise project to which an application belongs, click **Enterprise Project** on the application card to go to the enterprise project page and migrate the APM application. Enterprise Project Management Service (EPS) provides a unified method to manage cloud resources and personnel by enterprise project. The default project is **default**. For details about how to enable, create, and manage enterprise projects, see **Enterprise Management User Guide**.

You can delete a service card in the following scenarios:

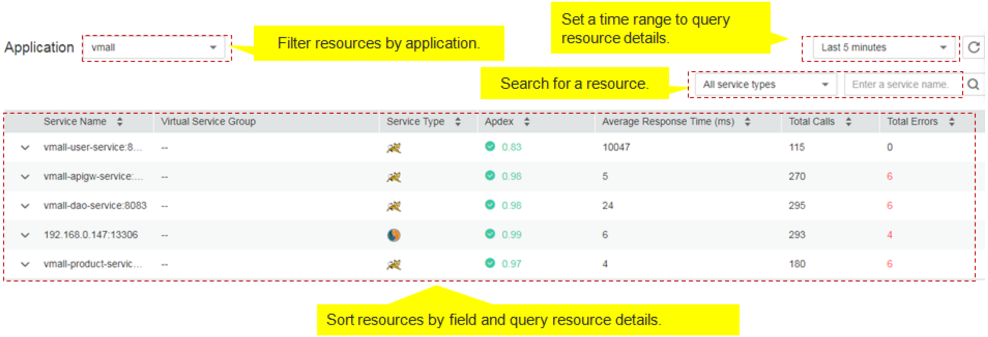
- The service connected to APM has been deleted.
- The ICAgent has been uninstalled and service data does not need to be collected.

If the service connected to APM is still running, the service card will be displayed again three minutes after it is deleted.

3.2 Inventory

The **Inventory** page displays metrics such as the service type, resource ID, response time, calls, and errors, facilitating fault locating.

Figure 3-2 Inventory page



Application vmall

Filter resources by application.

Set a time range to query resource details.

Last 5 minutes

Search for a resource.

All service types

Enter a service name.

Service Name	Virtual Service Group	Service Type	Apdex	Average Response Time (ms)	Total Calls	Total Errors
vmall-user-service:8...	--		0.83	10047	115	0
vmall-apigw-service:...	--		0.98	5	270	6
vmall-dao-service:8083	--		0.98	24	295	6
192.168.0.147:13306	--		0.99	6	293	4
vmall-product-servic...	--		0.97	4	180	6

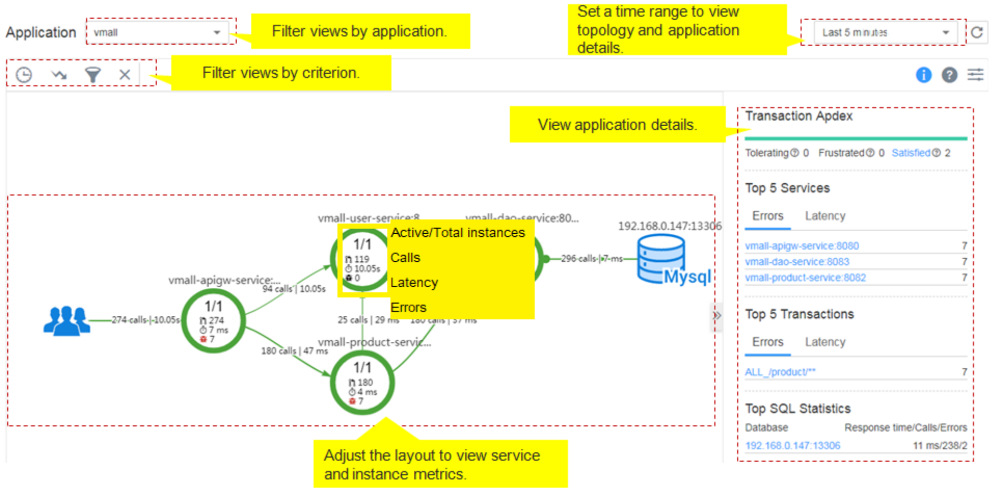
Sort resources by field and query resource details.

4 Topology

A topology graphically displays call and dependency relationships between applications. In a topology, each circle represents a service, each segment in a circle represents an instance, and each arrow represents a call relationship. APM supports calls between applications. The topology can display service call relationships across applications. When a circle represents an application, right-click the circle and choose **View Application** to go to the topology page.

Different colors on the circle represent different health statuses of instances. Colors are determined by **Application Performance Index (Apdex)** values. If an Apdex value is closer to **1**, the corresponding application is healthier.

Topology Page



1. **Table 4-1** provides topology description.

Table 4-1 Topology description

Color	Instance	Call
Green	0.75 ≤ Apdex ≤ 1 The instance responds quickly when it is called.	0.75 ≤ Apdex ≤ 1 Quick response.
Yellow	0.3 ≤ Apdex < 0.75 The instance responds slowly when it is called.	0.3 ≤ Apdex < 0.75 Slow response.
Red	0 ≤ Apdex < 0.3 The instance responds very slowly when it is called.	0 ≤ Apdex < 0.3 Very slow response.
Gray	The instance is not called.	N/A
Black	The instance is deleted.	N/A

2. On the right of the topology page, set a time range to view the following topology details of an application:
   - Transaction Apdex
   - Top 5 services ranked by errors and latency
   - Top 5 transactions ranked by errors and latency
   - Top 5 SQL statements ranked by response time, calls, and errors
3. In the topology, click a circle (a service) to view metric data, including Service Level Agreement (SLA) metrics, basic service metrics, and transaction details.
4. In the topology, click a segment (an instance) in a circle to view metric data, including basic instance metrics, JVM metrics, node metrics, and transaction details.

Locating Faults Using the Topology

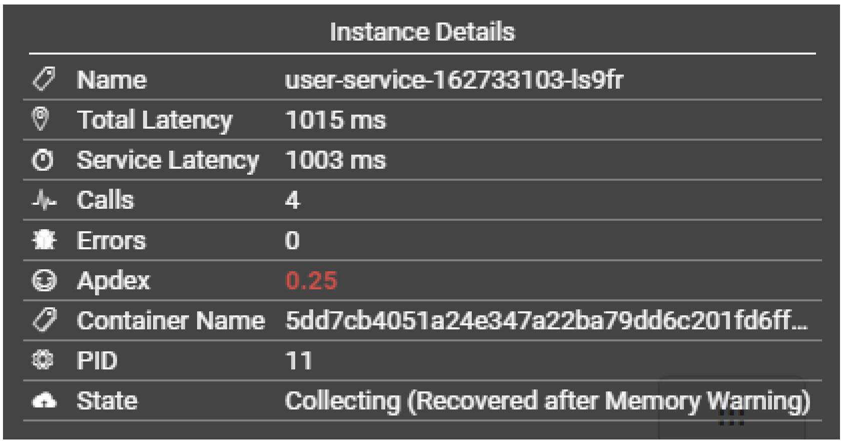
The following describes how to locate an instance with a slow response:

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

Step 2 In the navigation pane, choose **Topology**.

Step 3 In the upper right corner of the topology page, set a time range during which a problem occurs.

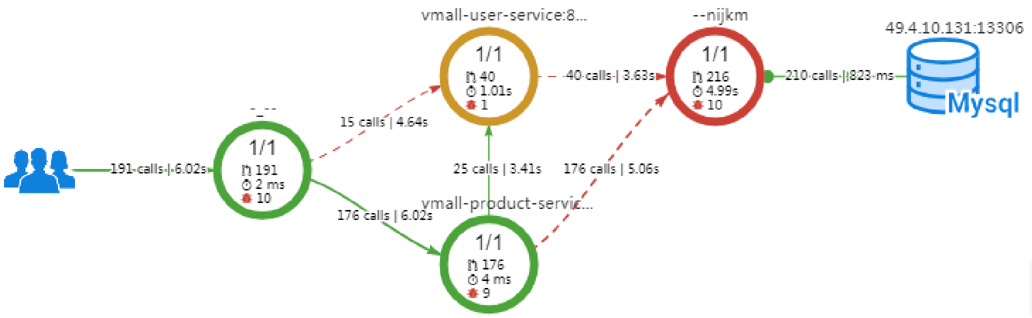
Step 4 Check the instance with a long execution time (that is, the instance highlighted in red) in the topology.



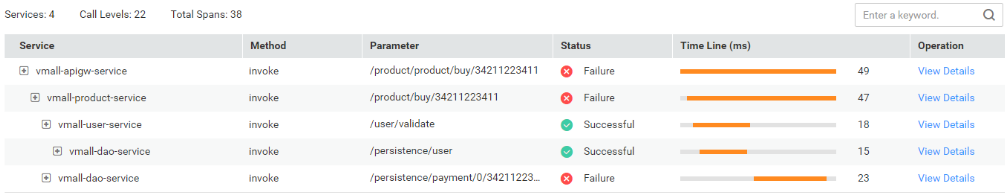
Instance Details

Name	user-service-162733103-ls9fr
Total Latency	1015 ms
Service Latency	1003 ms
Calls	4
Errors	0
Apdex	0.25
Container Name	5dd7cb4051a24e347a22ba79dd6c201fd6ff...
PID	11
State	Collecting (Recovered after Memory Warning)

Step 5 (Optional) For the service containing multiple instances, right-click the service and choose **Expand** from the shortcut menu to view call relationships between instances to preliminarily identify the abnormal instance.



Step 6 Choose **Find Call-Chain** from the shortcut menu. On the page that is displayed, further locate the fault based on call duration and other parameters.



Services: 4 Call Levels: 22 Total Spans: 38

Service	Method	Parameter	Status	Time Line (ms)	Operation
vmall-apigw-service	invoke	/product/product/buy/34211223411	Failure	49	View Details
vmall-product-service	invoke	/product/buy/34211223411	Failure	47	View Details
vmall-user-service	invoke	/user/validate	Successful	18	View Details
vmall-dao-service	invoke	/persistence/user	Successful	15	View Details
vmall-dao-service	invoke	/persistence/payment/0/34211223...	Failure	23	View Details

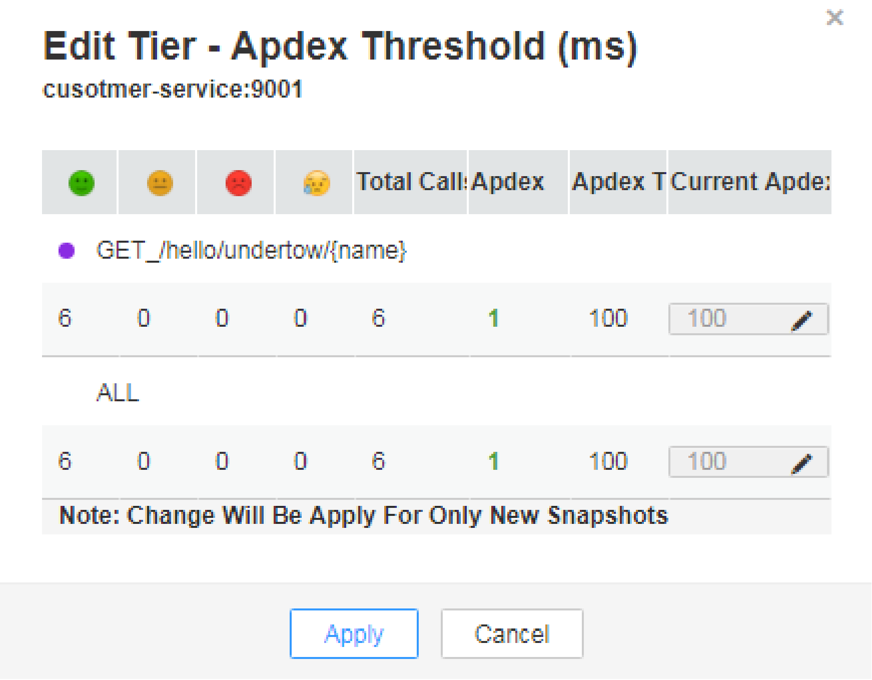
----End

Configuring Transaction Apdex Threshold

The response time of different transactions is different. APM enables you to configure different Apdex thresholds for different transactions. For example, if a login takes more than 50 ms, the response is slow. If a query transaction takes more than 10 ms, the response is slow. In this case, you need to set different Apdex thresholds for the login and query transactions.

Step 1 In the topology page, move the mouse cursor over a circle, right-click it, and click **Edit Threshold**.

Step 2 Modify the transaction Apdex threshold and click **Apply**.



Edit Tier - Apdex Threshold (ms)

cusotmer-service:9001

🙂	😐	☹	😥	Total Call:	Apdex	Apdex T	Current Apde:
● GET_/hello/undertow/{name}							
6	0	0	0	6	1	100	100
ALL							
6	0	0	0	6	1	100	100

Note: Change Will Be Apply For Only New Snapshots

----End

5 Tracing

5.1 Call Chain

With the tracing function, APM traces and records service calls, comprehensively monitors key metrics such as call status and latency, and visually restores the execution traces and statuses of service requests in distributed systems, so that you can quickly locate performance bottlenecks and faults.

Locating Performance Bottlenecks

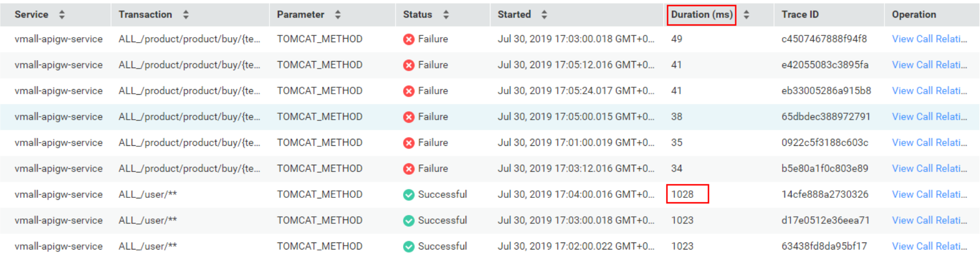
Step 1 Log in to the APM console.

