Application Performance Management 2.0

User Guide

Issue	01
Date	2024-12-26

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

1 Before You Start

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

Application List	The **Applications** page displays information such as components, environments, Agent status, and supported operations.
CMDB Management	APM has built-in CMDB for managing the application structure and related configurations.
Application Metric Monitoring	APM can manage tags and monitor the metric data of JVM, GC, service calls, exceptions, external calls, database access, and middleware, helping you comprehensively monitor application running. Application metrics can be reported to the AOM console through Prometheus instances.
Tracing	Information such as the call status, duration, and API is displayed, helping you further locate fault causes.
Application Topology	The call and dependency relationships between applications are displayed, and abnormal instances can be automatically discovered. There are two types of application topologies: • Single-component topology: topology of a single component under an environment. You can also view the call relationships of direct and indirect upstream and downstream components. • Global application topology: topology of some or all components under an application.
URL Tracing	Through URL tracing, you can monitor the call relationships between important APIs and downstream services, and then detect problems more precisely.
Resource Tag Management	You can tag resources under your account for classification.

Managing Tags	You can add tags for different environments and applications for easy management.
Alarm Management	When an application connected to APM meets a preset alarm condition, an alarm is triggered and reported in a timely manner. In this way, you can quickly learn about service exceptions and rectify faults to prevent loss.
AgentAgent Management	Agent Management allows you to check the deployment and running statuses of the Agents that are connected to APM, and to stop, start, or delete them.
Configuration Management	Configuration Management manages and displays the configurations supported by APM in a centralized manner. It consists of two parts: • Collection Center: displays collectors in a centralized manner. You can view and manage various collectors, metrics, and collection parameters supported by APM. • Data Masking: You can set policies to mask the data reported using APM 2.0 APIs.
System Management	System Management manages and displays system configurations in a centralized manner, including: • Access Keys: long-term identity credentials. They ensure that the requests are secret, complete, and correct. • General Configuration: You can determine whether to collect data through bytecode instrumentation, specify the slow request threshold and maximum number of rows to collect, and set web monitoring aggregation. • Agent Count: APM counts the number of Agents used by tenants.
Permissions Management	Enterprise Project Management Service (EPS) is used to control user access to APM resources.
Learn more	**Permissions Management** Create a user and grant permissions. **Getting Started** Learn how to connect applications to APM in different scenarios.

2 Application List

Application List

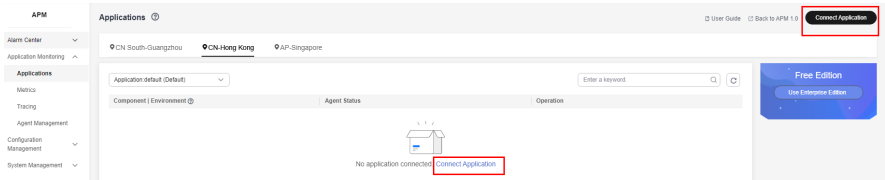
The **Applications** page displays information such as components, environments, Agent status, and supported operations.

Step 1 Log in to the management console.

Step 2 Click  on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane on the left, choose **Application Monitoring** > **Applications**.

Figure 2-1 Application list



Component|Environment: name of a component or environment. You can click the text in blue to go to the corresponding to component or environment page.

Agent Status: number of Agents in different statuses.

The following table describes the Agent statuses.

Status	Description
Enabled	The Agent is running properly.
Offline	• The Agent is offline due to network problems. Check and restore the network. • The Agent is offline if your process does not exist. • The Agent is disabled and offline if the trial period expires.

Status	Description
Disabled	The Agent is manually or globally disabled. Contact technical support.

----End

More Operations

Perform the operations listed in **Table 2-1** if needed.

Table 2-1 Related operations

Operation	Description
Selecting an application	Select an application from the **Application** drop-down list on the left of the page.
Viewing the topology of an environment	Click **Topology** in the **Operation** column of an environment.
Setting a component or environment	Click **Configure** in the **Operation** column. On the displayed **Instance** tab page, set the component or environment as required.
Deleting an environment	Click **Delete** in the **Operation** column of an environment.
Searching for a component or environment	Enter a component or environment keyword or name on the right.

Subscribing to Enterprise-Edition APM

After you subscribe to the enterprise-edition APM, preferential package information will be displayed. You can purchase preferential packages online.

Step 1 In the navigation pane on the left, choose **Application Monitoring** > **Applications**.

Step 2 Click **Buy Package** on the right. The **Buy Package** page is displayed.

Step 3 Select a region.

Step 4 Click a certain type of Agent package and click **+** or **-** to increase or decrease the number of packages as required. If needed, select Agent packages of multiple levels.

Step 5 Click **Buy Now**. The list of selected Agent packages is displayed.

Step 6 Read the **APM Service Agreement** and **Privacy Statement** and then select the checkbox to confirm that you have read them.

Step 7 Click **Submit**. The APM purchase information is displayed.

Step 8 Select a payment method and pay money.

NOTE

- The current edition is the enterprise edition. The pay-per-use price is $0.96 USD Agent × day. Select required preferential packages to save money.
- The Agent quota of your preferential package will be used first. If the quota is used up or your package expires, APM will charge by your usage.
- After you purchase a preferential package, it cannot be unsubscribed. After the package expires, you can continue using APM and your data is still secure.
- Please complete the payment within three days. Otherwise, the order will be automatically canceled.

----End

3 CMDB Management

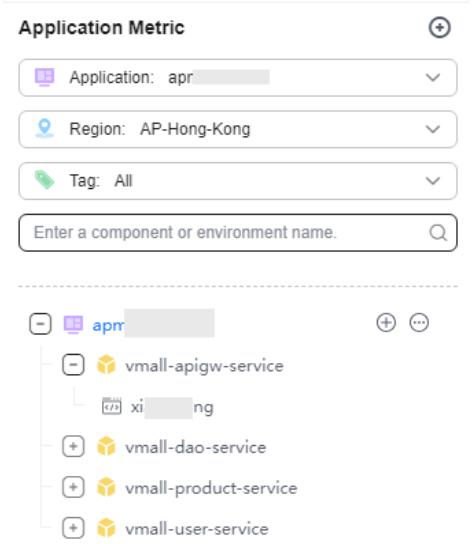
3.1 Introduction

APM has a built-in CMDB for managing application structure information and related configurations. It involves the following concepts:

- **Enterprise project**: An enterprise project can contain one or more applications.
- **Application** (global concept): a logical unit. An application can be an independent functional module. The same application information can be viewed in all regions. It is optional to associate an application with an enterprise project. The application associated with an enterprise project is managed based on enterprise project permissions. The application not associated with any enterprise project is managed based on the Identity and Access Management (IAM) permissions.
- **Sub-application** (global concept): similar to a folder. There can be up to three layers of sub-applications under an application.
- **Component** (global concept): a program or microservice. It is generally used together with environments. It may contain one or more environments. For example, an order app can be deployed in the function test environment, pressure test environment, pre-release environment, or live network environment.
- **Environment**: Components or programs with different configurations are deployed in different environments. Each environment has its own region attribute. You can filter environments by region. You can also add one or more tags to an environment and filter environments by tag.
- **Instance**: a process in an environment. It is named in the format of "host name+IP address+instance name". An environment is usually deployed on different hosts or containers. If an environment is deployed on one host, differentiation by instance is supported.
- **Environment tag**: an attribute for filtering environments. Different environments may have the same tag. Tags carry public configuration capabilities. For example, the configuration set on a tag can be shared by the environments with the same tag. Tags defined for environments of one application cannot be applied to other applications.

The following shows an example of the CMDB structure.

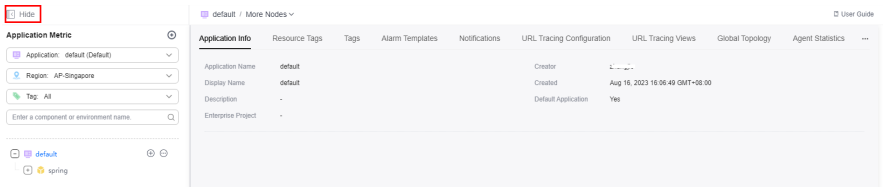
Figure 3-1 CMDB structure



The CMDB structure tree can be hidden.

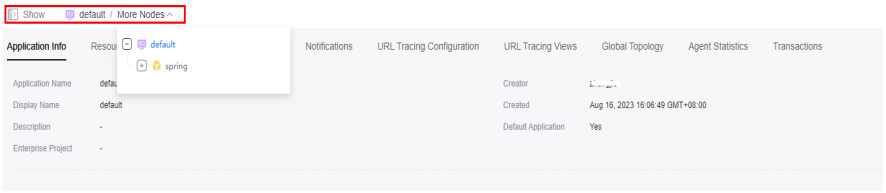
Step 1 Click **Hide** to hide the CMDB structure tree.

Figure 3-2 Hiding the CMDB structure tree



Step 2 Go to the path above in the upper part of the page and select your target node.

Figure 3-3 Selecting a node



Step 3 Click **Expand** to display the CMDB structure tree.

----End

3.2 Creating an Application

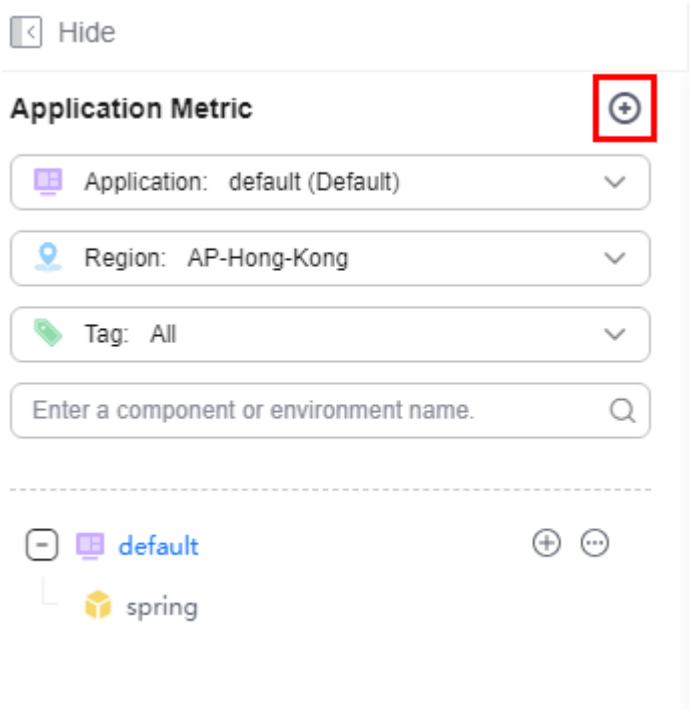
Step 1 Log in to the management console.

Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 Click ⊕ on the right of **Application Metric** to create an application.

Figure 3-4 Creating an application



Step 5 In the displayed dialog box, set application parameters.

Table 3-1 Parameters for creating an application

Parameter	Description
Application Name	Name of an application, which cannot be empty. Enter 1 to 128 characters and start with a letter. Only digits, letters, underscores (_), and hyphens (-) are allowed.
Display Name	Application alias. The alias takes precedence over the application name to display. Enter 1 to 128 characters. Only digits, letters, underscores (_), hyphens (-), brackets, and periods (.) are allowed.
Enterprise Project	Select an enterprise project from the drop-down list. This parameter is displayed only when you use the enterprise edition.
Description	Description of the application. Enter up to 1000 characters.

Step 6 Click **Confirm**.

NOTE

After an application is created, connect it to APM for monitoring. For details about the access method, see .

----End

3.3 Creating a Sub-application

Step 1 Log in to the management console.

Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 Click ⊕ next to your target application in the tree.

Step 5 In the displayed dialog box, set sub-application parameters.

Table 3-2 Parameters for creating a sub-application

Parameter	Description
Sub-application Name	Name of a sub-application, which cannot be empty. Enter 1 to 128 characters and start with a letter. Only digits, letters, underscores (_), and hyphens (-) are allowed.
Display Name	Display name of a sub-application, which cannot be empty. Enter 1 to 128 characters. Only digits, letters, underscores (_), hyphens (-), brackets, and periods (.) are allowed.
Description	Description of the sub-application. Enter up to 1000 characters.

Step 6 Click **Yes**.

NOTE

A maximum of three layers of sub-applications can be created.

----End

3.4 Configuring an Application and Sub-application

Step 1 Log in to the management console.

Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 Click  next to the application or sub-application name in the tree.

Step 5 Configure the application and sub-application according to **Table 3-3**.

Table 3-3 Parameters for configuring the application and sub-application

Operation	Description
Modify	Click **Modify**. In the displayed dialog box, modify the information about the application or sub-application.
Set as Default	If you select **Set as Default** for an application, it will become the default application. When you log in to the system, the default application will be selected. This option is not available for sub-applications.
Delete	Click **Delete**.

Step 6 Click **Yes**.

----End

3.5 Checking the Basic Information About an Application, Sub-Application, Component, and Environment

Checking the Basic Information About an Application

Step 1 Log in to the management console.

Step 2 Click  on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 Click an application in the tree on the left.

Step 5 In the right pane, click **Application Info** to check the basic information about the application.

Table 3-4 Basic information of the application

Parameter	Description
Application Name	Name of the application.
Display Name	Alias of the application.

Parameter	Description
Description	Description of the application. Enter up to 1,000 characters.
Enterprise Project	Enterprise project name. It is displayed only when you have enabled the enterprise edition.
Creator	User who creates the application.
Created	Time when the application is created.
Default Application	Whether the application is the default one. If it is a default application, **(Default)** will be displayed next to its name in the **Application** column in the tree on the left.

----End

Checking the Basic Information About a Sub-Application and Component

Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 2 Click a sub-application or component in the tree on the left. **Sub-application Info** or **Component Info** is displayed on the right.

Table 3-5 Basic information about the sub-application or component

Parameter	Description
Sub-Application/ Component Name	Name of the sub-application or component.
Display Name	Alias of the sub-application or component.
Description	Description of the sub-application or component. Enter up to 1,000 characters.
Creator	User who creates the sub-application or component.
Created	Time when the sub-application or component is created.

----End

NOTE

Environment and components are created when you connect an Agent. To monitor Java applications, see **Connecting Agents**.

Checking the Basic Information About an Environment

Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 2 In the tree on the left, click next to the target environment. The instance monitoring page is displayed.

Step 3 Click the **Basic Info** tab to check the basic information about the environment.

Table 3-6 Basic information about the environment

Basic Attributes	Parameter	Description
Component	Component Name	Name of a component.
	Created	Time when the component is created.
	Creator	User who creates the component.
Environment	Environment Name	Name of an environment.
	Environment Type	Type of the environment.
	Tag Name	Environment tag. For details about how to manage tags, see **Managing Tags**.
	Region	Region where the environment is located.
	Creator	User who creates the environment.
	Created	Time when the environment is created.
	UUID	Component ID.

----End

4 Application Metric Monitoring

4.1 Overview

APM Agents periodically collect performance metric data to measure the overall health status of applications. They can collect the metric data of JVM, GC, service calls, exceptions, external calls, database access, and middleware, helping you comprehensively monitor application running.

APM has strict definitions on metric data collection. Each type of data to be collected corresponds to a collector. For example, for JVM data of Java applications, a JVM collector is provided. A collector collects data of multiple metric sets. For details about collectors and metric sets, see **Collection Center**.

After collectors are deployed in the environment, monitoring items are generated. During data collection, the monitoring items determine data structures and collection behaviors.

- Collection period: A monitoring item has the same period attribute as a data collector. The default data collection period is 1 minute and cannot be changed.
- Monitoring item status: A monitoring item is enabled by default. You can disable it so that an Agent does not intercept or report the metric data. For details, see **Enabling or Disabling a Monitoring Item**.
- Collection status: Each collection instance or monitoring item has a collection status. If a collection error occurs, you can view it on the **Collection Status** tab page. A common error is that there are too many primary keys. As a result, data aggregation on the client is abnormal.

Monitoring Item Types

Agents automatically discover collection plug-ins and instantiate collectors to form monitoring items. Monitoring items are instantiated in an environment.

There are many types of collectors, which are hard to distinguish. The system backend groups collectors for easy data query.

Application monitoring enables you to monitor the overall health status of applications. Basic monitoring items include the topology, URL, JVM, and

exceptions. Other monitoring items, such as calls, communication protocols, databases, web containers, caches, and message queues, are automatically discovered and displayed.

> NOTE
>
> The **Metrics** page displays only the involved monitoring item metrics of connected applications.

Based on collector functions, monitoring items can be classified into:

- **Topology**: Displays the call relationships between services within a period. The statistics can be collected from the caller or the callee. You can also check the trend.
- **URL**: Monitors the external services that call the current application.
- **JVM**: Monitors basic system performance metrics.
- **Exception**: Monitors application exceptions.
- **Call**: Monitors the external services called by the current application.
- **SQL**: Monitors database access.
- **Web Container**: Monitors web containers such as Tomcat. Generally, the total number of threads, number of busy threads, and number of connections are collected to measure the overall system capacity.

Monitoring Item Configuration

Collectors corresponding to monitoring items define collection parameters. You can modify collection parameters on the page as required. These parameters will be delivered to Agents with heartbeat parameters to change collection behaviors. By default, Redis instruction content is not collected for security purposes. If necessary, modify collection parameters to collect specific instruction data. Collection parameters can also be defined on environment tags. Collectors automatically inherit collection parameter attributes of corresponding environment tags. In this way, configuration is automated.

Monitoring Item Views

On the metric monitoring details page, a monitoring item corresponds to one or more tab views, and each view corresponds to a metric set. APM provides summary tables, trend graphs, latest data tables, and original tables. For details, see **Monitoring Item Views**.

4.2 Application Monitoring Details

4.2.1 Topology

The topology displays the call relationships between services within a period. The statistics can be collected from the caller or the callee. You can also view the trend. On the topology, you can view the call relationships between services and check whether the calls between services are normal to quickly locate faults. The application relationships, call data (service and instance metrics), and health status are clearly displayed.

Viewing the Topology

Step 1 Log in to the management console.

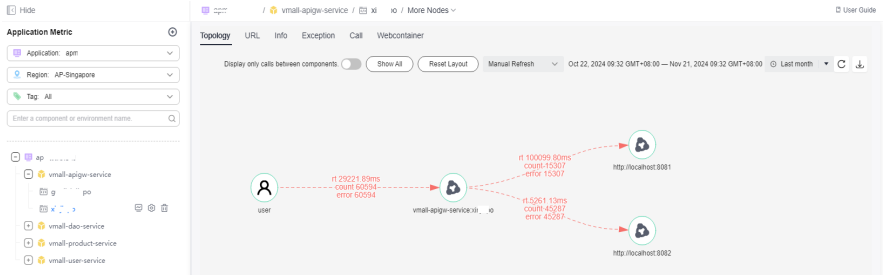
Step 2 Click  on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click  next to the target environment.

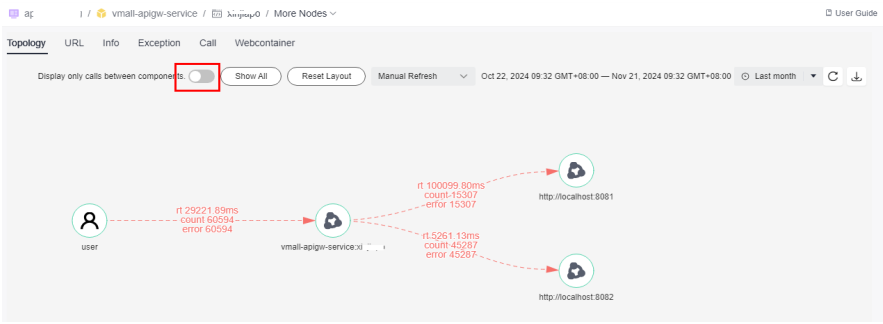
Step 5 Switch to the **Topology** tab page. The call trend of the selected instance is displayed.

Figure 4-1 Viewing the topology



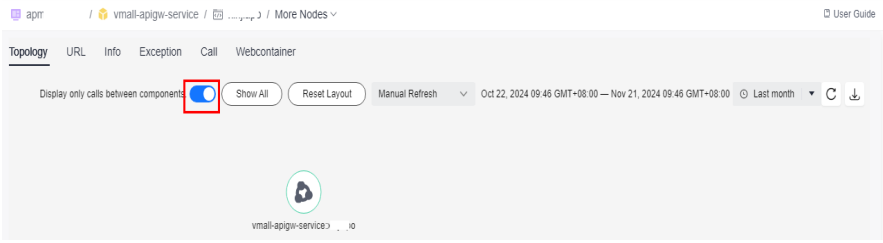
Step 6 Click  next to **Display only calls between components**.

Figure 4-2 Displaying only calls between components



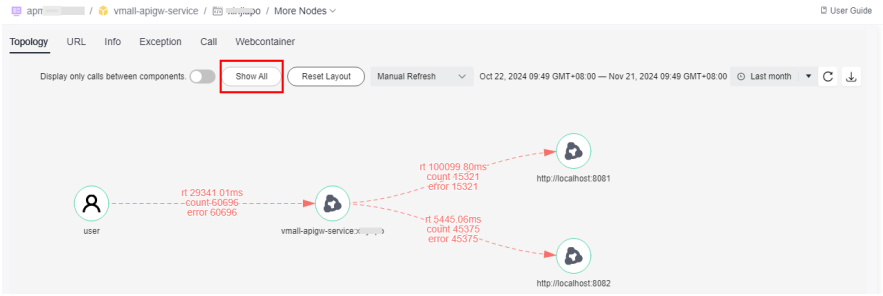
When the button turns blue, only the calls between components are displayed.

Figure 4-3 Calls between components



Step 7 Click **Show All** to display all call relationships of the selected instance in a specified time range.

