Application Performance Management 2.0

User Guide

Issue 01

Date 2023-07-20

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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.
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.
Agent Management	Agent Management allows you to view 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: Set the maximum number of rows for data collection, slow request threshold, and whether to stop collecting data through bytecode instrumentation. ● 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

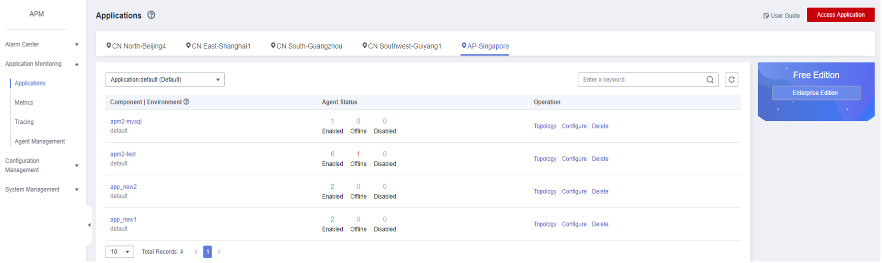
The **Applications** page displays information such as components, environments, Agent status, and supported operations.

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	Agent Status	Operation
apm2-mysql default	1 Enabled 0 Offline 0 Disabled	Topology | Configure | Delete
apm2-test default	0 Enabled 1 Offline 0 Disabled	Topology | Configure | Delete
app_new2 default	2 Enabled 0 Offline 0 Disabled	Topology | Configure | Delete
app_new1 default	2 Enabled 0 Offline 0 Disabled	Topology | Configure | Delete

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 abnormal due to a network error. Check and restore the network.

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 right 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.

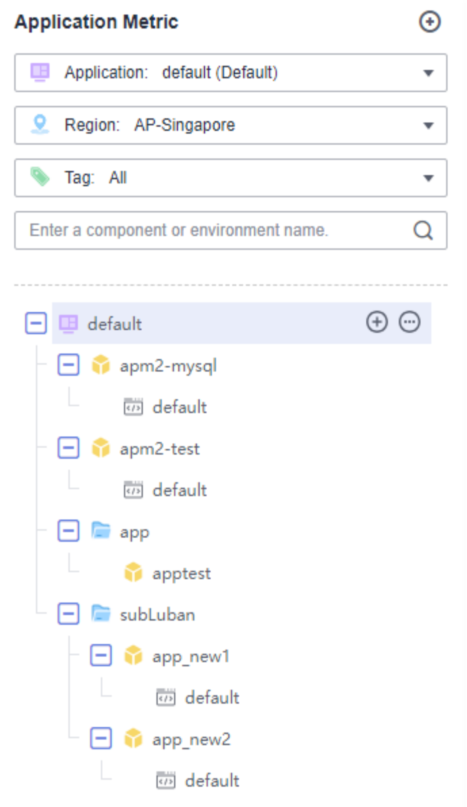
3 CMDB Management

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.

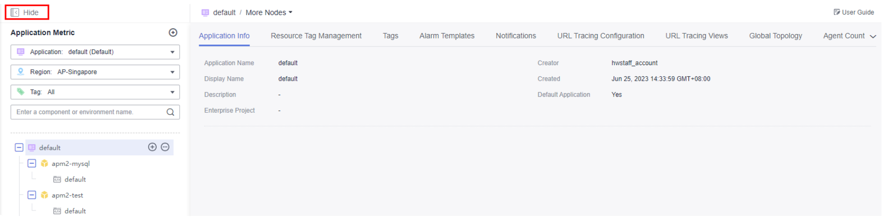
Figure 3-1 CMDB structure



The CMDB structure tree can be hidden.

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

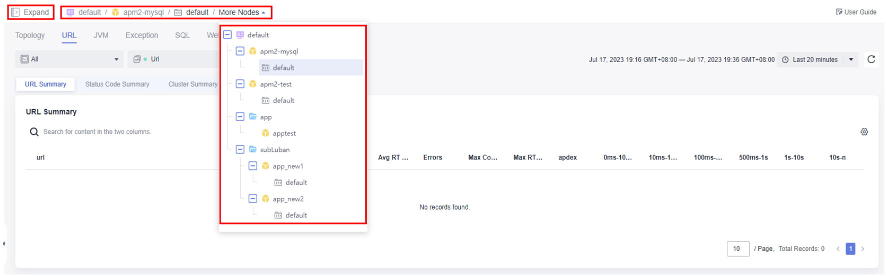
Figure 3-2 Hiding the CMDB structure tree



Application Name default
Display Name default
Description -
Enterprise Project -
Creator hwstaff_account
Created Jun 25, 2023 14:33:59 GMT+08:00
Default Application Yes

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



URL Summary

Jul 17, 2023 19:16 GMT+08:00 — Jul 17, 2023 19:36 GMT+08:00

10 / Page, Total Records: 0

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

----End

3.1 Creating an Application

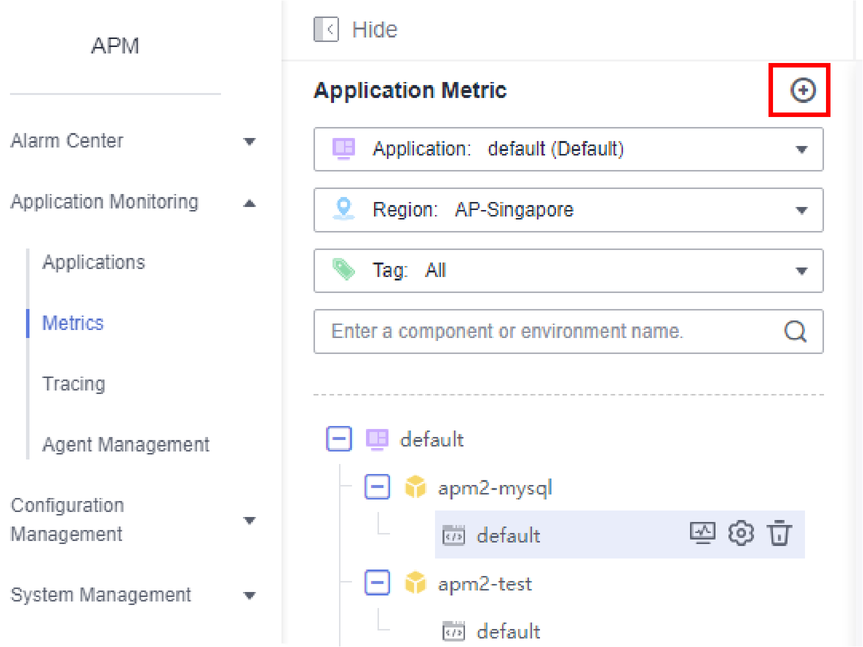
Step 1 Log in to the management console.

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



Application: default (Default)

Region: AP-Singapore

Tag: All

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	Display name of an application, which cannot be empty. Enter 1 to 128 characters. Only digits, letters, underscores (_), hyphens (-), brackets, and periods (.) are allowed.

Parameter	Description
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.

----End

3.2 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 on the left.

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

3.3 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 on the left.

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. This option is not available for sub-applications.
Delete	Click **Delete**.

Step 6 Click **Yes**.

----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.

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

- **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.
- **Cache**: Monitors cache systems such as Redis and collects instruction-level metric data.
- **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.
- **Message Queue**: Monitors message systems such as Kafka and RabbitMQ, including the sender and receiver. The processing function at the receive end can generate trace information.
- **Communication Protocol**: Monitors communication protocols such as WebSocket.

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

NOTE

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

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.

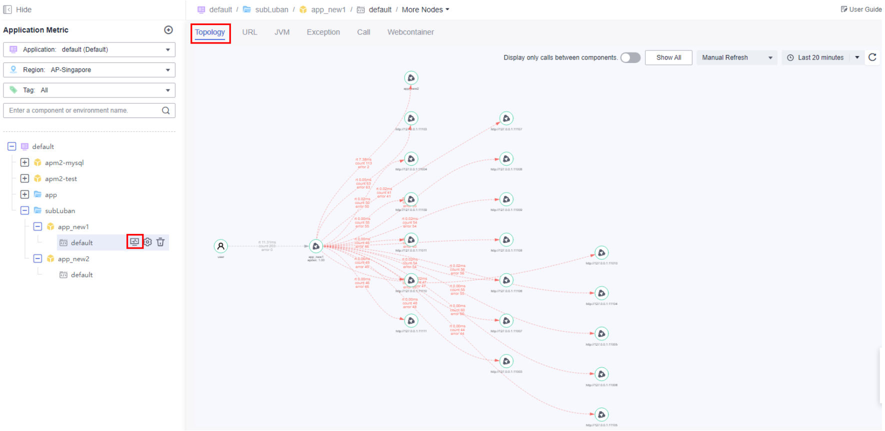


Figure 4-1 Viewing the topology

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

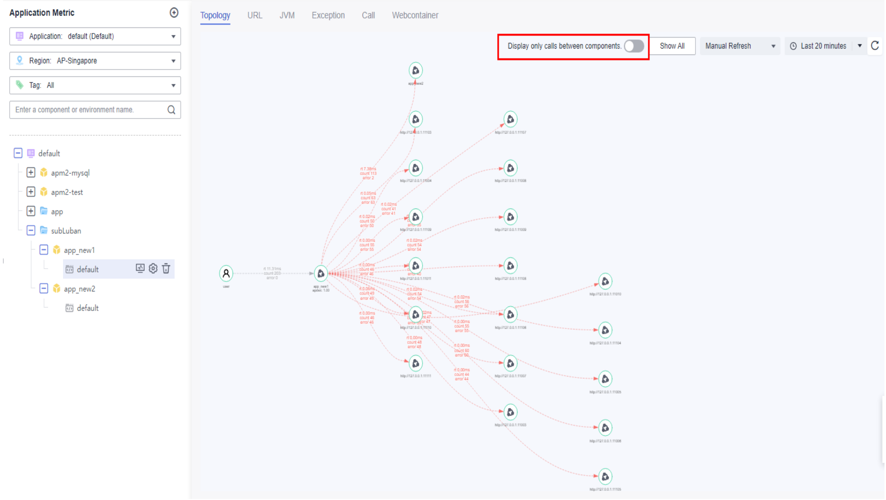
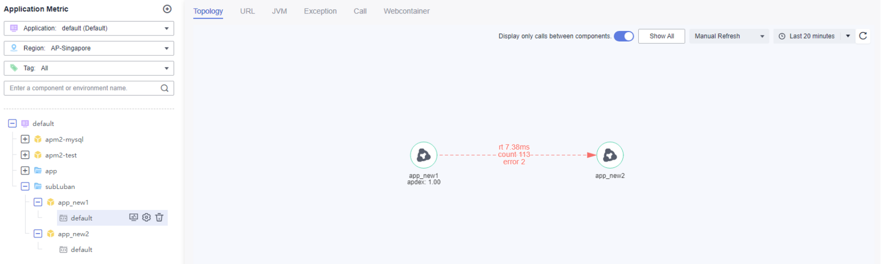


Figure 4-2 Displaying only calls between components

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

Figure 4-3 Calls between components



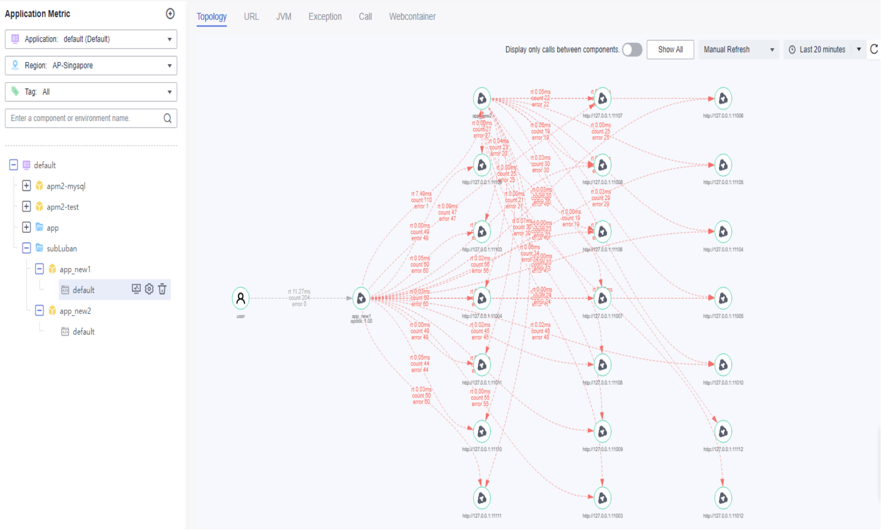
Application: default (Default)

Region: AP-Singapore

Tag: All

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

Figure 4-4 Showing all



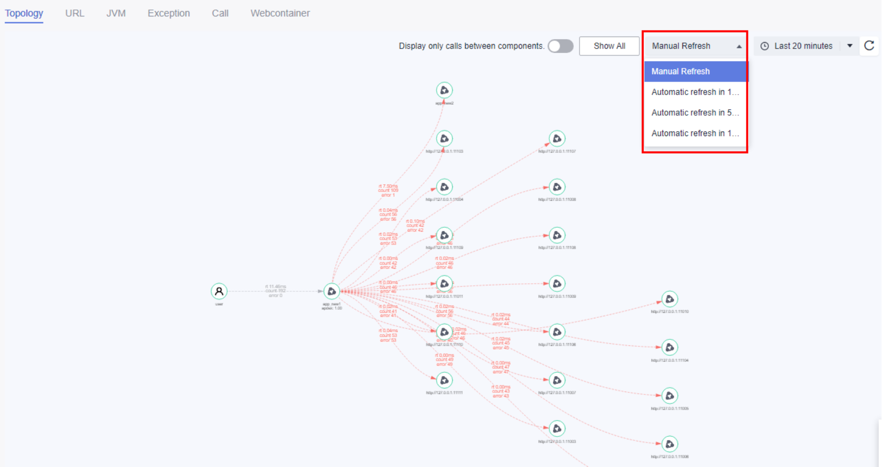
Application: default (Default)

Region: AP-Singapore

Tag: All

Step 8 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

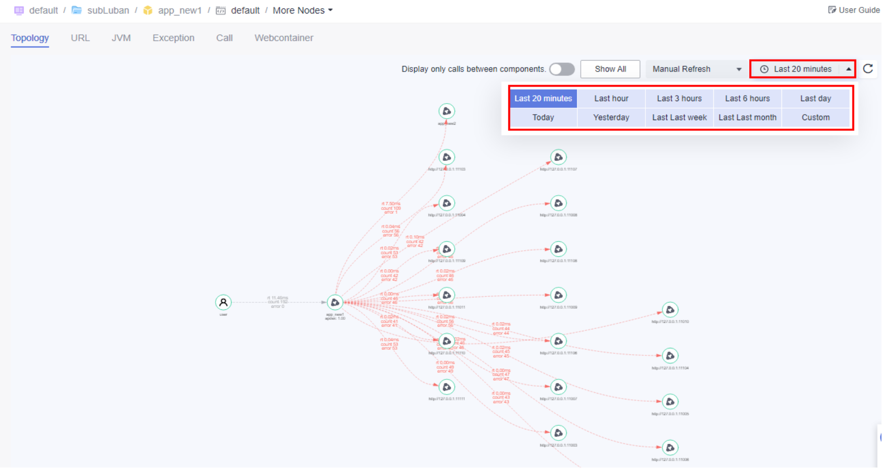


Topology
URL
JVM
Exception
Call
Webcontainer
Display only calls between components.
Show All
Manual Refresh
Manual Refresh
Automatic refresh in 1...
Automatic refresh in 5...
Automatic refresh in 1...
Last 20 minutes
user
app_new1

Step 9 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 7 days**, **Last 30 days**, 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 covers 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

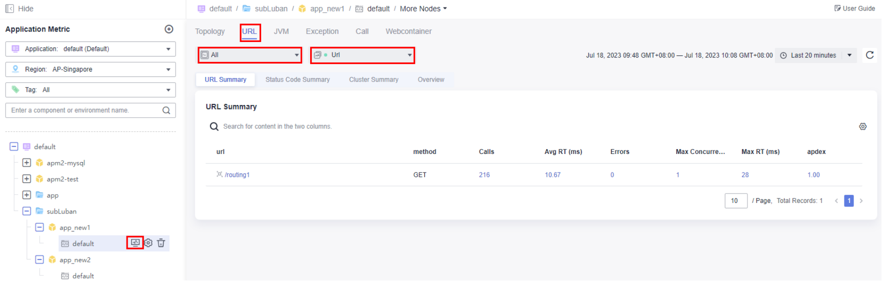
Step 1 Log in to the management console.

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, view URL monitoring information of all instances.