Step 2 In the navigation pane, choose **Tracing** > **Call Chain**.

Step 3 In the upper right of the **Call Chain** page, select the desired time range, application, and service from three drop-down lists, and click **Search**.

Step 4 (Optional) On the **Call Chain** page, click **Advanced** in the upper right corner, set filter criteria, and click **Search**.

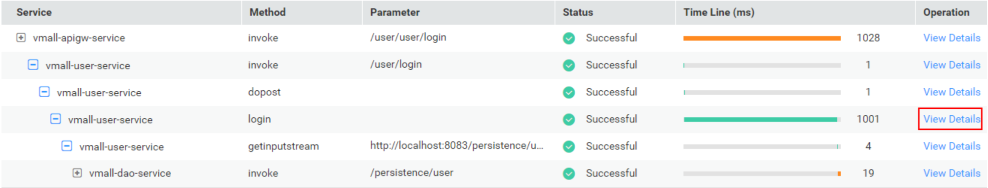
Step 5 Identify a service with long call duration and then locate the performance bottleneck.



Service	Transaction	Parameter	Status	Started	Duration (ms)	Trace ID	Operation
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	✗ Failure	Jul 30, 2019 17:03:00.018 GMT+0...	49	c4507467888f94f8	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	✗ Failure	Jul 30, 2019 17:05:12.016 GMT+0...	41	e42055083c3895fa	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	✗ Failure	Jul 30, 2019 17:05:24.017 GMT+0...	41	eb33005286a915b8	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	✗ Failure	Jul 30, 2019 17:05:00.015 GMT+0...	38	65dbdec388972791	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	✗ Failure	Jul 30, 2019 17:01:00.019 GMT+0...	35	0922c5f3188c603c	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	✗ Failure	Jul 30, 2019 17:03:12.016 GMT+0...	34	b5e80a1f0c803e89	View Call Relati...
vmall-apigw-service	ALL_/user/**	TOMCAT_METHOD	✓ Successful	Jul 30, 2019 17:04:00.016 GMT+0...	1028	14cfe888a2730326	View Call Relati...
vmall-apigw-service	ALL_/user/**	TOMCAT_METHOD	✓ Successful	Jul 30, 2019 17:03:00.018 GMT+0...	1023	d17e0512e36eea71	View Call Relati...
vmall-apigw-service	ALL_/user/**	TOMCAT_METHOD	✓ Successful	Jul 30, 2019 17:02:00.022 GMT+0...	1023	63438fd8da95bf17	View Call Relati...

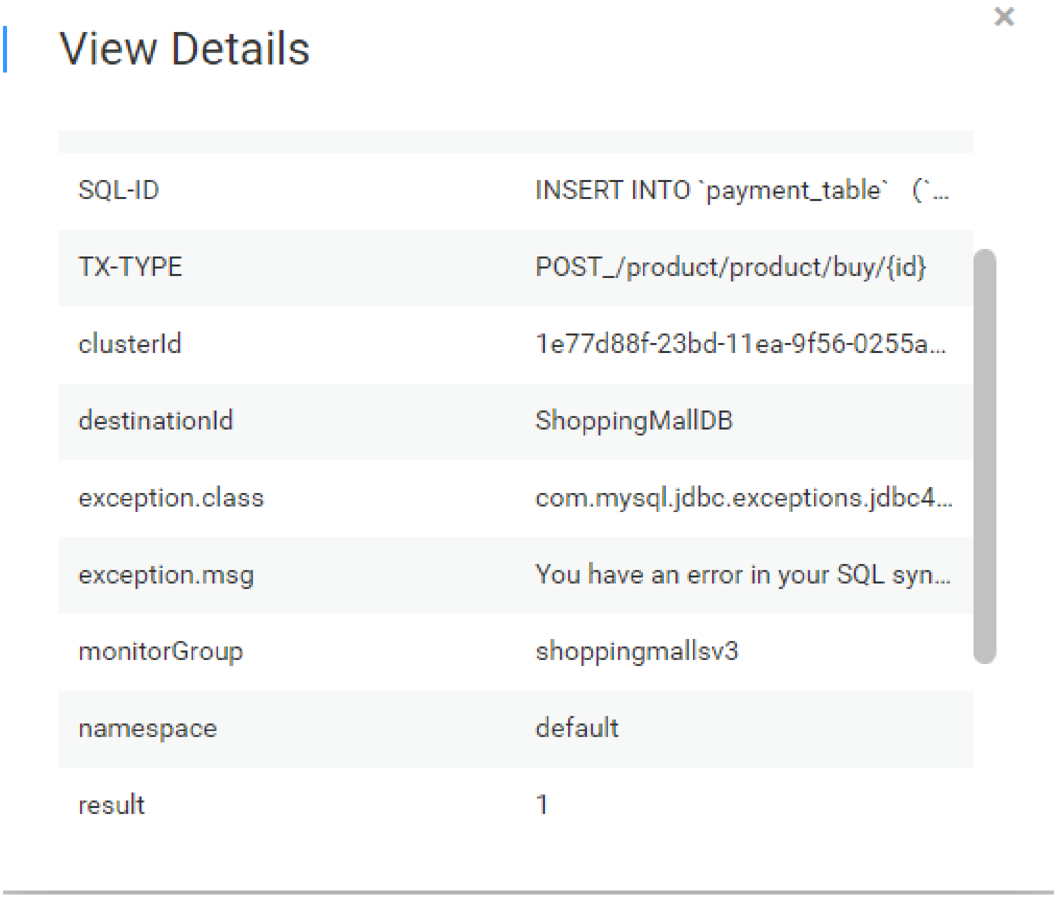
Step 6 Click **View Call Relationship** in the **Operation** column of the target service.

Step 7 (Optional) View additional information to further locate the cause.



Service	Method	Parameter	Status	Time Line (ms)	Operation
⊞ vmall-apigw-service	invoke	/user/user/login	✓ Successful	1028	View Details
⊟ vmall-user-service	invoke	/user/login	✓ Successful	1	View Details
⊟ vmall-user-service	dopost		✓ Successful	1	View Details
⊟ vmall-user-service	login		✓ Successful	1001	View Details
⊟ vmall-user-service	getinputstream	http://localhost:8083/persistence/u...	✓ Successful	4	View Details
⊞ vmall-dao-service	invoke	/persistence/user	✓ Successful	19	View Details

On the call relationship page that is displayed, click **View Details** in the **Operation** column to view call details.



View Details

SQL-ID	INSERT INTO `payment_table` (`...
TX-TYPE	POST_/product/product/buy/{id}
clusterId	1e77d88f-23bd-11ea-9f56-0255a...
destinationId	ShoppingMallDB
exception.class	com.mysql.jdbc.exceptions.jdbc4...
exception.msg	You have an error in your SQL syn...
monitorGroup	shoppingmallsv3
namespace	default
result	1

----End

Locating Faults

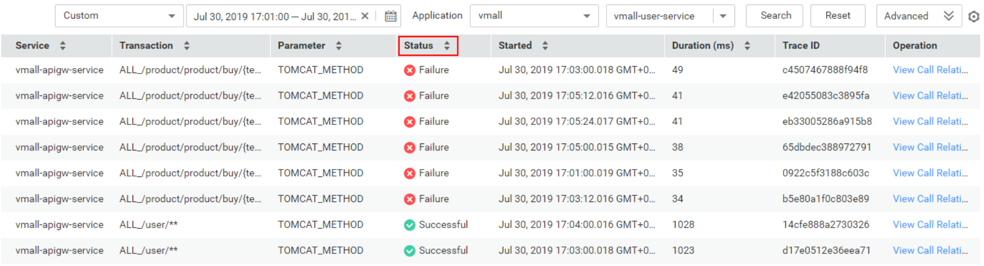
Step 1 Log in to the APM console.

Step 2 In the navigation pane, choose **Tracing** > **Call Chain**.

Step 3 In the upper right of the **Call Chain** page, select the desired time range, application, and service from three drop-down lists, and click **Search**.

Step 4 (Optional) On the **Call Chain** page, click **Advanced** in the upper right corner, set filter criteria, and click **Search**.

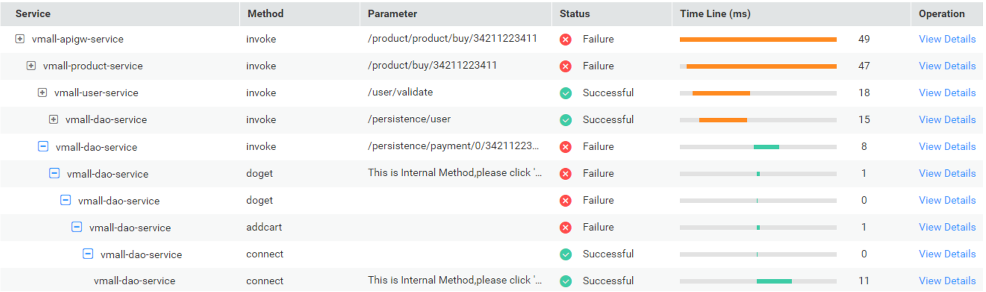
Step 5 Check the service status in the **Status** column and find out the faulty service.



Custom | Jul 30, 2019 17:01:00 — Jul 30, 201... | Application | vmall | vmall-user-service | Search | Reset | Advanced

Service	Transaction	Parameter	Status	Started	Duration (ms)	Trace ID	Operation
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	Failure	Jul 30, 2019 17:03:00.018 GMT+0...	49	c4507467888f94f8	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	Failure	Jul 30, 2019 17:05:12.016 GMT+0...	41	e42055083c3895fa	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	Failure	Jul 30, 2019 17:05:24.017 GMT+0...	41	eb33005286a915b8	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	Failure	Jul 30, 2019 17:05:00.015 GMT+0...	38	65dbdec388972791	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	Failure	Jul 30, 2019 17:01:00.019 GMT+0...	35	0922c5f3188c603c	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	Failure	Jul 30, 2019 17:03:12.016 GMT+0...	34	b5e80a1f0c803e89	View Call Relati...
vmall-apigw-service	ALL_/user/**	TOMCAT_METHOD	Successful	Jul 30, 2019 17:04:00.016 GMT+0...	1028	14cfe888a2730326	View Call Relati...
vmall-apigw-service	ALL_/user/**	TOMCAT_METHOD	Successful	Jul 30, 2019 17:03:00.018 GMT+0...	1023	d17e0512e36eea71	View Call Relati...

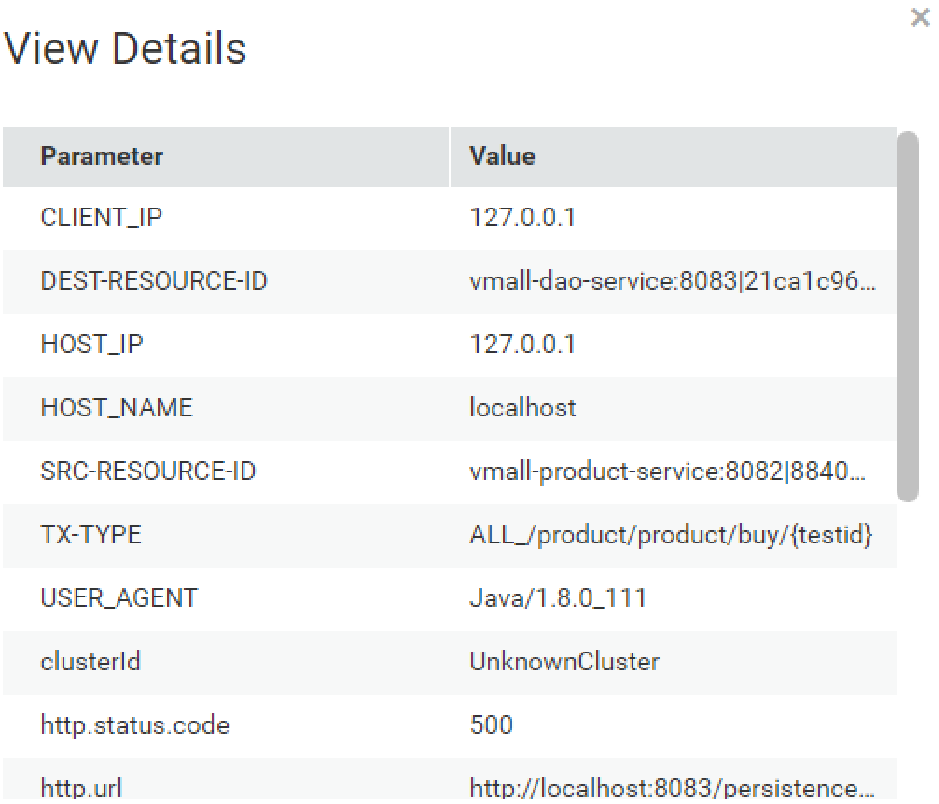
Step 6 Click **View Call Relationship** in the **Operation** column, check whether the return value is normal, and locate the fault.



Service	Method	Parameter	Status	Time Line (ms)	Operation
vmall-apigw-service	invoke	/product/product/buy/34211223411	Failure	49	View Details
vmall-product-service	invoke	/product/buy/34211223411	Failure	47	View Details
vmall-user-service	invoke	/user/validate	Successful	18	View Details
vmall-dao-service	invoke	/persistence/user	Successful	15	View Details
vmall-dao-service	invoke	/persistence/payment/0/34211223...	Failure	8	View Details
vmall-dao-service	doget	This is Internal Method,please click '...	Failure	1	View Details
vmall-dao-service	doget		Failure	0	View Details
vmall-dao-service	addcart		Failure	1	View Details
vmall-dao-service	connect		Successful	0	View Details
vmall-dao-service	connect	This is Internal Method,please click '...	Successful	11	View Details

Step 7 (Optional) View additional information to further locate the cause.