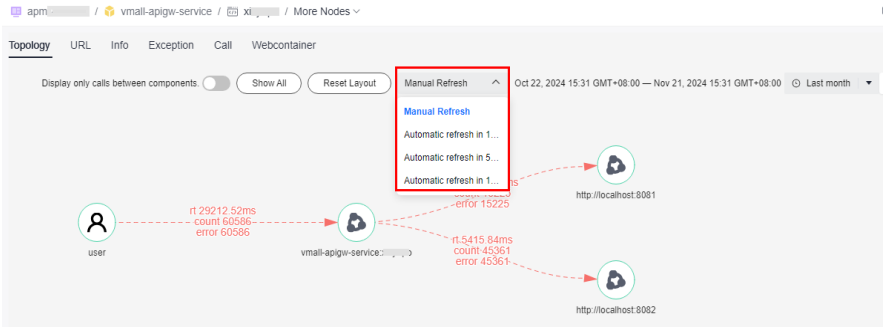
Figure 4-4 Showing all



Step 8 Click **Reset Layout** to restore to the initial topology.

Step 9 Select the refresh mode and time. Default: **Manual Refresh**. In addition, **Automatic refresh in 1 minute**, **Automatic refresh in 5 minutes**, and **Automatic refresh in 15 minutes** are supported.

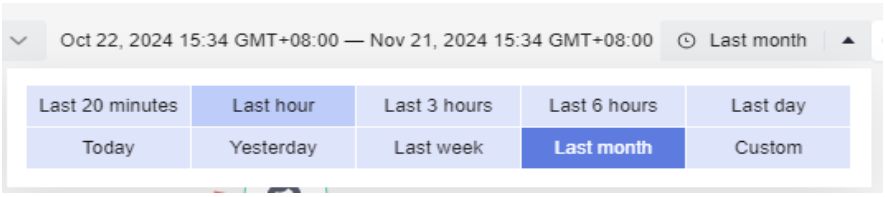
Figure 4-5 Selecting a refresh mode



Step 10 Select a time dimension. Default: **Last 20 minutes**.

Options: **Last 20 minutes**, **Last hour**, **Last 3 hours**, **Last 6 hours**, **Last day**, **Today**, **Yesterday**, **Last week**, **Last month**, or **Custom**.

Figure 4-6 Selecting a time dimension



----End

4.2.2 URL

This function monitors the calls of the current application by external services. It includes URL, Dubbo server, CSE server, CSEProvider cluster, and FunctionGraph monitoring. This type of monitoring item demonstrates the actual external status of the entire service. For example, if the average response time of a URL is long, it means that external users take a long time to query the corresponding data.

This section focuses on URL monitoring.

Going to the URL Page

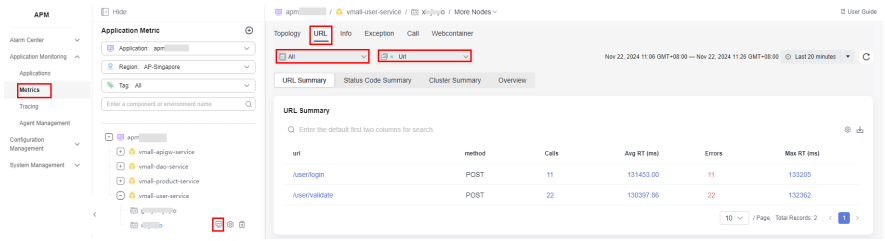
Step 1 Log in to the management console.

Step 2 Click  on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

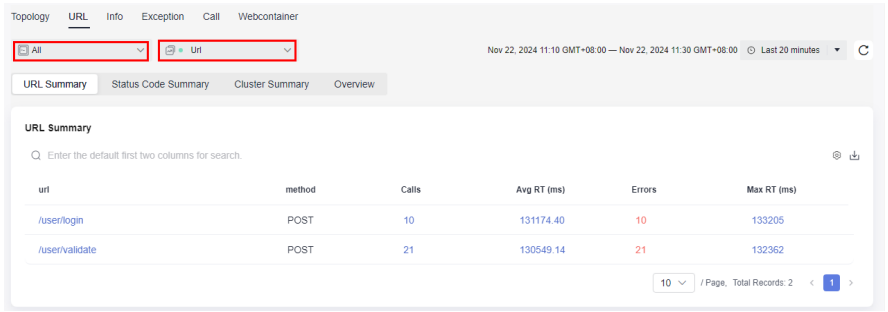
Step 4 In the tree on the left, click  next to the target environment. On the **URL** tab page that is displayed, check URL monitoring information of all instances.

Figure 4-7 Going to the URL page



Step 5 On the displayed **URL** tab page, select a target instance and monitoring item to view the monitoring data in different metric sets.

Figure 4-8 Selecting an instance and monitoring item



Step 6 Select a time range. Default: **Last 20 minutes**.

Options: **Last 20 minutes**, **Last hour**, **Last 3 hours**, **Last 6 hours**, **Last day**, **Today**, **Yesterday**, **Last week**, **Last month**, or **Custom**.

Step 7 Click  in the upper right corner of the list and select the metric data you want to view.

Step 8 Click  in the upper right corner of the list to export information. A maximum of 100 records can be exported.

----End

Viewing URL Monitoring Data

URL summary

For common URL calls, the system collects the metrics of each URL. For details about the metrics, see **Table 4-1**.

Figure 4-9 URL summary under URL monitoring

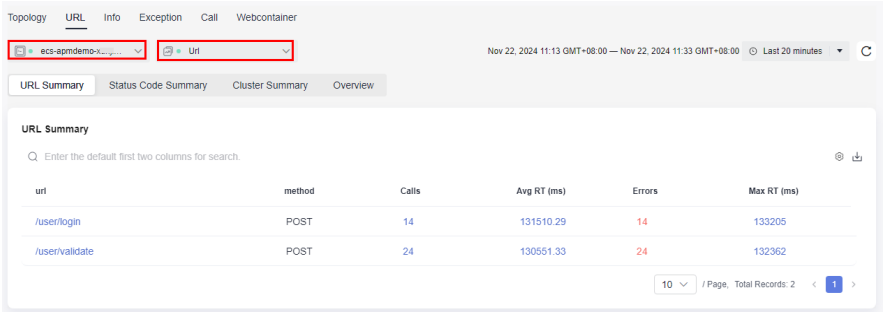


Table 4-1 Parameters of the URL summary

Metric Set	Metric	Description
URL summary	url	URL.
	method	Request HTTP method.
	Calls	Number of times that the URL is called.
	Avg RT (ms)	Average response time of the URL in a collection period.
	Errors	Number of call errors of the URL.
	Max Concurrency	Maximum concurrency of the URL.
	Max RT (ms)	Maximum response time of the URL in a collection period.
	Apdex	Application performance index (Apdex), which indicates users' satisfaction. The value ranges from 0 to 1. The closer the value is to 1, the higher the satisfaction is. For details, see **Basic Concepts - Apdex**.
	Exceptions	Number of exceptions of the URL.
	0 ms–10 ms	Number of requests with 0 ms–10 ms response time.
	10 ms–100 ms	Number of requests with 10 ms–100 ms response time.
	100 ms–500 ms	Number of requests with 100 ms–500 ms response time.
	500 ms–1s	Number of requests with 500 ms–1s response time.
	1s–10s	Number of requests with 1s–10s response time.

Metric Set	Metric	Description
	10s–n	Number of requests with response time longer than 10s.

- URL invocation is the starting point of tracing. When you click a URL, the tracing page is displayed, showing the URL invocation condition in a certain period (default: 20 minutes).
- You can add a URL for tracing by referring to **Configuring URL Tracing**.
- Click a number in blue (such as those in the **Calls** or **Avg RT (ms)** column) to view more details.

Status code summary

APM supports status code-based summary. The system collects the metrics of each URL. For details about the metrics, see **Table 4-2**.

Figure 4-10 Status code summary under URL monitoring

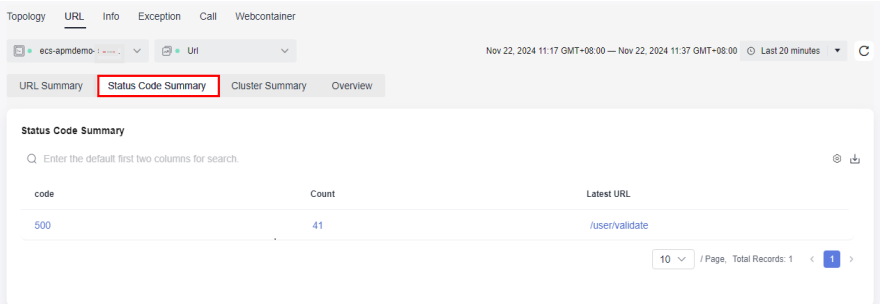


Table 4-2 Parameters of status code summary

Metric Set	Metric	Description
Status code summary	code	Status code.
	Count	Number of times that the status code occurred.
	Latest URL	Sample URL which returns the status code in a collection period.

- Click a status code in the **code** column. The tracing page is displayed, showing the invocation condition of the status code of the selected instance in the environment in last 20 minutes (default).
- Click a number in the **Count** column to view the trend of the status code in a specified period.
- Click the latest URL to view the invocation details of the corresponding status code.

Cluster summary

APM can summarize metrics by cluster. For details about the metrics, see **Table 4-3**.

Figure 4-11 Cluster summary under URL monitoring

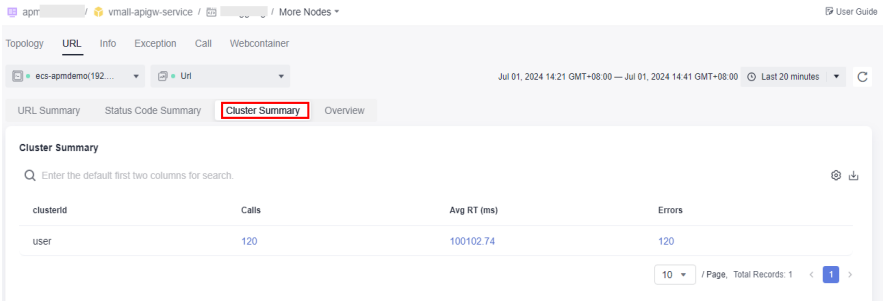


Table 4-3 Parameters of the cluster summary

Metric Set	Parameter	Description
Cluster summary	Cluster ID	Cluster ID of the caller.
	Calls	Number of times the cluster is called.
	Avg RT (ms)	Average response time in a collection period.
	Errors	Number of times that the cluster fails to be called.
	Max Concurrency	Maximum concurrency of the cluster.
	Max RT (ms)	Slowest call time in a collection period.

Click a number in blue (such as those in the **Calls** or **Avg RT (ms)** column) to view more details.

Overview

View the metric trend of the selected instance on the **Overview** tab page. For details about the metrics, see **Table 4-4**. When you hover over the graph, you can check the total requests, average RT (ms), errors, and Apdex in a specific time.

Figure 4-12 Overview under URL monitoring

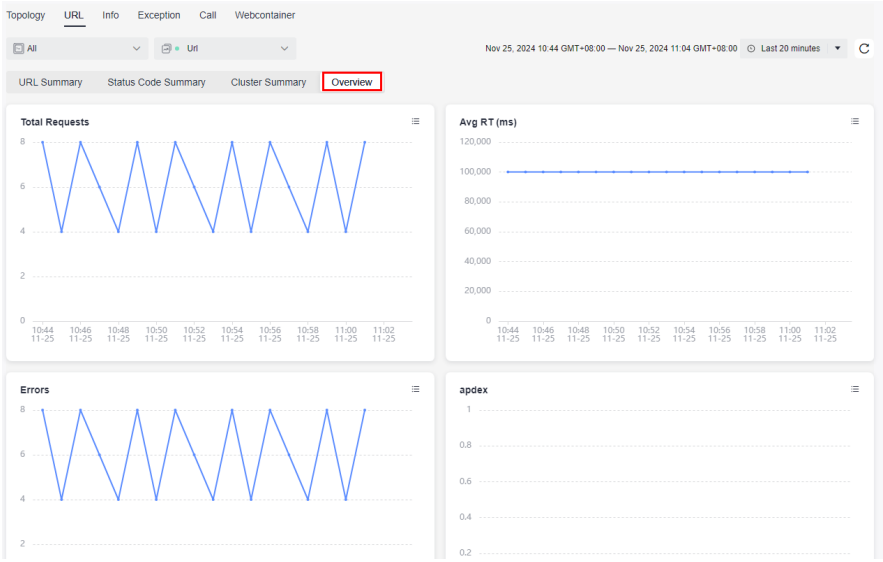


Table 4-4 Overview metrics

Metric Set	Metric	Description
Overview	Total Requests	Total number of URL requests.
	Avg RT (ms)	Average response time of the URL.
	Errors	Total number of URL errors.
	Apdex	Users' satisfaction with the URL.

4.2.3 JVM

This function monitors JVMInfo, JVMMonitor, GC, thread, and JavaMethod.

Going to the JVM Page

Step 1 Log in to the management console.

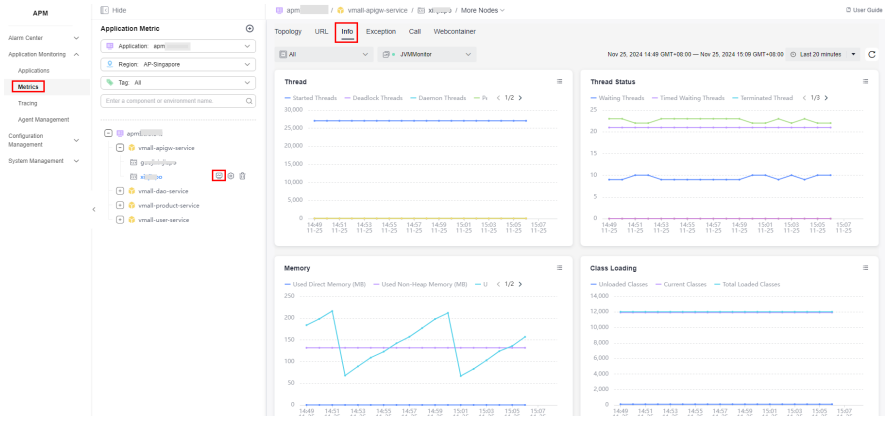
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click next to the target environment.

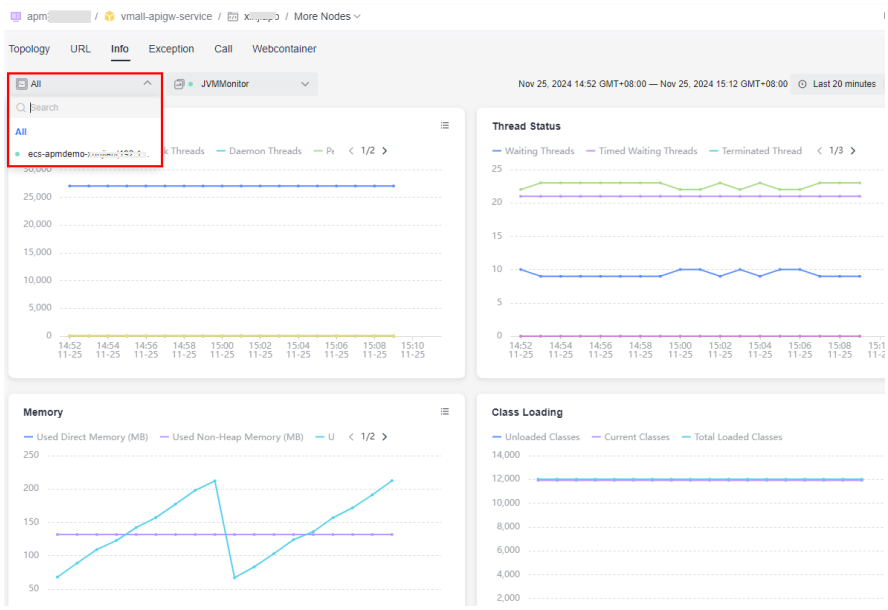
Step 5 Click the **JVM** tab. By default, the JVMMonitor information of all instances is displayed. When you hover over a graph, you can check the actual value of each metric in a specific time.

Figure 4-13 Going to the JVM page



Step 6 On the displayed **JVM** tab page, select a target instance and monitoring item to view the monitoring data in different metric sets.

Figure 4-14 Selecting an instance and monitoring item



Step 7 Select a time range. Default: **Last 20 minutes**.

Options: **Last 20 minutes**, **Last hour**, **Last 3 hours**, **Last 6 hours**, **Last day**, **Today**, **Yesterday**, **Last week**, **Last month**, or **Custom**.

----End

Viewing JVM Information

On the **JVM** tab page, view the JVMInfo metrics of the corresponding instance. For details about the metrics, see **Table 4-5**.

Figure 4-15 Viewing JVM information

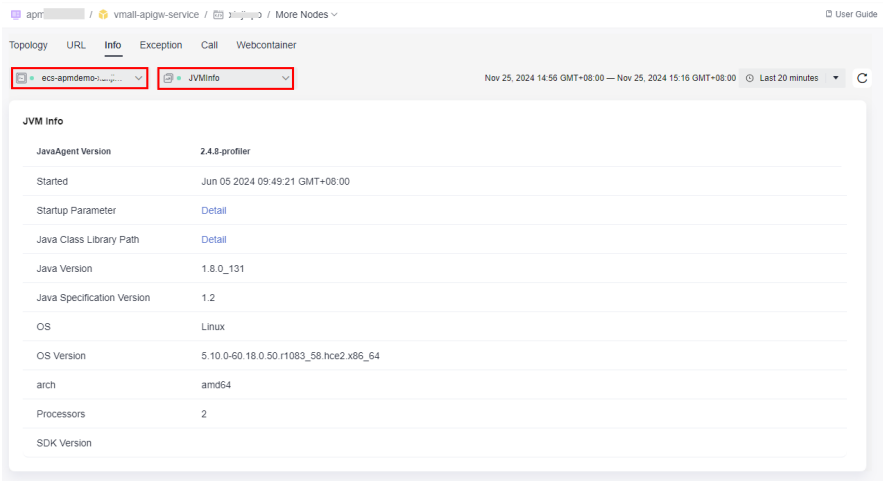


Table 4-5 JVMInfo metrics

Metric Set	Metric	Description
JVMInfo	JavaAgent Version	Java Agent version.
	Started	JVM startup time.
	Startup Parameter	JVM startup parameter. Click **Detail** to view JVM startup parameter details.
	Java Class Library Path	Java class library path. Click **Detail** to view Java class library path details.
	Java Version	Java version.
	Java Specification Version	Java specification version.
	OS	OS name.
	OS Version	OS version.
	arch	CPU architecture.
	Processors	Number of processors.
	SDK Version	SDK version.

Viewing JVM Monitoring Data

APM monitors JVM metrics. For details about the metrics, see **Table 4-6**. JVM monitoring metrics are displayed in graphs, so that you can view and analyze JVM monitoring data more easily.

- When you hover over a graph, you can check the actual value of each metric in a specific time.
- Click  in the upper right corner of the **Memory Pool** list and select the metric data you want to view.
- Click  in the upper right corner of the **Memory Pool** list to export information. A maximum of 100 records can be exported.

Figure 4-16 Viewing JVM monitoring data

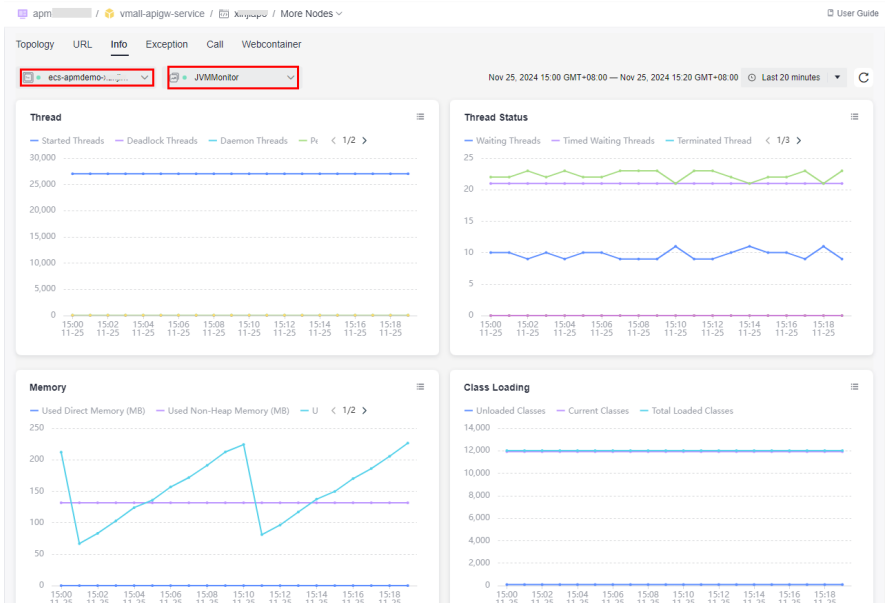


Table 4-6 JVM monitoring metrics

Metric Set	Metric	Description
Thread	Current Threads	Number of current threads.
	Deadlock Threads	Number of deadlock threads.
	Daemon Threads	Number of daemon threads.
	Started Threads	Number of started threads.
	Peak Threads	Peak number of threads.
Thread Status	Waiting Threads	Number of waiting threads.
	Terminated Threads	Number of threads in the terminated state.

Metric Set	Metric	Description
	Runnable Threads	Number of runnable threads.
	Blocked Threads	Number of blocked threads.
	New Threads	Number of new threads.
	Timed Waiting Threads	Number of threads that timed out.
Memory	Used Non-Heap Memory	Size of the used non-heap memory.
	Used Heap Memory	Size of the used heap memory.
	Used Direct Memory	Size of the used direct memory.
Class loading	Current Classes	Number of current classes.
	Total Loaded Classes	Total number of loaded classes.
	Unloaded Classes	Number of unloaded classes.
Memory pool	committed(M)	Size of available memory.
	init(M)	Size of the initialized memory.
	max(M)	Size of the maximum memory.
	name	Memory pool name.
	used(M)	Size of the used memory.
CPU	CPU Usage	CPU usage of the Java process.

Viewing GC Information

APM monitors GC metrics. For details about the metrics, see **Table 4-6**.