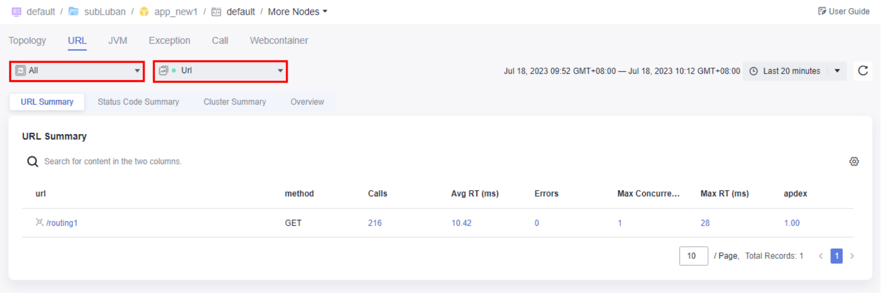
Figure 4-7 Going to the URL page



url	method	Calls	Avg RT (ms)	Errors	Max Concurre...	Max RT (ms)	apdex
/routing1	GET	216	10.67	0	1	28	1.00

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

Figure 4-8 Selecting a target instance and metric



default / subLuban / app_new1 / default / More Nodes ▾ User Guide

Topology URL JVM Exception Call Webcontainer

All ▾ | Url ▾ | Jul 18, 2023 09:52 GMT+08:00 — Jul 18, 2023 10:12 GMT+08:00 | Last 20 minutes ▾

URL Summary | Status Code Summary | Cluster Summary | Overview

URL Summary

Search for content in the two columns. ⚙

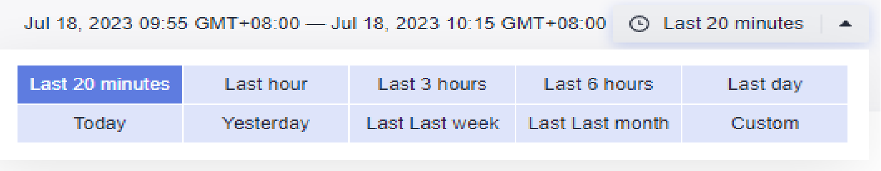
url	method	Calls	Avg RT (ms)	Errors	Max Concurre...	Max RT (ms)	apdex
/routing1	GET	216	10.42	0	1	28	1.00

10 / Page, Total Records: 1 ‹ 1 ›

Step 6 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 7 days**, **Last 30 days**, or **Custom**.

Figure 4-9 Selecting a time dimension



Jul 18, 2023 09:55 GMT+08:00 — Jul 18, 2023 10:15 GMT+08:00 | Last 20 minutes ▴

Last 20 minutes	Last hour	Last 3 hours	Last 6 hours	Last day
Today	Yesterday	Last Last week	Last Last month	Custom

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

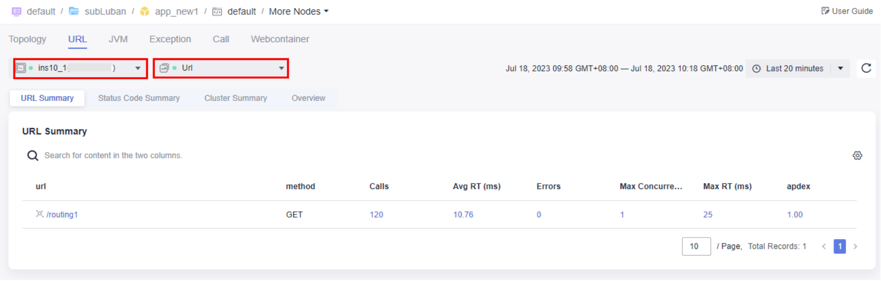
----End

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 4-10 URL summary under URL monitoring



default / subLuban / app_new1 / default / More Nodes ▾ User Guide

Topology URL JVM Exception Call Webcontainer

ins10_1[redacted]) ▾ | Url ▾ | Jul 18, 2023 09:58 GMT+08:00 — Jul 18, 2023 10:18 GMT+08:00 | Last 20 minutes ▾

URL Summary | Status Code Summary | Cluster Summary | Overview

URL Summary

Search for content in the two columns. ⚙

url	method	Calls	Avg RT (ms)	Errors	Max Concurre...	Max RT (ms)	apdex
/routing1	GET	120	10.76	0	1	25	1.00

10 / Page, Total Records: 1 ‹ 1 ›

Table 4-1 Parameters of the URL summary

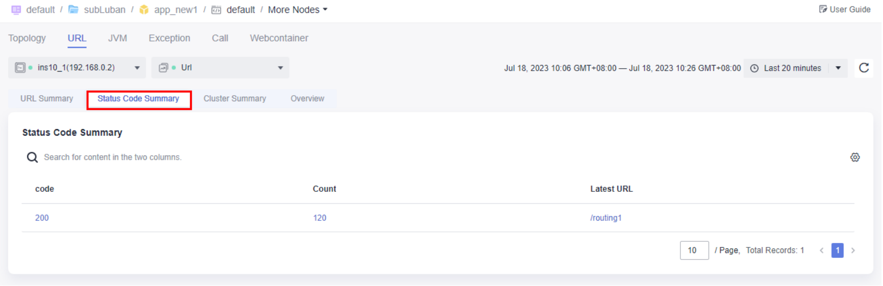
Metric Set	Metric	Description
URL summary	url	URL
	method	Request HTTP method
	Calls	Number of times that the URL is called
	Avg RT (ms)	Average response time of the URL in a collection period
	Errors	Number of call errors of the URL
	Max Concurrency	Maximum concurrency of the URL
	Max RT (ms)	Maximum 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.
	Exceptions	Number of exceptions of the URL
	0–10 ms	Number of requests with 0–10 ms response time
	10–100 ms	Number of requests with 10–100 ms response time
	100–500 ms	Number of requests with 100–500 ms response time
	500–1000 ms	Number of requests with 500–1000 ms response time
	1–10s	Number of requests with 1–10s response time
	> 10s	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 digits 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 4-11 Status code summary under URL monitoring



Status Code Summary

code	Count	Latest URL
200	120	/routing1

Table 4-2 Parameters of status code summary

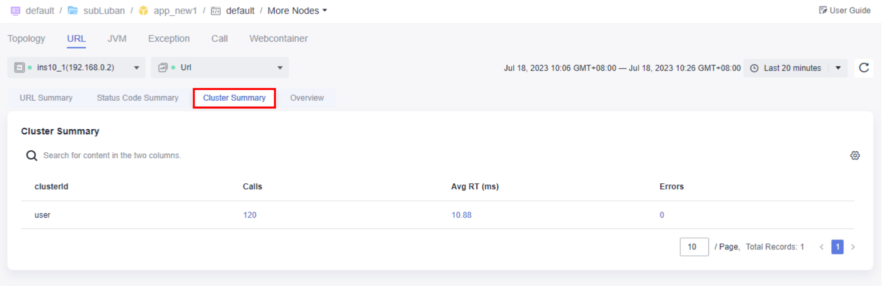
Metric Set	Metric	Description
Status code summary	code	Status code
	Count	Number of times that the status code has occurred
	Latest URL	Sample URL which returns the status code in a collection period

- 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 4-12 Cluster summary under URL monitoring



Cluster Summary

clusterId	Calls	Avg RT (ms)	Errors
user	120	10.88	0

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 digits 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**.

Figure 4-13 Overview under URL monitoring

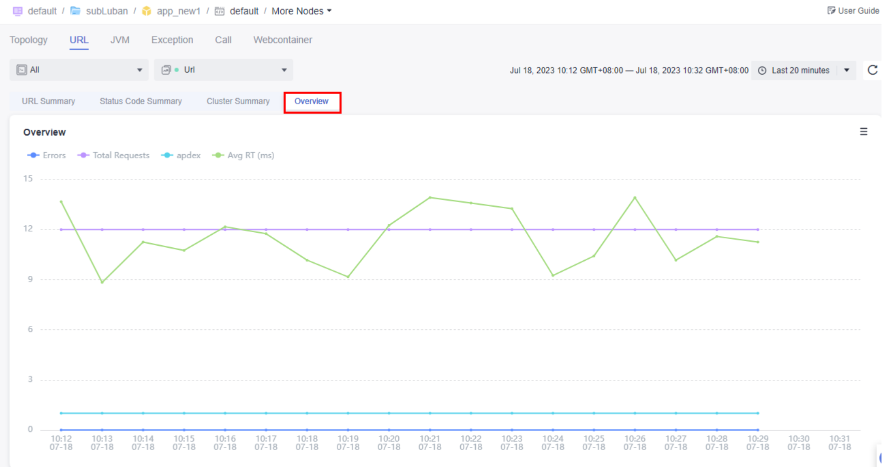


Table 4-4 Overview metrics

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

Metric Set	Metric	Description
	Apdex	Users' satisfaction towards 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.

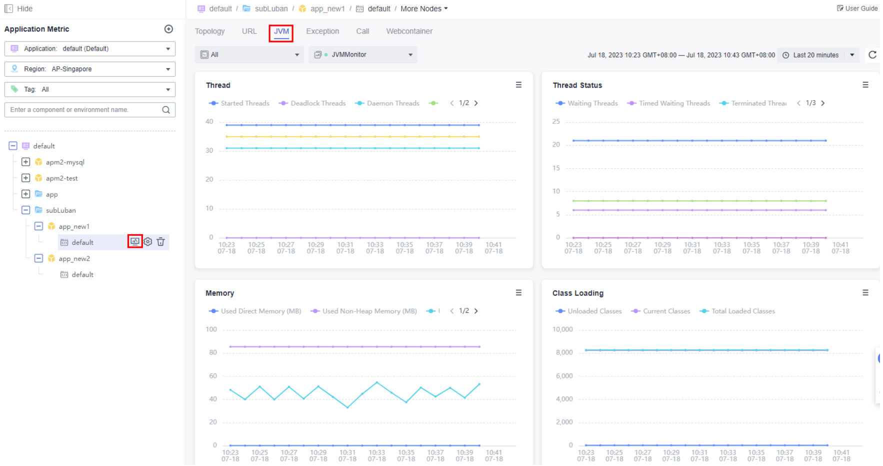
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

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.

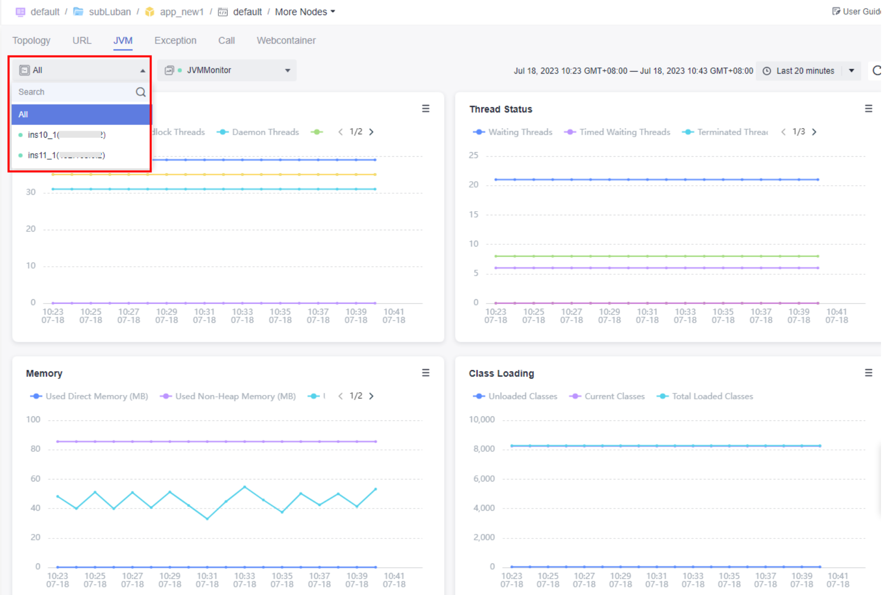
Figure 4-14 Going to the JVM page



Application: default (Default)
Region: AP-Singapore
Tag: All
All
JVMMonitor
Jul 18, 2023 10:23 GMT+08:00 — Jul 18, 2023 10:43 GMT+08:00
Last 20 minutes

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

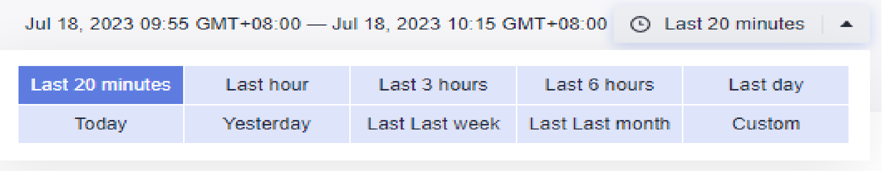
Figure 4-15 Selecting a target instance and metric



Step 7 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 7 days**, **Last 30 days**, or **Custom**.

Figure 4-16 Selecting a time dimension



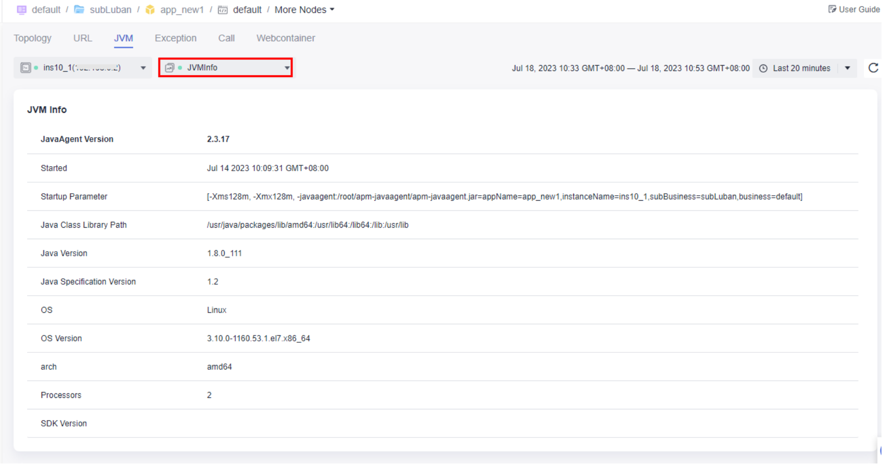
Step 8 Click ⚙ in the upper right corner of the list and select the metric data you want to view.

----End

Viewing JVM Information

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

Figure 4-17 Viewing JVM information


default / subLuban / app_new1 / default / More Nodes
User Guide
Topology
URL
JVM
Exception
Call
Webcontainer
ins10_1([redacted])
JVMInfo
Jul 18, 2023 10:33 GMT+08:00 — Jul 18, 2023 10:53 GMT+08:00
Last 20 minutes

JVM Info

JavaAgent Version	**2.3.17**
Started	Jul 14 2023 10:09:31 GMT+08:00
Startup Parameter	[-Xms128m, -Xmx128m, -javaagent:/root/apm-javaagent/apm-javaagent.jar=appName=app_new1,instanceName=ins10_1,subBusiness=subLuban,business=default]
Java Class Library Path	/usr/java/packages/lib/amd64:/usr/lib64:/lib64:/lib:/usr/lib
Java Version	1.8.0_111
Java Specification Version	1.2
OS	Linux
OS Version	3.10.0-1160.53.1.el7.x86_64
arch	amd64
Processors	2
SDK Version	

Table 4-5 JVMInfo metrics

Metric Set	Metric	Description
JVMInfo	JavaAgent Version	Java Agent version
	Started	JVM startup time
	Startup Parameter	JVM startup parameter
	Java Class Library Path	Java class library path
	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.