On the call relationship page that is displayed, click **View Details** in the **Operation** column to view call details.



View Details

Parameter	Value
CLIENT_IP	127.0.0.1
DEST-RESOURCE-ID	vmall-dao-service:8083|21ca1c96...
HOST_IP	127.0.0.1
HOST_NAME	localhost
SRC-RESOURCE-ID	vmall-product-service:8082|8840...
TX-TYPE	ALL_/product/product/buy/{testid}
USER_AGENT	Java/1.8.0_111
clusterId	UnknownCluster
http.status.code	500
http.url	http://localhost:8083/persistence...

----End

5.2 Method Tracing

Method tracing is used to dynamically trace a method of a class. When the method of this class is called, APM collects the call data of the method based on configured method tracing rules using probes, and displays the call data on the **Call Chain** page. Method tracing is used to help application developers locate method-level performance problems online.

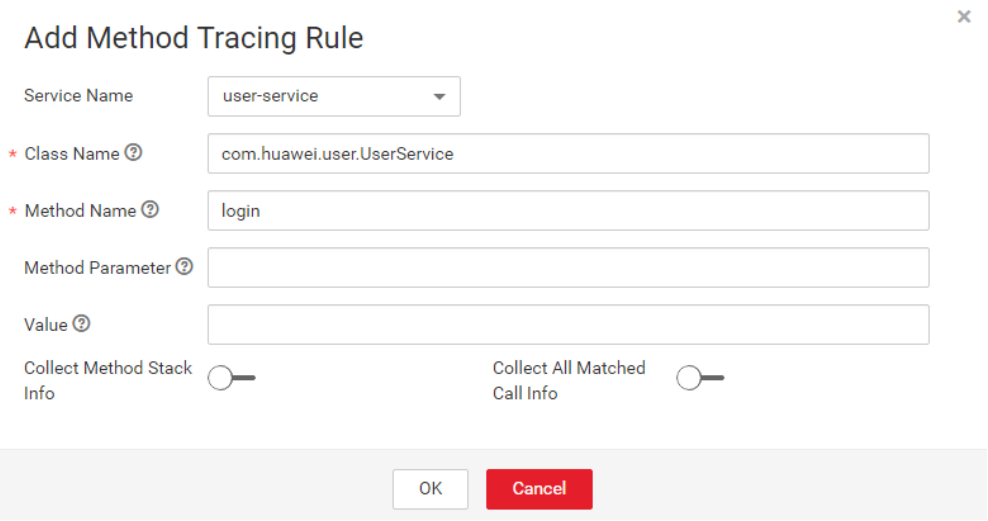
APM traces the APIs of most third-party open-source components, but does not trace specific methods in your applications. To monitor important methods in applications or methods of some third-party open-source components that are not supported by APM, you need to customize method tracing. After the configuration is complete, you can view the call data of the method on the **Call Chain** page.

Step 1 Log in to the APM console.

Step 2 In the navigation pane, choose **Tracing** > **Method Tracing**.

Step 3 Customize a method tracing rule and start method tracing.

On the **Method Tracing** page, click **Add Method Tracing Rule**, set parameters, and click **OK**.


Add Method Tracing Rule

Service Name: user-service

* Class Name: com.huawei.user.UserService

* Method Name: login

Method Parameter:

Value:

Collect Method Stack Info: ○ off

Collect All Matched Call Info: ○ off

NOTE

- If **Method Parameter** is not set, all information about the methods using the same name is collected by default.
- If **Value** is not set, the values of methods are not filtered during collection.
- If **Collect Method Stack Info** is enabled, the call stack information about methods is collected.
- If **Collect All Matched Call Info** is enabled, all tracing method information is collected. If this function is disabled, tracing method information is collected based on the sampling ratio set during **Collection Configuration**.

Step 4 Preliminarily locate service performance problems based on the displayed call duration and status.

Step 5 Click **View Call Relationship** in the **Operation** column to view the method-level call relationships.

----End

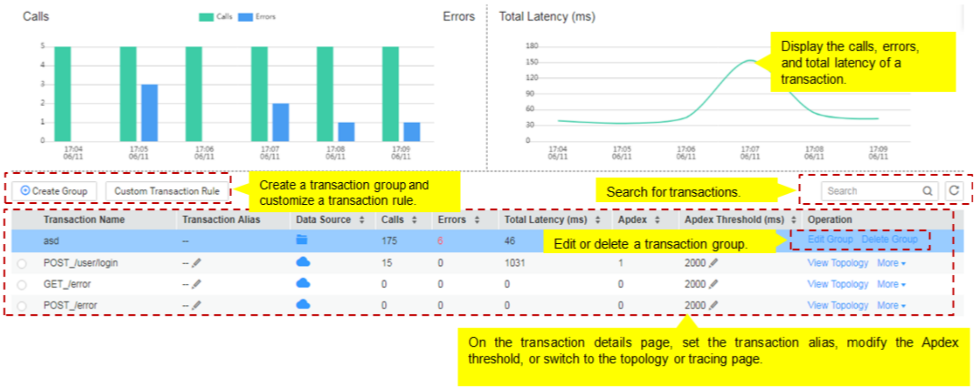
6 Transactions

A transaction is usually an HTTP request. The process is as follows: user request > web server > database > web server > user request. In real life, a transaction is a one-time task. A user completes a task by using an application. In the example of an e-commerce application, querying a product is a transaction, and making a payment is also a transaction.

To complete a transaction, you may call multiple services. Any slow or error call may lead to slow responses. During routine O&M, you can analyze the transactions with slow responses to locate and solve application problems, thereby improving user experience.

Transaction Insights Page

Figure 6-1 Transaction insights page



Display the calls, errors, and total latency of a transaction.

Create a transaction group and customize a transaction rule.

Search for transactions.

Transaction Name	Transaction Alias	Data Source	Calls	Errors	Total Latency (ms)	Apdex	Apdex Threshold (ms)	Operation
asd	--		175	6	46			Edit Group Delete Group
POST_/user/login	--		15	0	1031	1	2000	View Topology More
GET_/error	--		0	0	0	0	2000	View Topology More
POST_/error	--		0	0	0	0	2000	View Topology More

Edit or delete a transaction group.

On the transaction details page, set the transaction alias, modify the Apdex threshold, or switch to the topology or tracing page.

NOTE

On the **Transactions** page, **Errors** indicates the number of requests whose return code is greater than or equal to 400. Other requests are not included.

1. Set a time range to view the following transaction details of an application:
   - Calls and errors
   - Total latency

2. Click **Create Group**, select a transaction to move it to the new group, and then name the group.
3. Click **View Topology** to view the topology of the transaction.
4. Click **More** in the **Operation** column and select **View Call Relationship** from the drop-down list to view the tracing data of the transaction.

Analyzing Faults Based on Transactions

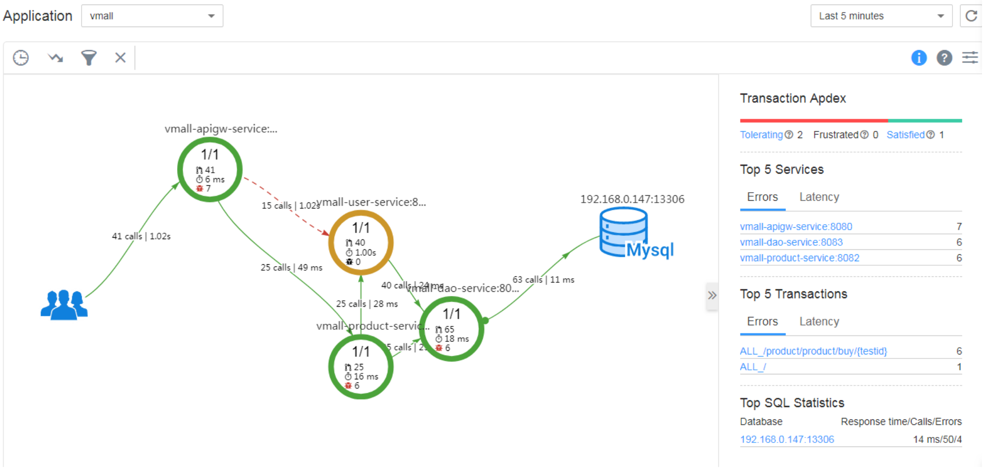
The following describes how to analyze a transaction with an extremely slow response:

Step 1 Log in to the APM console.

Step 2 In the navigation pane, choose **Transactions**.

Step 3 On the **Transactions** page, select a transaction with an extremely slow response from the transaction list.

Step 4 Click **View Topology** in the **Operation** column to view the topology and instance details of the transaction.



Application vmall

Last 5 minutes

Transaction Apdex

Tolerating 2 Frustrated 0 Satisfied 1

Top 5 Services

Errors Latency

vmall-apigw-service:8080	7
vmall-dao-service:8083	6
vmall-product-service:8082	6

Top 5 Transactions

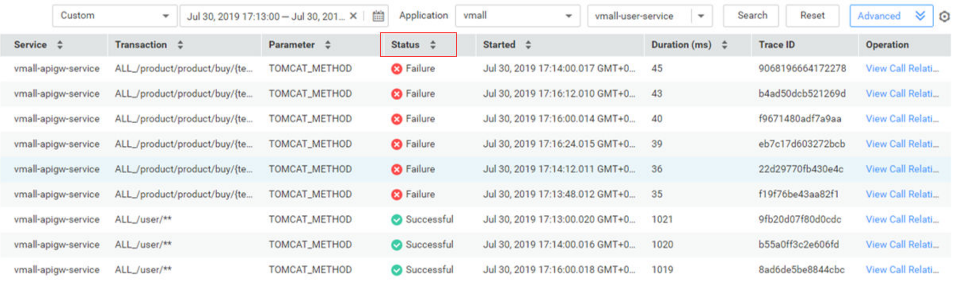
Errors Latency

ALL_/product/product/buy/{testid}	6
ALL_/	1

Top SQL Statistics

Database	Response time/Calls/Errors
192.168.0.147:13306	14 ms/50/4

Step 5 Right-click an instance with an extremely slow response and choose **Find Call-Chain** from the shortcut menu. On the page that is displayed, further locate the fault based on call duration and other parameters.



Custom | Jul 30, 2019 17:13:00 – Jul 30, 201... | Application vmall | vmall-user-service | Search | Reset | Advanced

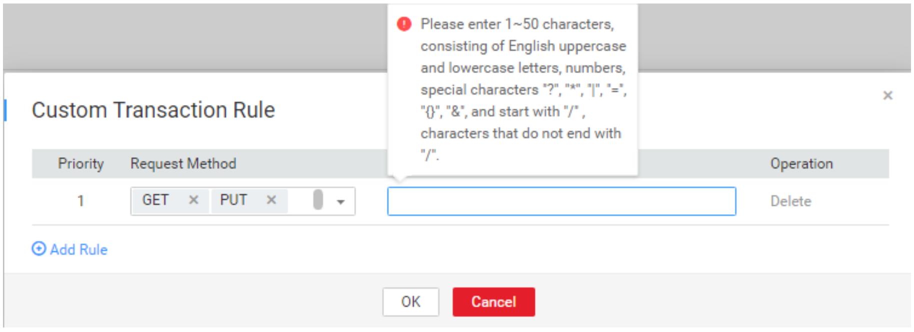
Service	Transaction	Parameter	Status	Started	Duration (ms)	Trace ID	Operation
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	✗ Failure	Jul 30, 2019 17:14:00.017 GMT+0...	45	9068196664172278	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	✗ Failure	Jul 30, 2019 17:16:12.010 GMT+0...	43	b4ad50dcb521269d	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	✗ Failure	Jul 30, 2019 17:16:00.014 GMT+0...	40	f9671480adf7a9aa	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	✗ Failure	Jul 30, 2019 17:16:24.015 GMT+0...	39	eb7c17d603272bcb	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	✗ Failure	Jul 30, 2019 17:14:12.011 GMT+0...	36	22d29770fb430e4c	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{te...	TOMCAT_METHOD	✗ Failure	Jul 30, 2019 17:13:48.012 GMT+0...	35	f19f76be43aa82f1	View Call Relati...
vmall-apigw-service	ALL_/user/**	TOMCAT_METHOD	✓ Successful	Jul 30, 2019 17:13:00.020 GMT+0...	1021	9fb20d07f80d0cdc	View Call Relati...
vmall-apigw-service	ALL_/user/**	TOMCAT_METHOD	✓ Successful	Jul 30, 2019 17:14:00.016 GMT+0...	1020	b55a0ff3c2e606fd	View Call Relati...
vmall-apigw-service	ALL_/user/**	TOMCAT_METHOD	✓ Successful	Jul 30, 2019 17:16:00.018 GMT+0...	1019	8ad6de5be8844cbc	View Call Relati...

----End

Customizing Transactions

To precisely define transactions and collect tracing data, use the URI template to customize transactions and classify requests into different transactions. When the collector receives requests, custom transactions will be calculated first.

Step 1 On the **Transactions** page, click **Custom Transaction Rule**. A transaction consists of the request method and regular expression. It is in the format of **{Request Method}_/{pattern}**. Example: When the request methods are **GET** and **POST** and the regular expression is **/{name}**, the transaction is **GET,POST_/{name}**.



Please enter 1~50 characters, consisting of English uppercase and lowercase letters, numbers, special characters "?", "*", "|", "=", "{}", "&", and start with "/" , characters that do not end with "/".

Step 2 Select one or more request methods. Request methods include **GET**, **PUT**, **DELETE**, **POST**, **HEAD**, **CONNECT**, **OPTIONS**, **PATCH**, **TRACE**, and **Select all**. **Select all** indicates all request methods.

Step 3 In the **Regular Expression** text box, enter a transaction rule and click **OK**. In this way, the custom transaction rule is added successfully.

The regular expression uses the **URI template** matching mode of the Spring MVC framework. Example: @RequestMapping(path="/owners/{ownerId}/pets/{petId}", method=RequestMethod.GET), where **ownerId** and **petId** are variables.