Figure 4-17 Viewing GC information

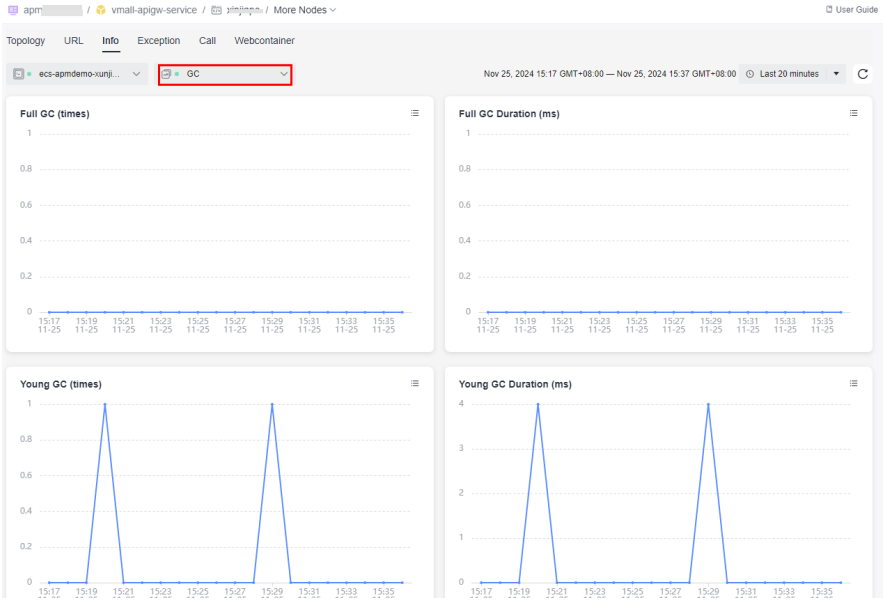


Table 4-7 GC metrics

Metric Set	Metric	Description
GC statistics	Full GC (times)	Number of full GC times in a collection period.
	Full GC Duration (ms)	Full GC duration in a collection period.
	Young GC (times)	Number of young GC times in a collection period.
	Young GC Duration (ms)	Young GC duration in a collection period.
GC Details	GC Type	GC type, which can be **major** or **minor**.
	GC Cause	GC cause.
	Count	Number of times that GC has occurred.
	Total GC Duration (ms)	GC duration.
	Max GC Duration (ms)	Time consumed by the slowest GC.
	GC Recycler	GC recycler name.
	Slowest GC Details	Details about the slowest GC.

- Click the digits in blue (such as those in the **Count**, **Total GC Duration (ms)**, or **Max GC Duration (ms)** column) to view the corresponding GC trend graph in a certain period (default: 20 minutes).

- When you hover over a graph, you can check the actual value of each metric in a specific time.
- On the GC details area, you can view the GC type, GC cause, count, total GC duration (ms), maximum GC duration (ms), GC recycler, and slowest GC details (details and history).
- Click in the upper right corner of the **GC Details** list and select the metric data you want to view.
- Click in the upper right corner of the **GC Details** list to export information. A maximum of 100 records can be exported.

Viewing Threads

You can view the thread details of the corresponding instance on APM. For details, see **Table 4-8**.

Figure 4-18 Viewing threads

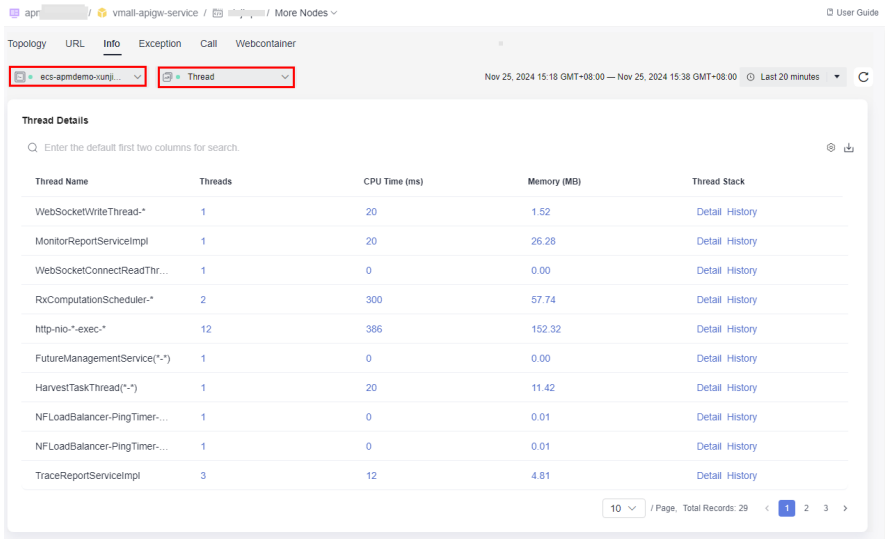


Table 4-8 Thread metrics

Metric Set	Metric	Description
Thread details	Thread Name	Thread name.
	Threads	Number of threads.
	CPU Time (ms)	Thread CPU time.
	Memory (MB)	Memory (MB).
	Thread Stack	Thread stack.

- Click a number in the **Threads** column to view the trend of the thread in a specified period.

- Click **Detail** in the **Thread Stack** column to view the thread details.
- Click **History** in the **Thread Stack** column to view the historical thread stack list.
- Click  in the upper right corner of the **Thread Details** list and select the metric data you want to view.
- Click  in the upper right corner of the **Thread Details** list to export information. A maximum of 100 records can be exported.

Viewing Java Methods

1. By default, APM does not monitor Java methods. To monitor them, **configure the JavaMethod monitoring item** first.
2. After the configuration is complete, the system monitors the methods and classes of JavaMethod.
3. On the **JVM** page, select a target instance and **JavaMethod** to view details. For details, see **Table 4-9**.

Table 4-9 JavaMethod metrics

Metric Set	Metric	Description
JavaMethod	Class	Class of a Java method.
	Method	Method.
	Calls	Number of times that the method is called.
	Avg RT (ms)	Average response time.
	Errors	Number of times that the method fails to be called.
	Max Concurrency	Maximum concurrency of the method.
	Max RT (ms)	Maximum response time of the method.
	0 ms–10 ms	Number of requests with 0 ms–10 ms response time.
	10 ms–100 ms	Number of requests with 10 ms–100 ms response time.
	100 ms–500 ms	Number of requests with 100 ms–500 ms response time.
	500 ms–1s	Number of requests with 500 ms–1s response time.
	1s–10s	Number of requests with 1s–10s response time.
	10s–n	Number of requests with response time longer than 10s.

- Click a number (such as those in the **Calls** or **Errors** column) to view the trend of the thread in a specified period.
- Click in the upper right corner of the **Method** list and select the metric data you want to view.
- Click in the upper right corner of the **Method** list to export information. A maximum of 100 records can be exported.

4.2.4 Exception

This function monitors application exception logs. Take the monitoring of Java exception logs as an example. Once you use the log system to print logs, they will be collected by APM. The exception collection type varies according to the collector type.

Viewing Exception Logs

Step 1 Log in to the management console.

Step 2 Click on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click next to the target environment.

Step 5 Click the **Exception** tab. By default, exception logs of all instances are displayed. For details about the metrics, see **Table 4-10**.

Figure 4-19 Exception monitoring data

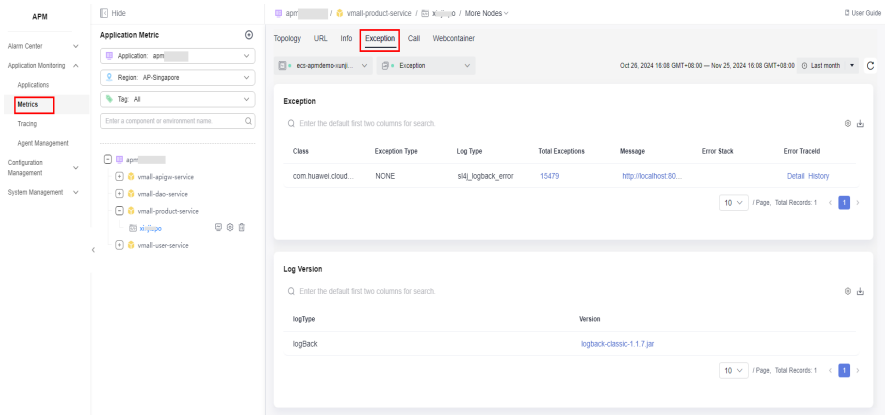


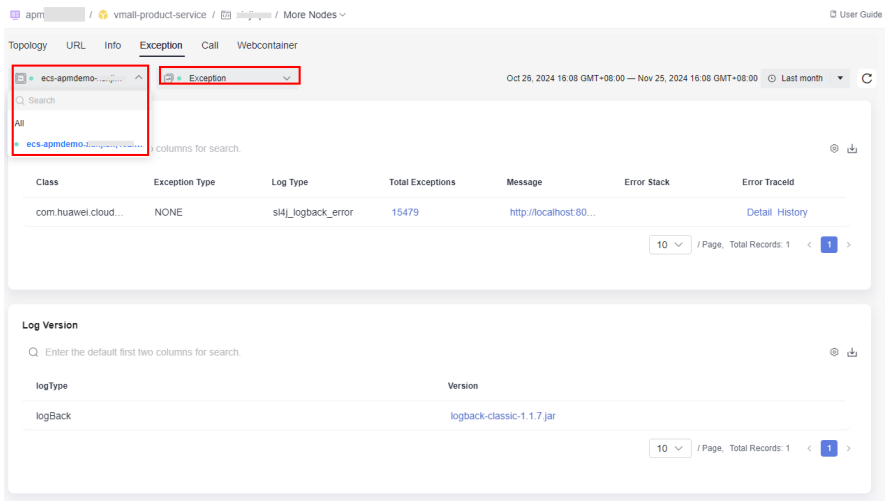
Table 4-10 Exception and log parameters

Metric Set	Parameter	Description
Exception	Class	Exception class
	Exception Type	Exception type
	Log Type	Exception log type
	Total Exceptions	Number of times that an exception has occurred
	Message	Message returned when the exception occurred
	Error Stack	Error stack
	Error Trace ID	Information about the error trace
Log Version	Log Type	Log type
	Version	Version

- Click a number in blue in the **Total Exceptions** column to view the trend of the total exceptions in a specified period.
- Click the blue text in the **Message** column to view the message time and content.
- Click **Detail** in the **Error Stack** column to view exception details.
- Click **History** in the **Error Stack** column to view the historical error stack list.
- Click **Detail** in the **Trace** column to view trace details.
- Click **History** in the **Trace** column to view the historical trace list.
- Click the blue text in the **Version** column to view details.

Step 6 On the **Exception** tab page, select a target instance and then select **Exception** to view the exception monitoring data.

Figure 4-20 Selecting a target instance and exception



Step 7 Select a time range. Default: **Last 20 minutes**.

Options: **Last 20 minutes**, **Last hour**, **Last 3 hours**, **Last 6 hours**, **Last day**, **Today**, **Yesterday**, **Last week**, **Last month**, or **Custom**.

Step 8 Click in the upper right corner of the list and select the metric data you want to view.

Step 9 Click in the upper right corner of the list to export information. A maximum of 100 records can be exported.

----End

4.2.5 Call

This function monitors the calls of external services by the current application. It covers CSEConsumer, ApacheHttpClient, ApacheHttpAsyncClient, DubboConsumer, and HttpClient monitoring.

This section focuses on HttpClient monitoring.

Going to the Call Page

Step 1 Log in to the management console.

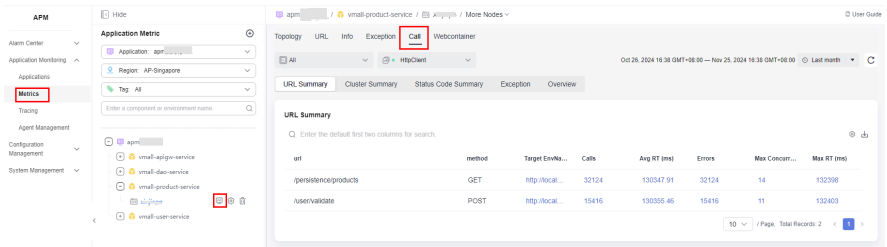
Step 2 Click on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click next to the target environment.

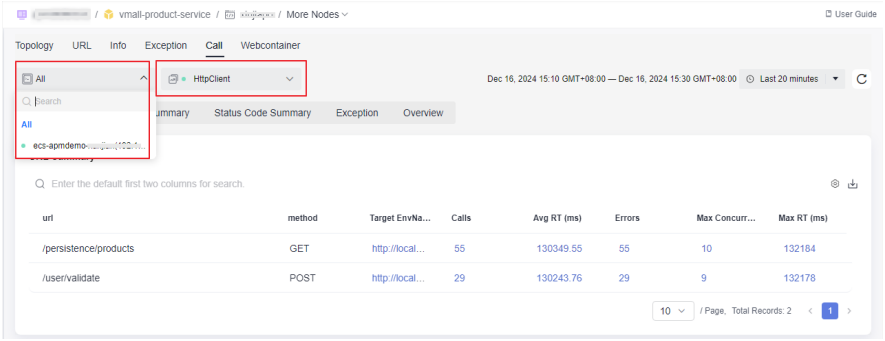
Step 5 Click the **Call** tab. By default, the HttpClient monitoring information of all instances is displayed.

Figure 4-21 External call data



Step 6 On the displayed **Call** tab page, select a target instance and monitoring item to view the monitoring data in different metric sets.

Figure 4-22 Selecting an instance and monitoring item



Step 7 Select a time range. Default: **Last 20 minutes**.

Options: **Last 20 minutes**, **Last hour**, **Last 3 hours**, **Last 6 hours**, **Last day**, **Today**, **Yesterday**, **Last week**, **Last month**, or **Custom**.

Step 8 Click in the upper right corner of the list and select the metric data you want to view.

Step 9 Click in the upper right corner of the list to export information. A maximum of 100 records can be exported.

----End

Viewing HttpClient Monitoring Data

URL summary

The HttpClient monitoring system collects the metrics of each URL. For details about the metrics, see **Table 4-11**. Click in the upper right corner of the list and select the metric data you want to view.

Figure 4-23 URL summary under HttpClient monitoring

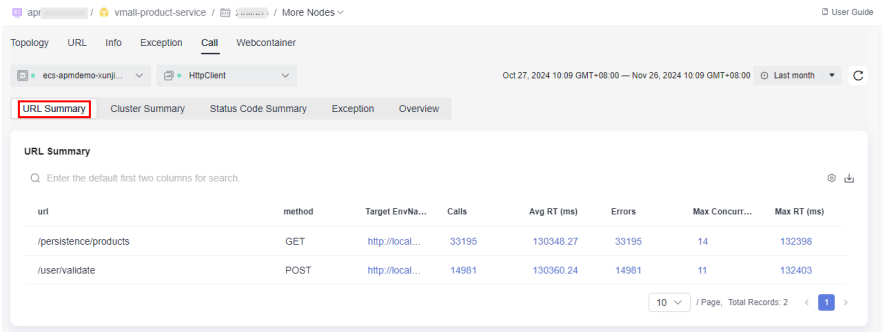


Table 4-11 Parameters of URL summary under HttpClient monitoring

Metric Set	Metric	Description
URL summary	url	Called URL.
	method	HTTP method of the URL.

Metric Set	Metric	Description
	TargetEnvName	Name of the component whose URL is called.
	Calls	Number of times that the URL is called.
	Avg RT (ms)	Average response time of the called URL.
	Errors	Number of call errors of the URL.
	Max Concurrency	Maximum concurrency of the URL.
	Max RT (ms)	Maximum response time of the called URL.
	0 ms–10 ms	Number of requests with 0 ms–10 ms response time.
	10 ms–100 ms	Number of requests with 10 ms–100 ms response time.
	100 ms–500 ms	Number of requests with 100 ms–500 ms response time.
	500 ms–1s	Number of requests with 500 ms–1s response time.
	1s–10s	Number of requests with 1s–10s response time.
	10s–n	Number of requests with response time longer than 10s.
	Error Trace	ID of the trace that encounters an error in a collection period.
	Slowest Trace	ID of the slowest trace in a collection period.

- Click a number in blue (such as those in the **Calls** or **Avg RT (ms)** column) to view more details.
- Click the address in the **TargetEnvName** column. The details about the called component are displayed in a list.
- Click the text in blue (such as those in the **Slowest Trace** or **Error Trace** column) to view more details.

Cluster summary

APM can summarize external call metrics by cluster. For details about the metrics, see **Table 4-12**.

Figure 4-24 Cluster summary under HttpClient monitoring

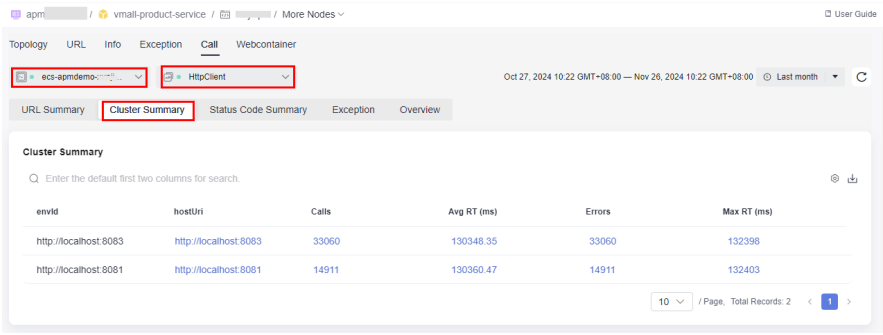


Table 4-12 Parameters of cluster summary under HttpClient monitoring

Metric Set	Metric	Description
Cluster summary	envId	Cluster ID of the called party.
	hostUri	URL of the called party.
	Calls	Number of times that the cluster URL is called.
	Avg RT (ms)	Average response time for calling the cluster URL.
	Errors	Number of call errors of the URL.
	Max RT (ms)	Maximum response time for calling the cluster URL.
	0 ms–10 ms	Number of requests with 0 ms–10 ms response time.
	10 ms–100 ms	Number of requests with 10 ms–100 ms response time.
	100 ms–500 ms	Number of requests with 100 ms–500 ms response time.
	500 ms–1s	Number of requests with 500 ms–1s response time.
	1s–10s	Number of requests with 1s–10s response time.
	10s–n	Number of requests with response time longer than 10s.

- Click a number in blue (such as those in the **Calls** or **Avg RT (ms)** column) to view more details.
- Click the address in the **hostUri** column. The details of the called party are displayed in a list.

Status code summary

APM can summarize external call metrics by status code. For details about the metrics, see **Table 4-13**.

Figure 4-25 Status code summary under HttpClient monitoring

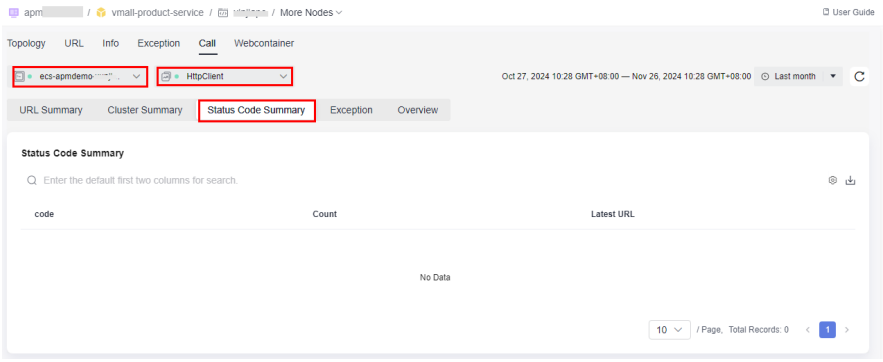


Table 4-13 Parameters of status code summary under HttpClient monitoring

Metric Set	Metric	Description
Status code summary	code	Status code.
	Count	Number of times that the status code occurred.
	Latest URL	URL that returns the status code.

- Click a status code in the **code** column. The tracing page is displayed, showing the invocation condition of the status code of the selected instance in the environment in last 20 minutes (default).
- Click a number in the **Count** column to view the trend of the status code in a specified period.
- Click the latest URL to view the invocation details of the corresponding status code.

Exception

On the **Exception** tab page, view the exception statistics about HttpClient calls. For details about the metrics, see **Table 4-14**.

Figure 4-26 HttpClient monitoring exceptions

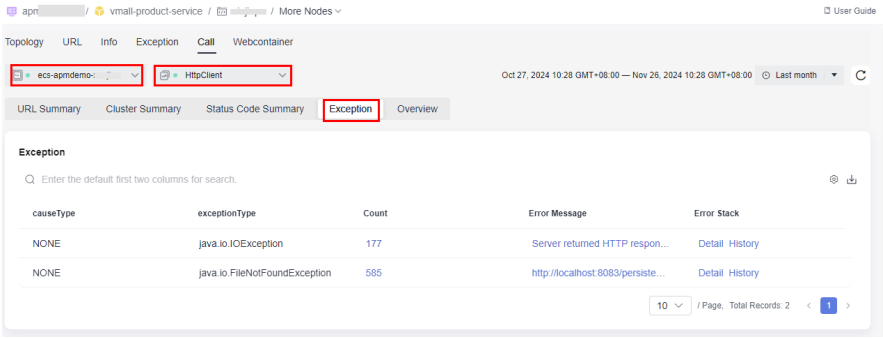


Table 4-14 Parameters of HttpClient monitoring exceptions

Metric Set	Metric	Description
Exception	causeType	Exception class.
	exceptionType	Exception type.
	Count	Number of times the exception occurred.
	Error Message	Message returned when the exception occurred.
	Error Stack	Exception stack information.

- Click a number in blue in the **Count** column to view the trend of the thread in a specified period.
- Click the text in blue in the **Error Message** column to view message details.
- Click **Detail** in the **Error Stack** column to view exception details.
- Click **History** in the **Error Stack** column to view the historical error stack list.

Overview

On the **Overview** tab page, view the metrics of the selected instance. For details about the metrics, see **Table 4-15**.

When you hover over a graph, you can check the actual value of each metric in a specific time.