Figure 4-18 Viewing JVM monitoring data

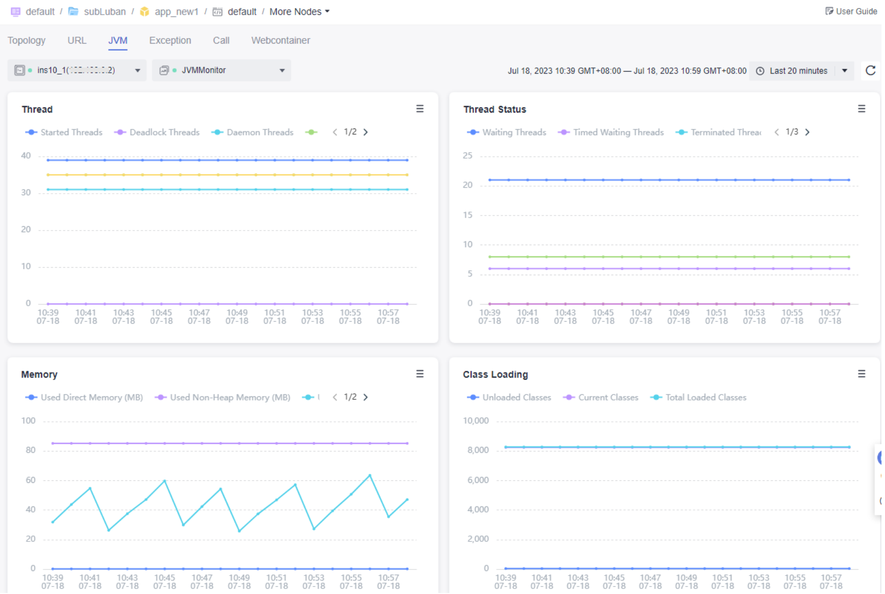


Table 4-6 JVM monitoring metrics

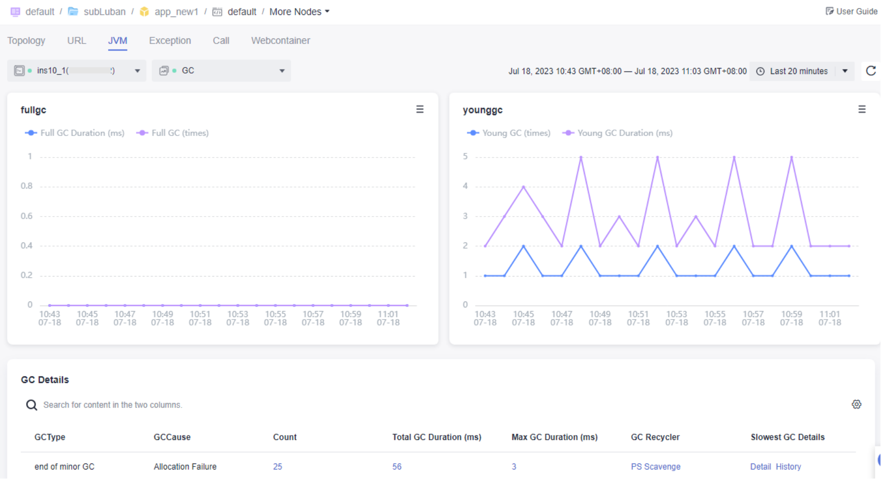
Metric Set	Metric	Description
Thread	Current Threads	Number of current threads
	Deadlock Threads	Number of deadlock threads
	Daemon Threads	Number of daemon threads
	Started Threads	Number of started threads
	Peak Threads	Peak number of threads
Thread Status	Waiting Threads	Number of waiting threads
	Initial Threads	Number of threads in the initial state
	Running Threads	Number of running threads
	Blocked Threads	Number of blocked threads
	Terminated Threads	Number of terminated threads
	Timed Waiting Threads	Number of threads that timed out
Memory	Used Non-Heap Memory	Size of the used non-heap memory

Metric Set	Metric	Description
	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	Available Memory	Size of available memory
	Initialized Memory	Size of the initialized memory
	Max. Memory	Size of the maximum memory
	Name	Memory pool name
	Used Memory	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 4-19 Viewing GC information



GCType	GCCause	Count	Total GC Duration (ms)	Max GC Duration (ms)	GC Recycler	Slowest GC Details
end of minor GC	Allocation Failure	25	56	3	PS Scavenge	Detail History

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

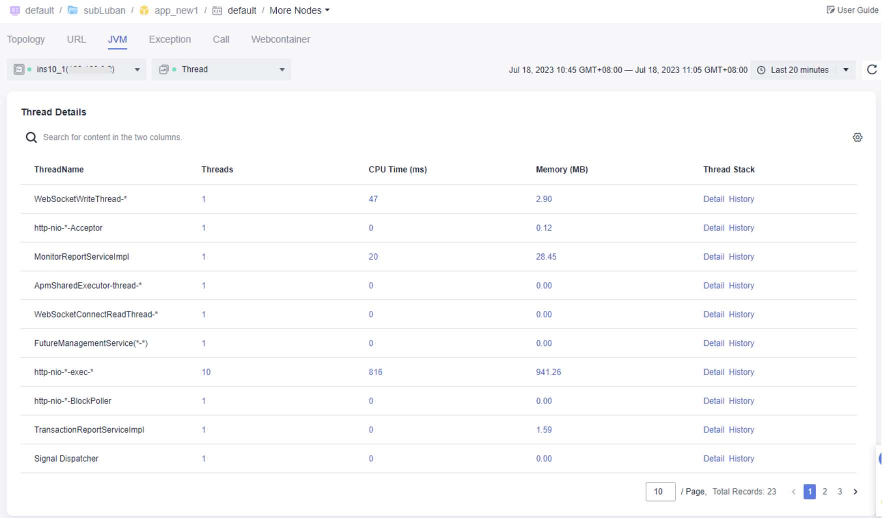
Metric Set	Metric	Description
	Young GC (times)	Number of young GC times in a collection period
	Young GC Duration (ms)	Young GC duration in a collection period
GC Details	GC Type	GC type, which can be **major** or **minor**
	GC Cause	GC cause
	Count	Number of times that GC has occurred
	Total GC Duration (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).
- 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).

Viewing Threads

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

Figure 4-20 Viewing threads


default / subLuban / app_new1 / default / More Nodes
User Guide
Topology
URL
JVM
Exception
Call
Webcontainer
ins10_1([redacted])
Thread
Last 20 minutes
Search for content in the two columns.

Jul 18, 2023 10:45 GMT+08:00 — Jul 18, 2023 11:05 GMT+08:00

Thread Details

ThreadName	Threads	CPU Time (ms)	Memory (MB)	Thread Stack
WebSocketWriteThread-*	1	47	2.90	Detail History
http-nio-*-Acceptor	1	0	0.12	Detail History
MonitorReportServiceImpl	1	20	28.45	Detail History
ApmSharedExecutor-thread-*	1	0	0.00	Detail History
WebSocketConnectReadThread-*	1	0	0.00	Detail History
FutureManagementService(*-*)	1	0	0.00	Detail History
http-nio-*-exec-*	10	816	941.26	Detail History
http-nio-*-BlockPoller	1	0	0.00	Detail History
TransactionReportServiceImpl	1	0	1.59	Detail History
Signal Dispatcher	1	0	0.00	Detail History

10 / Page, Total Records: 23 ‹ 1 2 3 ›

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 **Details** in the **Thread Stack** column to view the thread details.
- Click **History** in the **Thread Stack** column to view the historical thread stack list.

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
	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
	0–10 ms	Number of requests with 0–10 ms response time
	10–100 ms	Number of requests with 10–100 ms response time

Metric Set	Metric	Description
	100–500 ms	Number of requests with 100–500 ms response time
	500–1000 ms	Number of requests with 500–1000 ms response time
	1–10s	Number of requests with 1–10s response time
	> 10s	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.

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.

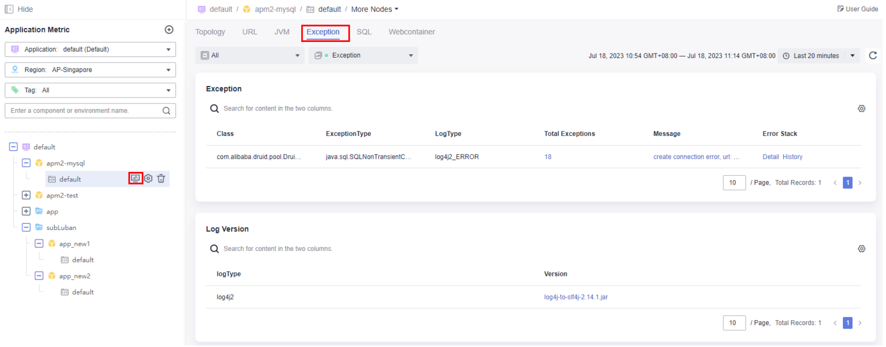
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

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 4-21 Exception monitoring data



Application: default (Default)

Region: AP-Singapore

Tag: All

Enter a component or environment name.

All

Exception

Jul 18, 2023 10:54 GMT+08:00 — Jul 18, 2023 11:14 GMT+08:00 Last 20 minutes

Exception

Class	ExceptionType	LogType	Total Exceptions	Message	Error Stack
com.alibaba.druid.pool.Drui...	java.sql.SQLNonTransientC...	log4j2_ERROR	18	create connection error, url: ...	Detail History

Log Version

logType	Version
log4j2	log4j-to-slf4j-2.14.1.jar

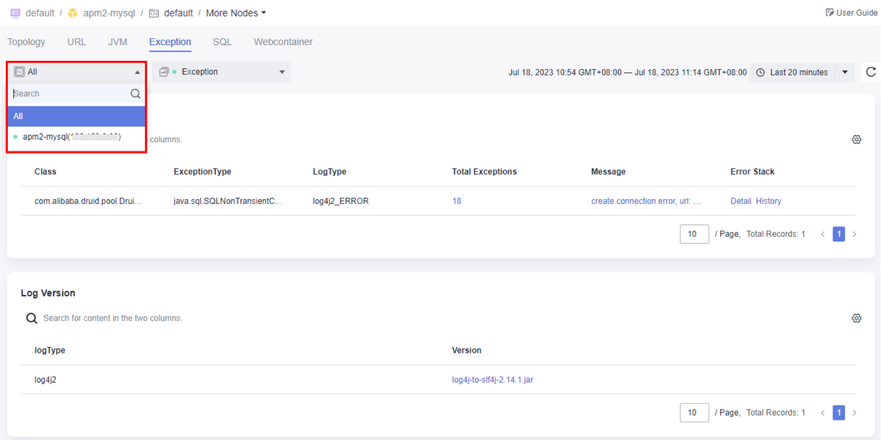
Table 4-10 Exception and log parameters

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 has occurred
	Error Stack	Error stack
Log Version	Log Type	Log type
	Version	Log version

- Click a number in blue in the **Total Exceptions** column to view the trend of the thread in a specified period.
- Click the blue text in the **Message** column to view the message time and content.
- Click **Details** in the **Error Stack** column to view exception details.
- Click **History** in the **Error Stack** column to view the historical error stack 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 4-22 Selecting a target instance and exception



Jul 18, 2023 10:54 GMT+08:00 — Jul 18, 2023 11:14 GMT+08:00

Class	ExceptionType	LogType	Total Exceptions	Message	Error Stack
com.alibaba.druid.pool.Drui...	java.sql.SQLNonTransientC...	log4j2_ERROR	18	create connection error, url: ...	Detail History

Total Records: 1

Log Version

Search for content in the two columns.

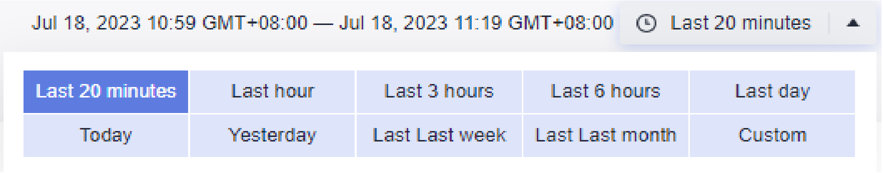
logType	Version
log4j2	log4j-to-slf4j-2.14.1.jar

Total Records: 1

Step 7 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 7 days**, **Last 30 days**, or **Custom**.

Figure 4-23 Selecting a time dimension



Jul 18, 2023 10:59 GMT+08:00 — Jul 18, 2023 11:19 GMT+08:00

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

----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.

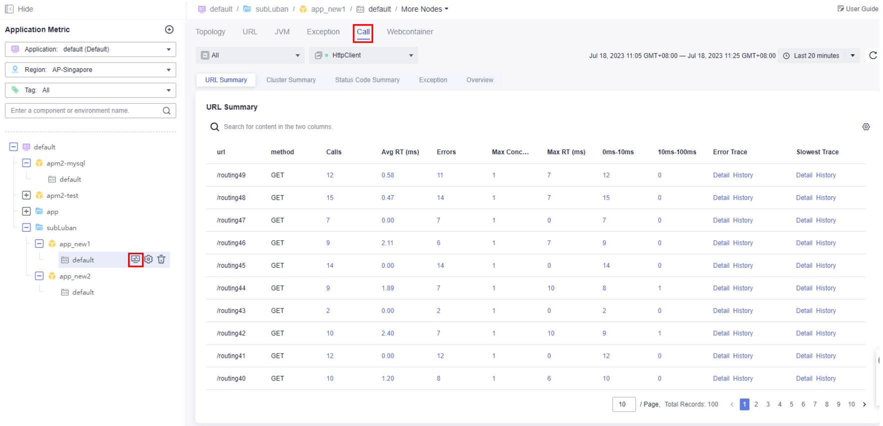
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

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 4-24 External call data



Jul 18, 2023 11:05 GMT+08:00 — Jul 18, 2023 11:25 GMT+08:00

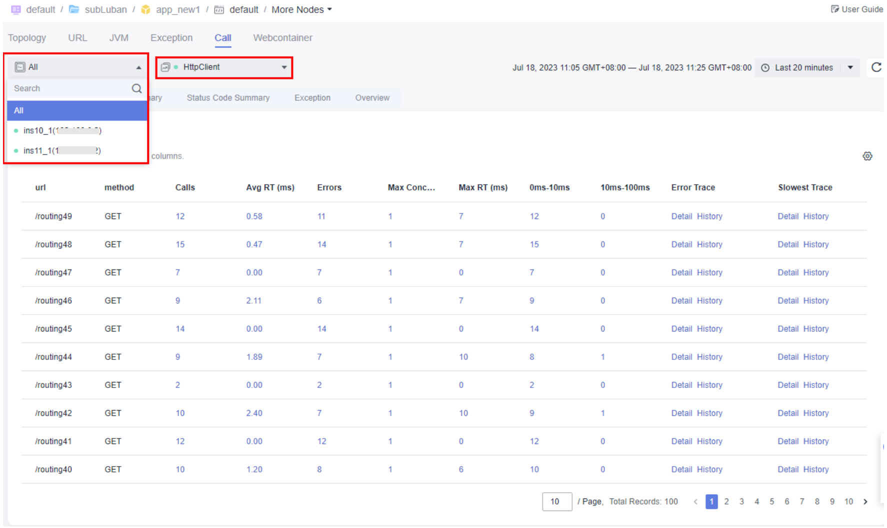
URL Summary

url	method	Calls	Avg RT (ms)	Errors	Max Conc...	Max RT (ms)	0ms-10ms	10ms-100ms	Error Trace	Slowest Trace
/routing49	GET	12	0.58	11	1	7	12	0	Detail History	Detail History
/routing48	GET	15	0.47	14	1	7	15	0	Detail History	Detail History
/routing47	GET	7	0.00	7	1	0	7	0	Detail History	Detail History
/routing46	GET	9	2.11	6	1	7	9	0	Detail History	Detail History
/routing45	GET	14	0.00	14	1	0	14	0	Detail History	Detail History
/routing44	GET	9	1.89	7	1	10	8	1	Detail History	Detail History
/routing43	GET	2	0.00	2	1	0	2	0	Detail History	Detail History
/routing42	GET	10	2.40	7	1	10	9	1	Detail History	Detail History
/routing41	GET	12	0.00	12	1	0	12	0	Detail History	Detail History
/routing40	GET	10	1.20	8	1	6	10	0	Detail History	Detail History

10 / Page, Total Records: 100 ‹ 1 2 3 4 5 6 7 8 9 10 ›

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

Figure 4-25 Selecting a target instance and metric



default / subLuban / app_new1 / default / More Nodes

User Guide

Topology | URL | JVM | Exception | Call | Webcontainer

All | HttpClient | Jul 18, 2023 11:05 GMT+08:00 — Jul 18, 2023 11:25 GMT+08:00 | Last 20 minutes

Search

All

- ins10_1([redacted])
- ins11_1([redacted])

...ary | Status Code Summary | Exception | Overview

columns.

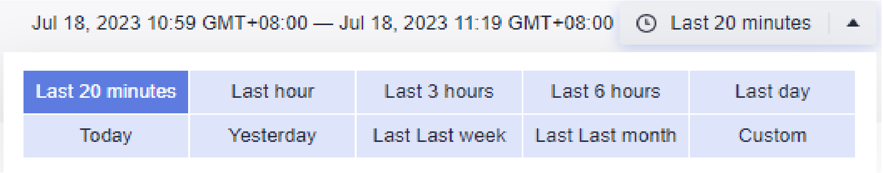
url	method	Calls	Avg RT (ms)	Errors	Max Conc...	Max RT (ms)	0ms-10ms	10ms-100ms	Error Trace	Slowest Trace
/routing49	GET	12	0.58	11	1	7	12	0	Detail History	Detail History
/routing48	GET	15	0.47	14	1	7	15	0	Detail History	Detail History
/routing47	GET	7	0.00	7	1	0	7	0	Detail History	Detail History
/routing46	GET	9	2.11	6	1	7	9	0	Detail History	Detail History
/routing45	GET	14	0.00	14	1	0	14	0	Detail History	Detail History
/routing44	GET	9	1.89	7	1	10	8	1	Detail History	Detail History
/routing43	GET	2	0.00	2	1	0	2	0	Detail History	Detail History
/routing42	GET	10	2.40	7	1	10	9	1	Detail History	Detail History
/routing41	GET	12	0.00	12	1	0	12	0	Detail History	Detail History
/routing40	GET	10	1.20	8	1	6	10	0	Detail History	Detail History

10 / Page, Total Records: 100 ‹ 1 2 3 4 5 6 7 8 9 10 ›

Step 7 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 7 days**, **Last 30 days**, or **Custom**.