To add multiple custom transaction rules, click **Add Rule**.

NOTE

- A transaction rule must be 1 to 50 characters long. It must start with a slash (/) but cannot end with a slash. Only letters, digits, and special characters (?*|={}&) are allowed.
- Both the question mark (?) and asterisk (*) can be used for fuzzy search. One question mark represents one character, one asterisk represents 0 to N characters between two slashes in a URI, and double asterisks represent infinite characters. Example: When you enter **/first/***, **/first/test** can be returned but **/first/test/test** cannot. When you enter **/first/****, both **/first/test** and **/first/test/test** can be returned.

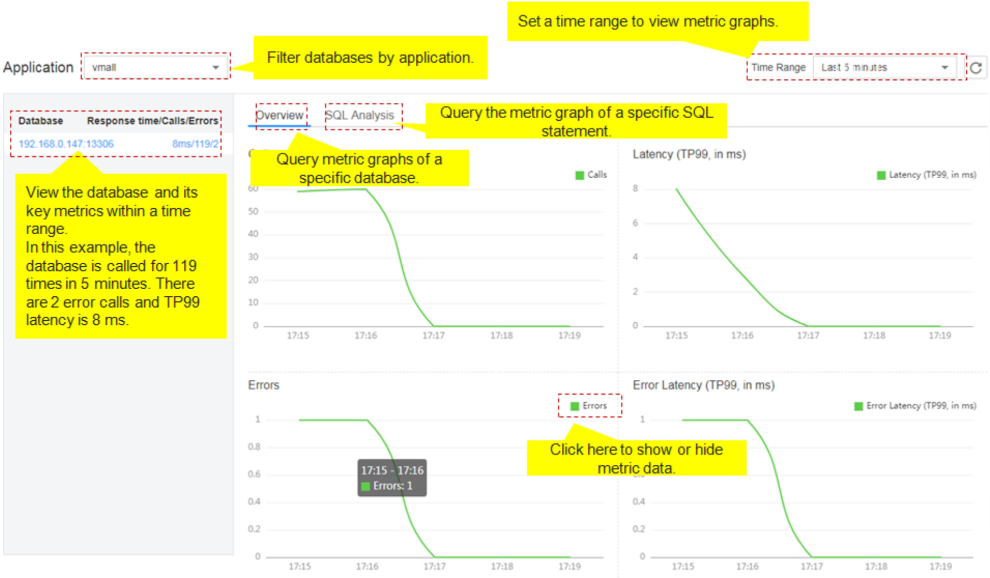
----End

7 SQL Analysis

APM displays key metrics, such as SQL statement calls, response time, and errors for analyzing database performance problems caused by slow or error SQL statements. SQL analysis supports MySQL, Oracle, and PostgreSQL relational databases only.

SQL Page

Figure 7-1 SQL page



Set a time range to view metric graphs.

Filter databases by application.

Query the metric graph of a specific SQL statement.

Query metric graphs of a specific database.

View the database and its key metrics within a time range.
In this example, the database is called for 119 times in 5 minutes. There are 2 error calls and TP99 latency is 8 ms.

Click here to show or hide metric data.

Analyzing Abnormal SQL Statements

When an SQL statement of a database is abnormal, performance problems such as service timeout may occur. During routine O&M, you can monitor key metrics, such as error duration and latency of databases, locate the SQL statements that take a long time to execute, operate at low efficiency, or fail to be called, and then analyze and optimize them.

The SQL analysis function determines whether to collect SQL data. Before performing the following operations, ensure that this function is enabled.

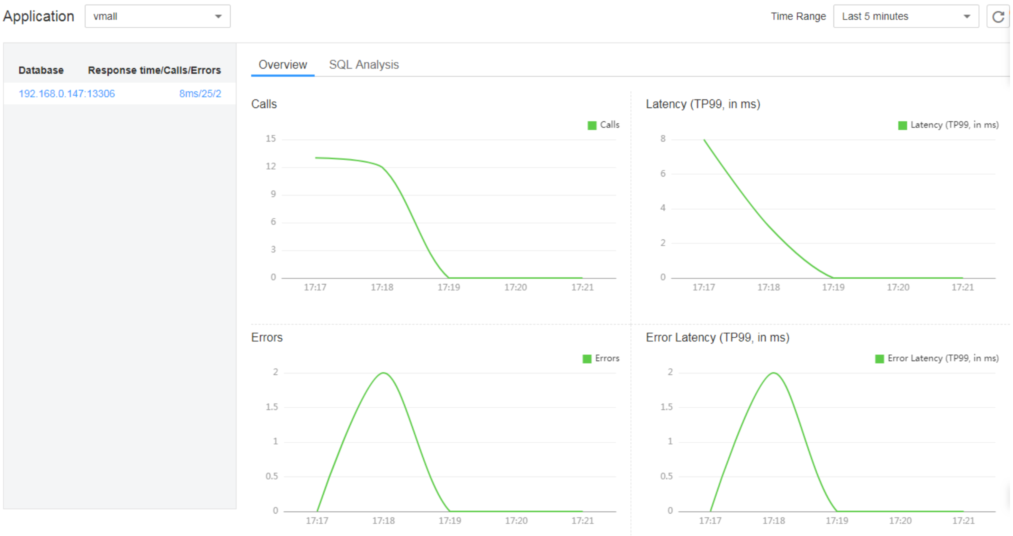
Otherwise, no SQL data can be queried. This function is enabled by default. If it is disabled, choose **Agent** > **Configuration** in the navigation pane and then enable it.

Step 1 Log in to the APM console.

Step 2 In the navigation pane, choose **SQL Analysis**.

Step 3 On the **SQL Analysis** page, select the time range during which a problem occurred.

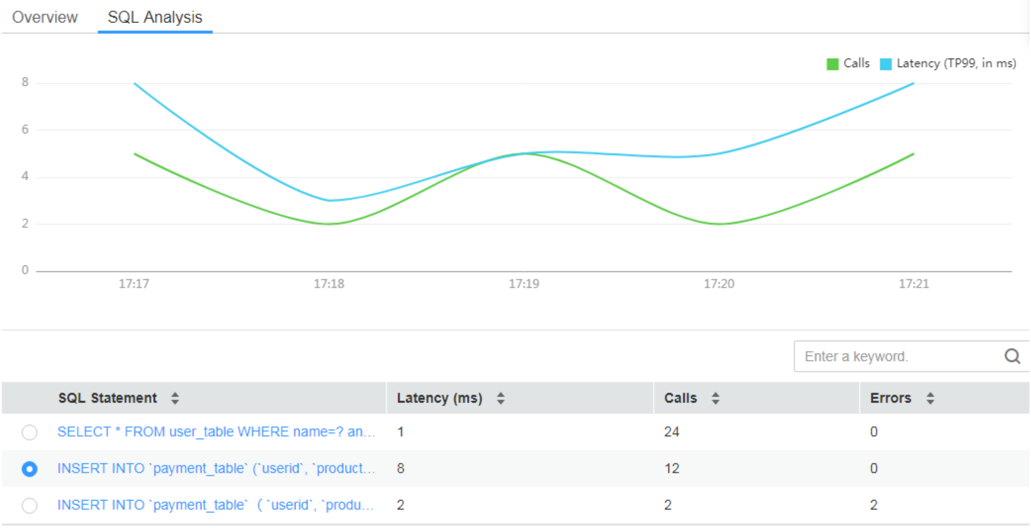
Step 4 On the **Overview** tab page, locate the faulty database in the application based on key metrics. If a database requires long response time and has many call errors, performance problems may occur.



Database	Response time/Calls/Errors
192.168.0.147:13306	8ms/25/2

Step 5 Analyze the problem cause.

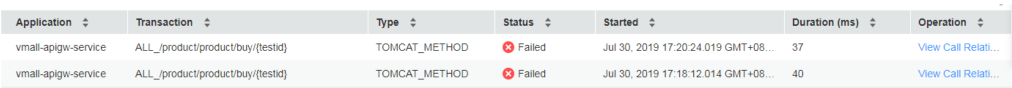
Click the **SQL Analysis** tab, and locate the abnormal SQL statement in the SQL statement list.



	SQL Statement	Latency (ms)	Calls	Errors
○	SELECT * FROM user_table WHERE name=? an...	1	24	0
●	INSERT INTO `payment_table` (`userid`, `product...	8	12	0
○	INSERT INTO `payment_table` (`userid`, `produ...	2	2	2

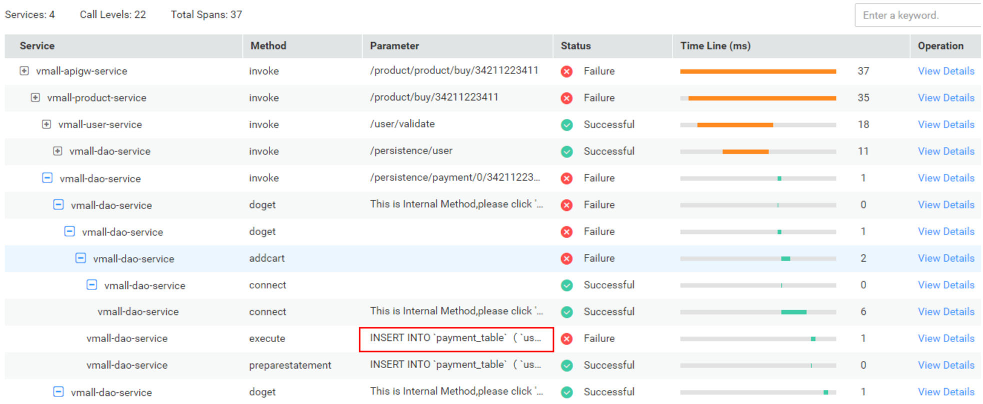
Step 6 Further analyze the cause.

1. Click the abnormal SQL statement to go to the **Call Chain** page and check the impact of this statement on the entire service.



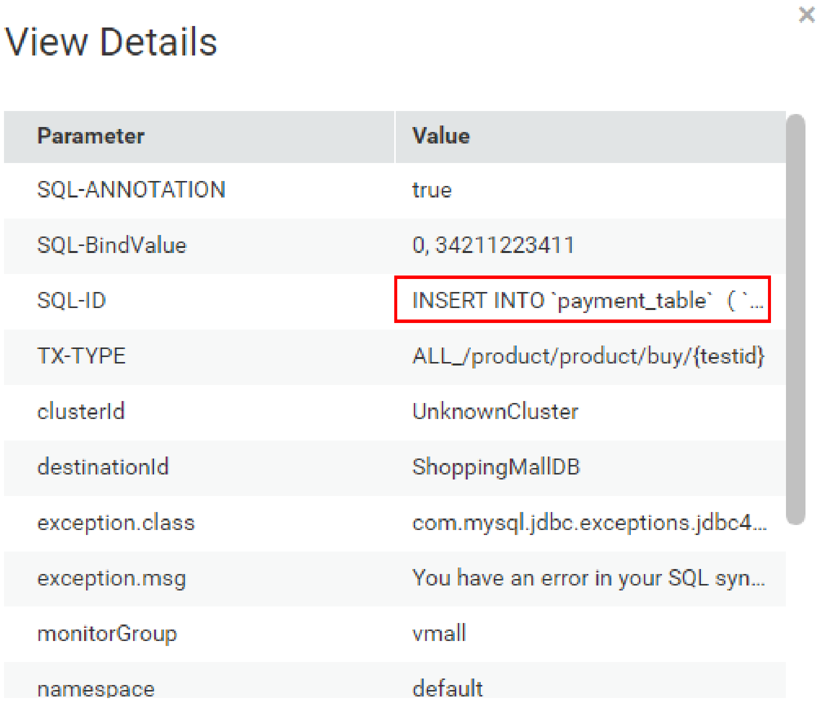
Application	Transaction	Type	Status	Started	Duration (ms)	Operation
vmall-apigw-service	ALL_/product/product/buy/{testid}	TOMCAT_METHOD	Failed	Jul 30, 2019 17:20:24.019 GMT+08...	37	View Call Relati...
vmall-apigw-service	ALL_/product/product/buy/{testid}	TOMCAT_METHOD	Failed	Jul 30, 2019 17:18:12.014 GMT+08...	40	View Call Relati...

2. Click **View Call Relationship** in the **Operation** column to find out the method of the abnormal SQL statement. Analyze the cause of the abnormal SQL statement in this method. For example, check whether the index is used, data volume is overlarge, syntax is correct, or deadlock occurs. Then, optimize the SQL statement accordingly.