Figure 4-27 Overview under HttpClient monitoring

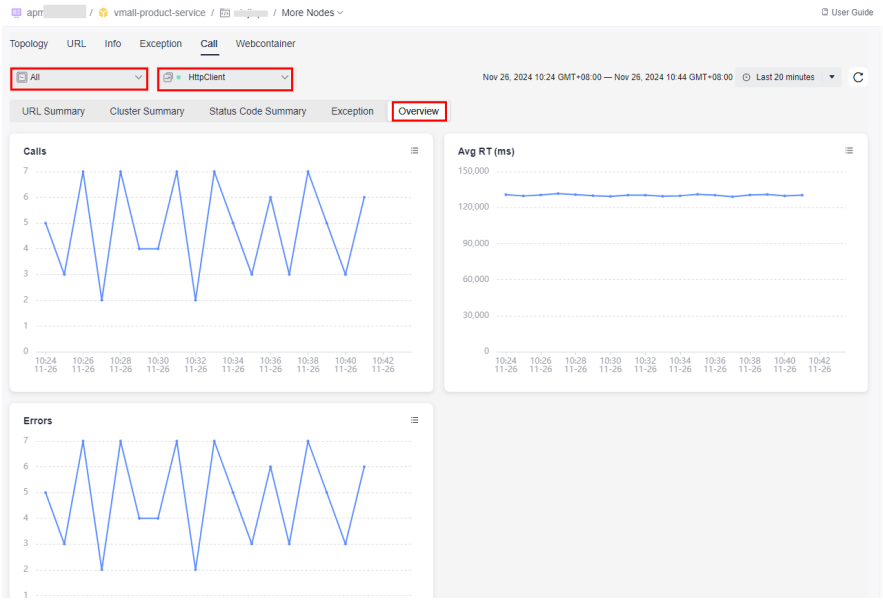


Table 4-15 Overview parameters of HttpClient monitoring

Metric Set	Metric	Description
Overview	Calls	Total number of calls.
	Avg RT (ms)	Average response time
	Errors	Total number of errors.

4.2.6 SQL

This function monitors database access. The databases that can be monitored include the C3P0, Cassandra, ClickHouse, DBCP, Druid, EsRestClient, GaussDB, Hikari, Jetcd, ObsClient, MySQL, PostgreSQL, Oracle, HBase, and MongoDB. APM collects details about executed statements to help you locate performance problems in code.

This section focuses on MySQL database monitoring.

Going to the SQL Page

Step 1 Log in to the management console.

Step 2 Click on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click next to the target environment.

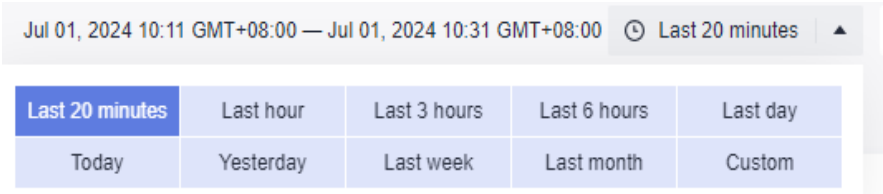
Step 5 Click the **SQL** tab. By default, the MySQL database information of all instances is displayed.

Step 6 On the displayed **SQL** tab page, select a target instance and monitoring item to view the monitoring data in different metric sets.

Step 7 Select a time range. Default: **Last 20 minutes**.

Options: **Last 20 minutes**, **Last hour**, **Last 3 hours**, **Last 6 hours**, **Last day**, **Today**, **Yesterday**, **Last week**, **Last month**, or **Custom**.

Figure 4-28 Selecting a time range



Step 8 Click in the upper right corner of the list and select the metric data you want to view.

----End

Viewing MySQL Database Monitoring Data

SQL summary

APM can monitor MySQL databases by SQL. For details about the metrics, see Table 4-16. Click  in the upper right corner of the list and select the metric data you want to view.

Table 4-16 SQL summary parameters

Metric Set	Metric	Description
SQL monitoring	sql	Unique ID of the SQL statement, which is used for alarm configuration.
	SQL Statement	SQL statement.
	Calls	Number of times that the SQL statement is called.
	Avg RT (ms)	Average response time (ms).
	Errors	Number of errors that the SQL statement encounters.
	Rows Read	Number of read rows of the SQL statement.
	Rows Updated	Number of updated rows of the SQL statement.
	Max Concurrency	Maximum concurrency of the SQL statement.
	Max RT (ms)	Maximum response time of the SQL statement.
	0 ms–10 ms	Number of requests with 0 ms–10 ms response time.
	10 ms–100 ms	Number of requests with 10 ms–100 ms response time.
	100 ms–200 ms	Number of requests with 100 ms–200 ms response time.
	200 ms–1s	Number of requests with 200 ms–1s response time.
	1s–10s	Number of requests with 1s–10s response time.
	10s–n	Number of requests with response time longer than 10s.

Metric Set	Metric	Description
	Slowest Trace	ID of the slowest trace in a collection period.
	Error Trace	ID of the trace that encounters an error in a collection period.

- Click an SQL statement to view details.
- Click a number in blue (such as those in the **Calls** or **Avg RT (ms)** column) to view more details.
- Click a slow or an error trace to view its details.

Database summary

APM can summarize MySQL database metrics by database. For details about the metrics, see **Table 4-17**.

Table 4-17 Database summary parameters

Metric Set	Metric	Description
Database connections	db	Database name.
	Connections Created	Number of connections created by the database.
	Connections Destroyed	Number of the database's connections that have been destroyed.
	Avg RT (ms)	Average response time (ms).
	Calls	Number of times that the database is called.
	Errors	Number of errors that the database encounters.
	Rows Read	Number of rows read from the database.
	Rows Updated	Number of rows updated in the database.
	Max RT (ms)	Maximum response time of the database.
	0 ms–10 ms	Number of requests with 0 ms–10 ms response time.
	10 ms–100 ms	Number of requests with 10 ms–100 ms response time.

Metric Set	Metric	Description
	100 ms–200 ms	Number of requests with 100 ms–200 ms response time.
	200 ms–1s	Number of requests with 200 ms–1s response time.
	1s–10s	Number of requests with 1s–10s response time.
	10s–n	Number of requests with response time longer than 10s.

Click a number in blue (such as those in the **Calls** or **Avg RT (ms)** column) to view more details.

Exception

On the **Exception** tab page, view exception statistics about SQL calls. For details about the metrics, see **Table 4-18**.

Table 4-18 Exception parameters

Metric Set	Metric	Description
Exception	causeType	Exception class.
	exceptionType	Exception type.
	Count	Number of exceptions.
	SQL	SQL statement that encounters an exception.
	Error Stack	Exception stack information.
	Message	Error message.

Overview

On the **Overview** tab page, view the call trend of the selected instance. For details about the metrics, see **Table 4-19**. When you hover over a graph, you can check the actual value of each metric in a specific time.

Table 4-19 Overview parameters

Metric Set	Metric	Description
Overview	Calls	Total number of calls.
	Rows Read	Total number of read rows.

Metric Set	Metric	Description
	Avg RT (ms)	Average response time (ms).
	Errors	Total number of errors.
	Rows Updated	Number of rows updated in the database.

Info

On the **Info** tab page, view the driver version information. Click the text in blue to view more details.

Viewing Druid Connection Pool Monitoring Data

The Druid connection pool monitoring system collects data sources, connection details, additional configurations, and exception information. You can click  in the upper right corner of the list to customize the columns you want to view. For details about the metrics, see **Table 4-20**.

Table 4-20 Druid connection pool parameters

Metric Set	Metric	Description
Data source	Connection Address	Connection address.
	Driver	Driver name.
	Initialized Connections	Number of initialized connections.
	Min Idle Connections in Pool	Minimum of idle connections in a pool.
	Max Idle Connections in Pool	Maximum number of idle connections in a pool.
	Max Connections in Pool	Maximum number of connections in a pool.
	Idle Connections	Number of idle connections.
	Max Idle Connections	Maximum number of idle connections.
	Active Connections	Number of active connections.
	Max Active Connections	Maximum number of active connections.
	Waiting Threads	Number of waiting threads.
	Max Waiting Threads	Maximum number of waiting threads.

Metric Set	Metric	Description
	Upper Limit for Waiting Threads	Upper limit for waiting threads.
	Total Connections	Total number of connections.
Connection details	Connection Address	Connection address.
	Calls	Number of calls.
	Total RT (ms)	Total response time (ms).
	Avg RT (ms)	Average response time (ms).
	Errors	Number of errors.
	Max Concurrency	Maximum number of concurrent connections.
	Max RT (ms)	Maximum response time.
	0 ms–10 ms	Number of requests with 0 ms–10 ms response time.
	10 ms–100 ms	Number of requests with 10 ms–100 ms response time.
	100 ms–500 ms	Number of requests with 100 ms–500 ms response time.
	500 ms–1s	Number of requests with 500 ms–1s response time.
	1s–10s	Number of requests with 1s–10s response time.
	10s–n	Number of requests with response time longer than 10s.
Additional configuration	Connection Address	Connection address.
	Max Wait (ms)	Maximum waiting time.
	Test on Borrow	Whether to verify the validity of a connection before obtaining it from the connection pool.
	Test on Return	Whether to verify the validity of a connection when it is returned.
	Test While Idle	Whether to verify the validity of an idle connection when an application applies for it from the pool
	Remove Abandoned	Whether to automatically reclaim timeout connections.

Metric Set	Metric	Description
	Remove Abandoned TimeoutMillis (ms)	If a connection in the pool is not returned within the specified duration, the connection will be reclaimed.
	Remove Abandoned Count	Number of timeout connection reclaims.
	Min Evictable Idle TimeMillis (ms)	Minimum idle time of a connection in the pool.
	Time Between EvictionRunsMillis (ms)	Interval for checking the validity of idle connections.
Exception	causeType	Exception class.
	Exception Type	Exception type.
	Count	Number of times the exception occurred.
	Error Message	Message returned when the exception occurred.
	Error Stack	Exception stack information.
Version	Driver Version	Driver version.

- Click a number in blue (such as those in the **Calls** or **Avg RT (ms)** column) to view more details.
- Click the text in blue (such as those in the **Driver** or **Driver Version** column) to view more details.

Viewing Hikari Connection Pool Monitoring Data

The Hikari connection pool monitoring system collects the pool details, connection details, and exception information. You can click  in the upper right corner of the list to customize the columns you want to view. For details about the metrics, see **Table 4-21**.

Table 4-21 Hikari connection pool parameters

Metric Set	Metric	Description
Connection pool details	Pool Address	Connection address.
	Driver Name	Driver name.
	Max Pool Size	Maximum number of connections that are allowed.
	Total Connections	Total number of current connections.

Metric Set	Metric	Description
	Active Connections	Number of active connections.
	Idle Connections	Number of idle connections.
	Threads Awaiting Connection	Number of waiting connections.
Connection details	Connection Address	Connection address.
	Calls	Number of calls.
	Total RT (ms)	Total response time (ms).
	Avg RT (ms)	Average response time (ms).
	Errors	Number of errors.
	Max Concurrency	Maximum number of concurrent connections.
	Max RT (ms)	Maximum response time.
	0 ms–10 ms	Number of requests with 0 ms–10 ms response time.
	10 ms–100 ms	Number of requests with 10 ms–100 ms response time.
	100 ms–500 ms	Number of requests with 100 ms–500 ms response time.
	500 ms–1s	Number of requests with 500 ms–1s response time.
	1s–10s	Number of requests with 1s–10s response time.
	10s–n	Number of requests with response time longer than 10s.
Exception	causeType	Exception class.
	Exception Type	Exception type.
	Count	Number of times the exception occurred.
	Error Message	Message returned when the exception occurred.
	Error Stack	Exception stack information.

- Click a number in blue (such as those in the **Calls** or **Avg RT (ms)** column) to view more details.

4.2.7 Web Container

This function monitors web containers, including Tomcat. This section focuses on Tomcat monitoring.

Going to the Web Container Page

Step 1 Log in to the management console.

Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click next to the target environment.

Step 5 Click the **Web Container** tab. By default, the Tomcat monitoring information of all instances is displayed. For details about the metrics, see **Table 4-22**.

Figure 4-29 Going to the web container page

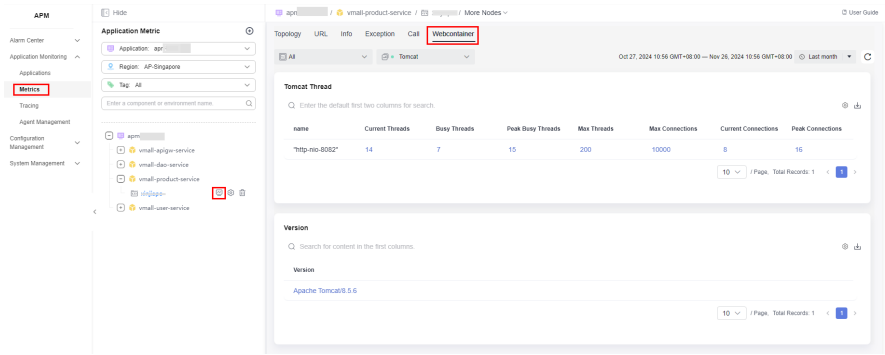


Table 4-22 Tomcat monitoring parameters

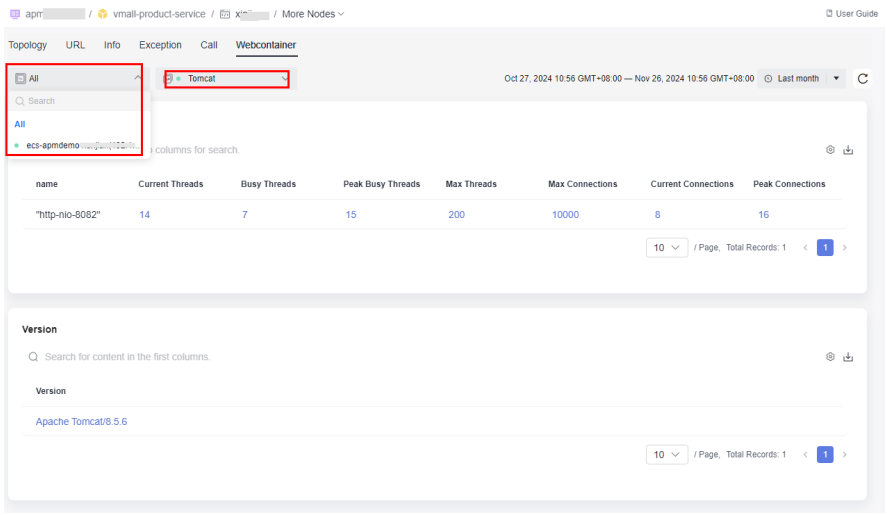
Metric Set	Metric	Description
Tomcat port monitoring	name	Port name.
	Current Threads	Number of current threads on the port.
	Busy Threads	Number of busy threads on the port at the time of collection.
	Peak Busy Threads	Maximum number of busy threads on the port in a collection period.
	Max Threads	Maximum number of threads on the port.
	Max Connections	Maximum number of connections on the port.
	Current Connections	Number of current connections of the port at the time of collection.

Metric Set	Metric	Description
	Peak Connections	Maximum number of connections on the port in a collection period.
Version	Version	Tomcat version.

- Click a number in blue (such as those in the **Current Threads**, **Busy Threads**, or **Peak Busy Threads** column) to view the trend graph of the target web container in the specified period.
- Click a version in the **Version** column to view details.

Step 6 On the displayed **Web Container** tab page, select a target instance and monitoring item to view the monitoring data in different metric sets.

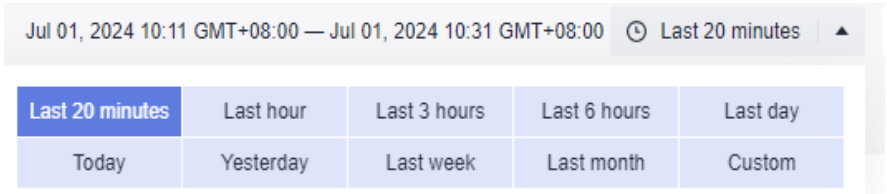
Figure 4-30 Selecting an instance and monitoring item



Step 7 Select a time range. Default: **Last 20 minutes**.

Options: **Last 20 minutes**, **Last hour**, **Last 3 hours**, **Last 6 hours**, **Last day**, **Today**, **Yesterday**, **Last week**, **Last month**, or **Custom**.

Figure 4-31 Selecting a time range



Step 8 Click in the upper right corner of the list and select the metric data you want to view.

Step 9 Click in the upper right corner of the list to export information. A maximum of 100 records can be exported.

----End

4.3 Application Monitoring Configuration

4.3.1 Configuration Details

You can define collection parameters for some collectors corresponding to monitoring items.

NOTE

On the **Monitoring Item** tab page, only monitoring items related to the connected application are displayed.

Configuring a Monitoring Item

Step 1 Log in to the management console.

Step 2 Click on the left and choose **Application** > **Application Performance Management**.

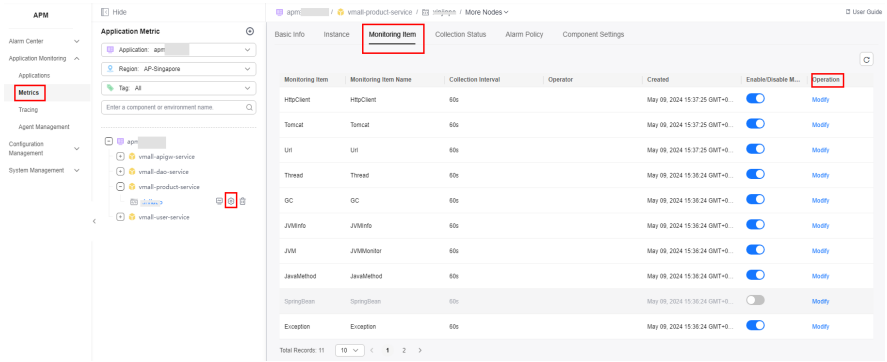
Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click next to the target environment. The instance monitoring page is displayed.

Step 5 Click the **Monitoring Item** tab.

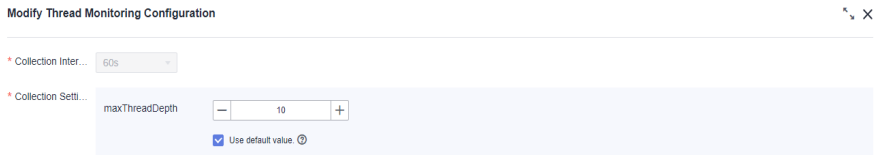
Step 6 Locate the row that contains the target monitoring item and click **Modify** in the **Operation** column.

Figure 4-32 Configuring a monitoring item



Step 7 On the displayed page, edit the monitoring configuration. For details, see the corresponding section.

Figure 4-33 Editing the thread monitoring configuration



Step 8 Click **Yes**.

----End

Enabling or Disabling a Monitoring Item

Step 1 Log in to the management console.

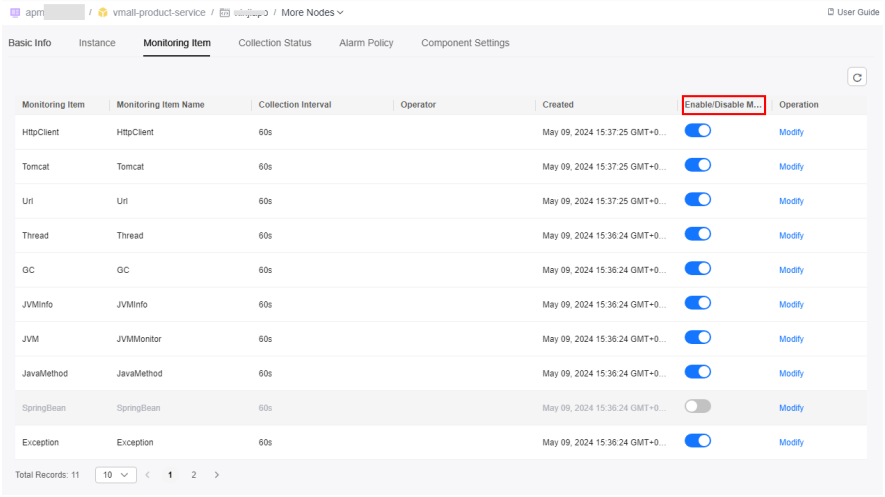
Step 2 Click  on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click  next to the target environment. The instance monitoring page is displayed.

Step 5 Click the **Monitoring Item** tab.

Figure 4-34 Enabling or disabling a monitoring item



Step 6 Locate the row that contains the target monitoring item and enable or disable it.

----End

4.3.2 Configuring the MySQL Monitoring Item

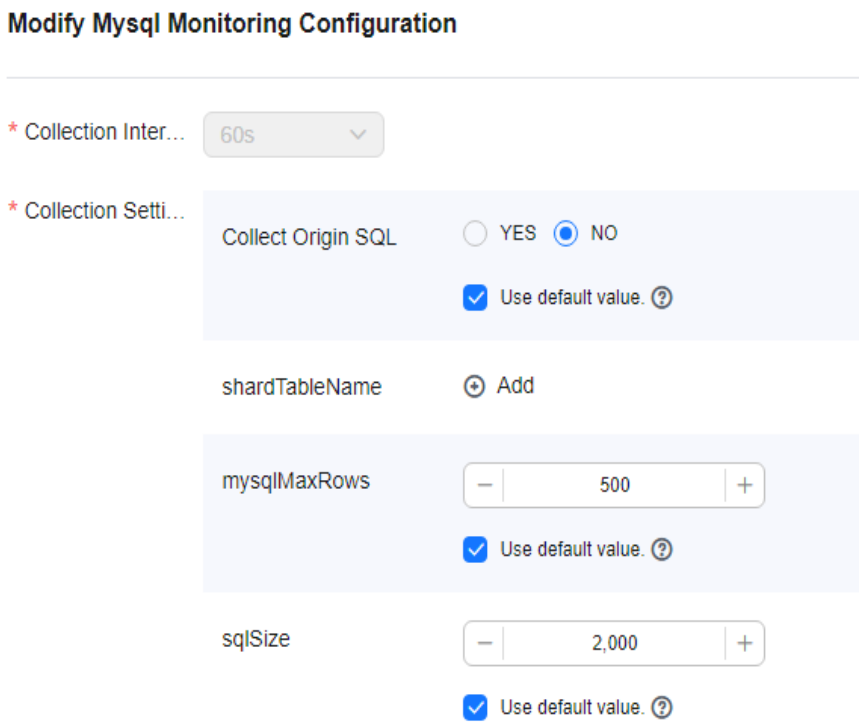
On the **Modify MySQL Monitoring Configuration** page, set the following parameters:

- **Collection Interval**: The default value is **60s** and cannot be changed.
- **Collect Original SQL**: This function is disabled by default. In that case, only SQL statements without values are collected, for example, **select name from**

user where id=?. When this function is enabled, SQL statements with values are collected, for example, **select name from user where id=1**.