Figure 4-26 Selecting a time dimension



Jul 18, 2023 10:59 GMT+08:00 — Jul 18, 2023 11:19 GMT+08:00 | Last 20 minutes

Last 20 minutes	Last hour	Last 3 hours	Last 6 hours	Last day
Today	Yesterday	Last Last week	Last Last month	Custom

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

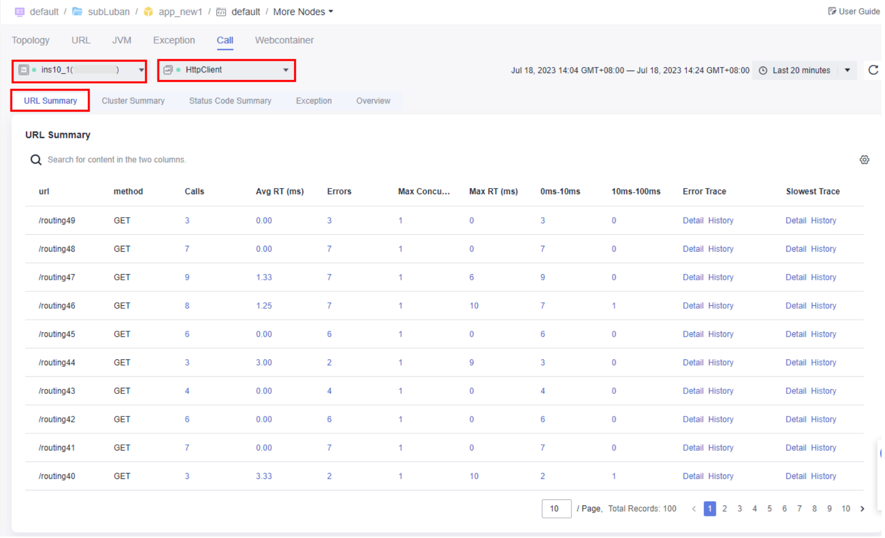
----End

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 4-27 URL summary under HttpClient monitoring



url	method	Calls	Avg RT (ms)	Errors	Max Concu...	Max RT (ms)	0ms-10ms	10ms-100ms	Error Trace	Slowest Trace
/routing49	GET	3	0.00	3	1	0	3	0	Detail History	Detail History
/routing48	GET	7	0.00	7	1	0	7	0	Detail History	Detail History
/routing47	GET	9	1.33	7	1	6	9	0	Detail History	Detail History
/routing46	GET	8	1.25	7	1	10	7	1	Detail History	Detail History
/routing45	GET	6	0.00	6	1	0	6	0	Detail History	Detail History
/routing44	GET	3	3.00	2	1	9	3	0	Detail History	Detail History
/routing43	GET	4	0.00	4	1	0	4	0	Detail History	Detail History
/routing42	GET	6	0.00	6	1	0	6	0	Detail History	Detail History
/routing41	GET	7	0.00	7	1	0	7	0	Detail History	Detail History
/routing40	GET	3	3.33	2	1	10	2	1	Detail History	Detail History

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
	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
	0–10 ms	Number of requests with 0–10 ms response time
	10–100 ms	Number of requests with 10–100 ms response time
	100–500 ms	Number of requests with 100–500 ms response time
	500–1000 ms	Number of requests with 500–1000 ms response time
	1–10s	Number of requests with 1–10s response time
	> 10s	Number of requests with response time longer than 10s

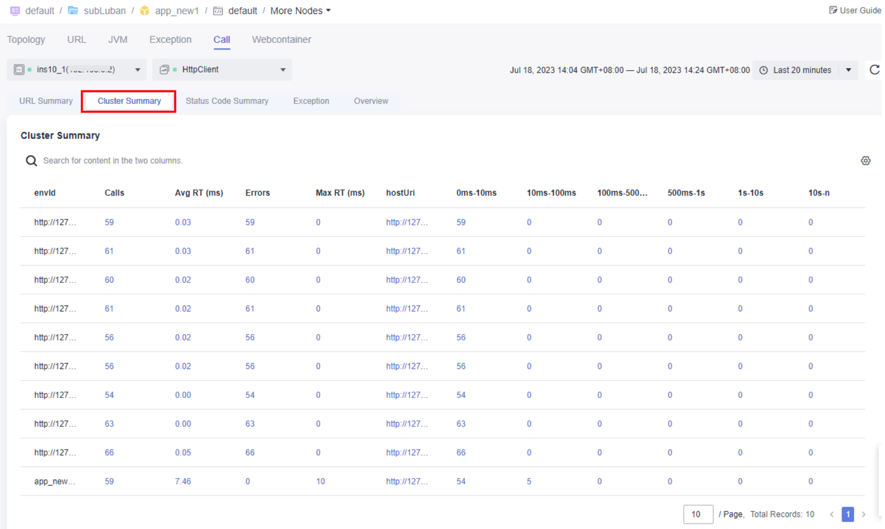
Metric Set	Metric	Description
	Error Trace	ID of the trace that encounters an error in a collection period
	Slowest Trace	ID of the slowest trace in a collection period

- Click digits 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 **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 4-28 Cluster summary under HttpClient monitoring



Cluster Summary

Search for content in the two columns.

envId	Calls	Avg RT (ms)	Errors	Max RT (ms)	hostUri	0ms-10ms	10ms-100ms	100ms-500...	500ms-1s	1s-10s	10s-n
http://127...	59	0.03	59	0	http://127...	59	0	0	0	0	0
http://127...	61	0.03	61	0	http://127...	61	0	0	0	0	0
http://127...	60	0.02	60	0	http://127...	60	0	0	0	0	0
http://127...	61	0.02	61	0	http://127...	61	0	0	0	0	0
http://127...	56	0.02	56	0	http://127...	56	0	0	0	0	0
http://127...	56	0.02	56	0	http://127...	56	0	0	0	0	0
http://127...	54	0.00	54	0	http://127...	54	0	0	0	0	0
http://127...	63	0.00	63	0	http://127...	63	0	0	0	0	0
http://127...	66	0.05	66	0	http://127...	66	0	0	0	0	0
app_new...	59	7.46	0	10	http://127...	54	5	0	0	0	0

10 / Page, Total Records: 10 ‹ 1 ›

Table 4-12 Parameters of cluster summary under HttpClient monitoring

Metric Set	Metric	Description
Cluster summary	envId	Cluster ID 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

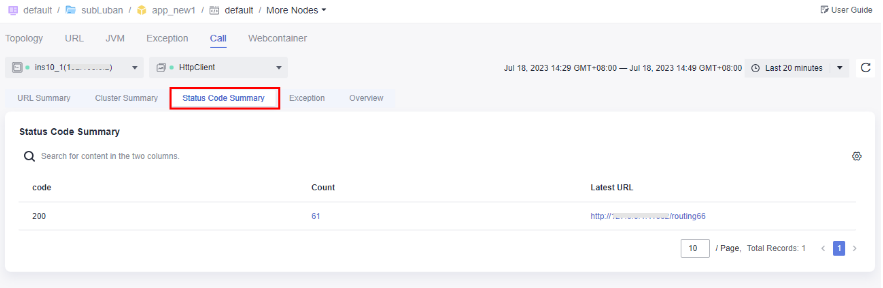
Metric Set	Metric	Description
	0–10 ms	Number of requests with 0–10 ms response time
	10–100 ms	Number of requests with 10–100 ms response time
	100–500 ms	Number of requests with 100–500 ms response time
	500–1000 ms	Number of requests with 500–1000 ms response time
	1–10s	Number of requests with 1–10s response time
	> 10s	Number of requests with response time longer than 10s

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

Status code summary

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

Figure 4-29 Status code summary under HttpClient monitoring



Jul 18, 2023 14:29 GMT+08:00 — Jul 18, 2023 14:49 GMT+08:00

Status Code Summary

code	Count	Latest URL
200	61	http://[redacted]/routing66

Total Records: 1

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

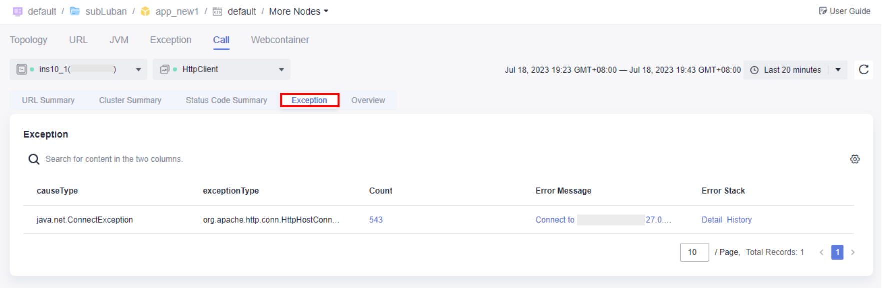
Metric Set	Metric	Description
Status code summary	code	Status code
	Count	Number of times that the status code has occurred
	Latest URL	URL that returns the status code

- 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 4-30 HttpClient monitoring exceptions



Exception

causeType	exceptionType	Count	Error Message	Error Stack
java.net.ConnectException	org.apache.http.conn.HttpHostConn...	543	Connect to [redacted] 27.0....	Detail History

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 has occurred
	Error Message	Message returned when the exception has 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 **Details** 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**.

Figure 4-31 Overview under HttpClient monitoring

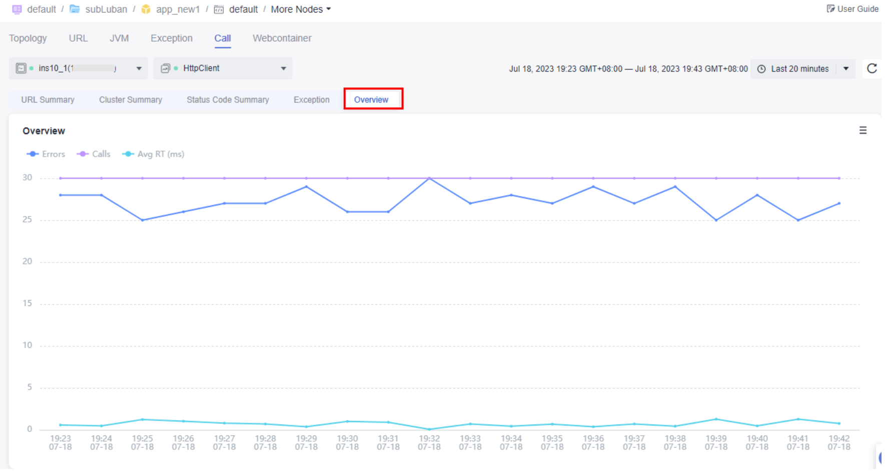


Table 4-15 Overview parameters of HttpClient monitoring

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.

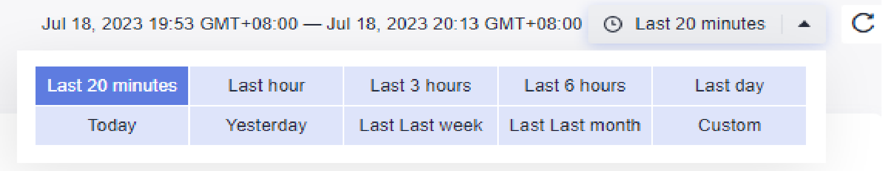
Step 5 Click the **SQL** tab. By default, the MySQL database information of all instances is displayed.

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

Step 7 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 7 days**, **Last 30 days**, or **Custom**.

Figure 4-32 Selecting a time dimension



Jul 18, 2023 19:53 GMT+08:00 — Jul 18, 2023 20:13 GMT+08:00 Last 20 minutes

Last 20 minutes	Last hour	Last 3 hours	Last 6 hours	Last day
Today	Yesterday	Last Last week	Last Last month	Custom

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

Metric Set	Metric	Description
	Max RT (ms)	Maximum response time of the SQL statement
	0–10 ms	Number of requests with 0–10 ms response time
	10–100 ms	Number of requests with 10–100 ms response time
	100–200 ms	Number of requests with 100–200 ms response time
	200–1000 ms	Number of requests with 200–1000 ms response time
	1–10s	Number of requests with 1–10s response time
	> 10s	Number of requests with response time longer than 10s
	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 digits in blue (such as **Calls** or **Avg RT (ms)**) 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

Metric Set	Metric	Description
	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
	0–10 ms	Number of requests with 0–10 ms response time
	10–100 ms	Number of requests with 10–100 ms response time
	100–200 ms	Number of requests with 100–200 ms response time
	200–1000 ms	Number of requests with 200–1000 ms response time
	1–10s	Number of requests with 1–10s response time
	> 10s	Number of requests with response time longer than 10s

Click digits in blue (such as **Calls** or **Avg RT (ms)**) 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**.

Table 4-19 Overview parameters

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

Metric Set	Metric	Description
	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
	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
	Avg RT (ms)	Average response time (ms)
	Errors	Number of errors
	Max Concurrency	Maximum number of concurrent connections
	Max RT (ms)	Maximum response time
	0–10 ms	Number of requests with 0–10 ms response time
	10–100 ms	Number of requests with 10–100 ms response time
	100–500 ms	Number of requests with 100–500 ms response time
	500–1000 ms	Number of requests with 500–1000 ms response time
	1–10s	Number of requests with 1–10s response time
	> 10s	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

Metric Set	Metric	Description
	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
	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
	exceptionType	Exception type
	Count	Number of times the exception has occurred
	Error Message	Message returned when the exception has occurred
	Error Stack	Exception stack information
Version	Driver Version	Driver version

- Click digits 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.

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.

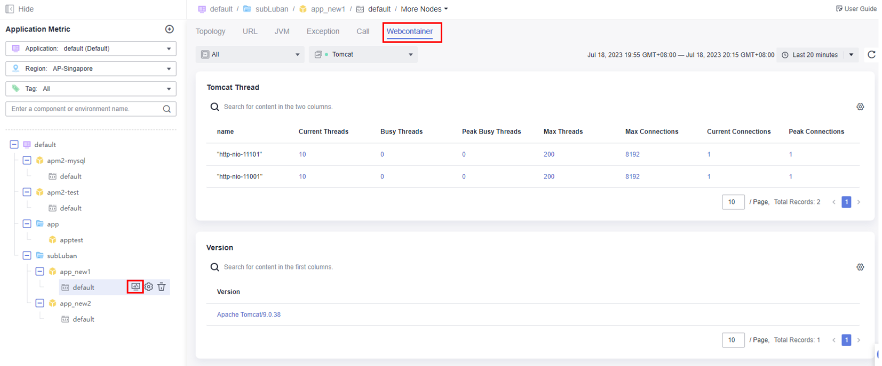
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

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 4-21**.

Figure 4-33 Going to the web container page


Hide
Application Metric
Application: default (Default)
Region: AP-Singapore
Tag: All
Enter a component or environment name.
default
apm2-mysql
default
apm2-test
default
app
apptest
subLuban
app_new1
default
app_new2
default
default / subLuban / app_new1 / default / More Nodes
User Guide
Topology
URL
JVM
Exception
Call
Webcontainer
All
Tomcat
Jul 18, 2023 19:55 GMT+08:00 — Jul 18, 2023 20:15 GMT+08:00
Last 20 minutes
Search for content in the two columns.
Search for content in the first columns.

Tomcat Thread

name	Current Threads	Busy Threads	Peak Busy Threads	Max Threads	Max Connections	Current Connections	Peak Connections
"http-nio-11101"	10	0	0	200	8192	1	1
"http-nio-11001"	10	0	0	200	8192	1	1

10 / Page, Total Records: 2 ‹ 1 ›

Version

Version
Apache Tomcat/9.0.38

10 / Page, Total Records: 1 ‹ 1 ›

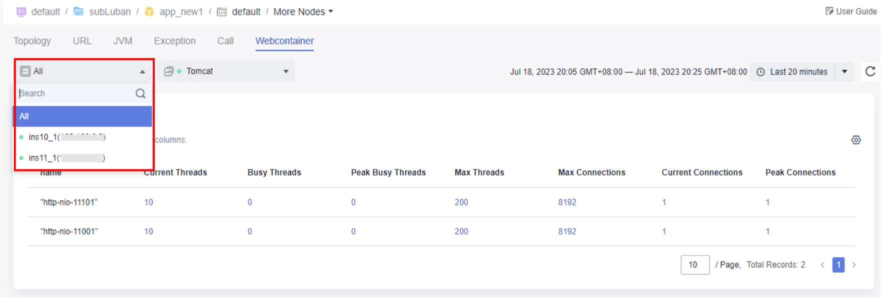
Table 4-21 Tomcat monitoring parameters

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

- Click digits in blue (such as **Current Threads**, **Busy Threads**, and **Peak Busy Threads**) 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 metric to view the monitoring data in different metric sets.

Figure 4-34 Selecting a target instance and metric



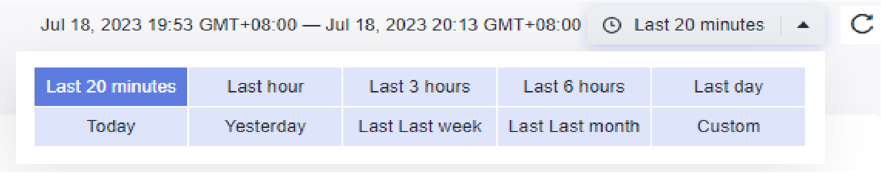
name	Current Threads	Busy Threads	Peak Busy Threads	Max Threads	Max Connections	Current Connections	Peak Connections
"http-nio-11101"	10	0	0	200	8192	1	1
"http-nio-11001"	10	0	0	200	8192	1	1

10 / Page, Total Records: 2 1

Step 7 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 7 days**, **Last 30 days**, or **Custom**.

Figure 4-35 Selecting a time dimension



Jul 18, 2023 19:53 GMT+08:00 — Jul 18, 2023 20:13 GMT+08:00 Last 20 minutes

Last 20 minutes	Last hour	Last 3 hours	Last 6 hours	Last day
Today	Yesterday	Last Last week	Last Last month	Custom

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

----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**.