Services: 4 Call Levels: 22 Total Spans: 37

Service	Method	Parameter	Status	Time Line (ms)	Operation
vmall-apigw-service	invoke	/product/product/buy/34211223411	Failure	37	View Details
vmall-product-service	invoke	/product/buy/34211223411	Failure	35	View Details
vmall-user-service	invoke	/user/validate	Successful	18	View Details
vmall-dao-service	invoke	/persistence/user	Successful	11	View Details
vmall-dao-service	invoke	/persistence/payment/0/34211223...	Failure	1	View Details
vmall-dao-service	doget	This is Internal Method,please click '...	Failure	0	View Details
vmall-dao-service	doget		Failure	1	View Details
vmall-dao-service	addcart		Failure	2	View Details
vmall-dao-service	connect		Successful	0	View Details
vmall-dao-service	connect	This is Internal Method,please click '...	Successful	6	View Details
vmall-dao-service	execute	INSERT INTO `payment_table` (`us...	Failure	1	View Details
vmall-dao-service	preparestatement	INSERT INTO `payment_table` (`us...	Successful	0	View Details
vmall-dao-service	doget	This is Internal Method,please click '...	Successful	1	View Details



View Details

Parameter	Value
SQL-ANNOTATION	true
SQL-BindValue	0, 34211223411
SQL-ID	INSERT INTO `payment_table` (`...
TX-TYPE	ALL_/product/product/buy/{testid}
clusterId	UnknownCluster
destinationId	ShoppingMallDB
exception.class	com.mysql.jdbc.exceptions.jdbc4...
exception.msg	You have an error in your SQL syn...
monitorGroup	vmall
namespace	default

----End

8 JVM Monitoring

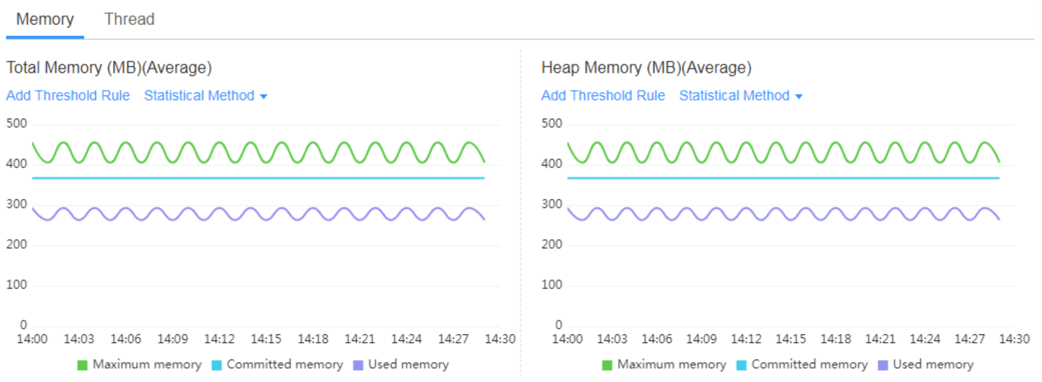
JVM monitoring displays the memory and thread metrics of the JVM running environment based on Java applications. You can monitor metric trends in real time for performance analysis.

On the **Memory** and **Thread** tab pages, you can respectively view the memory and thread graphs to quickly locate problems such as memory leakage and thread exceptions.

Memory Graphs

As shown in **Figure 8-1**, in a selected time range, the trends of the maximum, committed, and used memory in different JVM memory spaces (such as the total memory, heap memory, and non-heap memory spaces) of an instance are displayed. In addition, the garbage collection (GC) duration and times are also displayed.

Figure 8-1 Memory graphs



JVM memory

JVM memory consists of heap and non-heap memory.

- Heap memory: A heap is the data area where the JVM is running. It allocates memory for all instances and arrays. Heap memory of objects is reclaimed by an automatic memory management system called garbage collector. Heap space consists of eden space, survivor space, and tenured space.

- Non-heap memory: Memory (excluding heap memory) managed by JVM. Non-heap space consists of code cache and permanent space (or meta space).

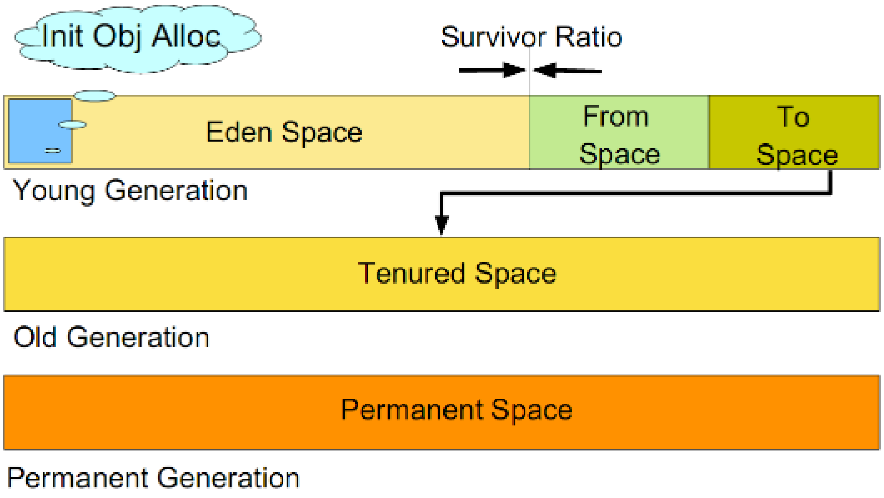
Java heap is the main area managed by the garbage collector. It is also called garbage collection heap. GC mode includes full GC and minor GC.

Table 8-1 Memory spaces

Space Name	Description
Eden space	Initially allocates memory from the thread pool to most objects.
Survivor space	Stores the eden space's objects that are not reclaimed during GC.
Tenured space	Maintains objects that have been stored in the survivor space for a period of time.
Code cache	Compiles and stores local code.
Permanent space	Stores static data of VMs, for example, classes and method objects.
Meta space	Stores local class metadata. In versions later than Java 8, permanent space is replaced by meta space.
Direct Buffer	Resource usage of the direct buffer is monitored.
Full GC	Indicates the GC performed in the entire heap space (covering young-, old-, and permanent-generation spaces) when the memory space is still insufficient after memory reclamation.
Minor GC	Indicates the GC performed in the young-generation space (including eden and survivor spaces) when the allocated memory is insufficient.

JVM collects garbage based on generations. JVM heap space is divided into old- and young-generation spaces. More than 90% objects that exist only for a short period of time are stored in the young-generation space, whereas objects that have long life cycles are stored in the old-generation space. Young-generation space is further divided into eden space and two survivor spaces. New objects are initially allocated to the eden space. The survivor spaces are used as the buffer between eden space and tenured space. Objects that are survived after several rounds of GC in the survivor spaces are then transferred to the old-generation space, as shown in **Figure 8-2**.

Figure 8-2 Memory spaces



NOTE

There are two survivor spaces, which are represented by **from** and **to** pointers. The **to** pointer points to the empty survivor space.

Thread Graphs

As shown in **Figure 8-3**, in a selected time range, the trends of new, runnable, blocked, and waiting threads are displayed.

Figure 8-3 Thread graphs

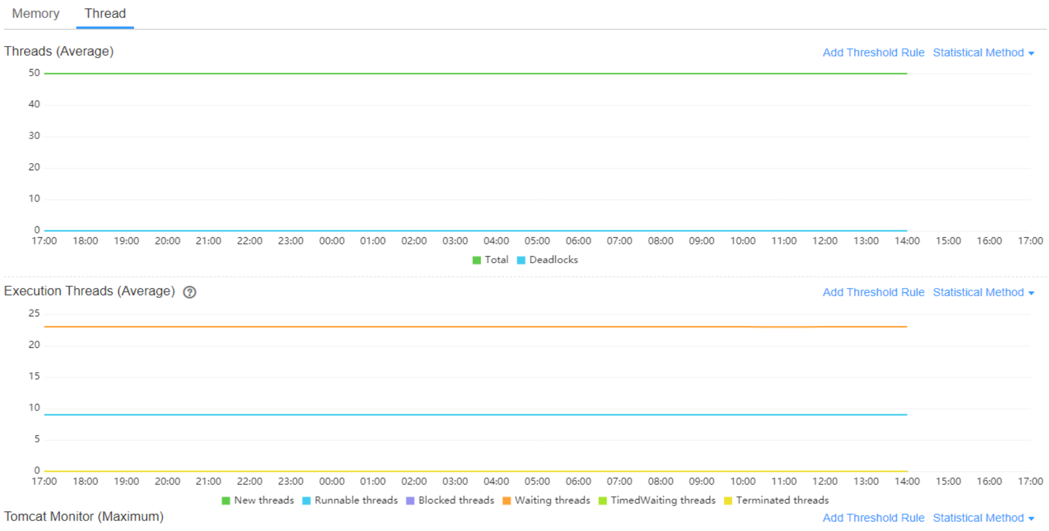


Table 8-2 Threads

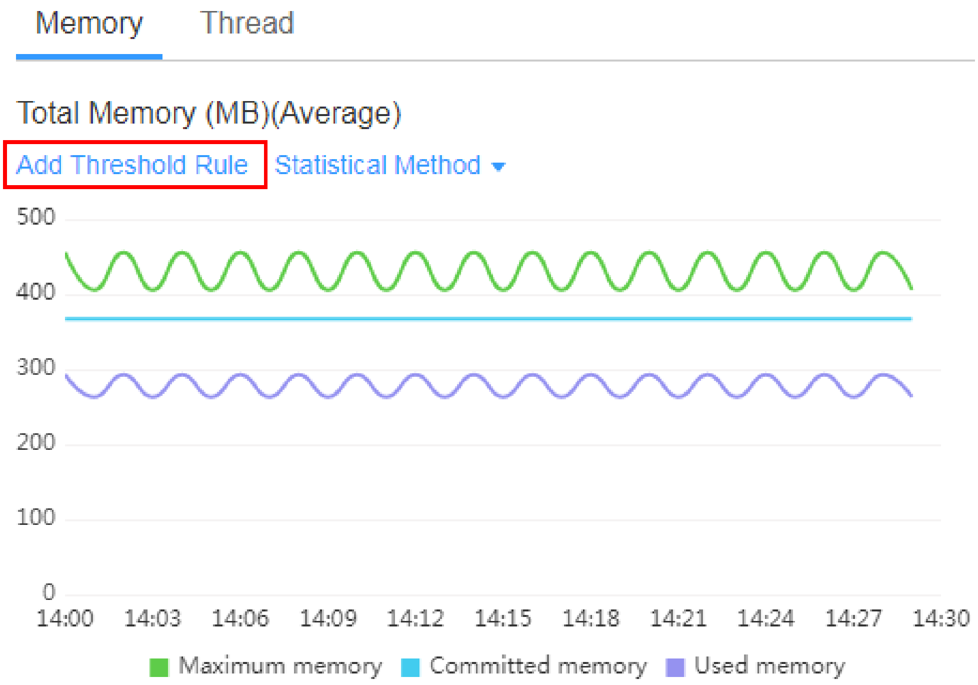
Thread Name	Description
Total threads	Both active and standby threads are included. Sticky threads and dedicated threads become standby threads after being executed.
Deadlock threads	When two or more threads encounter resource conflicts or the communication between them is abnormal, the system enters the deadlock state.
New threads	Number of threads that are newly created.
Runnable threads	Number of threads that can run.
Blocked threads	Number of threads that are blocked.
Waiting threads	Number of threads that are in the waiting state.
Timed waiting threads	Number of threads that are waiting for another thread to perform an action for a specified waiting time.
Terminated threads	Number of threads that are terminated.
Max connections	Maximum number of connections that are supported by Tomcat.
Current connections	Number of connections that are being occupied on Tomcat.
Max threads	Maximum number of threads that can be executed on Tomcat.
Current threads	Number of threads that are being executed on Tomcat.
Busy threads	Number of threads executed on Tomcat for processing tasks.

Adding a Threshold Rule

You can add threshold rules for all JVM memory and thread metrics. When the rules are met, alarms are reported, altering you to risks.

Step 1 On the **JVM Monitoring** page, select an application in the upper left corner, and then select an instance.

Step 2 In the trend graph of a memory or thread metric on the right, set a threshold rule. Specifically, click **Add Threshold Rule** on the top of the trend graph.

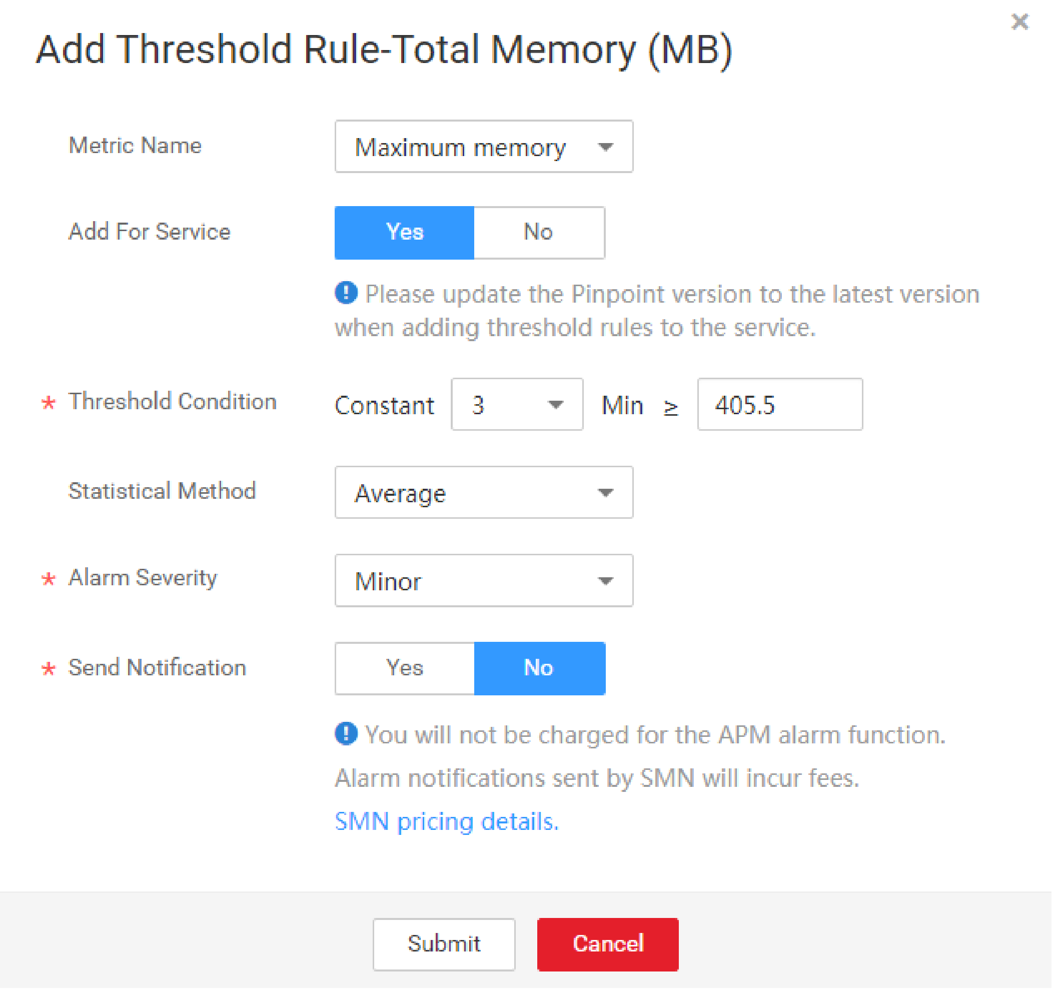


Step 3 Set rule parameters and click **Submit**, as shown in the following figure. If you want to receive alarm notifications, select **Yes** when setting **Send Notification** and then select a topic.