- **shardTableName**: specified when you need to aggregate multiple tables into one table. For example, there are two tables: **UserTable_1** and **UserTable_2**. By default, two SQL statements (**select name from UserTable_1** and **select name from UserTable_2**) are displayed on the SQL monitoring page. If you set **shardTableName** to **UserTable**, tables starting with **UserTable** are aggregated into the same table. Only one SQL statement (**select name from UserTable**) is displayed on the SQL monitoring page.
- **mysqlMaxRows**: the maximum number of MySQL rows that can be collected by the Agent. If this value has been reached, the Agent stops collecting data immediately. The default value is **500**. The value ranges from 10 to 2000.
- **sqlSize**: the maximum number of SQL statement bytes that can be collected by the Agent. Only when the number of bytes is within **sqlSize**, can SQL statements be collected. The default value is **2000**. The value ranges from 10 to 4096.

Figure 4-35 Configuring the MySQL monitoring item



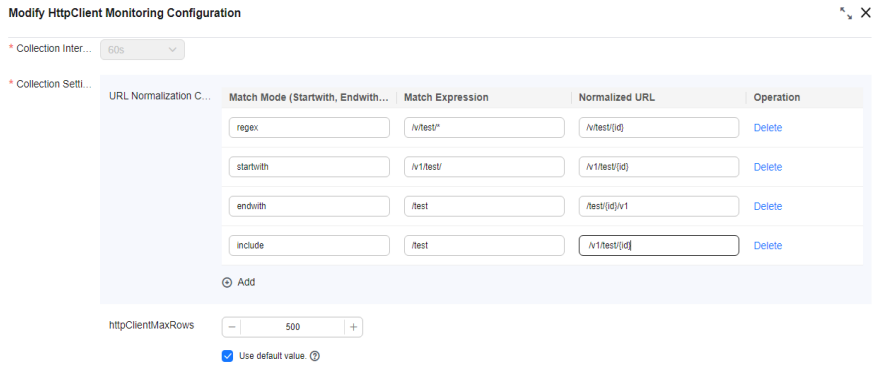
4.3.3 Configuring the HttpClient Monitoring Item

On the **Modify HttpClient Monitoring Configuration** page, set the following URL normalization parameters:

- **Collection Interval**: The default value is **60s** and cannot be changed.
- URL normalization is used to aggregate URLs that meet the conditions you set. For example, **http://localhost/rest/v1/test/123** and **http://localhost/rest/v1/test/234** can be aggregated into **http://localhost/rest/v1/test/*{id}***.

- **httpClientMaxRows**: the maximum number of HttpClient rows that can be collected by the Agent. If this value has been reached, the Agent stops collecting data immediately. The default value is **500**. The value ranges from 10 to 2000.

Figure 4-36 Configuring the HttpClient monitoring item



Normalization Methods

There are four normalization methods: **Startwith**, **Endwith**, **Include**, and **Regex**.

- **Startwith**: URLs starting with a certain expression are counted as normalized URLs. For example, URLs starting with **http://127.0.0.1/v1** are aggregated into **/v1/test/***{id}*, as shown in **Figure 4-36**.
- **Endwith**: URLs ending with a certain expression are counted as normalized URLs. For example, URLs ending with **/test** are aggregated into **/***{id}***/test**, as shown in **Figure 4-36**.
- **Include**: URLs containing a certain expression are counted as normalized URLs. For example, URLs containing **test** are aggregated into **/test/***{id}*, as shown in **Figure 4-36**.
- **Regex**: URLs that meet the wildcard expression are counted as normalized URLs. For details about the wildcard rules, see **Table 4-23**.

Table 4-23 Wildcard description

Wildcard	Description
?	Matches any character.
*	Matches zero, one, or more characters.
**	Matches zero, one, or more directories.

Usage Example

The following is an example:

URL Path	Description
/app/p?ttern	Matches files such as **/app/pattern** and **/app/pAttern**, excluding **/app/pttern**.
/app/*.x	Matches all **.x** files in the **app** directory.
/**/example	Matches **/app/example**, **/app/foo/example**, and **/example**.
/app/**/dir/file.*	Matches **/app/dir/file.jsp**, **/app/foo/dir/file.htm**, **/app/foo/bar/dir/file.pdf**, and **/app/dir/file.c**.
/**/*.jsp	Matches all **.jsp** files.

4.3.4 Configuring the URL Monitoring Item

On the **Modify URL Monitoring Configuration** page, set the following parameters:

CAUTION

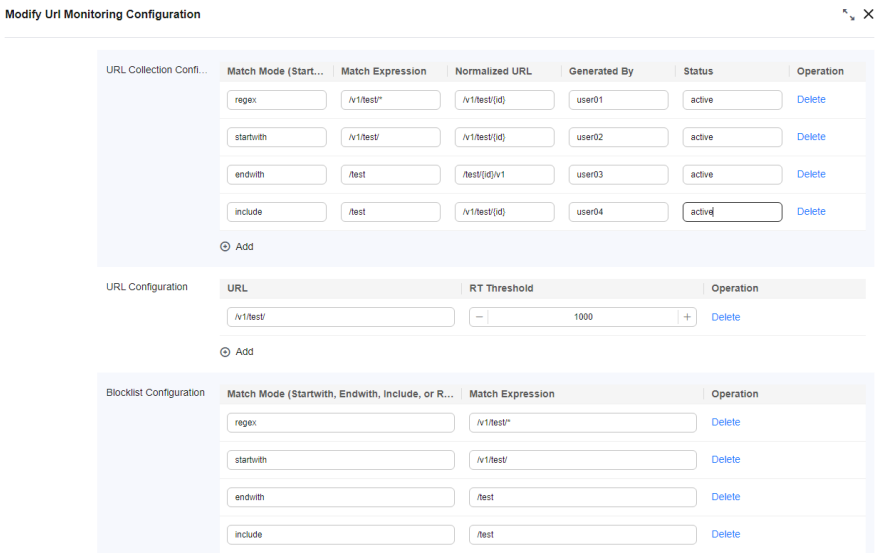
For security purposes, do not contain sensitive data in headers, URL parameters, cookies, or other parameters.

Parameter	Description	Example
Collection Interval	The default value is **60s** and cannot be changed.	60s
Key for Header Value Interception	Key specified for collecting values in headers. The collected information can be seen in the trace parameters.	Host
Key for Parameter Value Interception	Key specified for collecting values in URLs. The collected information can be seen in the trace parameters. Take **http://127.0.0.1/test?param=123** as an example. If the key is set to **param**, value **123** can be seen in the trace parameters.	param
Key for Cookie Value Interception	Key specified for collecting values in cookies. The collected information can be seen in the trace parameters.	testKey

Parameter	Description	Example
URL Collection Configuration	URLs that meet the conditions you set are aggregated. For example, **/rest/v1/test/123** and **/rest/v1/test/234** can be aggregated into **/rest/v1/test/***{id}*. The configuration method is the same as that described in **HttpClient URL Normalization**. **Generated By**: **user** or **automatic**. If **Generated By** is set to **automatic**, the normalization mode can only be **regex**. **Status**: **active** or **inactive**. If **Status** is set to **inactive**, the current URL collection configuration does not take effect.	**Figure 4-37**
Blocklist Configuration	Data of URLs that meet the conditions you set will not be collected. The configuration method is the same as that described in **HttpClient URL Normalization**.	**Figure 4-37**
Service Code Length	Maximum length of the response body to be parsed to prevent the performance from being affected. Content that beyond this limit will not be parsed, but corresponding service status codes are regarded as normal by default.	-
Key for Service Code Interception	Key specified for collecting service status codes. If the custom API returned content is **{"errorCode":500,"errorMsg":"error msg"}**, set this parameter to **errorCode**.	errorCode
Normal Service Code	If this status code is returned, traces are regarded as normal. If other codes are returned, traces are regarded as abnormal.	-
Slow Request Threshold	Global response time threshold. The default value is **800**. Requests with the response time longer than 800 ms are regarded as slow requests. The sampling ratio of slow requests will be increased.	-
URL Configuration	Response time threshold separately set for a URL. If the response time of this URL exceeds the threshold, the sampling rate of this URL will be increased. If this parameter is not set, the global slow request threshold is used by default.	**Figure 4-37**
Error Code	Options: **400 or greater** and **500 or greater** (default). By default, if status code 500 or greater occurs, the system regards that there is an error.	-

Parameter	Description	Example
URL Automatic Normalization	Example: There are three URL invocations: /get/xxx/a /get/xxx/b /get/xxx/b • If this parameter is set to **Yes**, URL automatic normalization is enabled. After normalization: /get/xxx/a 1 /get/xxx/b 2 • If this parameter is set to **No**, URL automatic normalization is disabled. /get/xxx/{p} 3 • **Use default value**: The inherited tag value is preferentially used.	-

Figure 4-37 Example



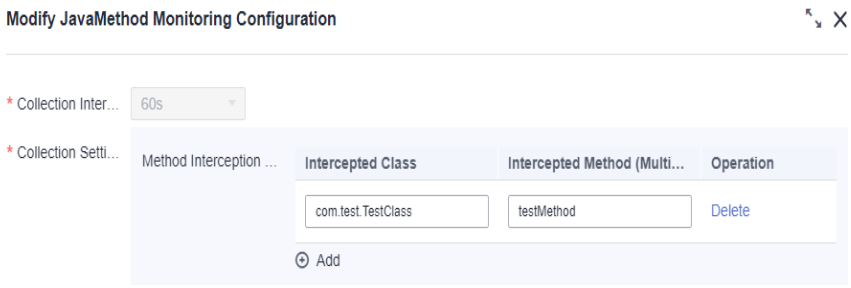
4.3.5 Configuring the JavaMethod Monitoring Item

On the **Modify JavaMethod Monitoring Configuration** page, set method interception parameters.

- **Collection Interval**: The default value is **60s** and cannot be changed.
- **Method Interception Configuration**: is used to collect specified service methods. The method data is displayed on the JavaMethod metric page and in traces.
- **Intercepted Class**: name of the fully-qualified class to be collected. Both the package name and class name need to be specified.

- **Intercepted Method**: name of the method to be collected. If multiple methods exist, separate them by commas (,), for example, **testMethod1,testMethod2**.

Figure 4-38 Configuring the JavaMethod monitoring item



4.3.6 Configuring the Druid Monitoring Item

On the **Modify Druid Monitoring Configuration** page, set the following parameters:

- **Collection Interval**: The default value is **60s** and cannot be changed.
- **TraceReportTimeSpanThreshold(ms)**: threshold for reporting getConnection method traces. If the threshold is not exceeded, such traces will not be reported. The default value is **1**. If you select **Use default value**, the value of the inherited tag is preferentially used.
- **Get pool info when calling getConnection**: specifies whether to obtain the pool information when calling the **getConnection** method. The default value is **No**. If you select **Use default value**, the value of the inherited tag is preferentially used.

4.3.7 Configuring the ApacheHttpAsyncClient Monitoring Item

On the **Modify ApacheHttpAsyncClient Monitoring Configuration** page, set the following parameters:

- **Collection Interval**: The default value is **60s** and cannot be changed.

4.3.8 Configuring the Redis Monitoring Item

On the **Modify Redis Monitoring Configuration** page, set the following parameters:

- **Collection Interval**: The default value is **60s** and cannot be changed.
- **Parameter Parsing**: The default value is **No**. If you select **Use default value**, the value of the inherited tag is preferentially used.
- **Parameter Length**: The default value is **1000**. If you select **Use default value**, the value of the inherited tag is preferentially used.
- **Distinguish Redis Ports**: The default value is **No**. If you select **Use default value**, the value of the inherited tag is preferentially used.

4.3.9 Configuring the Jedis Monitoring Item

On the **Modify Jedis Monitoring Configuration** page, set the following parameter:

Collection Interval: The default value is **60s** and cannot be changed.

4.3.10 Configuring the HBase Monitoring Item

On the **Modify HBase Monitoring Configuration** page, set the following parameter:

Collection Interval: The default value is **60s** and cannot be changed.

4.3.11 Configuring the ApacheHttpClient Monitoring Item

On the **Modify ApacheHttpClient Monitoring Configuration** page, set the following parameter:

Collection Interval: The default value is **60s** and cannot be changed.

4.3.12 Configuring the Tomcat Monitoring Item

On the **Modify Tomcat Monitoring Configuration** page, set the following parameter:

Collection Interval: The default value is **60s** and cannot be changed.

4.3.13 Configuring the EsRestClient Monitoring Item

On the **Modify EsRestClient Monitoring Configuration** page, set the following parameter:

- **Collection Interval**: The default value is **60s** and cannot be changed.
- **Index Normalization Configuration**: The system matches indexes based on a regular expression and then normalizes them.

4.3.14 Configuring the WebSocket Monitoring Item

On the **Modify WebSocket Monitoring Configuration** page, set the following parameter:

Collection Interval: The default value is **60s** and cannot be changed.

4.3.15 Configuring the KafkaProducer Monitoring Item

On the **Modify KafkaProducer Monitoring Configuration** page, set the following parameter:

Collection Interval: The default value is **60s** and cannot be changed.

4.3.16 Configuring the Hikari Monitoring Item

On the **Modify Hikari Monitoring Configuration** page, set the following parameters:

- **Collection Interval**: The default value is **60s** and cannot be changed.
- **TraceReportTimeSpanThreshold(ms)**: The default value is **1**. If **Use default value** is selected, the value of the inherited tag is preferentially used.
- **Get pool info when calling getConnection**: The default value is **No**. If **Use default value** is selected, the value of the inherited tag is preferentially used.

4.3.17 Configuring the Exception Monitoring Item

On the **Modify Exception Monitoring Configuration** page, set the following parameters:

- **Collection Interval**: The default value is **60s** and cannot be changed.
- **Determine Trace Exception upon Log Error Detection**: The default value is **Yes**. If **Use default value** is selected, the value of the inherited tag is preferentially used.
- **Associating Service Logs with TraceId**: The default value is **No**. If **Use default value** is selected, the value of the inherited tag is preferentially used.

4.3.18 Configuring the Thread Monitoring Item

On the **Modify Thread Monitoring Configuration** page, set the following parameters:

- **Collection Interval**: The default value is **60s** and cannot be changed.
- **maxThreadDepth**: The default value is **10** and the maximum number is **50**. If you select **Use default value**, the value of the inherited tag is preferentially used.

4.3.19 Configuring the GC Monitoring Item

On the **Modify GC Monitoring Configuration** page, set the following parameter:

Collection Interval: The default value is **60s** and cannot be changed.

4.3.20 Configuring the JVMInfo Monitoring Item

On the **Modify JVMInfo Monitoring Configuration** page, set the following parameter:

Collection Interval: The default value is **60s** and cannot be changed.

4.3.21 Configuring the JVMMonitor Monitoring Item

On the **Modify JVMMonitor Monitoring Configuration** page, set the following parameters:

- **Collection Interval**: The default value is **60s** and cannot be changed.
- **Call Chain Stack Collection Threshold**: When the request latency exceeds the threshold, the stack is automatically printed. The default value is **0** and the maximum value is **10000**.

4.3.22 Configuring ProbeInfo Monitoring Item

On the **Modify ProbeInfo Monitoring Configuration** page, set the following parameter:

Collection Interval: The default value is **60s** and cannot be changed.

4.4 Monitoring Item Views

APM supports summary tables, trend graphs, latest data tables, and original data tables.

- Summary table: records the summary calculation results based on the primary key metric within a period. You can click a number or character string in the summary table to view the trend graph of the primary key metric.
- Trend graph: displays the trend of a primary key metric in a period. A trend graph may have breakpoints, indicating that no data is collected in this period. There are multiple reasons why data is not collected. For example, collectors do not collect the metrics with zero calls or the data may be lost.
- Original data table: For character strings, no trend graphs can be generated. Therefore, original data tables are used. Each row indicates the mapping between a time and a value.
- Latest data table: displays the latest data. You can click a data record to view its trend graph.

NOTE

The view of each monitoring item is configured in the background and has not been opened. You can check views together with corresponding background metric sets. For details, see **Metric Sets**.

4.5 Instance

On the **Instance** page, you can view instance information, and stop, start, or delete Agents on instances.

Viewing Instances

Step 1 Log in to the management console.

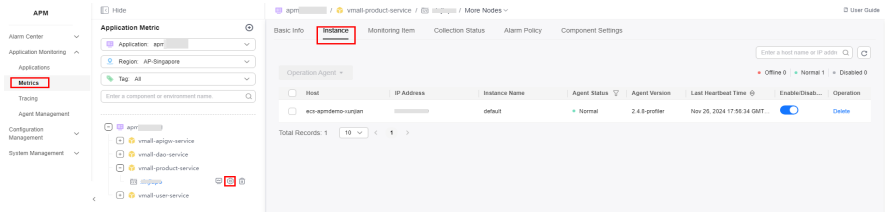
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click ⚙ next to the target environment. The instance monitoring page is displayed.

Step 5 On the displayed page, click the **Instance** tab to view the instance list.

Figure 4-39 Instance



1. Set the search criteria and click in the search box in the upper right corner of the page to filter instances.
2. In the upper right corner of the page, view the number of offline, normal, or disabled instances.

Table 4-24 Instance parameters

Parameter	Description
Host	Host name.
IP Address	IP address of an instance.
Instance Name	Instance name.
Agent Status	Agent status. Options: **Offline**, **Normal**, and **Disabled**. • By default, normal Agents are displayed first, then disabled ones, and offline ones. • You can click in the **Agent Status** column to filter data by Agent status.
Agent Version	Agent version.
Last Heartbeat Time	Latest time when instance data was collected. • You can click in the **Last Heartbeat Time** column to sort data.
Enable/Disable Agent	Enable or disable the Agent.
Operation	Operation performed on the instance. You can click **Delete** to delete the instance.

----End

Enabling or Disabling Agents

NOTE

When the Agent is enabled, is displayed. When the Agent is disabled, is displayed.

Disabling an Agent

Step 1 In the instance list, locate the instance for which you want to disable an Agent and click .

Step 2 In the displayed dialog box, click **Yes**.

----End

Enabling an Agent

Step 1 In the instance list, locate the instance for which you want to enable an Agent and click .

Step 2 In the displayed dialog box, click **Yes**.

----End

Operating Agents in Batches

Step 1 In the instance list, select desired instances.

Step 2 Click **Operate Agent**.

Step 3 In the drop-down list, select **Enable Agent**, **Disable Agent**, or **Delete Agent**.

Step 4 In the displayed dialog box, click **Confirm** to enable, disable, or delete the Agents.

----End

4.6 Collection Status

On the **Collection Status** page, you can view the collection status of hosts.

Step 1 Log in to the management console.

Step 2 Click on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click next to the target environment. The instance monitoring page is displayed.

Step 5 On the displayed page, click the **Collection Status** tab to view the collection status of hosts.

Figure 4-40 Viewing the collection status

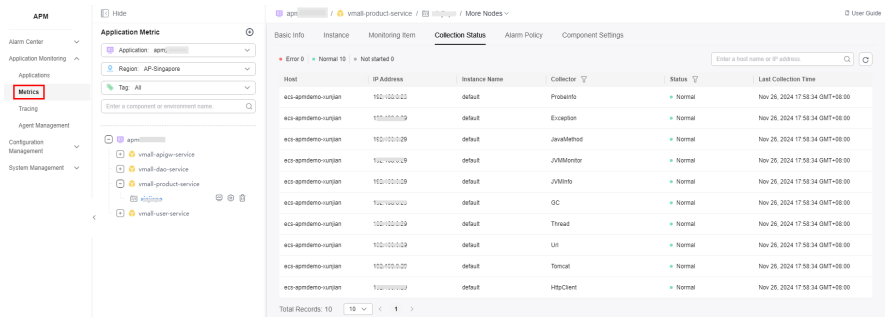


Table 4-25 Collection status description

Parameter	Description
Host	Host name.
IP Address	IP address of an instance.
Instance Name	Instance name.
Collector	Collector name. You can click in the **Collector** column to filter data by collector name.
Status	Collection status. Options: **Normal**, **Error**, and **Not started**. You can click in the **Status** column to filter data by status.
Last Collection Time	Latest time when the collector collected data.

----End

4.7 Component Settings

Component settings include log association, Profiler, and full sampling settings.

Step 1 Log in to the management console.

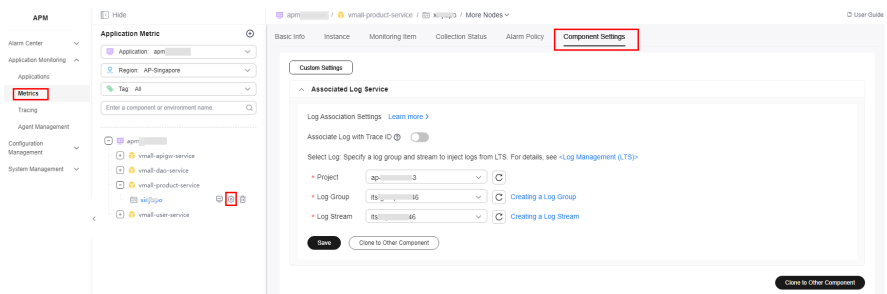
Step 2 Click on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click next to the target environment. The instance monitoring page is displayed.

Step 5 Click the **Component Settings** tab. Currently, you can set log association.

Figure 4-41 Component settings



Step 6 Click **Clone to Other Component**.

Step 7 In the displayed dialog box, select one or more components and click **Clone to Other Component**. The log association settings are then successfully copied to the selected components.

----End

Associating Traces with Logs

Trace IDs can be associated with logs in Log Tank Service (LTS). Then you can find out the logs based on the associated trace IDs for fast troubleshooting.