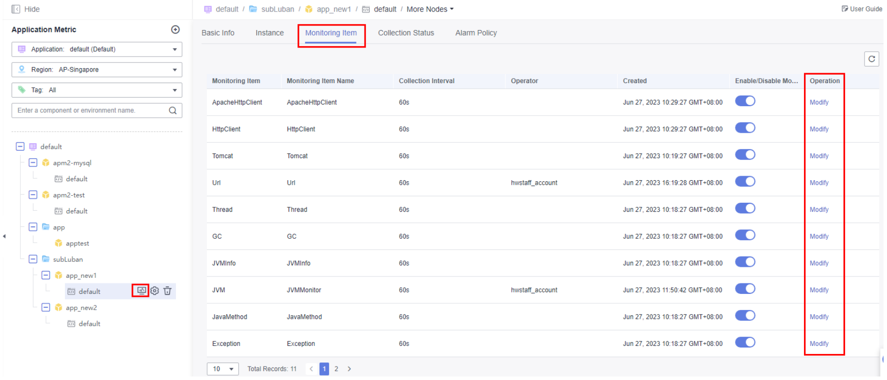
Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

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 4-36 Configuring a monitoring item

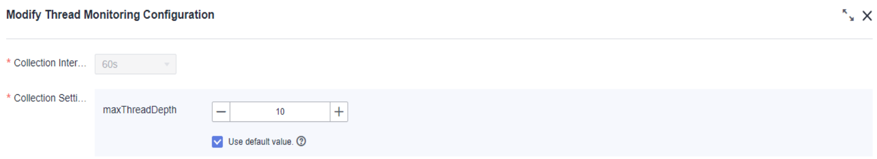


Monitoring Item	Monitoring Item Name	Collection Interval	Operator	Created	Enable/Disable Mo...	Operation
ApacheHttpClient	ApacheHttpClient	60s		Jun 27, 2023 10:29:27 GMT+08:00		Modify
HttpClient	HttpClient	60s		Jun 27, 2023 10:29:27 GMT+08:00		Modify
Tomcat	Tomcat	60s		Jun 27, 2023 10:19:27 GMT+08:00		Modify
Url	Url	60s	hwstaff_account	Jun 27, 2023 16:19:28 GMT+08:00		Modify
Thread	Thread	60s		Jun 27, 2023 10:18:27 GMT+08:00		Modify
GC	GC	60s		Jun 27, 2023 10:18:27 GMT+08:00		Modify
JVMInfo	JVMInfo	60s		Jun 27, 2023 10:18:27 GMT+08:00		Modify
JVM	JVMMonitor	60s	hwstaff_account	Jun 27, 2023 11:50:42 GMT+08:00		Modify
JavaMethod	JavaMethod	60s		Jun 27, 2023 10:18:27 GMT+08:00		Modify
Exception	Exception	60s		Jun 27, 2023 10:18:27 GMT+08:00		Modify

10 Total Records: 11 < 1 2 >

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

Figure 4-37 Editing the thread monitoring configuration



Modify Thread Monitoring Configuration

* Collection Inter... 60s

* Collection Setti... maxThreadDepth 10

☑ Use default value

Step 8 Click **Yes**.

----End

Enabling or Disabling a Monitoring Item

Step 1 Log in to the management console.

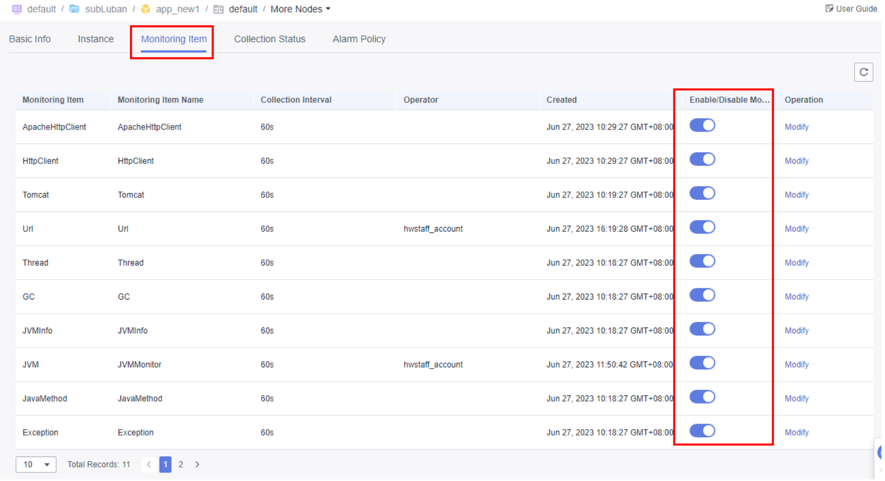
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

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 4-38 Enabling or disabling a monitoring item



Monitoring Item	Monitoring Item Name	Collection Interval	Operator	Created	Enable/Disable Mo...	Operation
ApacheHttpClient	ApacheHttpClient	60s		Jun 27, 2023 10:29:27 GMT+08:00	●	Modify
HttpClient	HttpClient	60s		Jun 27, 2023 10:29:27 GMT+08:00	●	Modify
Tomcat	Tomcat	60s		Jun 27, 2023 10:19:27 GMT+08:00	●	Modify
Url	Url	60s	hwstaff_account	Jun 27, 2023 16:19:28 GMT+08:00	●	Modify
Thread	Thread	60s		Jun 27, 2023 10:18:27 GMT+08:00	●	Modify
GC	GC	60s		Jun 27, 2023 10:18:27 GMT+08:00	●	Modify
JVMInfo	JVMInfo	60s		Jun 27, 2023 10:18:27 GMT+08:00	●	Modify
JVM	JVMMonitor	60s	hwstaff_account	Jun 27, 2023 11:50:42 GMT+08:00	●	Modify
JavaMethod	JavaMethod	60s		Jun 27, 2023 10:18:27 GMT+08:00	●	Modify
Exception	Exception	60s		Jun 27, 2023 10:18:27 GMT+08:00	●	Modify

10 Total Records: 11 < 1 2 >

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

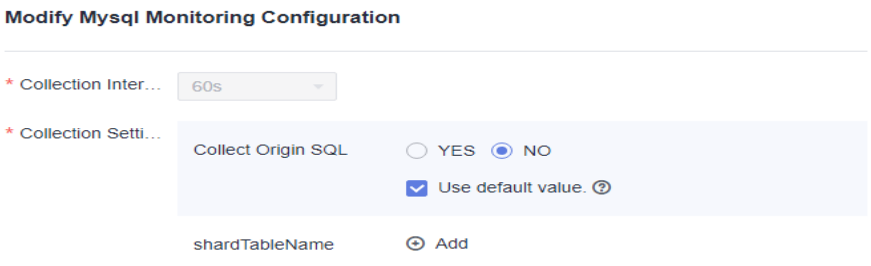
----End

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.

Figure 4-39 Configuring the MySQL monitoring item



Modify Mysql Monitoring Configuration

* Collection Inter... 60s

* Collection Setti...

Collect Origin SQL ○ YES ● NO

☑ Use default value.

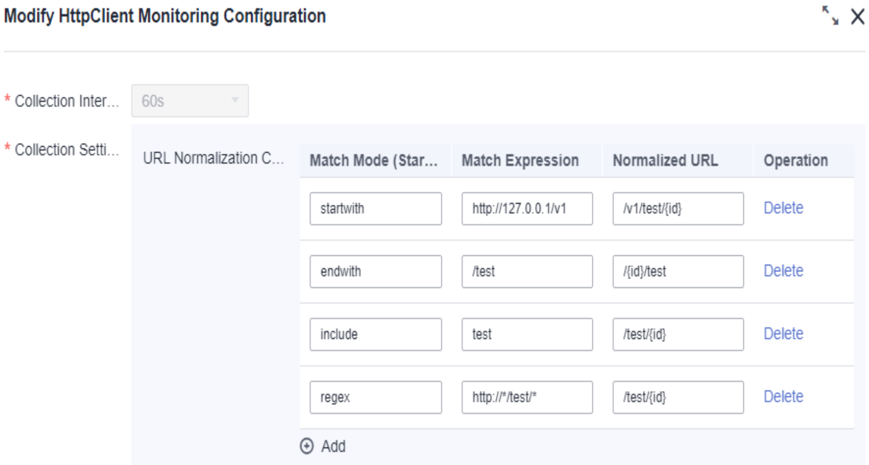
shardTableName Add

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}*.

Figure 4-40 Configuring the HttpClient monitoring item



Modify HttpClient Monitoring Configuration

* Collection Inter... 60s

* Collection Setti... URL Normalization C...

Match Mode (Star...	Match Expression	Normalized URL	Operation
startwith	http://127.0.0.1/v1	/v1/test/{id}	Delete
endwith	/test	/{id}/test	Delete
include	test	/test/{id}	Delete
regex	http://*/test/*	/test/{id}	Delete

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 4-40**.
- **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 4-40**.
- **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 4-40**.
- **regex**: URLs that meet the wildcard expression are counted as normalized URLs. For details about the wildcard rules, see **Table 4-22**.

Table 4-22 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

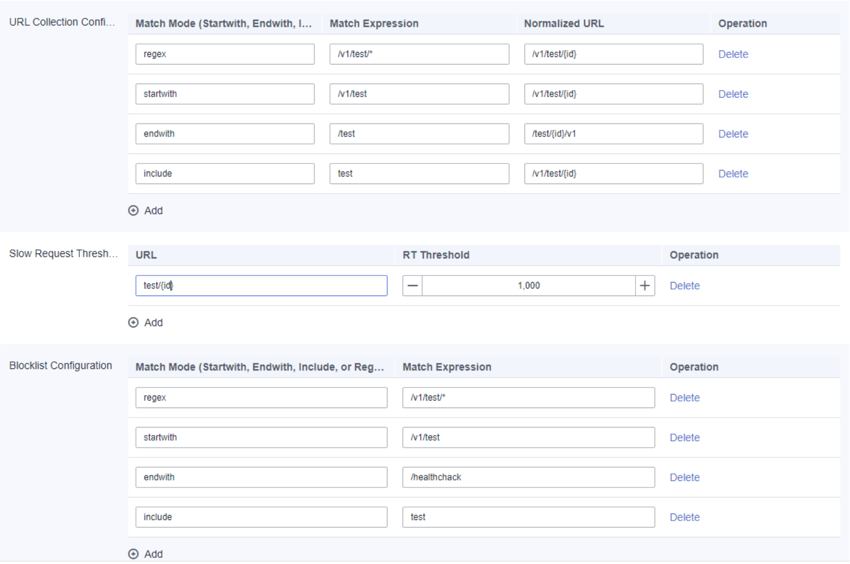
For security purposes, do not contain sensitive data in headers, URL parameters, cookies, or other parameters.

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

Parameter	Description	Example
Key for Cookie Value Interception	Key specified for collecting values in cookies. The collected information can be seen in the trace parameters.	testKey
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**.	**Figure 4-41**
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 4-41**
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 4-41**
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 the default value: The inherited tag value is preferentially used.	-

Figure 4-41 Example



URL Collection Confi...

Match Mode (Startwith, Endwith, I...	Match Expression	Normalized URL	Operation
regex	/v1/test/*	/v1/test/{id}	Delete
startwith	/v1/test	/v1/test/{id}	Delete
endwith	/test	/test/{id}/v1	Delete
include	test	/v1/test/{id}	Delete

⊕ Add

Slow Request Thresh...

URL	RT Threshold	Operation
test/{id}	− 1,000 +	Delete

⊕ Add

Blocklist Configuration

Match Mode (Startwith, Endwith, Include, or Reg...	Match Expression	Operation
regex	/v1/test/*	Delete
startwith	/v1/test	Delete
endwith	/healthchack	Delete
include	test	Delete

⊕ Add

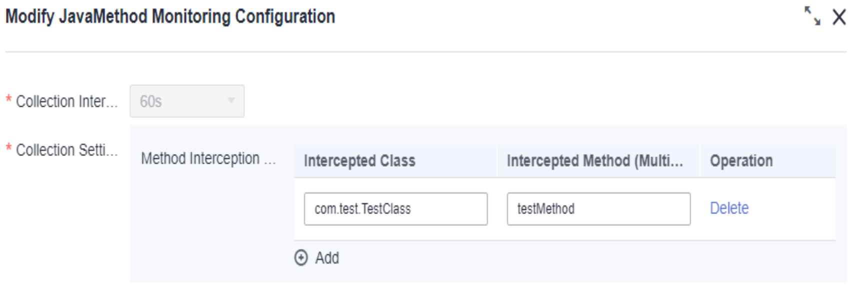
4.3.5 Configuring the JavaMethod Monitoring Item

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 4-42 Configuring the JavaMethod monitoring item



Modify JavaMethod Monitoring Configuration

* Collection Inter... 60s

* Collection Setti... Method Interception ...

Intercepted Class	Intercepted Method (Multi...	Operation
com.test.TestClass	testMethod	Delete

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 **No**. If **Use default value** is selected, the value of the inherited tag is preferentially used.
- **Determine Print TraceId In Log**: 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 **1** 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**.

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 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
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

Search Criterion	Description	Mandatory
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	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
Application Code	If you have configured **Service Code Length**, **Key for Service Code Interception**, and **Normal Service Code** for URL monitoring, responses' 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

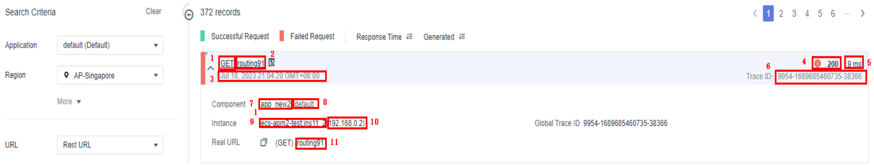
----End

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



Search Criteria Clear

Application: default (Default)

Region: AP-Singapore

URL: Rest URL

372 records

Successful Request | Failed Request | Response Time | Generated

GET routing91

Jul 18, 2023 21:04:20 GMT+08:00

200 9 ms

Trace ID: 9954-1689685460735-38366

Component: app_new2 default

Instance: ecs-apm2-test:ins11_1 (192.168.0.2)

Global Trace ID: 9954-1689685460735-38366

Real URL: (GET) routing91

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.

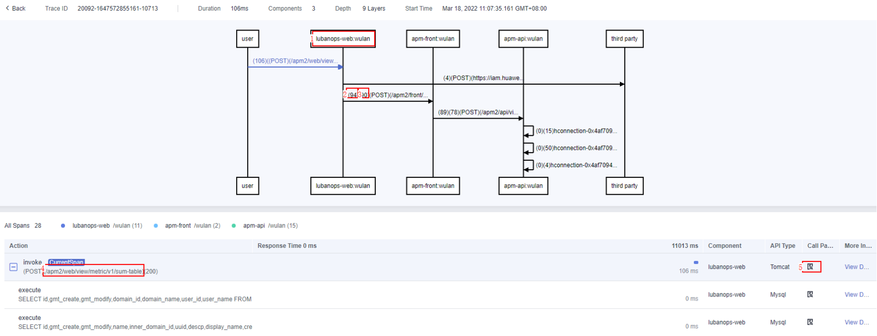
You can also click a specific URL on the monitoring item view page, for example, the table view of the URL monitoring item. In this way, you can quickly search for required trace information based on preset search criteria.

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


< Back
user
1
lubanops-web:wulan
apm-front:wulan
apm-api:wulan
third party
(106)((POST)(/apm2/web/view...
(4)(POST)(https://iam.huawe...
2
(94
3
0)(POST)(/apm2/front/...
(89)(78)(POST)(/apm2/api/vi...
(0)(15)hconnection-0x4af709...
(0)(50)hconnection-0x4af709...
(0)(4)hconnection-0x4af7094...
user
lubanops-web:wulan
apm-front:wulan
apm-api:wulan
third party
4
5

Trace ID 20092-1647572855161-10713 | Duration 106ms Components 3 Depth 9 Layers Start Time Mar 18, 2022 11:07:35.161 GMT+08:00

All Spans 28 ● lubanops-web /wulan (11) ● apm-front /wulan (2) ● apm-api /wulan (15)

Action	Response Time 0 ms	11013 ms	Component	API Type	Call Pa...	More In...
invoke CurrentSpan (POST)(/apm2/web/view/metric/v1/sum-table)(200)		106 ms	lubanops-web	Tomcat		View D...
execute SELECT id,gmt_create,gmt_modify,domain_id,domain_name,user_id,user_name FROM		0 ms	lubanops-web	Mysql		View D...
execute SELECT id,gmt_create,gmt_modify,name,inner_domain_id,uuid,descp,display_name,cre		0 ms	lubanops-web	Mysql		View D...

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. Extended data of the trace method. Generally, parameters related to the method are displayed.

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**.