NOTE

Description of the **Add For Service** parameter:

- If this parameter is set to **Yes**, the threshold rule is applied to the entire service.
- If this parameter is set to **No**, the threshold rule is applied to a single instance.



Add Threshold Rule-Total Memory (MB)

Metric Name: Maximum memory

Add For Service: [✓ Yes] No

Please update the Pinpoint version to the latest version when adding threshold rules to the service.

* Threshold Condition: Constant 3 Min ≥ 405.5

Statistical Method: Average

* Alarm Severity: Minor

* Send Notification: Yes [✓ No]

You will not be charged for the APM alarm function. Alarm notifications sent by SMN will incur fees. SMN pricing details.

----End

9 ICAgent Installation and Configuration

9.1 Agent Management

9.1.1 Installing the ICAgent (Linux)

Prerequisites

Before installing the ICAgent, ensure that the time and time zone of the local browser are consistent with those of the desired server. If multiple servers are deployed, ensure that the local browser and multiple servers use the same time zone and time. Otherwise, the application topology and tracing data on the console may be incorrect.

Installation Methods

There are two methods to install the ICAgent. The two methods are not applicable to container nodes created using ServiceStage, or Cloud Container Engine (CCE). To monitor container nodes through APM, see **Application Performance Management Getting Started**. **Table 9-1** lists the ICAgent installation methods.

Table 9-1 Installation methods

Method	Application Scenario
Initial installation	This installation method is used when the following conditions are met: 1. An Elastic IP Address (EIP) has been bound to the server. For details, see **Assigning an EIP and Binding It to an ECS**. 2. The ICAgent has never been installed on the server.

Method	Application Scenario
Inherited installation	This installation method is used when the following conditions are met: You have multiple servers on which the ICAgent is to be installed. One server is bound to an EIP, but others are not bound to an EIP. The ICAgent has been installed on the server bound to an EIP. You can use this method to install the ICAgent on the servers that are not bound to an EIP.

Initial Installation

After you apply for a server on the cloud and install the ICAgent in the Linux environment, perform the following operations:

Step 1 Obtain an Access Key ID/Secret Access Key (AK/SK) by using either of the following methods:

- Obtain a temporary AK/SK by creating an agency. For details, see **How Do I Obtain the AK/SK by Creating an Agency?**.

  NOTE

  For each ECS server where the ICAgent is to be installed, you need to bind it to an agency on the ECS console. The agency relationship takes effect 5 minutes later.

- Obtain a permanent AK/SK by adding access keys. For details, see **How Do I Obtain the AK/SK and Project ID?**.

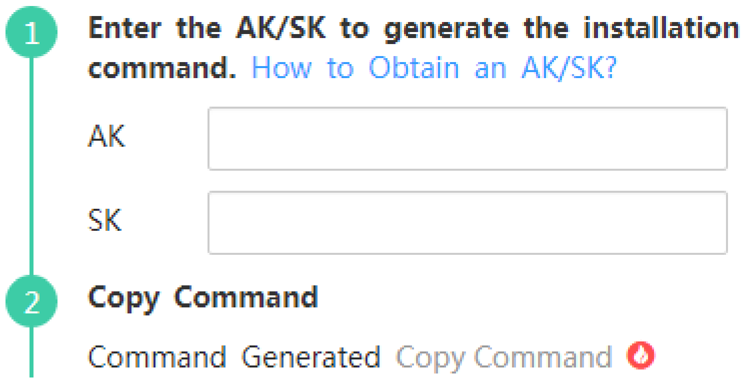
Step 2 Log in to the APM console. In the navigation pane, choose **Agent** > **Management**.

Step 3 Click **Install ICAgent**. On the page that is displayed, set **Host** to **HUAWEI CLOUD host** and **OS** to **Linux**.

Step 4 Generate the ICAgent installation command and copy it.

- As shown in **Figure 9-1**, if you have obtained the permanent AK/SK, set **Installation Mode** to **Obtain AK/SK** and enter the AK/SK in the text box to generate the ICAgent installation command. Then, click **Copy Command**.

Figure 9-1 Entering the AK/SK



1 Enter the AK/SK to generate the installation command. How to Obtain an AK/SK?

AK

SK

2 Copy Command

Command Generated Copy Command

NOTE

Ensure that the AK/SK are correct. Otherwise, the ICAgent cannot be installed.

- If you have obtained the temporary AK/SK, set **Installation Mode** to **Create Agency** and click **Copy Command** to copy the ICAgent installation command.

Step 5 Use a remote login tool to log in to the server where the ICAgent is to be installed as the **root** user and run the preceding command to install the ICAgent.

NOTE

- If the message "ICAgent install success" is displayed, the ICAgent is successfully installed in the **/opt/oss/servicemgr/** directory. After the ICAgent is successfully installed, choose **Agent** > **Management** in the navigation pane to view the ICAgent status.
- If the installation fails, uninstall the ICAgent according to **Uninstalling the ICAgent (Linux)** and then install it again. If the problem persists, contact technical support.

----End

Inherited Installation

If the ICAgent has been installed on a server and the installation package **ICProbeAgent.tar.gz** exists in the **/opt/ICAgent/** directory of the server, use this method to install the ICAgent on a remote server with a few clicks.

Step 1 Run the following command (***x.x.x.x*** indicates the server IP address) on the server where the ICAgent has been installed:

bash /opt/oss/servicemgr/ICAgent/bin/remoteInstall/remote_install.sh -ip x.x.x.x

Step 2 Enter the password of the **root** user of the server where the ICAgent is to be installed as prompted.

NOTE

- If both the expect tool and ICAgent have been installed on a server, the ICAgent is successfully installed on the remote server after the preceding command is run. If the ICAgent has been installed on a server, but the expect tool has not, enter the information as prompted.
- Ensure that the **root** user can run the **SSH** and **SCP** commands on the ECS server where the ICAgent has been installed to communicate with the remote ECS server where the ICAgent is to be installed.
- If the message "ICAgent install success" is displayed, the ICAgent is successfully installed in the **/opt/oss/servicemgr/** directory. After the ICAgent is successfully installed, choose **Agent** > **Management** in the navigation pane to view the ICAgent status.
- If the installation fails, uninstall the ICAgent according to **Uninstalling the ICAgent (Linux)** and then install it again. If the problem persists, contact technical support.

----End

Inherited Batch Installation

If the ICAgent has been installed on a server and the installation package **ICProbeAgent.tar.gz** exists in the **/opt/ICAgent/** directory of the server, use this method to install the ICAgent on multiple remote ECS servers with a few clicks.

NOTICE

1. Ensure that you can run the **SSH** and **SCP** commands on the ECS server where the ICAgent has been installed to communicate with the remote ECS servers where the ICAgent is to be installed.
2. If you have installed the ICAgent in a server through an agency, you also need to set an agency for other servers where the ICAgent is to be installed. For details, see **Creating an Agency**.
3. Batch installation scripts depend on Python versions. You are advised to implement batch installation on hosts running Python 2.x. Python 3.x does not support batch installation.

Prerequisites

The IP addresses and passwords of all ECS servers where the ICAgent is to be installed have been collected, sorted in the **iplist.cfg** file, and uploaded to the **/opt/ICAgent/** directory on the ECS server where the ICAgent has been installed. As shown in the following example, each IP address and password in the **iplist.cfg** file must be separated by a space.

192.168.0.109 password (Enter the actual password.)

192.168.0.39 password (Enter the actual password.)

NOTE

- Because the **iplist.cfg** file contains sensitive information, you are advised to clear it in time.
- If the passwords of all servers are the same, you only need to list IP addresses in the **iplist.cfg** file and enter the password once during execution. If the password of an IP address is different from those of other IP addresses, you need to list both passwords and IP addresses in the **iplist.cfg** file.
- The batch installation function depends on Python 2.7.*. If the system displays a message indicating that Python cannot be found during the installation, install Python 2.7.* and try again.

Procedure

Step 1 Run the following command on the server where the ICAgent has been installed:

bash /opt/oss/servicemgr/ICAgent/bin/remoteInstall/remote_install.sh -batchModeConfig /opt/ICAgent/iplist.cfg

Enter the default password of the **root** user of the servers where the ICAgent is to be installed as prompted. If the passwords of all IP addresses have been configured in the **iplist.cfg** file, press **Enter** to skip this step. Otherwise, enter the default password.

```
batch install begin
Please input default passwd:
send cmd to 192.168.0.109
send cmd to 192.168.0.39
2 tasks running, please wait...
2 tasks running, please wait...
2 tasks running, please wait...
End of install agent: 192.168.0.39
End of install agent: 192.168.0.109
All hosts install icagent finish.
```

Wait until the message "All hosts install icagent finish." is displayed, which indicates that the ICAgent has been successfully installed on all the hosts listed in the configuration file.

Step 2 After the ICAgent is successfully installed, choose **Agent** > **Management** in the navigation pane to view the ICAgent status.

----End

ICAgent Statuses

The following table lists the ICAgent statuses.

Table 9-2 ICAgent statuses

Status	Description
Running	The ICAgent is running properly.
Uninstalled	The ICAgent is not installed. For details about how to install the ICAgent, see **Installing the ICAgent (Linux)**.
Installing	The ICAgent is being installed. This operation takes about 1 minute to complete.
Installation failed	Failed to install the ICAgent. Uninstall the ICAgent according to **Uninstalling the ICAgent Through Logging In to a Server** and then install it again.
Upgrading	The ICAgent is being upgraded. This operation takes about 1 minute to complete.
Upgrade failed	Failed to upgrade the ICAgent. Uninstall the ICAgent according to **Uninstalling the ICAgent Through Logging In to a Server** and then install it again.
Offline	The AK/SK or ECS agency configurations are incorrect. Ensure that such configurations are correct.
Faulty	The ICAgent is faulty. Contact technical support.

9.1.2 Upgrading the ICAgent (Linux)

To ensure better collection experience, APM will continuously upgrade ICAgent versions. When the Linux system displays a message indicating that a new ICAgent version is available, perform the following operations:

Step 1 Log in to the APM console.

Step 2 In the navigation pane, choose **Agent** > **Management**.

Step 3 Select **Cluster: XXX** or **Other: user-defined nodes** from the drop-down list on the right of the page.

Step 4 Upgrade the ICAgent.

- If you select **Cluster: xxx** in **Step 3**, directly click **Upgrade ICAgent**. In this way, the ICAgent on all hosts in the cluster can be upgraded at a time.
- If you select **Other: user-defined nodes** in **Step 3**, select a desired host and then click **Upgrade ICAgent**.

Step 5 In the displayed **Upgrade ICAgent** dialog box, click **Yes**. Wait for about 1 minute to complete the ICAgent upgrade. When the ICAgent status changes from **Upgrading** to **Running**, the ICAgent is successfully upgraded.

----End

9.1.3 Uninstalling the ICAgent (Linux)

If the ICAgent on a server is uninstalled, server O&M will be affected, making topology and tracing functions unavailable. Exercise caution when performing this operation.

You can uninstall the ICAgent using either of the following methods:

- **Uninstalling the ICAgent Through the APM Console**: The ICAgent has been successfully installed, and needs to be uninstalled.
- **Uninstalling the ICAgent Through Logging In to a Server**: The ICAgent fails to be installed, and needs to be uninstalled.
- **Remotely Uninstalling the ICAgent**: The ICAgent has been successfully installed, and needs to be remotely uninstalled.
- **Uninstalling the ICAgent in Batches**: The ICAgent has been successfully installed, and needs to be uninstalled in batches.

Uninstalling the ICAgent Through the APM Console

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

Step 2 Select **Other: user-defined nodes** from the drop-down list on the right of the page.

Step 3 Select one or more servers whose ICAgent is to be uninstalled, and click **Uninstall ICAgent**. In the **Uninstall ICAgent** dialog box, click **Yes**.

Wait for about 1 minute to complete the uninstallation. When the ICAgent status changes from **Uninstalling** to **Uninstall**, the ICAgent is successfully uninstalled.

NOTE

To reinstall the ICAgent, wait for 5 minutes after it is uninstalled. Otherwise, the ICAgent may be automatically uninstalled.

----End

Uninstalling the ICAgent Through Logging In to a Server

Step 1 Log in to the server from which the ICAgent is to be uninstalled as the **root** user.

Step 2 Run the following command to uninstall the ICAgent:

```
bash /opt/oss/servicemgr/ICAgent/bin/manual/uninstall.sh;
```

Step 3 Wait until the message "ICAgent uninstall success" is displayed.

----End

Remotely Uninstalling the ICAgent

In addition to the preceding methods, you can use a method similar to **Inherited Installation** to remotely uninstall the ICAgent.

Step 1 Run the following command (***x.x.x.x*** indicates the server IP address) on the server where the ICAgent has been installed:

```
bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -ip x.x.x.x
```

Step 2 Enter the password of the **root** user of the server where the ICAgent is to be uninstalled as prompted.

NOTE

- If both the expect tool and ICAgent have been installed on a server, the ICAgent is successfully uninstalled from the remote server after the preceding command is run. If the ICAgent has been installed on a server, but the expect tool has not, enter the information as prompted.
- Ensure that the **root** user can run the **SSH** and **SCP** commands on the Elastic Cloud Server (ECS) server where the ICAgent has been installed to communicate with the remote ECS server where the ICAgent is to be uninstalled.
- If the message "ICAgent uninstall success" is displayed, the ICAgent is successfully uninstalled. After the ICAgent is successfully uninstalled, choose **Agent** > **Management** in the navigation pane to view the ICAgent status.