NOTE

- If you enable the function of recording trace IDs to service logs, trace IDs will be automatically generated in the logs. If this function is disabled, the log association settings will not take effect.
- The Log4j, Log4j2, and Logback log components are supported for associating service logs.
- Only the Java type is supported.

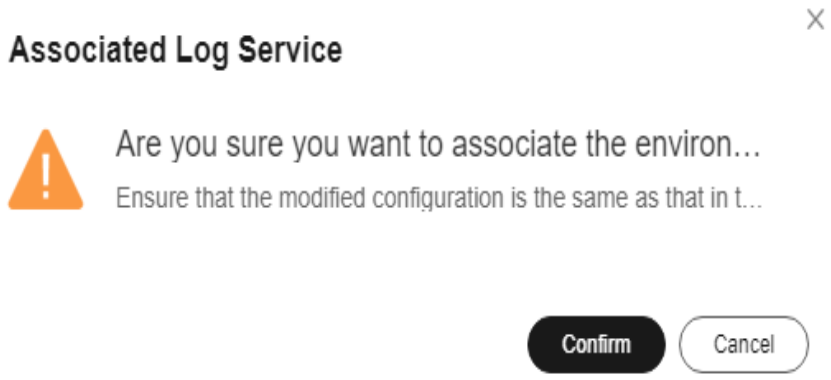
Step 1 Under log association settings, enter related information.

Table 4-26 Parameters for log association settings

Parameter	Description
Project	Select a project from the drop-down list.
Log Group	A log group is a group of log streams which share the same log retention settings. Up to 100 log groups can be created for a single account. For how to create a log group, see **Creating a Log Group**.
Log Stream	A log stream is the basic unit for reading and writing logs. You can put different types of logs into different streams to ease management. For how to create a log stream, see **Creating a Log Stream**.

Step 2 Click **Save**.

Figure 4-42 Saving log association settings



Step 3 In the displayed dialog box, click **Confirm**.

Step 4 Click **Clone to Other Component**.

Step 5 On the displayed page, select one or more components and click **Save and Clone to Other Component**. The current settings will then be copied to the components you have selected.

----End

5 Tracing

When the calls between enterprise microservices are complex, APM Agents sample some requests, and intercept corresponding requests and subsequent call information. For example, in the scenario where service A calls service B and then calls service C, after service A receives a request, APM determines whether to trace the request based on the intelligent sampling algorithm.

Intelligent Sampling Algorithm

APM uses the intelligent sampling algorithm to determine whether to trace requests.

- If a request needs to be traced, a trace ID is generated and details (events) about some important methods (generally the tree structure with the parent-child relationship) under service A are intercepted. At the same time, the trace ID is transparently transmitted to service B. The important methods under service B are also intercepted. The trace ID is also transparently transmitted to service C. Some methods under service C are intercepted in a similar way as those under services B and A. Each node respectively reports event information and an association relationship can be formed based on the trace ID. In this way, you can view the call details of the entire request based on the trace ID.
- If a request does not need to be traced, no trace ID is generated. Service B does not receive the trace ID and uses the same algorithm as service A to determine whether to perform tracing.
- After data is reported, APM stores not only all event details, but also the root event (called span) information of each service for subsequent trace search. Generally, you search for the span information and then obtain the overall trace details based on the trace ID in the span information.
- By default, the intelligent sampling policy is used. There are three types of URLs: error URLs, slow URLs (use the default 800 ms or customize a threshold), and normal URLs. The sampling ratio of each type of URL is calculated separately. For APM, statistics are collected and reported every minute. In the first collection period, all URLs are regarded as normal for sampling. In the second collection period, URLs are classified into error, slow, and normal URLs based on the statistics collected in the previous period.
  - Sampling rate of error URLs: If the CPU usage is less than 30%, 100 records are collected per minute. If the CPU usage is greater than or

equal to 30% but less than 60%, 50 records are collected per minute. If the CPU usage is greater than or equal to 60%, 10 records are collected per minute. At least two records are collected for each URL.

- Sampling rate of slow URLs: If the CPU usage is less than 30%, 100 records are collected per minute. If the CPU usage is greater than or equal to 30% but less than 60%, 50 records are collected per minute. If the CPU usage is greater than or equal to 60%, 10 records are collected per minute. At least two records are collected for each URL.
- Sampling rate of normal URLs: If the CPU usage is less than 30%, 20 records are collected per minute. If the CPU usage is greater than or equal to 30% but less than 60%, 10 records are collected per minute. If the CPU usage is greater than or equal to 60%, 5 records are collected per minute. At least one record is collected for each URL.

The advantage of the preceding algorithm is that once the trace information is generated, the link is complete, helping you make correct decisions. If a large number of URLs are called, abnormal requests may fail to be collected. In this case, you can collect metrics to locate system exceptions.

Trace Search

This function is used to search for span information, that is, the root event of a node. A trace can be found in multiple environments. For example, in the scenario where service A calls service B and then calls service C, the same trace may be found from services A, B, and C.

Step 1 Log in to the management console.

Step 2 Click  on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Tracing**.

Step 4 Select a time range in the upper right corner of the page. Default: **Last 20 minutes**. Options: **Last 20 minutes**, **Last hour**, **Last 3 hours**, **Last 6 hours**, **Last day**, **Today**, **Yesterday**, or **Custom**.

Step 5 Specify the following search criteria or add custom criteria to query traces.

Table 5-1 Search criteria of traces

Search Criterion	Description	Mandatory
Application	Application to which the trace belongs.	Yes
Region	Region where the trace is located.	Yes
Component	Component to which the trace belongs.	No
Environment	Environment to which the trace belongs.	No
Instance	Instance to which the trace belongs.	No

Search Criterion	Description	Mandatory
URL	Trace URL, which can be a REST URL or real URL. A REST URL contains a variable name, for example, **/apm/get/{*id*}**. A real URL indicates an actual URL.	No
Exact Search	Whether to perform exact match on URLs. If this option is selected, exact match is performed. If this option is not selected, fuzzy match is performed.	No
Call Method	HTTP method of the trace.	No
Status Code	HTTP status code returned by the trace.	No
Response Time	Response time range of the trace. You can specify the minimum and maximum response time to search for the trace or leave them empty.	No
Exception or Not	Whether to filter the traces that are regarded as exceptions.	No
Trace ID	If you specify this parameter, other search criteria become invalid and the search will be performed based on the trace ID you specify.	No
Custom Parameter	• Search for traces by call parameter. The format is **key=value**. Example: **exceptionMsg=failed**. • Configure required parameters before you search for traces by custom parameter. For example, if you have configured **Key for Header Value Interception**, **Key for Parameter Value Interception**, and **Key for Cookie Value Interception** for URL monitoring, you can set **key=value** to search, for example, **httpMethod=POST**. For details about how to configure URL monitoring, see **Configuring the URL Monitoring Item**.	No
Global Trace ID	Global ID of a trace. If you specify this parameter, other search criteria become invalid and the search will be performed based on the trace ID you specify.	No

Search Criterion	Description	Mandatory
Application Code	If you have configured **Service Code Length**, **Key for Service Code Interception**, and **Normal Service Code**, corresponding application codes will be collected. You can search information based on application codes. Generally, the value of **Application Code** is the same as the value of **Normal Service Code**. For details about how to configure URL monitoring, see **Configuring the URL Monitoring Item**.	No

----End

Viewing Trace Details

Viewing Basic Information About the Trace Filtered Based on the Search Criteria

In the displayed trace list, click > next to the target trace to view its basic information, as shown in the following figure.

Figure 5-1 Basic information about a trace

Parameter description:

1. HTTP method of the trace.
2. REST URL of the trace. A REST URL contains a variable name, for example, **/apm/get/{*id*}**. You can click the URL to go to the trace details page.
3. Start time of the trace.
4. HTTP status code returned by the trace.
5. Response time of the trace.
6. Trace ID.
7. Component to which the trace belongs.
8. Environment to which the trace belongs.
9. Host of the instance to which the trace belongs.
10. IP address of the instance to which the trace belongs.
11. Actual URL of the trace.
12. Logs.

a. On the LTS console, configure the collection. For details, see **Ingesting ECS Text Logs to LTS**.

b. Click **View Logs** to go to the LTS page based on the trace ID. For details, see **Searching Logs**.

NOTE

If the function of associating trace IDs with logs is not enabled, a warning dialog box is displayed. Click **Associate Now** to go to the log association settings page. For details about how to associate logs with trace IDs, see **Component Settings**.

13. Only the traces of successful or failed requests can be displayed. The following uses **Successful Request** as an example.
    - Click the green button next to **Successful Request**, only the traces of successful requests are displayed. The red button next to **Failed Request** becomes dimmed.
    - If you click the green button again, both the traces of successful and failed requests are displayed. The red button is no longer dimmed.
    - The green and red buttons cannot be dimmed at the same time.

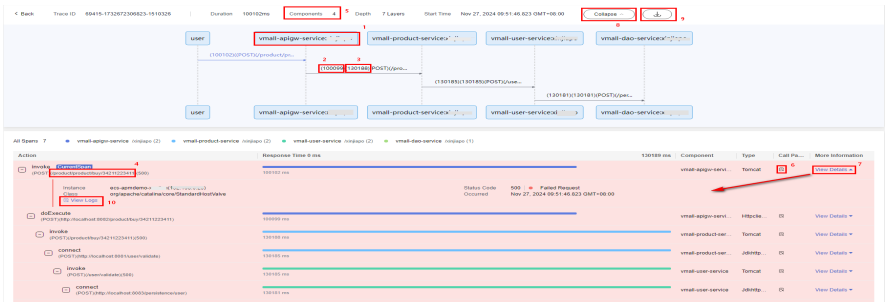
You can also click a specific URL on the monitoring item view page, for example, the table view of the URL monitoring item. In this way, you can quickly search for required trace information based on preset search criteria.

Viewing the Complete Information About the Trace, Including Local Method Stacks and Remote Call Relationships

Click the name of a trace to view its details, as shown in the following figure.

- The upper part is the sequence diagram of the trace, which shows complete call relationships between components. This diagram contains the information about the client and server corresponding to each call. The lower the line is, the later a call occurs.
- The lower part lists the method stack details of the trace. Each line indicates a method call. You can view the detailed method call relationships of the trace. By default, only component methods supported by JavaAgents are displayed. To display application methods, configure the application methods to be intercepted during JavaMethod configuration.

Figure 5-2 Call relationship



Parameter description:

1. Component and environment to which the called API belongs

2. Response time (unit: ms) of the client. You can hover the mouse pointer over this digit to view more details.
3. Response time (unit: ms) of the server.
4. Key parameter of the method in the trace method stack. For example, for a Tomcat entry method, a real URL is displayed. For a MySQL call method, an executed SQL statement is displayed.
5. Number of components that are involved.
6. Call parameters. Click  to view the call parameters.
7. Click **View Details**. The span details are displayed.
8. Click  to download the sequence diagram.
9. Click **View Logs** to go to the LTS page based on the trace ID. For details, see **Viewing Logs**.
10. Traces are displayed in a tree. **Depth** indicates the number of layers in the tree.

Figure 5-3 Depth

6 Application Topology

On the tracing page, you can view the topology of a single call, as well as the overall topology between different services based on collected metric data. There are two types of application topologies:

- Single-component topology: topology of a single component under an environment. You can also view the call relationships of direct and indirect upstream and downstream components.
- Global application topology: topology of some or all components under an application.

Each line in the topology indicates the call relationship between services within a period. The statistics can be collected from the calling or called party. You can click a line to view the call trend on the right. The topology can also display the call relationships between middleware. On the topology, you can view the call relationships between services and check whether the calls between services are normal to quickly locate faults.

Viewing the Topology of a Component

Step 1 Log in to the management console.

Step 2 Click  on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

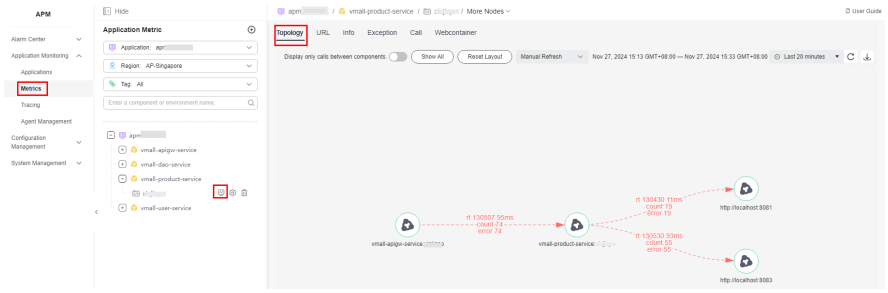
Step 4 In the tree on the left, click  next to the target environment.

Step 5 Click the **Topology** tab to view the call and dependency relationships of the component.

Click a line between components. The detailed data is displayed on the right.

Enable **Display only calls between components** to shield the calls of external components, or click **Show All** to display the calls between all components except the central node.

Figure 6-1 Viewing the topology of a component



Step 6 Right-click a component and then click **View Traces** or **View Metrics**.

Figure 6-2 Viewing the traces or metrics of the component

- Downloading the topology

  Click  to download the topology to the default path.
- Viewing a call chain

  Click **Viewing a Call Chain** to go to the trace page of the component. For details, see **Tracing**.
- Viewing indicators

  Click **Viewing Indicators** to go to the URL page of the component. For details, see **URL**.

----End

Viewing the Global Topology

Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

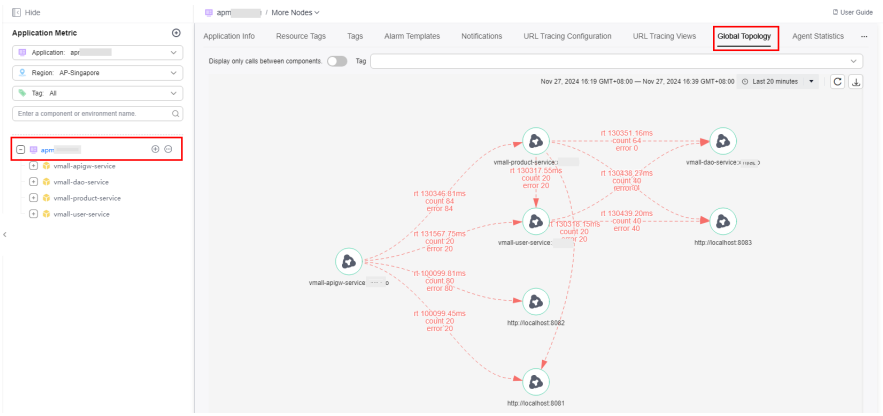
Step 2 In the tree on the left, click an application. The application details page is displayed.

Step 3 Click the **Global Topology** tab to view the call and dependency relationships of all components under the application.

- Click a line between components. The detailed data is displayed on the right.
- Enable **Display only calls between components** to shield the calls of external components.

- Use tags to filter calls.

Figure 6-3 Viewing the global topology



Step 4 Right-click a component and then click **View Traces** or **View Metrics**. For details, see **Step 6**.

----End

7 URL Tracing

You can view the topology of a single call, as well as the overall topology between different services. In some scenarios, the call relationships of an important business need to be traced. This process is called URL tracing. For example, to trace the API for creating online shopping orders. In APM, URL tracing consumes a large number of resources. Therefore, an entry URL will not be added for tracing by default. However, you can set that if necessary. APM has a limit on the total number of URLs added for tracing. It focuses on tracing the downstream calls for the APIs that are added for tracing. Through URL tracing, you can monitor the call relationships between important APIs and downstream services, and then detect problems more precisely.

Configuring URL Tracing

Step 1 Log in to the management console.

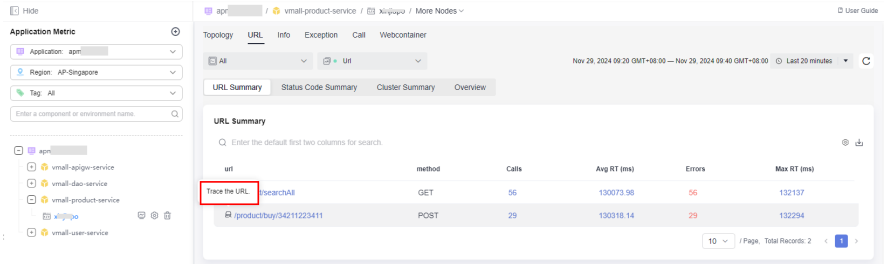
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click the environment that needs URL tracing. The environment details page is displayed. By default, the **URL** tab page is displayed.

Step 5 Move the mouse pointer to the target URL, click , and add it for URL tracing.

Figure 7-1 Configuring URL tracing



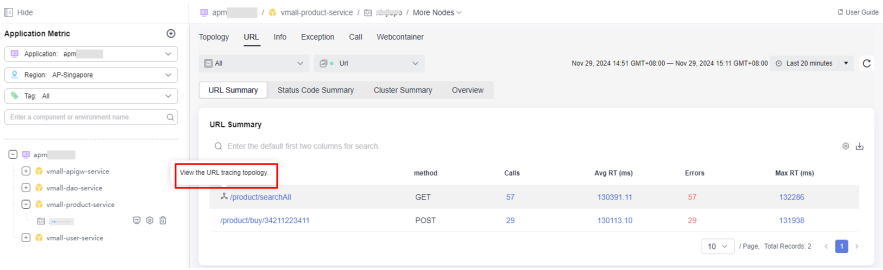
----End

Checking the URL Tracing View

- On the **URL** tab page:

  For the URL added for tracing, click next to it to view its topology.

  Figure 7-2 Viewing URL tracing details



- On the **URL Tracing Views** tab page:

Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

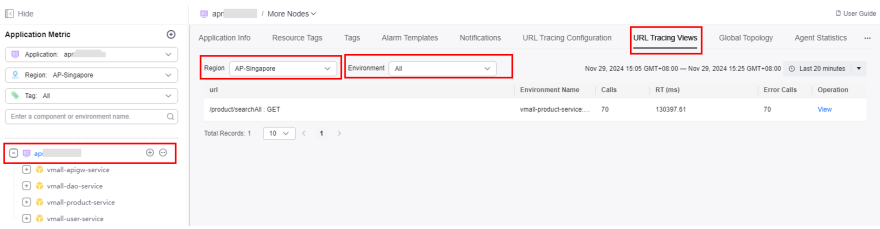
Step 2 In the tree on the left, click an application. The application details page is displayed.

Step 3 Click the **URL Tracing Views** tab to check all URL tracing views of the application.

Step 4 Filter transaction views by region and environment.

Step 5 Click **View** in the **Operation** column of the row that contains the URL you want to view.

Figure 7-3 Checking the URL tracing view



----End

Viewing the URL Tracing Configuration

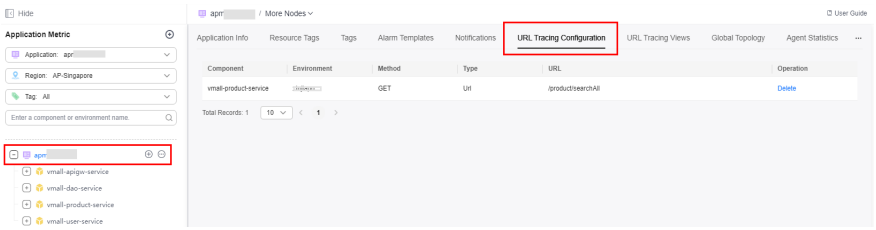
The URL which has been added for tracing will be displayed in the URL tracing configuration list.

Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 2 In the tree on the left, click an application. The application details page is displayed.

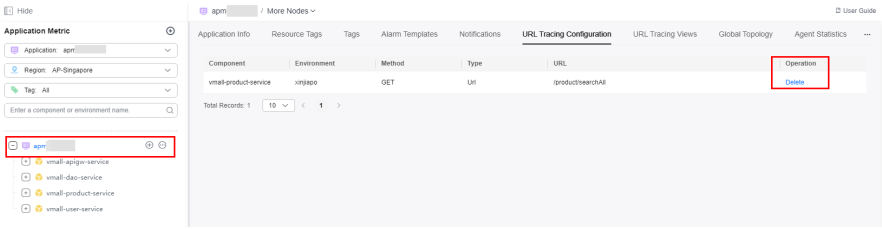
Step 3 Click the **URL Tracing Configuration** tab to check all URL tracing configurations of the application.

Figure 7-4 Viewing the URL tracing configuration list



Step 4 To delete a URL tracing configuration, click **Delete** in the **Operation** column.

Figure 7-5 Deleting a URL tracing configuration



----End

Viewing Transactions

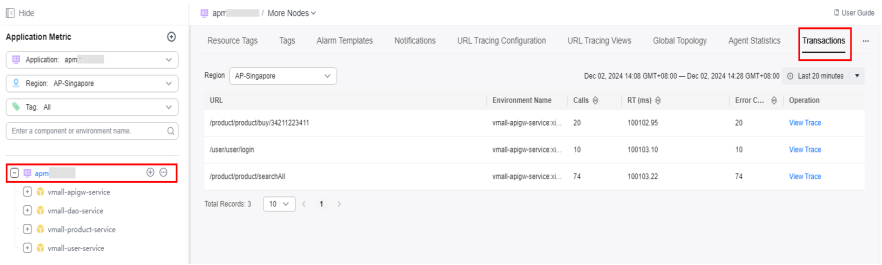
Transaction URLs are displayed in a list. By default, the system displays the invocation of all entries.

Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 2 In the tree on the left, click an application. The application details page is displayed.

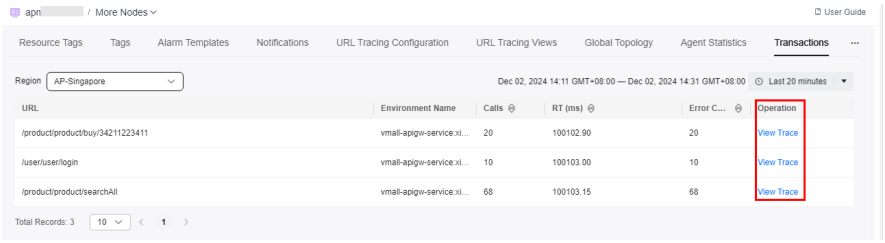
Step 3 Click the **Transactions** tab to view all transactions of the application.