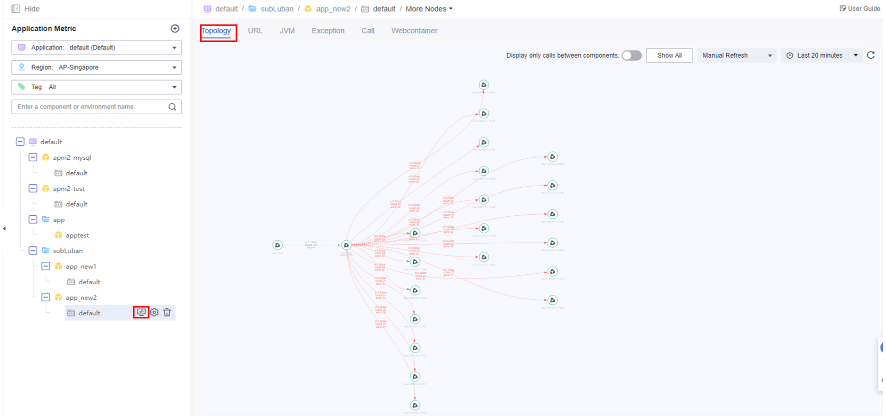
Step 4 In the tree on the left, click 🖥 next to the environment whose topology you want to view.

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



----End

Viewing the Global Topology

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

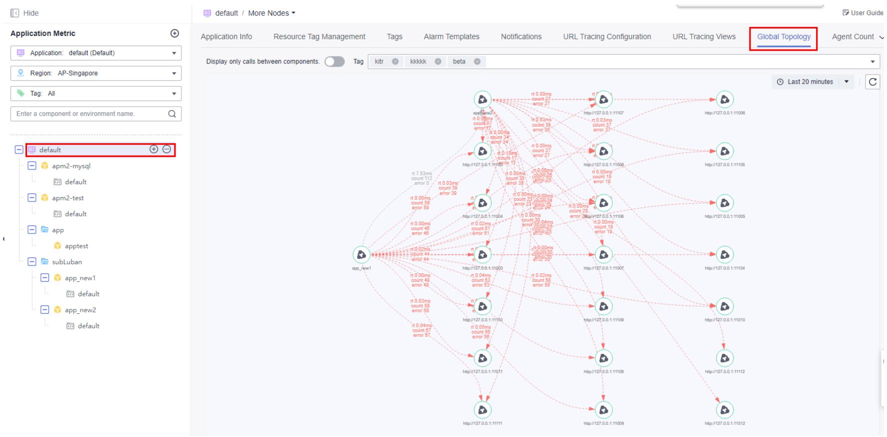
Step 2 In the tree on the left, click an application. The application details page is displayed.

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.

Use tags to filter calls or enable **Display only calls between components** to shield the calls of external components.

Figure 6-2 Viewing the global topology



----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.

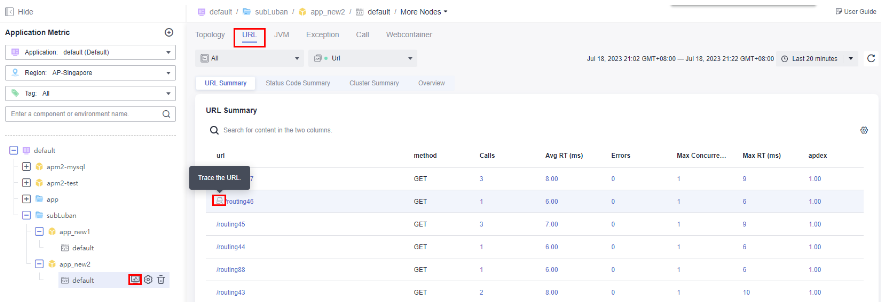
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

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



url	method	Calls	Avg RT (ms)	Errors	Max Concurre...	Max RT (ms)	apdex
[illegible]7	GET	3	8.00	0	1	9	1.00
/routing46	GET	1	6.00	0	1	6	1.00
/routing45	GET	3	7.00	0	1	9	1.00
/routing44	GET	1	6.00	0	1	6	1.00
/routing88	GET	1	6.00	0	1	6	1.00
/routing43	GET	2	8.00	0	1	10	1.00

Step 6 If there are more than five instances, click **More Instances**. Select up to five instances to monitor each time. If you select one more instance than the allowed limit (5), the first instance will be deselected by default.

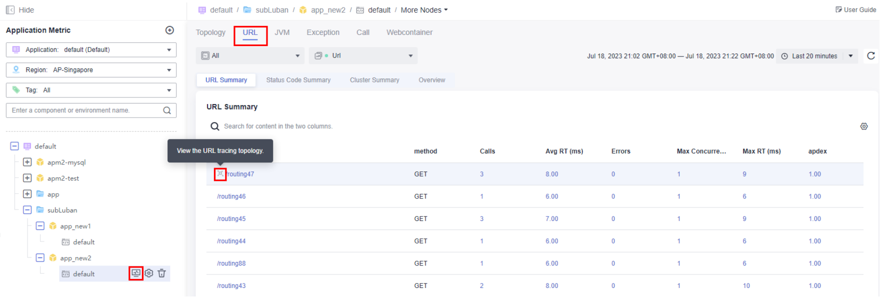
----End

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



	method	Calls	Avg RT (ms)	Errors	Max Concurre...	Max RT (ms)	apdex
/routing47	GET	3	8.00	0	1	9	1.00
/routing46	GET	1	6.00	0	1	6	1.00
/routing45	GET	3	7.00	0	1	9	1.00
/routing44	GET	1	6.00	0	1	6	1.00
/routing88	GET	1	6.00	0	1	6	1.00
/routing43	GET	2	8.00	0	1	10	1.00

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

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

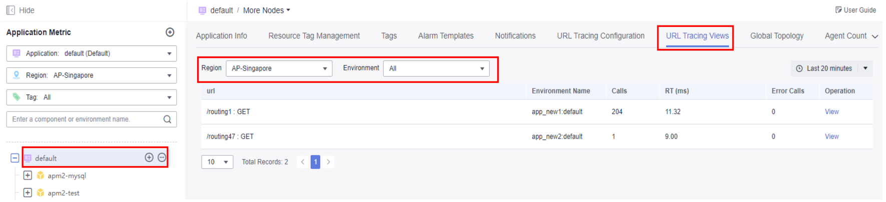
Step 2 In the tree on the left, click an application. The application details page is displayed.

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



url	Environment Name	Calls	RT (ms)	Error Calls	Operation
/routing1 : GET	app_new1:default	204	11.32	0	View
/routing47 : GET	app_new2:default	1	9.00	0	View

----End

Viewing the URL Tracing Configuration

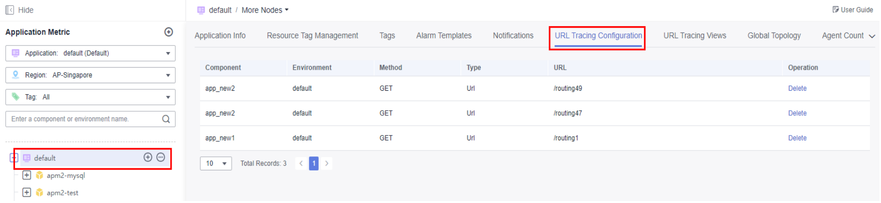
The URL which has been added for tracing will be displayed in the URL tracing configuration list.

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.

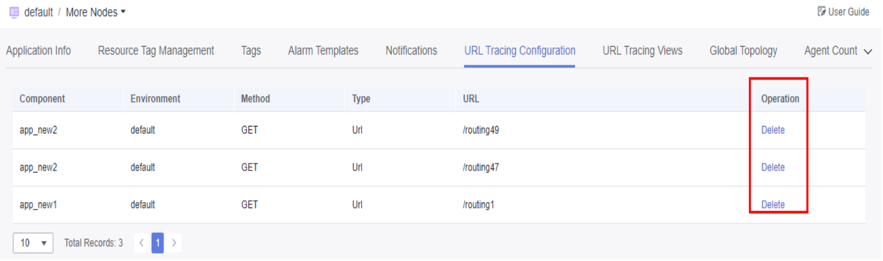
Figure 7-4 Viewing the URL tracing configuration list



Component	Environment	Method	Type	URL	Operation
app_new2	default	GET	Url	/routing49	Delete
app_new2	default	GET	Url	/routing47	Delete
app_new1	default	GET	Url	/routing1	Delete

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

Figure 7-5 Deleting a URL tracing configuration



Component	Environment	Method	Type	URL	Operation
app_new2	default	GET	Url	/routing49	Delete
app_new2	default	GET	Url	/routing47	Delete
app_new1	default	GET	Url	/routing1	Delete

----End

Viewing Transactions

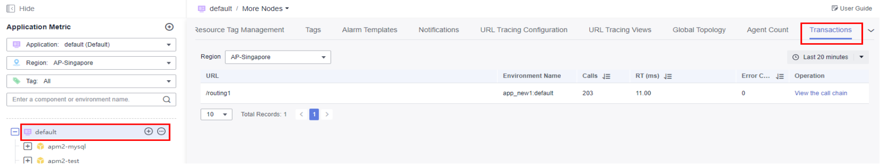
Transaction URLs are displayed in a list. By default, the system displays the invocation of all entries.

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.

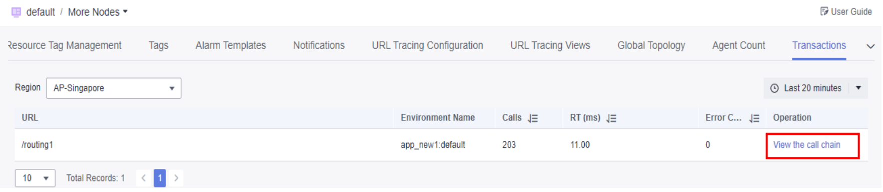
Figure 7-6 Viewing transactions



URL	Environment Name	Calls	RT (ms)	Error C...	Operation
/routing1	app_new1:default	203	11.00	0	View the call chain

Step 4 Click **View the call chain** in the **Operation** column of the target transaction. For details about trace operations, see **Tracing**.

Figure 7-7 Viewing traces



Region AP-Singapore

URL	Environment Name	Calls	RT (ms)	Error C...	Operation
/routing1	app_new1:default	203	11.00	0	View the call chain

10 Total Records: 1 < 1 >

----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**.

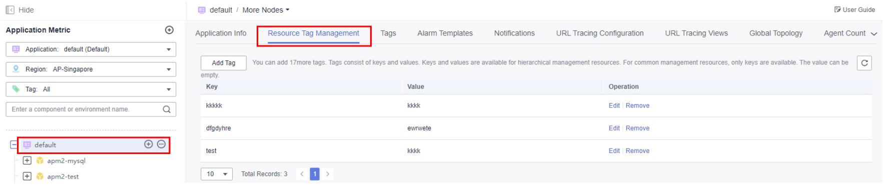
Viewing Tags

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 Viewing the tag list of the current application, as shown in the following figure.

Figure 8-1 Viewing the tag list



You can add 17more tags. Tags consist of keys and values. Keys and values are available for hierarchical management resources. For common management resources, only keys are available. The value can be empty.

Key	Value	Operation
kkkkk	kkkk	Edit | Remove
dfgdyhre	ewrwete	Edit | Remove
test	kkkk	Edit | Remove

----End

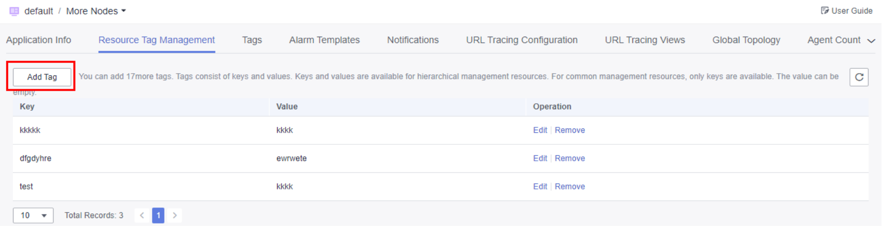
Adding a Tag

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



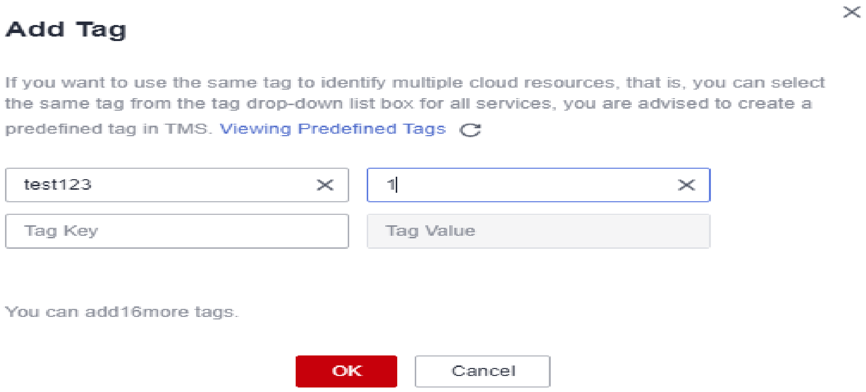
You can add 17more tags. Tags consist of keys and values. Keys and values are available for hierarchical management resources. For common management resources, only keys are available. The value can be empty.

Key	Value	Operation
kkkkk	kkkk	Edit | Remove
dfgdyhre	ewrwete	Edit | Remove
test	kkkk	Edit | Remove

10 Total Records: 3 1

Step 3 Set tag parameters.

Figure 8-3 Setting tag parameters



If you want to use the same tag to identify multiple cloud resources, that is, you can select the same tag from the tag drop-down list box for all services, you are advised to create a predefined tag in TMS. Viewing Predefined Tags

test123	1
Tag Key	Tag Value

You can add16more tags.

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 value 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 a Tag

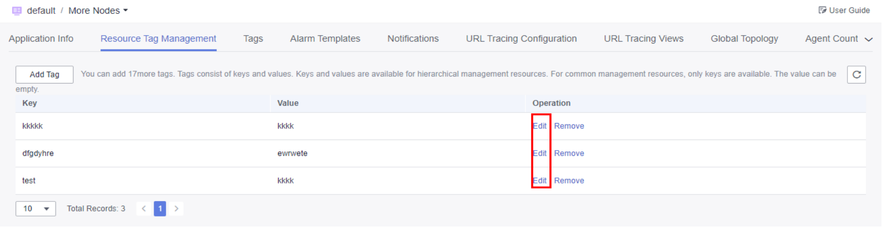
When modifying a tag for a single resource, you can modify only the cloud resources that contain the tag. To modify a tag, perform the following steps:

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.

Figure 8-4 Editing a tag



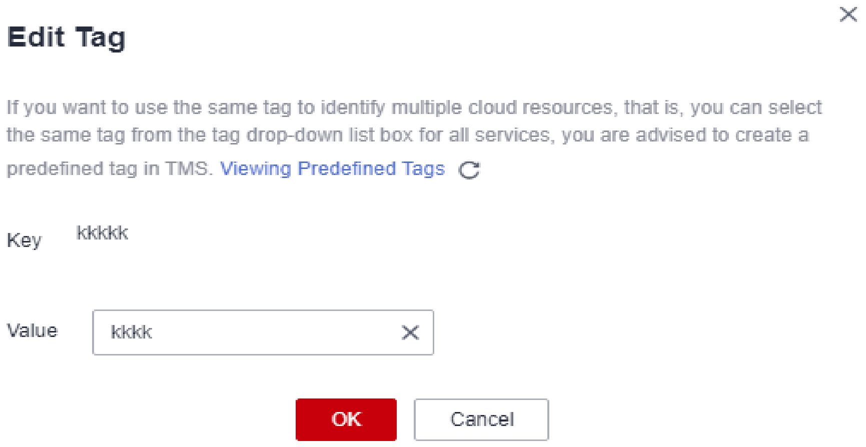
You can add 17more tags. Tags consist of keys and values. Keys and values are available for hierarchical management resources. For common management resources, only keys are available. The value can be empty.

Key	Value	Operation
kkkkk	kkkk	Edit Remove
dfgdyhre	ewrwete	Edit Remove
test	kkkk	Edit Remove

10 Total Records: 3 1

Step 4 Click **OK**.

Figure 8-5 Confirming the modification



Edit Tag

If you want to use the same tag to identify multiple cloud resources, that is, you can select the same tag from the tag drop-down list box for all services, you are advised to create a predefined tag in TMS. Viewing Predefined Tags

Key kkkkk

Value kkkk

----End

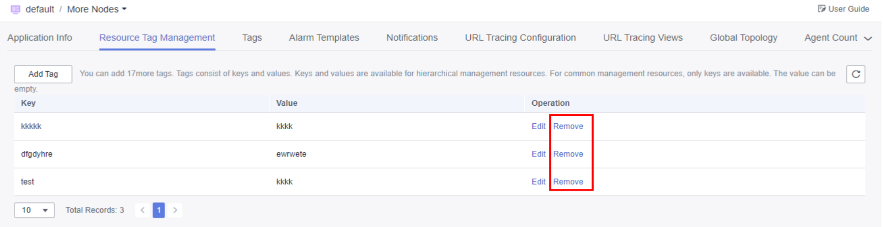
Deleting a Tag

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.