----End

Uninstalling the ICAgent in Batches

If the ICAgent has been installed on a server and the installation package **ICProbeAgent.zip** exists in the **/opt/ICAgent/** directory of the server, use this method to uninstall the ICAgent from multiple remote ECS servers with a few clicks.

NOTICE

The ECS servers must belong to the same Virtual Private Cloud (VPC) and network segment.

Prerequisites

The IP addresses and passwords of all ECS servers where the ICAgent is to be uninstalled have been collected, sorted in the **iplist.cfg** file, and uploaded to the **/opt/ICAgent/** directory on the ECS server where the ICAgent has been installed. As shown in the following example, each IP address and password in the **iplist.cfg** file must be separated by a space.

192.168.0.109 password (Enter the actual password.)

192.168.0.39 password (Enter the actual password.)

NOTE

- Because the **iplist.cfg** file contains sensitive information, you are advised to clear it in time.
- If the passwords of all servers are the same, you only need to list IP addresses in the **iplist.cfg** file and enter the password once during execution. If the password of an IP address is different from those of other IP addresses, you need to list both passwords and IP addresses in the **iplist.cfg** file.

Procedure

Step 1 Run the following command on the server where the ICAgent has been installed:

```
bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -batchModeConfig /opt/ICAgent/iplist.cfg
```

Enter the default password of the **root** user of the servers where the ICAgent is to be uninstalled as prompted. If the passwords of all IP addresses have been configured in the **iplist.cfg** file, press **Enter** to skip this step. Otherwise, enter the default password.

```
batch uninstall begin
Please input default passwd:
send cmd to 192.168.0.109
send cmd to 192.168.0.39
2 tasks running, please wait...
End of uninstall agent: 192.168.0.109
End of uninstall agent: 192.168.0.39
All hosts uninstall icagent finish.
```

Wait until the message "All hosts uninstall icagent finish." is displayed, which indicates that the ICAgent has been successfully uninstalled from all the hosts listed in the configuration file.

Step 2 After the ICAgent is successfully uninstalled, choose **Agent** > **Management** in the navigation pane to view the ICAgent status.

----End

9.2 Collection Configuration

To reduce memory, database, and disk space usage, you can implement collection configuration as required. The collection configuration takes effect for selected applications.

Procedure

Step 1 Log in to the APM. In the navigation pane, choose **Agent** > **Configuration**.

Step 2 Select an application from the **Application** drop-down list.

Step 3 Click ○— to enable data collection.

NOTE

This function is enabled by default. When you do not need to collect tracing and topology data of a specific application, disable this function to reduce resource usage.

Step 4 Click ○ to enable the function of collecting normal call chain data.

To reduce the resources consumed by probes, APM collects one more data record every minute when a transaction is abnormal or the latency is greater than **Application Performance Index (Apdex) Threshold**. If this function is enabled, normal call chain data is sampled and collected. If this function is disabled, normal call chain data is not collected.

Step 5 Click ○ to enable memory monitoring.

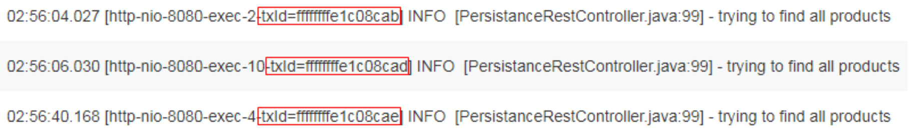
To prevent probes from affecting service performance in peak hours, enable memory monitoring. When the instance memory usage is excessively high, probes enter the hibernation state. You can also click ✎ to set the duration and memory usage.

NOTE

- Memory usage = Used memory of the Java process/Maximum available memory
- Maximum available memory: Use the smaller value between the available memory quota of the container and the maximum heap memory of the JVM. The maximum heap memory of the JVM is the value of **-Xmx**. The default value is 25% of the maximum available memory of the JVM.
- The memory usage during collection suspension must be greater than or equal to that during collection restoration.

Step 6 Click ○ to enable the function of adding trace IDs to logs.

A trace ID uniquely identifies a tracing. When this function is enabled, the system adds trace IDs to logs. You can accurately search for logs based on trace IDs, such as **ffffffffe1c08cab**, **ffffffffe1c08cad**, and **ffffffffe1c08cae**, as shown in the following figure.



```
02:56:04.027 [http-nio-8080-exec-2-txId=ffffffffe1c08cab] INFO  [PersistanceRestController.java:99] - trying to find all products
02:56:06.030 [http-nio-8080-exec-10-txId=ffffffffe1c08cad] INFO  [PersistanceRestController.java:99] - trying to find all products
02:56:40.168 [http-nio-8080-exec-4-txId=ffffffffe1c08cae] INFO  [PersistanceRestController.java:99] - trying to find all products
```

Step 7 Click ○ to enable SQL analysis.

When this function is disabled, no SQL data is affected, but you cannot implement SQL analysis.

Step 8 Set the HTTP response codes to be ignored.

To prevent unnecessary error reporting, and quickly and accurately locate faulty tracing, set the HTTP response codes to be ignored. They will not be recorded in error record tables. Click ✎, enter the HTTP response codes to be ignored, and click ✓. If there are multiple HTTP response codes, separate them by commas (,).

Step 9 Set the errors and exceptions to be ignored.

To prevent unnecessary error reporting, and quickly and accurately locate faulty tracing, set the errors and exceptions to be ignored. They will not be recorded in error record tables. Click ✎, enter the errors and exceptions to be ignored, and click ✓. If there are multiple types of Java exceptions, separate them by commas (,). The default value is null.

----End

9.3 Configuration Center

Setting Apdex Thresholds

Step 1 Log in to the APM console. In the navigation pane, choose **Configuration Center**.

Step 2 Select an application from the drop-down list.

Step 3 Set Application Performance Index (Apdex) thresholds. For details, see **Basic Concepts**.

- Click ✎ next to **Topology Apdex Threshold (ms)**, enter a topology Apdex threshold, and click ✓ to save the threshold.

  NOTE

  The default topology Apdex threshold is 100 ms.

- Click ✎ next to **Transaction Apdex Threshold (ms)**, enter a transaction Apdex threshold, and click ✓ to save the threshold.

  NOTE

  - The default transaction Apdex threshold is 500 ms.
  - This setting takes effect for all transactions of the application. If an Apdex threshold has been separately set for a transaction, the currently set Apdex threshold takes effect for all transactions except this transaction. To separately set an Apdex threshold for a transaction, do as follows:
    1. In the navigation pane, choose **Transactions**.
    2. In the drop-down list in the upper left corner, select the application to which the transaction belongs.
    3. In the transaction list, click ✓ in the **Apdex Threshold (ms)** column of the desired transaction, enter an Apdex threshold, and then click ✓ to save the threshold.

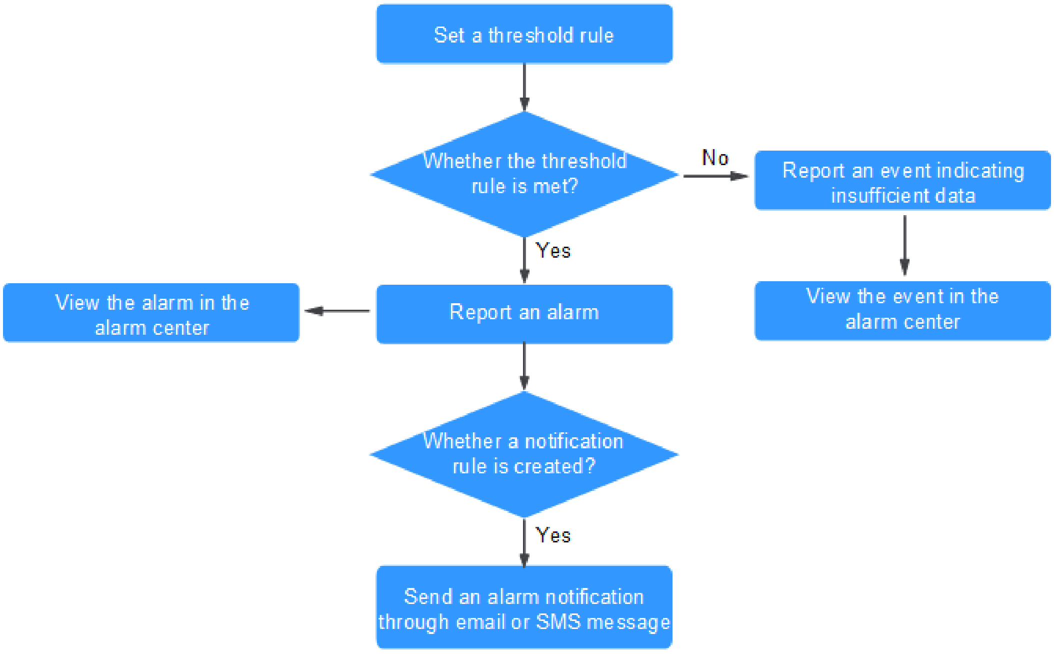
----End

10 Alarm Center

10.1 Viewing Alarms

Alarms are reported when APM or an external service, such as ServiceStage, or Cloud Container Engine (CCE), is abnormal or may cause exceptions. Alarms need to be handled. Otherwise, service exceptions may occur.

Flowchart


Set a threshold rule
Whether the threshold rule is met?
No
Report an event indicating insufficient data
View the event in the alarm center
Yes
Report an alarm
View the alarm in the alarm center
Whether a notification rule is created?
Yes
Send an alarm notification through email or SMS message

Procedure

Step 1 Log in to the APM console.

Step 2 In the navigation pane, choose **Alarm Center** > **Alarm List**.

Step 3 View alarms on the **Alarm List** page.

1. Set a time range to view alarms. There are two methods to set a time range:

   Method 1: Use the predefined time label, for example, **Last 1 hour**, **Last 6 hours**, or **Last 1 day**. You can choose one based on service requirements.

   Method 2: Customize a time range. The time range can be 30 days at most.

2. Set filter criteria and click **Search** to view alarms.

   Click **Reset** to reset filter criteria.

Step 4 Perform the operations described in **Table 10-1** if needed.

Table 10-1 Operations

Operation	Method	Description
Viewing alarm statistics	View alarm statistics that meet specific filter criteria within a specific time range through a bar graph.	-
Clearing alarms	Click **Clear** in the **Operation** column of a target alarm.	● You can clear an alarm after the problem that causes this alarm is resolved. ● Cleared alarms cannot be queried.
Viewing alarm details	Click **View Details** in the **Operation** column of the target alarm to view alarm details.	-
Viewing the latest alarms	Click 🔔 on the right of the page to view the latest three alarms.	-

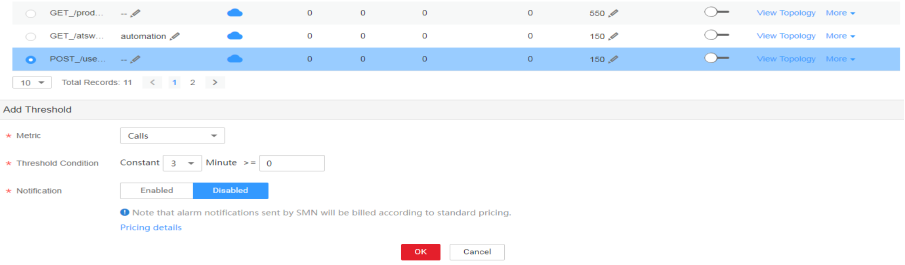
----End

Setting Threshold Rules for Transaction Metrics

APM supports alarm reporting when transaction exceptions occur. You can set threshold rules for transaction metrics. When metric values meet the threshold rules, alarms will be reported to the alarm center. To view alarms, choose **Alarm Center** > **Alarm List** in the navigation pane. The following uses the **Calls** metric of transactions as an example.

Step 1 On the **Transactions** page, choose **More** > **Modify Threshold** in the **Operation** column. The **Add Threshold** page is displayed.

Figure 10-1 Adding a threshold rule for a transaction metric



○	GET_/prod...	--		0	0	0	0	550		View Topology	More ▾
○	GET_/atsw...	automation		0	0	0	0	150		View Topology	More ▾
●	POST_/use...	--		0	0	0	0	150		View Topology	More ▾

10 ▾ Total Records: 11 < 1 2 >

Add Threshold

* Metric: Calls

* Threshold Condition: Constant 3 Minute >= 0

* Notification: Enabled [✓ Disabled]

Note that alarm notifications sent by SMN will be billed according to standard pricing.

Pricing details

OK Cancel

Step 2 Select the **Calls** metric. Transaction metrics include **Calls**, **Total latency**, **Errors**, and **Apdex**.

Step 3 Set the threshold condition: When there are 15 or more calls in 3 minutes, an alarm will be reported.

Step 4 If you do not need to receive notifications, select **Disabled** for **Notification** and then click **OK**.

NOTE

If you want to receive notifications, select **Enabled**. For details, see **Setting Alarm Notification**.