Figure 7-6 Viewing transactions



Step 4 Click **View the call chain** in the **Operation** column of the target transaction. For operations related to call chains, see **Tracing**.

Figure 7-7 Viewing the call chain



----End

8 Resource Tag Management

You can tag resources under your account for classification. This section describes how to use tags to query resources and how to modify and delete tags.

NOTE

Resource tag management is related to **Tag Management Service**, **Cost Center**, and **Billing Center**.

Checking Resource Tags

Step 1 Log in to the management console.

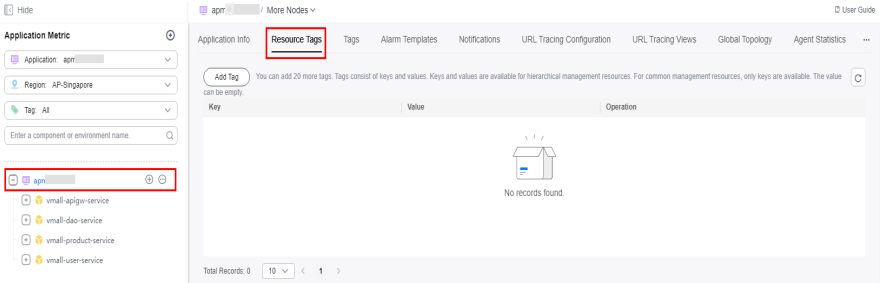
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the navigation tree on the left, click a target application and click the **Resource Tag Management** tab.

Step 5 Checking the tag list of the current application, as shown in the following figure.

Figure 8-1 Checking the tag list



----End

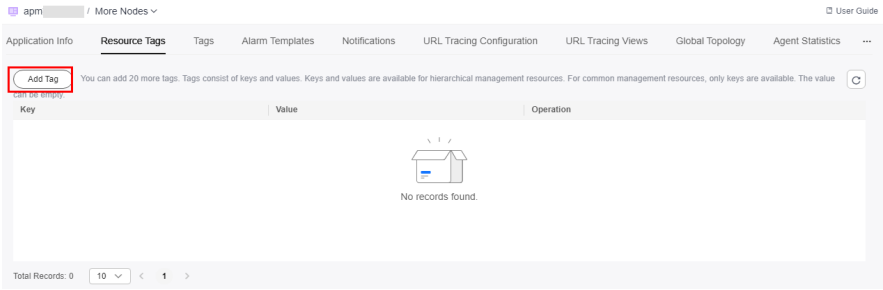
Adding Resource Tags

To add a tag with the same key to all resources in the search result list, click **Add Tag**.

Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 2 In the navigation tree on the left, click the application to which you want to add a tag and choose **Resource Tag Management** > **Add Tag**.

Figure 8-2 Adding a tag



Step 3 Set tag parameters.

Figure 8-3 Setting tag parameters

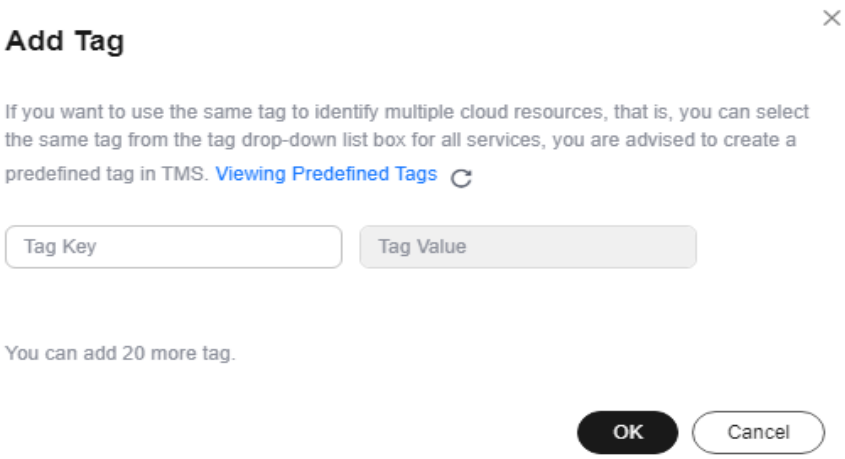


Table 8-1 Tag parameters

Parameter	Description
Tag Key	• The tag key cannot be empty or start or end with a space. • Enter 1 to 128 characters. Only letters, digits, spaces, and special characters (_.:=+-@) are allowed. • Each tag key must be unique.
Tag Value	• Enter up to 255 characters. Only letters, digits, spaces, and special characters (_.:=+-@) are allowed. • The resource tag value can be empty, but the predefined tag value cannot be empty.

NOTE

1. Each application supports up to 20 tags.
2. It is recommended that you use the TMS predefined tag function to add the same tag to different cloud resources. For details, see **Creating Predefined Tags**.

Step 4 Click **OK**.

----End

Editing Resource Tags

When you modify a tag, the modification applies only to the cloud resources that contain this tag. To modify a tag, perform the following steps:

Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 2 In the navigation tree on the left, click a target application and click the **Resource Tag Management** tab.

Step 3 Click **Edit** in the **Operation** column to modify the tag content, as shown in the following figure.

Step 4 Click **OK**.

----End

Deleting Resource Tags

Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 2 In the navigation tree on the left, click a target application and click the **Resource Tag Management** tab.

Step 3 Click **Remove** in the **Operation** column to delete the target tag, as shown in the following figure.

Step 4 Click **Yes**.

----End

9 Managing Tags

You can add tags for different environments and applications for easy management.

Tag management covers tags and global tags.

A tag is used to set a collector corresponding to the monitoring item under one or more environments of an application.

A global tag is used to set a collector corresponding to the monitoring item under all environments of an application.

NOTE

Priority: Global tag collector configuration > Tag collector configuration > Collector configuration of a monitoring item under an environment

Adding a Tag

Step 1 Log in to the management console.

Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

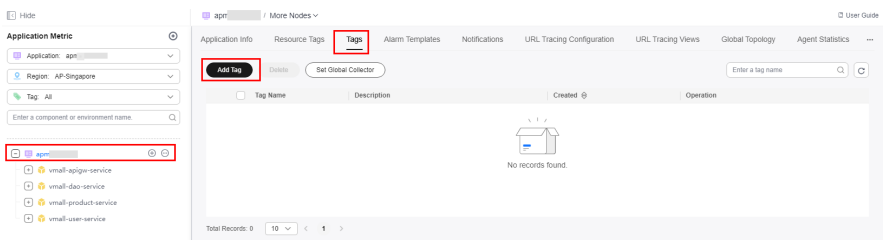
Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the navigation tree, select a target application.

Step 5 Click the **Tags** tab.

Step 6 Click **Add Tag**.

Figure 9-1 Adding a tag



Step 7 On the page that is displayed, set **Tag** and **Description**, and select the environment to be associated.

Table 9-1 Tag parameters

Parameter	Description
Tag	Enter 1 to 128 characters. Only digits, letters, underscores (_), hyphens (-), brackets, and periods (.) are allowed.
Description	Enter up to 1000 characters. Only digits, letters, underscores (_), hyphens (-), brackets, and periods (.) are allowed.
Bind Environment	• Search by component, environment, or application name is supported. • You can select one or more environments.

Step 8 Click **Yes**.

----End

Modifying a Tag

Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 2 In the navigation tree, select a target application.

Step 3 Click the **Tags** tab.

Step 4 Locate the row that contains the tag to be modified and click **Collector Configuration** in the **Operation** column. In the dialog box that is displayed, select your desired collector from the drop-down list and click **Yes**.

Locate the row that contains the tag to be modified and click **Change Environment** in the **Operation** column. In the dialog box that is displayed, select your desired environment and click **Yes**.

Locate the row that contains the tag to be modified and click **Modify Tag** in the **Operation** column. In the dialog box that is displayed, modify the tag and description.

----End

Deleting a Tag

Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 2 In the navigation tree, select a target application.

Step 3 Click the **Tags** tab.

Step 4 Locate the row that contains the target tag and click **Delete** in the **Operation** column. Alternatively, select the tags to delete and click **Delete** above the tag list.

Step 5 In the dialog box that is displayed, click **Yes**.

----End

Global Tag Collector Configuration

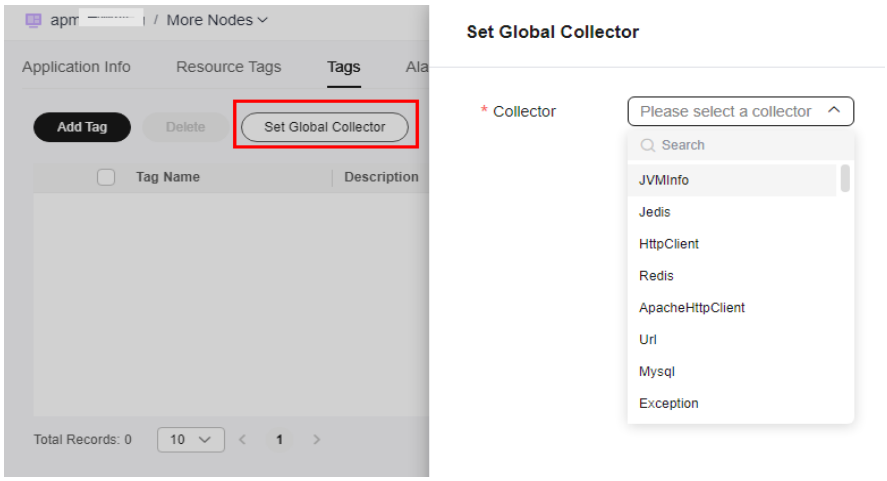
Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 2 In the navigation tree, select a target application.

Step 3 Click the **Tags** tab.

Step 4 Click **Global tag collector configuration**.

Figure 9-2 Global tag collector configuration



Step 5 Select a collector from the drop-down list and click **Yes**. For details about how to configure monitoring items, see **Application Monitoring Configuration**.

----End

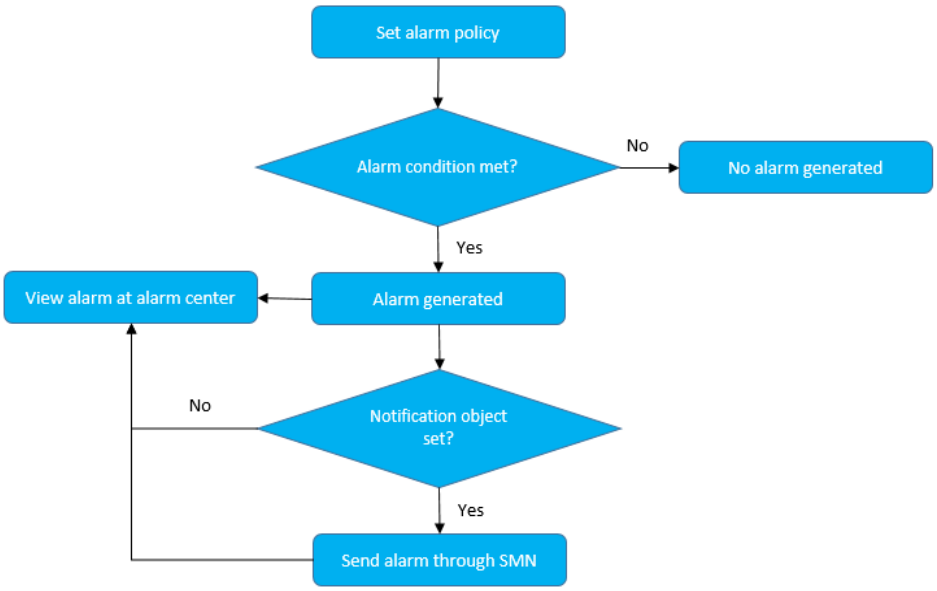
10 Alarm Management

10.1 Alarm List

Alarms are reported by services connected to APM Agents when specified conditions are met. You can learn about service exceptions in a timely manner and quickly rectify faults to prevent service loss.

Alarm process

Figure 10-1 Alarm process



Viewing Alarms

Step 1 Log in to the management console.

Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Alarm Center** > **Alarm List**.

Step 4 View alarms on the **Alarm List** page.

1. Select an application from the application drop-down list to view its alarms.
2. In the search text box, set search criteria, and click 🔍 to view the alarms that meet the criteria.
3. Click ▽ next to **Alarm Status** to filter alarms by alarm status.
4. When necessary, enable **Scheduled Refresh**. In that case, the alarm list is refreshed every 5s.
5. Click ⓘ in the **Operation** column to view the alarm details and notification.

----End

10.2 Alarm Policies

10.2.1 Configuring an Alarm Template

APM allows you to configure alarm templates. You can create multiple alarm policies under a template and bind them to nodes.

Procedure

Step 1 Log in to the management console.

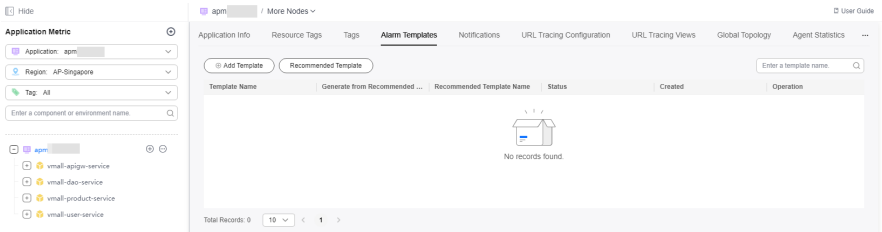
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click an application. The metric details page of the application is displayed.

Step 5 Click the **Alarm Templates** tab.

Figure 10-2 Adding an alarm template



Step 6 Click **Add Template** to add an alarm template as prompted.

1. Enter basic information and then click **Next**.

Template Name: Enter up to 64 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Remarks: Enter up to 512 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.

2. Click **Add Alarm Policy** to add an alarm policy.

   a. Basic information

   Table 10-1 Basic information about an alarm policy

Parameter	Description
Policy Name	Custom name, which cannot be left blank. Only letters, digits, underscores (_), and hyphens (-) are allowed. Enter up to 512 characters.
Alarm Severity	Severity of an alarm. Options: **COMMON** and **CRITICAL**.
Alarm Policy Type	Options: **Single-node** and **Aggregate**. **Single-node** indicates single-instance metric alarms, and **Aggregate** indicates aggregated metric alarms of all instances under a component.
Monitoring Item	Select a target monitoring item. The information about the selected item is displayed on the right.
Metric Set	Select a target metric set. The information about the selected metric set is displayed on the right.

   b. Alarm rule

   Table 10-2 Alarm rule parameters

Parameter	Description
Dimension	(Optional) A category of metrics.
Metric	Metric for which you want to define one or more alarm rules. **Metric**: a metric in the metric set. For example, if **Monitoring Item** is set to **Url** and **Metric Set** is set to **total**, you can select the **errorCount** metric. **Operator**: operation to be performed. **Threshold**: threshold of the metric.

Parameter	Description
Alarm Condition	Condition for triggering an alarm. A: the number of collection periods. Range: 1–10. B: the number of times the alarm is triggered. Range: 1–10. This value cannot be greater than that of A. C: period (in minutes) during which identical alarms will not be sent. This period cannot be shorter than 10 minutes.
Recovery Policy	Condition for clearing an alarm. For example, if this parameter is set to **3**, the alarm status will change to "Cleared" if no alarm is generated within 3 minutes.
Notification upon Recovery	Whether to notify recipients of alarm clearance.
Multi-Line Matching	(Optional) Whether to define data in the alarm notification content line by line.
Notification Content	Alarm details, which contain up to 500 characters. ■ If **Multi-Line Matching** is enabled, the alarm notification content supports both **Variable** and **Loop**. If **Multi-Line Matching** is disabled, only **Variable** can be selected. ■ Alarm notification content. You can customize the content or select metrics as required. ■ Alarm details, which contain up to 500 characters. ■ Select required metrics. Specifically, on the right of the page, click next to the target metric. The metric will then be displayed in the notification content. 

c. Notification object

Figure 10-3 Notification object

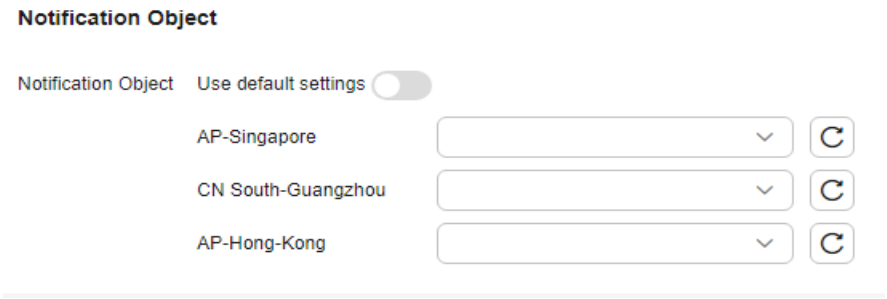


Table 10-3 Alarm notification parameters

Parameter	Description
Use default settings	– If this option is enabled, alarms will be sent to one or more default notification objects. For details about how to set notification objects, see **Alarm Notification**. – After this option is enabled, you can no longer select notification objects from the **Notification Object** drop-down list. – If all the values in the **Default** column of the **Notifications** page are **No**, no default notification objects have been set. In this case, the **Use default settings** option on the alarm policy creation page is dimmed and cannot be enabled.
Notification Object	Select a notification object from the drop-down list. Alarms will only be sent to the selected notification objects.

3. Click **Yes**.
4. Click **Next**. The **Bind Node** page is displayed.
5. Click **Bind Node** to bind nodes by environment, environment tag, or region.

Table 10-4 Node parameters

Parameter	Description
All	All nodes (including those added subsequently) in all regions will be bound.
Environment	All nodes in the selected environment will be bound.
Environment Tag	All nodes with the same tag will be bound.
Region	All nodes in the selected region will be bound.

Step 7 Click **Yes**. The information about the bound nodes is displayed in the lower part of the page, including the environment, tag, and region names.

NOTE

If there are multiple types of bound nodes, only information about the nodes with the same environment, tag, and region is displayed.

Step 8 Click **Complete**.

----End

More Operations

After the alarm template is created, perform the operations listed in **Table 10-5** if needed.

Table 10-5 Related operations

Operation	Description
Copying a template	Click **Copy** in the **Operation** column in the row that contains the template you want to copy.
Modifying a template	Click **Modify** in the **Operation** column in the row that contains the template you want to modify.
Deleting a template	Click **Delete** in the **Operation** column in the row that contains the template you want to delete.
Starting and stopping a template	Turn on or off the button ( ) in the **Operation** column in the row that contains the template you want to start or stop.

10.2.2 Creating a Custom Alarm Policy

You can create a custom alarm policy for a single component.

Procedure

Step 1 Log in to the management console.

Step 2 Click on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click next to the target environment. The instance monitoring page is displayed.

Step 5 Click the **Alarm Policy** tab.

Step 6 Click **Add Custom Alarm Policy** and set the alarm condition in the same way as that when you create an alarm template.

----End

Create an Alarm Policy Based on a Template

Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 2 In the tree on the left, click next to the target environment. The instance monitoring page is displayed.

Step 3 Click the **Alarm Policy** tab.

Step 4 In the template list, click **Copy** in the **Operation** column in the row that contains the template you want to copy.

----End

More Operations

After the alarm policy is created, perform the operations listed in **Table 10-6** if needed.

Table 10-6 Related operations

Operation	Description
Starting or stopping a policy	In the custom alarm policy list, start (in the **Operation** column) or stop the target policy.
Modifying a policy	Click **Edit** in the **Operation** column in the row that contains the policy you want to modify.
Deleting a policy	Click **Delete** in the **Operation** column in the row that contains the policy you want to delete.

10.2.3 Recommended Alarm Templates

APM provides recommended alarm templates.

Using Recommended Alarm Templates

Step 1 Log in to the management console.

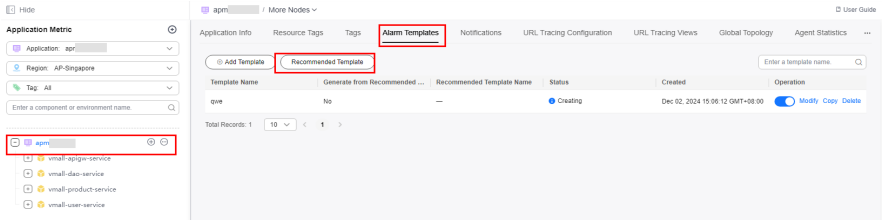
Step 2 Click on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click an application. The metric details page of the application is displayed.

Step 5 Choose **Alarm Templates** > **Recommendation Template** to view the configured alarm templates.

Figure 10-4 Viewing recommended alarm templates



Step 6 Click **View Details** in the **Operation** column in the row that contains the target alarm template.

Step 7 Click **Copy** to copy the recommended template to the template list. You can customize the template name as required.

Step 8 Click **Yes**. The copied alarm template is displayed on the template list.

Step 9 Click **Modify** in the **Operation** column and **bind nodes** to make the copied template to take effect.

----End

10.3 Alarm Notification

Alarms can be sent to specified terminals by SMS message, email, or function. In this way, you can obtain component exceptions in a timely manner and quickly rectify faults to avoid service loss. Ensure that you have the SMN permission. For details, see **Permissions Management**.

If you do not create any notification object, no alarm notifications will be received. To view alarms, log in to the APM console and choose **Alarm Center** > **Alarm List** in the navigation pane.

Creating a Notification Object

Step 1 Log in to the management console.

Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

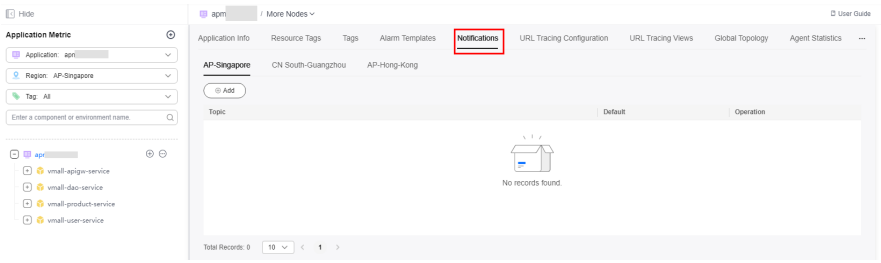
Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 4 In the tree on the left, click an application. The metric details page of the application is displayed.

Step 5 Click the **Notifications** tab.