Figure 8-6 Deleting a tag

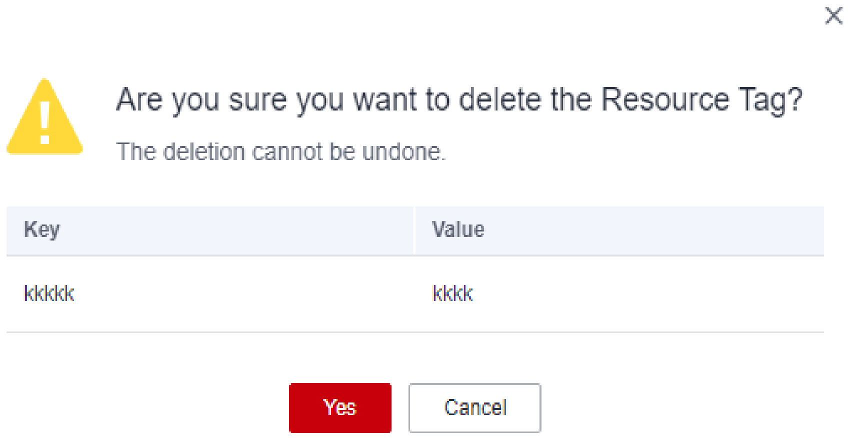


You can add 17more tags. Tags consist of keys and values. Keys and values are available for hierarchical management resources. For common management resources, only keys are available. The value can be empty.

Key	Value	Operation
kkkkk	kkkk	Edit Remove
dfgdyhre	ewrwete	Edit Remove
test	kkkk	Edit Remove

Step 4 Click **Yes**.

Figure 8-7 Confirming the deletion



Are you sure you want to delete the Resource Tag?

The deletion cannot be undone.

Key	Value
kkkkk	kkkk

----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**.

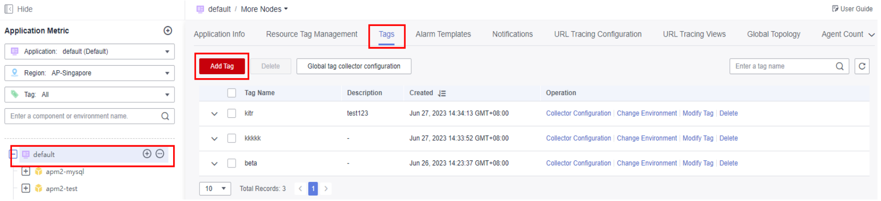
Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

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



Tag Name	Description	Created	Operation
kitr	test123	Jun 27, 2023 14:34:13 GMT+08:00	Collector Configuration | Change Environment | Modify Tag | Delete
kkkkk	-	Jun 27, 2023 14:33:52 GMT+08:00	Collector Configuration | Change Environment | Modify Tag | Delete
beta	-	Jun 26, 2023 14:23:37 GMT+08:00	Collector Configuration | Change Environment | Modify Tag | Delete

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

Step 8 Click **OK**.

----End

Modifying a Tag

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

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

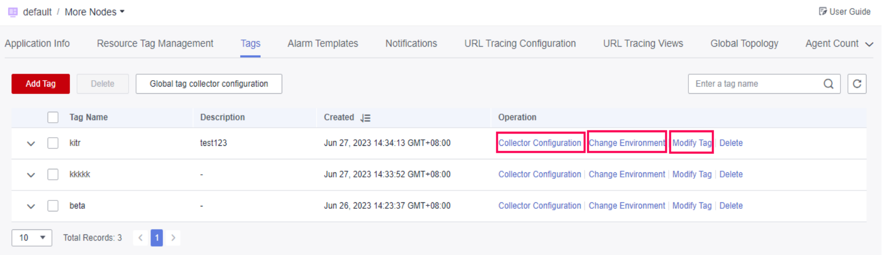
Step 3 Click the **Tags** tab.

Step 4 Locate the row that contains the tag to be modified and click **Collector Configuration**. In the dialog box that is displayed, select the collector to be associated from the drop-down list and click **OK**.

Locate the row that contains the tag to be modified and click **Change Environment**. In the dialog box that is displayed, select the environments to bind and click **OK**.

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

Figure 9-2 Modifying a tag



Tag Name	Description	Created	Operation
kitr	test123	Jun 27, 2023 14:34:13 GMT+08:00	Collector Configuration | Change Environment | Modify Tag | Delete
kkkkk	-	Jun 27, 2023 14:33:52 GMT+08:00	Collector Configuration | Change Environment | Modify Tag | Delete
beta	-	Jun 26, 2023 14:23:37 GMT+08:00	Collector Configuration | Change Environment | Modify Tag | Delete

----End

Deleting a Tag

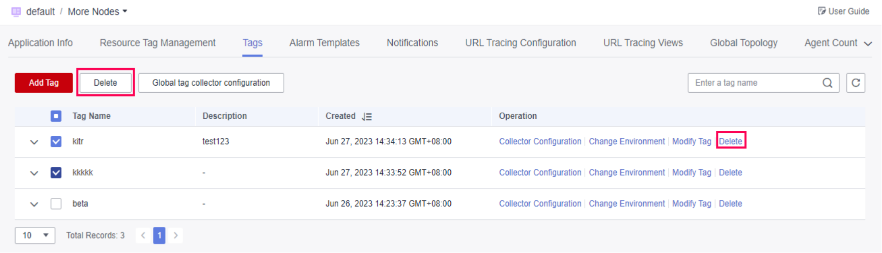
Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

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**.

Figure 9-3 Deleting a tag



	Tag Name	Description	Created	Operation
☑	kitr	test123	Jun 27, 2023 14:34:13 GMT+08:00	Collector Configuration | Change Environment | Modify Tag | Delete
☑	kkkkk	-	Jun 27, 2023 14:33:52 GMT+08:00	Collector Configuration | Change Environment | Modify Tag | Delete
□	beta	-	Jun 26, 2023 14:23:37 GMT+08:00	Collector Configuration | Change Environment | Modify Tag | Delete

10 Total Records: 3 < 1 >

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

----End

Global Tag Collector Configuration

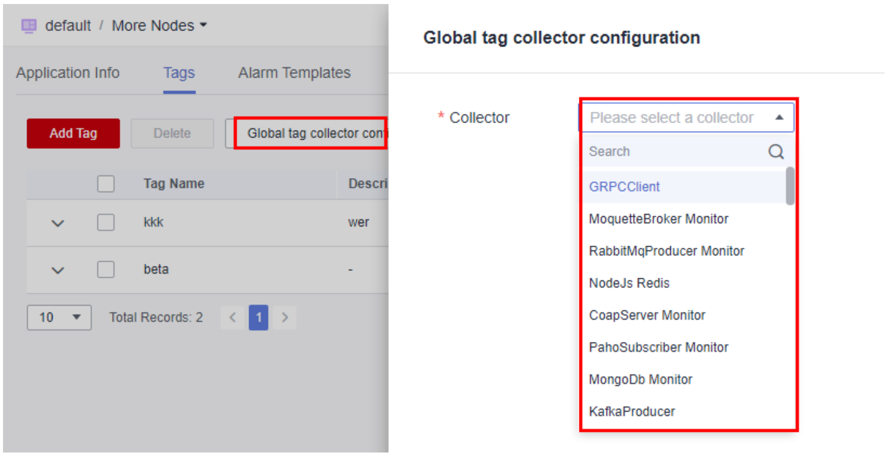
Step 1 In the navigation pane, choose **Application Monitoring** > **Metrics**.

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

Step 3 Click the **Tags** tab.

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

Figure 9-4 Global tag collector configuration



	Tag Name	Descri
□	kkk	wer
□	beta	-

10 Total Records: 2 < 1 >

* Collector: Please select a collector

GRPCClient
MoquetteBroker Monitor
RabbitMqProducer Monitor
NodeJs Redis
CoapServer Monitor
PahoSubscriber Monitor
MongoDb Monitor
KafkaProducer

Step 5 Select a collector from the drop-down list and click **OK**.

----End

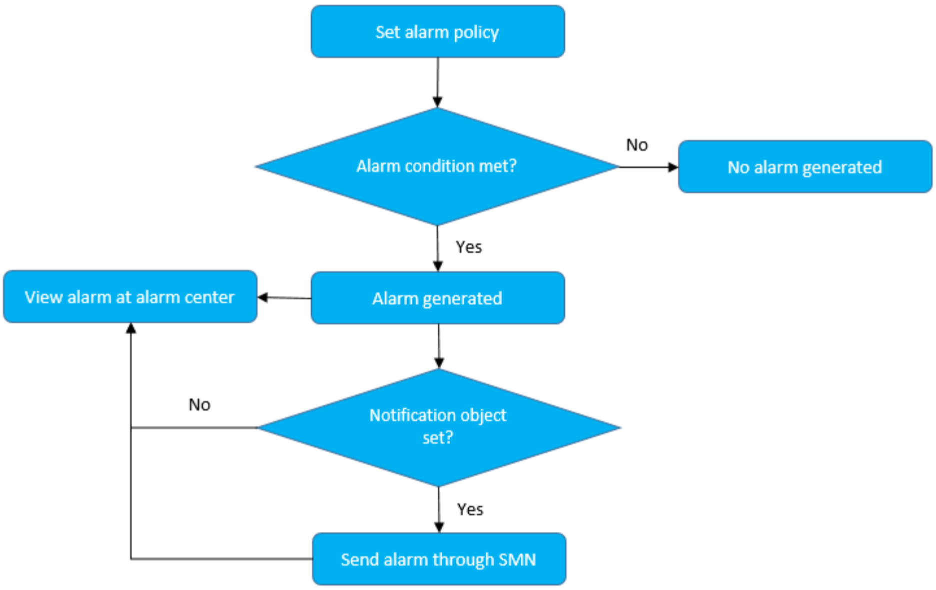
10 Alarm Management

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.

----End

10.2 Alarm Policies

10.2.1 Creating 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.

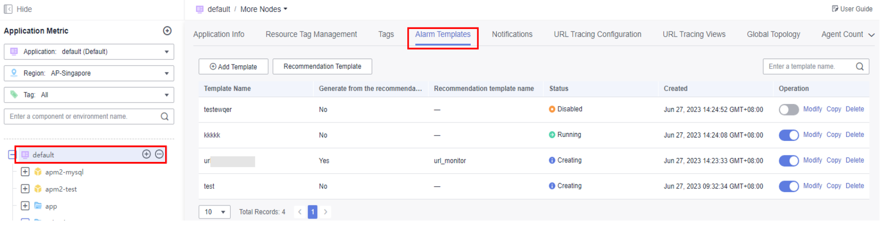
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

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 Creating an alarm template



Template Name	Generate from the recommenda...	Recommendation template name	Status	Created	Operation
testewqer	No	—	Disabled	Jun 27, 2023 14:24:52 GMT+08:00	Modify Copy Delete
kkkkk	No	—	Running	Jun 27, 2023 14:24:08 GMT+08:00	Modify Copy Delete
ur[redacted]	Yes	url_monitor	Creating	Jun 27, 2023 14:23:33 GMT+08:00	Modify Copy Delete
test	No	—	Creating	Jun 27, 2023 09:32:34 GMT+08:00	Modify Copy Delete

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

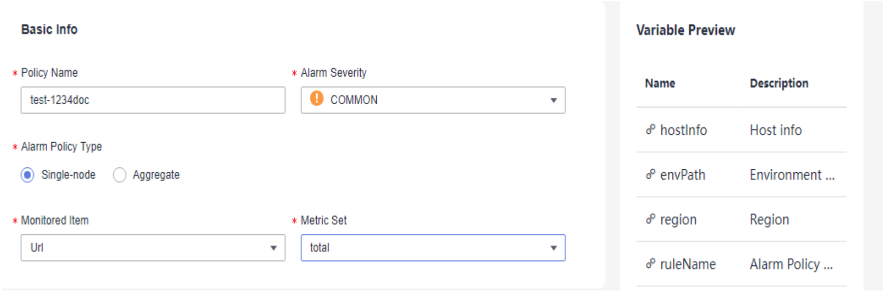
1. Enter basic information.

   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

Figure 10-3 Basic information



Basic Info

* Policy Name: test-1234doc

* Alarm Severity: COMMON

* Alarm Policy Type: ● Single-node ○ Aggregate

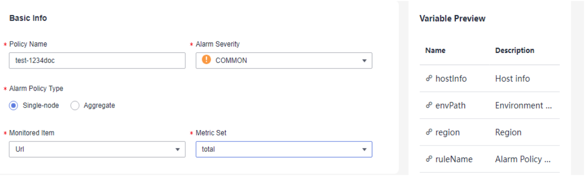
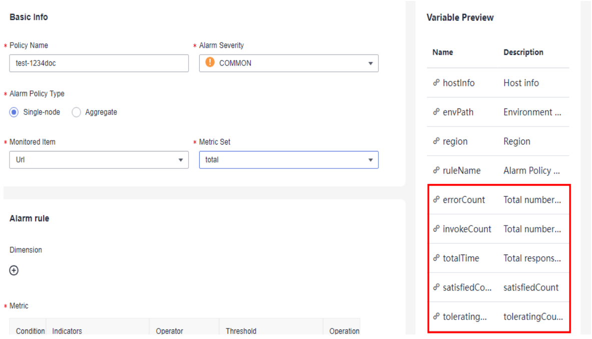
* Monitored Item: Url

* Metric Set: total

Variable Preview

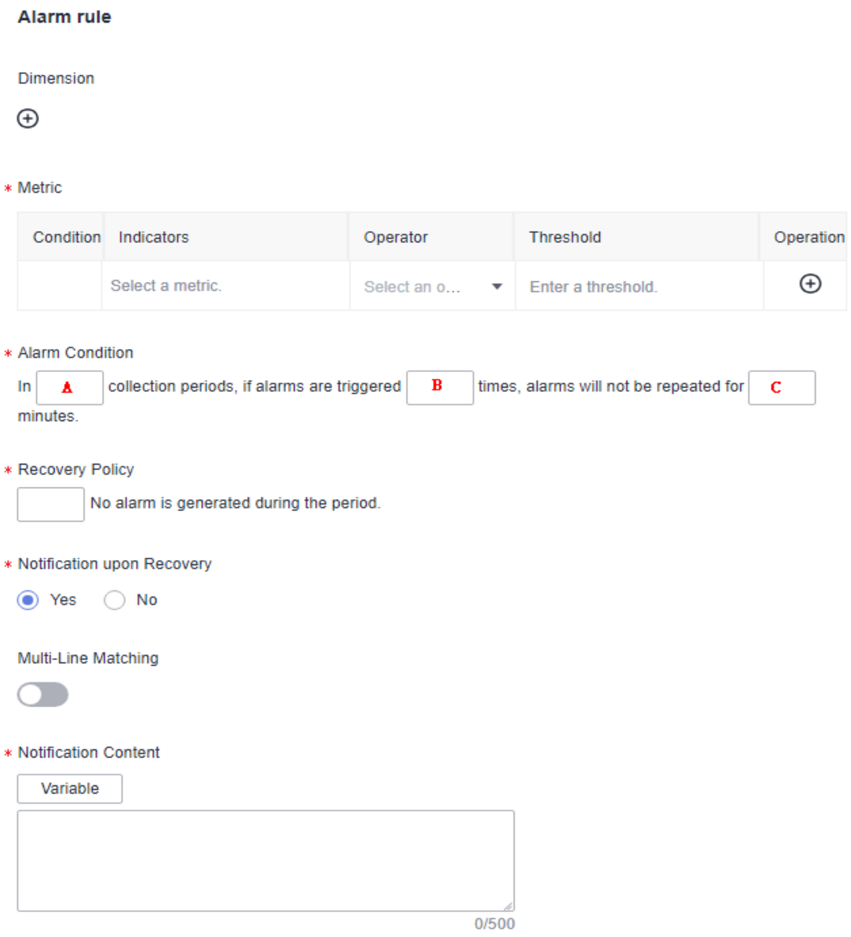
Name	Description
hostInfo	Host info
envPath	Environment ...
region	Region
ruleName	Alarm Policy ...

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.  Basic Info * Policy Name: test-1234doc * Alarm Severity: COMMON * Alarm Policy Type: ● Single-node ○ Aggregate * Monitored Item: Url * Metric Set: total Variable Preview Name: Description hostInfo: Host info envPath: Environment ... region: Region ruleName: Alarm Policy ...
Metric Set	Select a target metric set. The information about the selected metric set is displayed on the right.  Basic Info * Policy Name: test-1234doc * Alarm Severity: COMMON * Alarm Policy Type: ● Single-node ○ Aggregate * Monitored Item: Url * Metric Set: total Alarm rule Dimension ⊕ * Metric Condition, Indicators, Operator, Threshold, Operation Variable Preview Name: Description hostInfo: Host info envPath: Environment ... region: Region ruleName: Alarm Policy ... errorCount: Total number... invokeCount: Total number... totalTime: Total respons... satisfiedCo...: satisfiedCount tolerating...: toleratingCou...

b. Alarm rule

Figure 10-4 Alarm rule



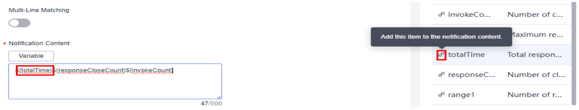
Condition	Indicators	Operator	Threshold	Operation
	Select a metric.	Select an o... ▾	Enter a threshold.	⊕

In A collection periods, if alarms are triggered B times, alarms will not be repeated for C minutes.

No alarm is generated during the period.