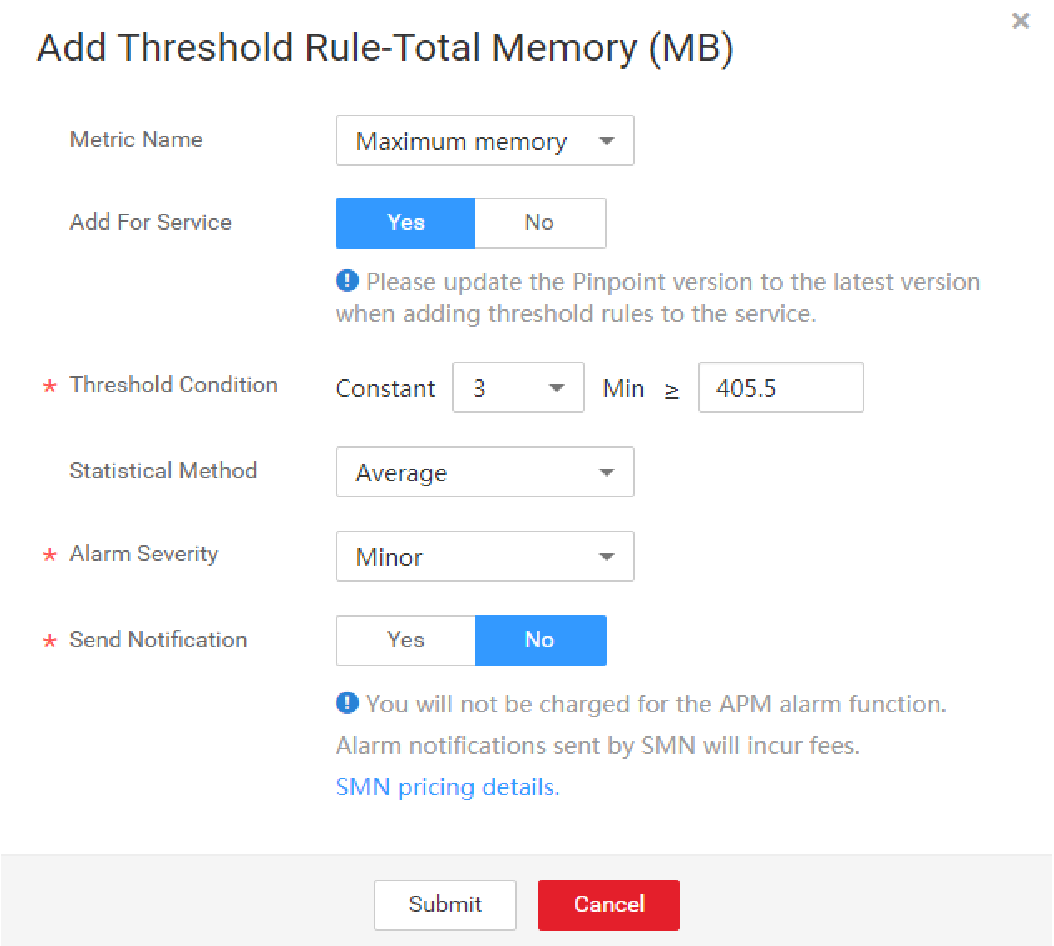
----End

Setting Threshold Rules for JVM Metrics

APM supports alarm reporting when JVM memory and thread metrics are abnormal. You can set threshold rules for JVM metrics. When metric values meet the threshold rules, alarms will be reported to the alarm center. To view alarms, choose **Alarm Center** > **Alarm List** in the navigation pane. The following uses the **Maximum memory** metric of the total memory as an example.

Step 1 On the **JVM Monitoring** page, click **Add Threshold Rule**.

Figure 10-2 Adding a threshold rule



Add Threshold Rule-Total Memory (MB)

Metric Name: Maximum memory

Add For Service: Yes

Please update the Pinpoint version to the latest version when adding threshold rules to the service.

* Threshold Condition: Constant 3 Min ≥ 405.5

Statistical Method: Average

* Alarm Severity: Minor

* Send Notification: No

You will not be charged for the APM alarm function. Alarm notifications sent by SMN will incur fees. SMN pricing details.

Step 2 On the page that is displayed, select the **Maximum memory** metric name. Other options are **Committed memory** and **Used memory**.

Step 3 Set the threshold condition: When the total memory is greater than or equal to 15 MB for 3 minutes, an alarm will be reported.

Step 4 Select the **Average** statistical method. Other options are **Maximum** and **Minimum**.

Step 5 Select the **Minor** alarm severity. Other options are **Critical**, **Major**, and **Warning**.

Step 6 If you do not need to receive notifications, select **No** for **Send Notification** and click **Submit**.

NOTE

If you want to receive notifications, select **Yes**. For details, see **Setting Alarm Notification**.

----End

10.2 Viewing Events

Events generally carry some important information. They are reported when APM or an external service, such as ServiceStage, or Cloud Container Engine (CCE) encounters some changes. Such changes do not necessarily cause service exceptions. Events do not need to be handled.

Procedure

Step 1 Log in to the APM console.

Step 2 In the navigation pane, choose **Alarm Center** > **Event List**.

Step 3 View events on the **Event List** page.

1. Set a time range to view events. There are two methods to set a time range:

   Method 1: Use the predefined time label, for example, **Last 1 hour**, **Last 6 hours**, or **Last 1 day**. You can choose one based on service requirements.

   Method 2: Customize a time range. The time range can be 30 days at most.

2. Set filter criteria and click **Search** to view events.

   Click **Reset** to reset filter criteria.

Step 4 Perform the operations described in **Table 10-2** if needed.

Table 10-2 Operations

Operation	Method	Description
Viewing event statistics	View event statistics that meet filter criteria within a specific time range through a bar graph.	-

----End

10.3 Setting Alarm Notification

APM supports alarm notification. That is, a certain type of alarms can be sent to specified users by Short Message Service (SMS) message or email. In this way, they can identify and rectify cluster exceptions at the earliest time, avoiding service loss.

You can create a maximum of 10 notification rules. If the number of notification rules reaches 10, delete unnecessary notification rules and create new ones.

If you do not create any notification rule, you cannot receive alarm notifications. In that case, you can only log in to the APM console and choose **Alarm Center** > **Alarm List** to view alarms.

APM enables you to create notification rules only for the alarms listed in **Table 10-3**.

Table 10-3 Alarm types

Alarm Type	Description
Probe hibernation alarm	Generated when the probe is in hibernation state.
Collector installation alarm	Generated when the ICAgent fails to be installed, upgraded, or uninstalled, or is abnormal.
Threshold alarm	Generated when a threshold rule is triggered.

NOTE

More types of alarms are being developed.

Creating a Notification Rule

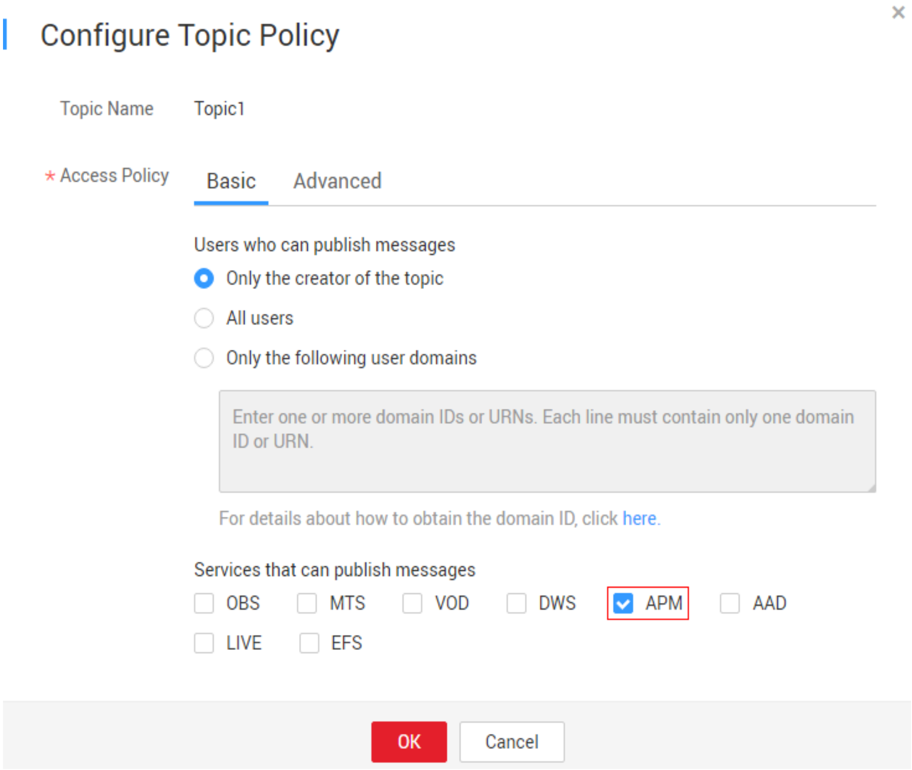
Step 1 Log in to the APM console.

Step 2 In the navigation pane, choose **Alarm Center** > **Notification Rules**, and click **Create Notification Rule**.

Step 3 Create a topic, configure a topic policy, and add subscribers to the topic. If you have made such configurations, skip this step.

1. Access the Simple Message Notification (SMN) console: When APM is interconnected with SMN, click **Create SMN Topic** to access the SMN console.
2. Create a topic: In the navigation pane of the SMN console, choose **Topic Management** > **Topics**. Then click **Create Topic**. On the page that is displayed, enter a topic name and click **OK**. For details, see **Creating a Topic**.
3. Configure a topic policy according to **Figure 10-3**. Otherwise, alarm notifications will fail to be sent. Then, add subscribers, that is, SMS message or email receivers of alarm notifications. For details, see **Configuring Topic Policies**, and **Adding a Subscription**. In this way, when an exception occurs in a cluster, APM can broadcast the alarm information to the subscribers in real time.

Figure 10-3 Configuring a topic policy



Configure Topic Policy

Topic Name Topic1

* Access Policy Basic Advanced

Users who can publish messages

● Only the creator of the topic

○ All users

○ Only the following user domains

Enter one or more domain IDs or URNs. Each line must contain only one domain ID or URN.

For details about how to obtain the domain ID, click here.

Services that can publish messages

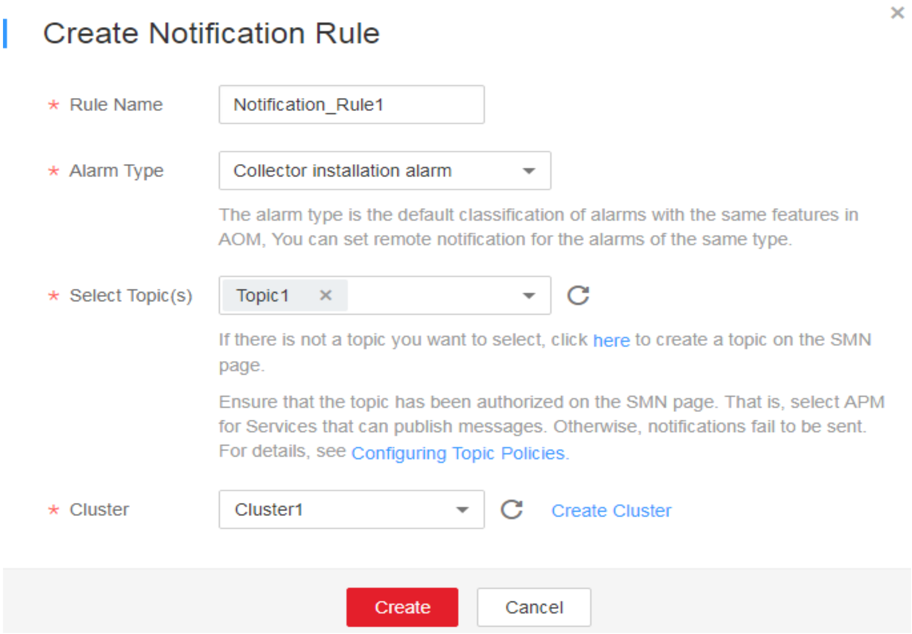
□ OBS □ MTS □ VOD □ DWS ☑ APM □ AAD

□ LIVE □ EFS

Step 4 Enter a rule name, select an alarm type (for details, see **Table 10-3**), select the topic created in **Step 3**, customize a cluster to be monitored, and click **Create**, as shown in **Figure 10-4**.

After the notification rule is created, if an alarm that meets the notification rule is generated, APM automatically sends notifications by SMS message or email.

Figure 10-4 Creating a notification rule



Create Notification Rule

* Rule Name Notification_Rule1

* Alarm Type Collector installation alarm

The alarm type is the default classification of alarms with the same features in AOM, You can set remote notification for the alarms of the same type.

* Select Topic(s) Topic1

If there is not a topic you want to select, click here to create a topic on the SMN page.

Ensure that the topic has been authorized on the SMN page. That is, select APM for Services that can publish messages. Otherwise, notifications fail to be sent. For details, see Configuring Topic Policies.

* Cluster Cluster1

----End

More Operations

After creating a notification rule, you can also perform the operations described in **Table 10-4**.

Table 10-4 Related operations

Operation	Description
Modifying a notification rule	Click **Modify** in the **Operation** column.
Deleting a notification rule	● To delete a notification rule, click **Delete** in the **Operation** column. ● To delete one or more notification rules, select it or them and click **Delete** above the notification rule list.
Searching for a notification rule	Enter a keyword of the notification rule name in the search box in the upper right corner and click 🔍.

11 Auditing

11.1 Operations Logged by CTS

With CTS, you can record operations associated with APM for future query, audit, and backtracking.

Table 11-1 Operations logged by CTS

Operation	Resource Type	Trace Name
Deleting an application	APM	clearApps
Setting a transaction alias	APM	setAlias
Modifying the VM service group	APM	updateVirtualService
Modifying the transaction configuration	APM	updateTxTypeSettings
Modifying the topology Apdex threshold	APM	updateThresholds
Setting the transaction group	APM	txtypeGroupOperation
Deleting the application configuration	apm	deleteAppGroup
Modifying the data collection configuration	apm	setAppPpswitcherConfig
Modifying the intelligent sampling configuration	apm	setAppCallChainConfig

Operation	Resource Type	Trace Name
Modifying the configuration of the memory monitoring mechanism	apm	setAppMwsConfig
Modifying the configuration for adding trace IDs to logs	apm	setAppLogTransacConfig
Modifying the SQL analysis configuration	apm	setAppSqlConfig
Modifying the configuration of errors and exceptions or HTTP response codes to be ignored	apm	setAppIgnoreConfig

11.2 Viewing Audit Logs

For details, see **Querying Real-Time Traces**.