Step 6 Click **Add**.

Figure 10-5 Creating a notification object



Step 7 On the displayed page, specify **Region** and **Topic**, and determine whether to enable default notification. If it is enabled, alarm notifications will be sent based on the topic and region you specify.

- If no topic is available, **create one**.
- If default notification is enabled, alarms will be sent to the specified region when you create an alarm policy.

Step 8 Click **Yes**.

----End

11 AgentAgent Management

11.1 Introduction

APM AgentsAgents use bytecode enhancement technology to collect application performance data in real time. They run on the server where applications are deployed.

Install Agents before using APM. For details, see section "Manually Installing Agents for Java Applications" in *APM Getting Started*.

APM can count the number of Agents used by tenants. For details, see **Agent Count**.

11.2 Agent Download Addresses

Region	Latest Version	Earlier Versions				
CN-Hong Kong	**2.4.5** sha256:37b155626f46f3a8b19772e3fd6597ece92bb255fdffa21e3e9e1467cc009392	**2.4.4** sha256:f60b55d646fe592c427143f1c8d8e8f277a647a3dd73dcdca43d7d37655ec573	**2.4.3** sha256:73de7b49e148b102b74a6075c3d8b25e76f43d6144ec5aafe6ac190ab3c1ef0b	-	-	-

Region	Latest Version	Earlier Versions				
AP-Singapore	2.4.5 sha256:37b155626f46f3a8b19772e3fd6597ece92bb255fdffa21e3e9e1467cc009392	2.4.4 sha256:f60b55d646fe592c427143f1c8d8e8f277a647a3dd73dcdca43d7d37655ec573	2.4.3 sha256:73de7b49e148b102b74a6075c3d8b25e76f43d6144ec5aafe6ac190ab3c1ef0b	2.4.1 sha256:c31cd55ead0b2172eb694fe402242b09caeb67d7059aaf40602586 33d9ade9f8	2.3.19 sha256:8755abcd541797ebf900f8f1767d62678b3cd57a6d8e045dcfb2f8c24885bfce	2.3.17 sha256:8893e89cd31748792327048 28027fd63647152 5d6e5772ff77e33 13f79a4b6b5
LA-Sao Paulo1	2.4.3 sha256:73de7b49e148b102b74a6075c3d8b25e76f43d6144ec5aafe6ac190ab3c1ef0b	-	-	-	-	-
TR-Istanbul	2.4.8 sha256:8893e89cd3174879232704828027fd636471525d6e5772ff77e3313f79a4b6b5	-	-	-	-	-
AF-Johannesburg	2.4.8 sha256:029c57990339f2a9de418b4d19e6f7349106a630b7eae559abc9d6d9ea8776d7	-	-	-	-	-

11.3 Agent Access Addresses

Table 11-1 Access addresses of Enhanced Agents

Region	Access Address
LA-Sao Paulo1	https://100.125.11.27:41333
CN-Hong Kong	https://100.125.6.106:41333
AP-Singapore	https://100.125.4.25:41333
LA-Mexico City2	https://100.125.2.18:41333
TR-Istanbul	https://100.125.8.18:41333
ME-Riyadh	https://100.125.250.39:41333
AF-Johannesburg	https://100.125.255.21:41333

11.4 Performing Operations on Agents

Agent Management allows you to check the deployment and running statuses of the Agents that are connected to APM, and to stop, start, or delete them.

Viewing Agents

Step 1 Log in to the management console.

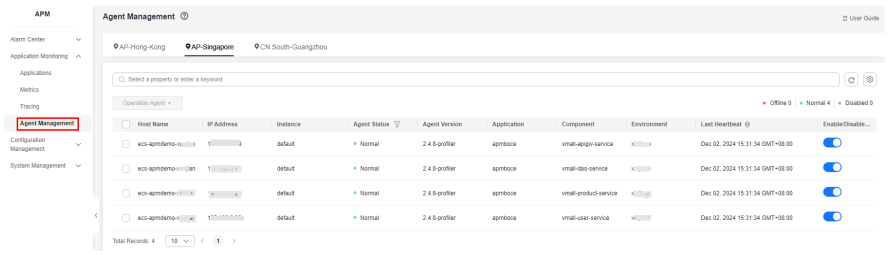
Step 2 Click  on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Application Monitoring** > **Agent Management**.

Step 4 On the Agent management page, view the Agent list.

1. In the upper left corner of the page, select a target region and application.
2. Set the search criteria and click  in the search box in the upper right corner of the page to filter Agents.

Figure 11-1 Viewing Agents



----End

The following table describes the Agent statuses.

Status	Description
Enabled	The Agent is running properly.
Offline	The Agent is abnormal due to a network error. Check and restore the network.
Disabled	The Agent is manually or globally disabled. Contact technical support.

Batch Operations

Step 1 In the navigation pane, choose **Application Monitoring** > **Agent Management**.

Step 2 Select target objects and click **Operation**.

Step 3 Select **Disable Agent**, **Enable Agent**, or **Delete Agent**.

Step 4 In the dialog box that is displayed, click **Yes** to disable, enable, or delete the Agents for the selected hosts.

----End

11.5 Upgrading Agents

Update Agent versions according to the following procedure.

Upgrading the Manually Installed Agents

To upgrade the manually installed Agent, download the new Agent by referring to **JavaAgent Download Addresses**. For details, see section "Manually Installing Agents for Java Applications" in *APM Getting Started*.

Upgrading the Agents for Java Applications Deployed in CCE Containers

To upgrade the Agents for the Java applications deployed in CCE containers, select the new version for installation. For details, see section "Installing Agents for the Java Applications Deployed in CCE Containers" in *APM Getting Started*.

Upgrading Agents of Other Types

Install new Agents. For details, see **Manually Installing Agents for Java Applications**.

12 Configuration Management

12.1 Collection Center

Collection Center displays collectors in a centralized manner. You can view and manage various collectors, metrics, and collection parameters supported by APM.

Viewing Collector Details

Step 1 Log in to the management console.

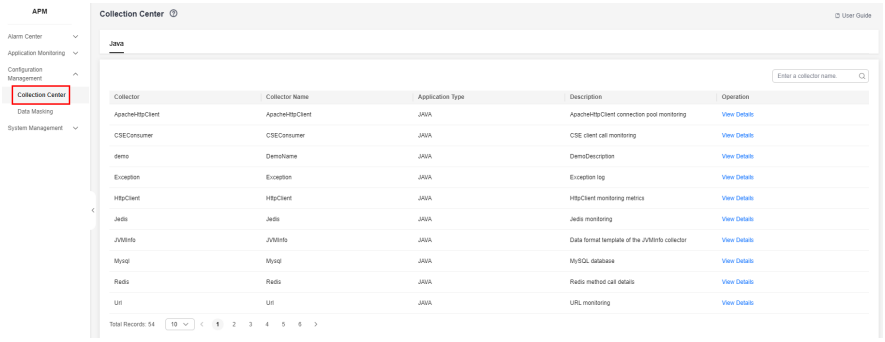
Step 2 Click  on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **Configuration Management** > **Collection Center**.

All the supported collectors are displayed.

Step 4 In the collector list, click **View Details** in the **Operation** column in the row that contains the target collector. The collector details page is displayed.

Figure 12-1 Viewing collector details



Step 5 The collector details page consists of three modules: basic information, collection parameters, and metric set.

- Basic information

  This module displays collector information such as collector name and type.

- Collection parameters

  This module displays the custom parameter settings supported by the collector. The settings take effect after being delivered to JavaAgents and are used for custom collection.

- Metric sets

  This module displays information about the metrics collected by the collector.

----End

Collector

A collector is a plug-in for collecting metric data. It consists of the collector description, metric set, and collection parameters. Collector description describes the data collected by a collector. Metric set is the data collected according to specifications. Collection parameters are the custom data to be collected.

- Data is collected by APM Agents. For example, Java performance data is collected by JavaAgents. The data collected by APM Agents must correspond to the data models of collectors' metric sets so that servers can process the data.
- The Agent of each language and framework defines its own collector.
- After a collector is added to an environment, it is instantiated as a monitoring item. This process is generally automated. APM Agents automatically discover collection plug-ins used by applications and add collectors to the environment to form monitoring items. For example, if a Java application connects to a database through the JDBC driver for MySQL, the MySQL collector is automatically added to the environment to form a monitoring item.

Collection Parameters

Collectors corresponding to monitoring items define collection parameters. You can modify collection parameters on the page as required. These parameters will be delivered to Agents with heartbeat parameters to change collection behaviors. By default, Redis instruction content is not collected for security purposes. If necessary, modify collection parameters to collect specific instruction data. Collection parameters can also be defined on environment tags. Collectors automatically inherit collection parameter attributes of corresponding environment tags. In this way, configuration is automated. For details about how to set collection parameters, see **Application Monitoring Configuration**.

Metric Sets

A collector collects data of multiple metric sets. For example, the URL collector collects URL details, overall call condition, and status statistics. Each type of statistics corresponds to a metric set. Each metric set contains multiple metrics. For example, the metric set of URL details contains metrics such as the URL, method, number of calls, number of errors, and slowest call. Each metric corresponds to a data type.

APM supports the following types of metric data:

Table 12-1 APM metric data types

Data Type	Description	Remarks
ENUM	Enumeration	Primary key type. In the example of URL monitoring, the URL and method metrics are primary keys, and other metrics such as the number of calls correspond to the URL and method.
INT	Integer	Maximum size: 8 bytes
DOUBLE	Floating-point number	8-byte floating-point number
STRING	Character string	Maximum length: 1,024 characters
CLOB	Large character string	Maximum size: 1 MB
DATETIME	Time	Time is automatically displayed on the page.

12.2 Data Masking

You can set policies to mask the data reported using APM 2.0.

NOTICE

APM will collect and store masked data. Do not upload privacy or sensitive data to APM. If you need to upload such data, encrypt them.

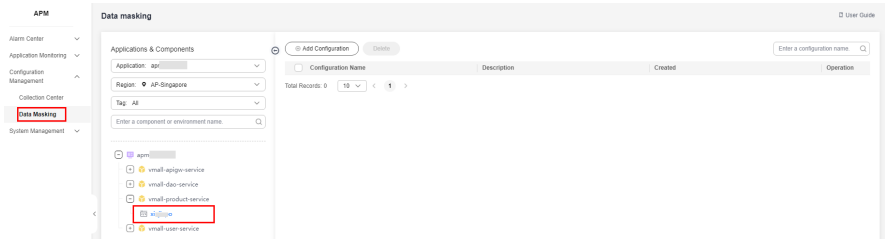
Querying a Data Masking Configuration

Step 1 Log in to the management console.

Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation tree on the left, choose **Configuration Management** > **Data Masking** and select your target node. The configuration information is displayed.

Figure 12-2 Viewing a data masking configuration



Step 4 In the search box, enter a configuration name keyword and click the search icon or press **Enter**.

----End

Adding a Data Masking Configuration

Step 1 In the navigation tree on the left, choose **Configuration Management** > **Data Masking** and select your target node.

Step 2 Click **Add** and set configuration parameters.

Table 12-2 Configuration parameters

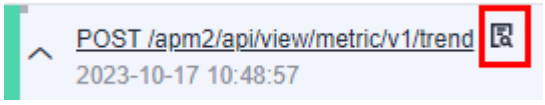
Parameter	Description
Configuration Name	Used to identify a data masking configuration. This parameter cannot be empty. Enter up to 30 characters. Only letters, digits, and special characters are allowed.
Configuration Description	Used to describe the data masking configuration. This parameter cannot be empty. Enter up to 1000 characters. Only letters, digits, and special characters are allowed.
Configuration Items	• Enter up to 32 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. • The configuration item cannot be empty. By default, an empty configuration item is displayed. If you select **Hash code**, content will be replaced with a globally unique random character string. If you select **Mask**, content will be replaced with a fixed number of asterisks (*). By default, **Mask** is selected. • Click the plus sign (+) to add a configuration item, or click the minus sign (–) to delete one. • Each configuration can contain up to 20 configuration items. • The **httpMethod**, **remoteAddr**, **exceptionType**, **content-type**, **charset**, **api_address**, **url**, **method**, **requestBody**, **responseBody**, **exceptionMsg**, **cookie**, and **Cookie** fields have special functions in APM traces and do not support masking. • If you use one of these fields as a key, the system will display a message indicating that an invalid name exists.

Step 3 Click **Yes**.

Step 4 In the navigation pane, choose **Application Monitoring** > **Tracing**.

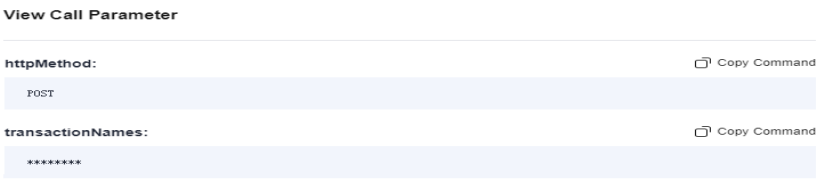
Step 5 Specify criteria to query traces and click  to view call parameters.

Figure 12-3 Viewing call parameters



Step 6 On the **View Call Parameter** page, check the value of **transactionNames**. It is displayed as **********.

Figure 12-4 Data masking going into effect



----End

Modifying a Data Masking Configuration

Step 1 In the navigation tree on the left, choose **Configuration Management** > **Data Masking** and select your target node.

Step 2 Click **Modify** in the **Operation** column to modify the configuration.

Step 3 Click **Yes**.

----End

Deleting Data Masking Configurations

Step 1 In the navigation tree on the left, choose **Configuration Management** > **Data Masking** and select your target node.

Step 2 Click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes** to delete the configuration.

Step 3 Select multiple data masking configurations and click **Delete** above the list. In the displayed dialog box, click **Yes** to delete multiple data masking configurations at a time.

----End

13 System Management

13.1 Access Keys

Access Key ID (AK) and Secret Access Key (SK) are your long-term identity credentials. JavaAgents report data with an AK. An AK is used together with an SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct.

Precautions

A user can create a maximum of two access keys with identical permissions and unlimited validity. Keep your access keys secure and change them periodically for security purposes. To change an access key, delete it and create a new one.

NOTE

APM allows you to encrypt and decrypt the SK in the **apm.config** file.

The encryption and decryption process is as follows:

1. Compile a Java class, for example, **com.demo.DecryptDemo**, and add a decryption method, for example, decrypt both the input and output to character strings.
2. Compile the decryption method to decrypt the SK and return the decrypted value.
3. Pack the **com.demo.DecryptDemo** class into a JAR package and place this JAR package and its dependent packages in the **apm-javaagent/ext** folder of JavaAgent.
4. Add the following content to the **apm.config** file:

   decrypt.className=com.demo.DecryptDemo

   decrypt.methodName=decrypt

   secret.key={*Character string encrypted by users***}**

Adding an Access Key

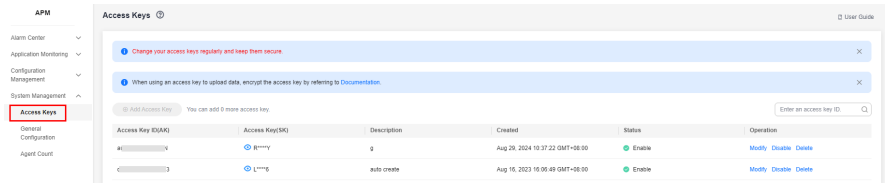
Step 1 Log in to the management console.

Step 2 Click  on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **System Management** > **Access Keys**.

Step 4 On the page that is displayed, click **Add Access Key**.

Figure 13-1 Adding an AK/SK



Step 5 Add an access key description and click **Yes** to generate an access key.

To modify the description, click **Modify** in the **Operation** column in the row that contains the target access key.

----End

Deleting an Access Key

Step 1 In the navigation pane, choose **System Management** > **Access Keys**.

Step 2 On the **Access Keys** page, locate the row that contains the target access key and click **Delete** in the **Operation** column.

Step 3 On the page that is displayed, click **Yes** to delete the access key.

----End

Enabling or Disabling an Access Key

Each access key is enabled by default. To disable it, do as follows:

Step 1 In the navigation pane, choose **System Management** > **Access Keys**.

Step 2 On the **Access Keys** page, locate the row that contains the target access key and click **Disable** in the **Operation** column.

Step 3 On the page that is displayed, click **Yes** to disable the access key.

To enable it again, click **Enable** in the row that contains the access key. On the page that is displayed, click **Yes**.

----End

13.2 General Configuration

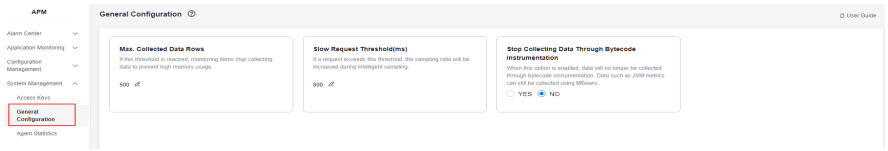
On the **General Configuration** page, you can determine whether to collect data through bytecode instrumentation, and specify the slow request threshold and maximum number of rows to collect.

Step 1 Log in to the management console.

Step 2 Click  on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation pane, choose **System Management** > **General Configuration**.

Figure 13-2 Modifying general configuration



- Stop Collecting Data Through Bytecode Instrumentation

  Enable or disable this function as required. Data such as JVM metrics will always be collected using MBeans. The default value is **No**.

  NOTE

  When the **Stop Collecting Data Through Bytecode Instrumentation** option is enabled, data will no longer be collected through bytecode instrumentation. Data such as JVM, GC, and Tomcat thread metrics can still be collected using MBeans.

- Slow Request Threshold

  If this threshold is reached, more samples will be collected during intelligent sampling. The default value is **800**.

- Max. Collected Data Rows

  If this value is reached, data will not be collected to prevent excessive memory usage. The default value is **499**.

----End

13.3 Agent Count

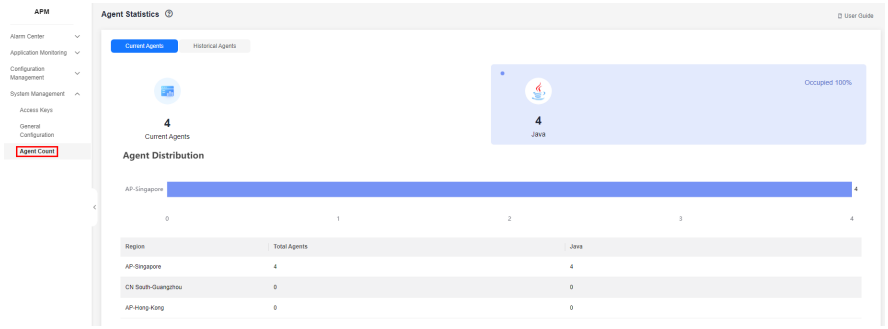
APM can count the Agents used by tenants. You can view the number of Agents by time, region, or Agent type.

Step 1 Log in to the management console.

Step 2 Click  on the left and choose **Application** > **Application Performance Management**.

Step 3 In the navigation tree, choose **System Management** > **Agent Count**.

Figure 13-3 Agent counting



- **Current Agent**: number of Agents used by the current tenant.
- **Historical Agent**: number of Agents used in each hour of today, yesterday, or a custom day.

----End

Checking the Number of Agents Used by an Application

Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

Step 2 On the displayed page, select an application to view. The **Application Info** tab page is displayed by default.

Step 3 Switch to the **Agent Count** tab page to view the number of Agents used by the current application.

- **Current Agent**: number of Agents used by the current application.
- **Historical Agent**: number of Agents used in each hour of today, yesterday, or a custom day.

----End

14 Permissions Management

14.1 Authorizing Users and User Groups Using Enterprise Projects

Enterprise Project Management Service (EPS) is used to control user access to APM resources.

After creating IAM user groups for employees, you can create enterprise projects on the Enterprise Management console and grant permissions to the user groups in the enterprise projects to implement personnel authorization and permission control.

You can create enterprise projects. Then you can manage resources across different regions by enterprise project, grant different permissions to user groups, and add them to enterprise projects.

Enterprise Management is a resource management service on Huawei Cloud. You can apply for it after registration. For details about how to enable and authorize an enterprise project, see **Project Management**.

14.2 Creating a User and Granting Permissions

This chapter describes how to use IAM for fine-grained permissions control for your APM resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing APM resources.
- Manage permissions on a principle of least permissions (PoLP) basis.
- Entrust an account or cloud service to perform efficient O&M on your APM resources.

If your account does not need individual IAM users, skip this chapter.

This section describes the procedure for granting permissions (see **Figure 14-1**).

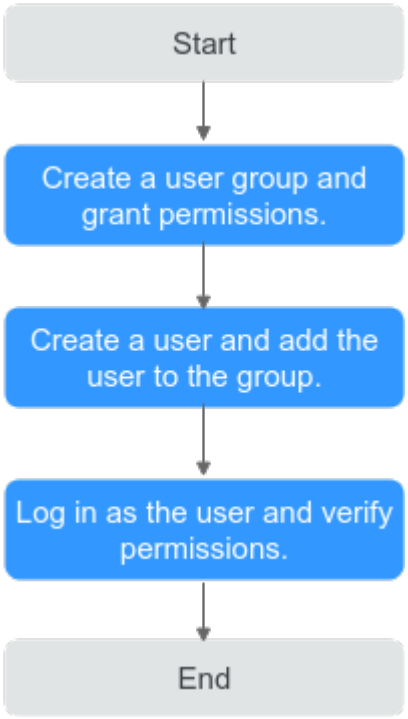
Prerequisite

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

Process Flow

Supported Cloud Services

Figure 14-1 Process for granting APM permissions



1. **Creating a User Group and Assigning Permissions**

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

2. **Creating an IAM User**

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

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

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

A Change History

Table A-1 Change history

Released On	Description
2024-12-26	1. Optimized frontend pages. 2. Added sections **Subscribing to Enterprise-Edition APM**, **Checking the Basic Information About an Application, Sub-Application, Component, and Environment**, **Instance**, **Collection Status**, **Component Settings**, **Agent Download Addresses**, and **Agent Access Addresses**. 3. Added the function of associating traces with logs.
2023-07-20	This issue is the first official release.