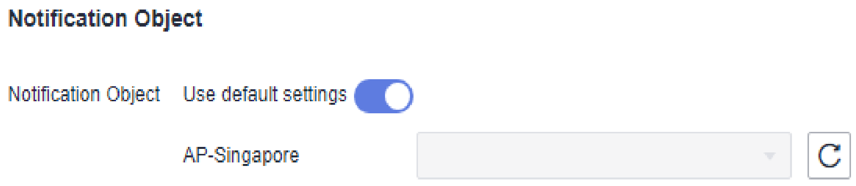
Table 10-2 Alarm rule parameters

Parameter	Description
Dimension	(Optional) A category of metrics.
Metric	Metric for which you want to define one or more alarm rules.
Alarm Condition	Condition for triggering an alarm. A: 1–10 B: 1–10; not greater than A C: ≥ 10
Recovery Policy	Condition for clearing an alarm.

Parameter	Description
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.  Multi-Line Matching * Notification Content Variable ${totalTime}${responseCloseCount}${invokeCount} 47/500 Add this item to the notification content. invokeCo... Number of c... Maximum re... totalTime Total respon... responseC... Number of cl... range1 Number of r...

c. Notification object

Figure 10-5 Notification object



Notification Object

Notification Object Use default settings

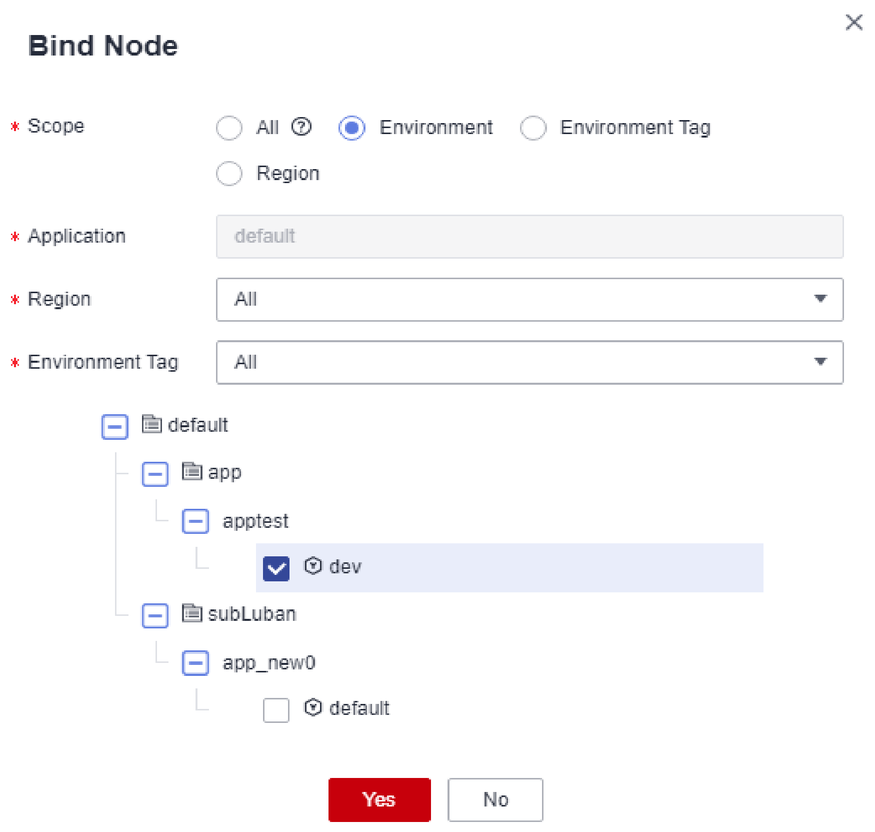
AP-Singapore

Table 10-3 Alarm notification parameters

Parameter	Description
Notification Object	Select a notification object from the drop-down list. The alarm will only be sent to the selected notification object.

3. Click **Yes**.
4. Bind nodes based on the environment, environment tag, or region.

Figure 10-6 Binding nodes



Bind Node

* Scope ○ All ● Environment ○ Environment Tag ○ Region

* Application: default

* Region: All

* Environment Tag: All

- default
  - app
    - apptest
      - ☑ dev
  - subLuban
    - app_new0
      - □ default

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 alarm template is created.

----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.

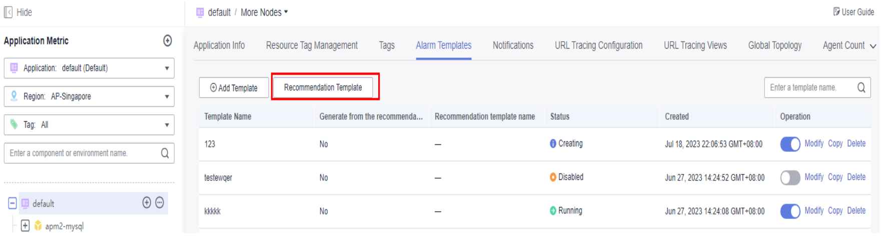
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

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.

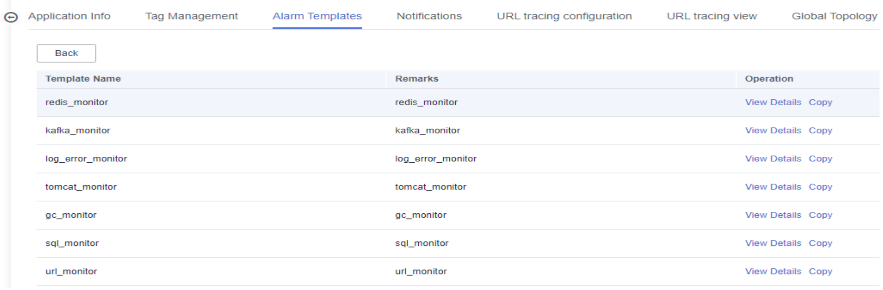
Figure 10-7 Viewing recommended alarm templates



Template Name	Generate from the recommenda...	Recommendation template name	Status	Created	Operation
123	No	–	Creating	Jul 18, 2023 22:06:53 GMT+08:00	Modify Copy Delete
testewqer	No	–	Disabled	Jun 27, 2023 14:24:52 GMT+08:00	Modify Copy Delete
kkkkk	No	–	Running	Jun 27, 2023 14:24:08 GMT+08:00	Modify Copy Delete

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

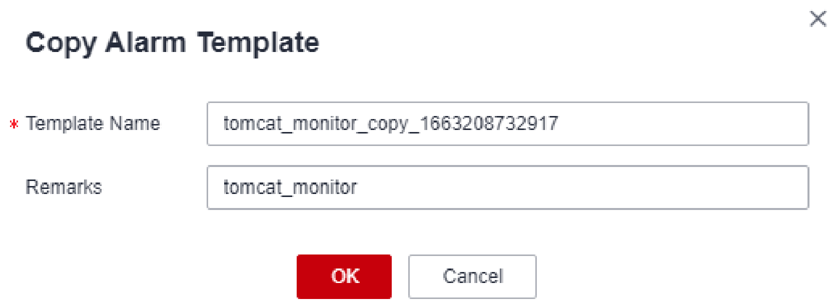
Figure 10-8 Recommended template list



Template Name	Remarks	Operation
redis_monitor	redis_monitor	View Details Copy
kafka_monitor	kafka_monitor	View Details Copy
log_error_monitor	log_error_monitor	View Details Copy
tomcat_monitor	tomcat_monitor	View Details Copy
gc_monitor	gc_monitor	View Details Copy
sql_monitor	sql_monitor	View Details Copy
url_monitor	url_monitor	View Details Copy

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

Figure 10-9 Copying an alarm template

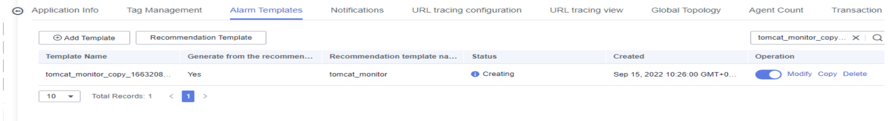


* Template Name: tomcat_monitor_copy_1663208732917

Remarks: tomcat_monitor

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

Figure 10-10 Returning to the alarm template page



Template Name	Generate from the recommen...	Recommendation template na...	Status	Created	Operation
tomcat_monitor_copy_1663208...	Yes	tomcat_monitor	Creating	Sep 15, 2022 10:26:00 GMT+0...	Modify Copy Delete

10 Total Records: 1 < 1 >

Step 9 Click **Modify** in the **Operation** column and **bind the template** to the node again for the copied template to take effect.

----End

10.3 Alarm Notification

Component alarms can be sent to specified terminals by text message, function, or email. In this way, you can learn about component exceptions in a timely manner and quickly rectify faults to prevent loss. Ensure that you have permissions for Simple Message Notification (SMN). 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**.

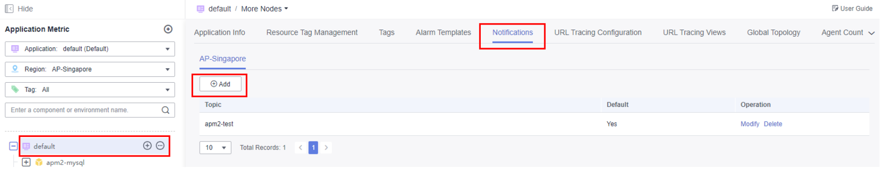
Step 3 In the navigation pane, choose **Application Monitoring** > **Metrics**.

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 10-11 Creating a notification object



Application: default (Default)

Region: AP-Singapore

Tag: All

Enter a component or environment name.

Topic	Default	Operation
apm2-test	Yes	Modify Delete

10 Total Records: 1 < 1 >

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 **OK**.

----End

11 Agent Management

11.1 Operating Agents

Agent Management allows you to view 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.

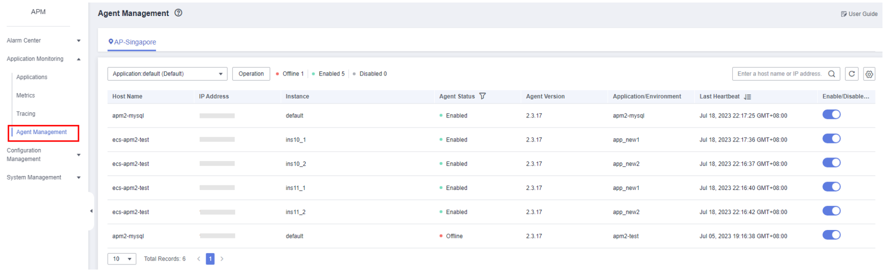
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

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

Step 4 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



Host Name	IP Address	Instance	Agent Status	Agent Version	Application/Environment	Last Heartbeat	Enable/Disable...
apm2-mysql	[redacted]	default	Enabled	2.3.17	apm2-mysql	Jul 18, 2023 22:17:25 GMT+08:00	●
ecs-apm2-test	[redacted]	ins10_1	Enabled	2.3.17	app_new1	Jul 18, 2023 22:17:36 GMT+08:00	●
ecs-apm2-test	[redacted]	ins10_2	Enabled	2.3.17	app_new2	Jul 18, 2023 22:16:37 GMT+08:00	●
ecs-apm2-test	[redacted]	ins11_1	Enabled	2.3.17	app_new1	Jul 18, 2023 22:16:40 GMT+08:00	●
ecs-apm2-test	[redacted]	ins11_2	Enabled	2.3.17	app_new2	Jul 18, 2023 22:16:42 GMT+08:00	●
apm2-mysql	[redacted]	default	Offline	2.3.17	apm2-test	Jul 05, 2023 19:16:38 GMT+08:00	●

----End

The following table describes the Agent statuses.

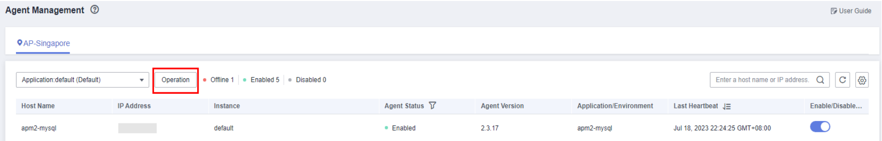
Status	Description
Enabled	The Agent is running properly.
Offline	The Agent is abnormal due to a network error. Check and restore the network.
Disabled	The Agent is manually or globally disabled. Contact technical support.

Batch Operations

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

Step 2 Click **Operation**.

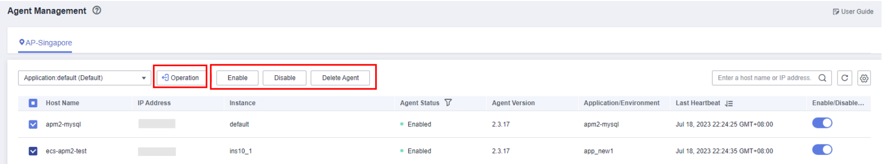
Figure 11-2 Batch operations



Host Name	IP Address	Instance	Agent Status	Agent Version	Application/Environment	Last Heartbeat	Enable/Disable...
apm2-mysql	[redacted]	default	● Enabled	2.3.17	apm2-mysql	Jul 18, 2023 22:24:25 GMT+08:00	

Step 3 Select the desired objects, and click **Disable**, **Enable**, or **Delete**.

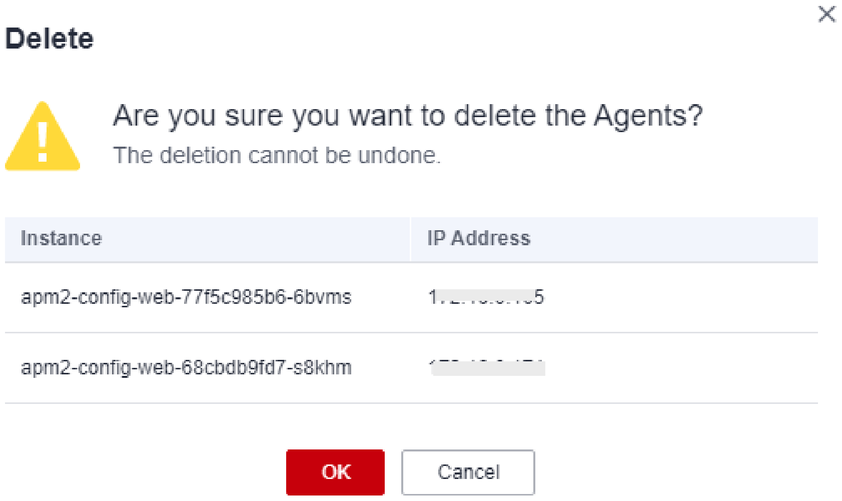
Figure 11-3 Operating Agents in batches



	Host Name	IP Address	Instance	Agent Status	Agent Version	Application/Environment	Last Heartbeat	Enable/Disable...
☑	apm2-mysql	[redacted]	default	● Enabled	2.3.17	apm2-mysql	Jul 18, 2023 22:24:25 GMT+08:00	
☑	ecs-apm2-test	[redacted]	ins10_1	● Enabled	2.3.17	app_new1	Jul 18, 2023 22:24:35 GMT+08:00	

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

Figure 11-4 Deleting Agents



Delete

Are you sure you want to delete the Agents?

The deletion cannot be undone.

Instance	IP Address
apm2-config-web-77f5c985b6-6bvms	[redacted]
apm2-config-web-68cbdb9fd7-s8khm	[redacted]

----End

11.2 Upgrading Agents

Update Agent versions according to the following procedure.

Upgrading the Manually Installed Agents

To upgrade the manually installed Agents, obtain the JavaAgent download addresses from the *APM Getting Started*, decompress them to the previous directory, and delete the original Agents from the directory.

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 **Getting Started** > **Monitoring Java Applications** > **Installing Agents for the Java Applications Deployed in CCE Containers**.

Upgrading Agents of Other Types

Install new Agents.

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.

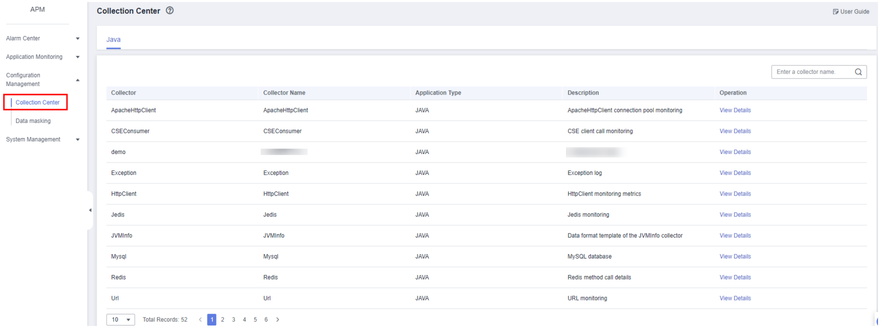
Step 2 Click ☰ on the left and choose **Application** > **Application Performance Management**.

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



Collector	Collector Name	Application Type	Description	Operation
ApacheHttpClient	ApacheHttpClient	JAVA	ApacheHttpClient connection pool monitoring	View Details
CSEConsumer	CSEConsumer	JAVA	CSE client call monitoring	View Details
demo	[redacted]	JAVA	[redacted]	View Details
Exception	Exception	JAVA	Exception log	View Details
HttpClient	HttpClient	JAVA	HttpClient monitoring metrics	View Details
Jedis	Jedis	JAVA	Jedis monitoring	View Details
JVMInfo	JVMInfo	JAVA	Data format template of the JVMInfo collector	View Details
Mysql	Mysql	JAVA	MySQL database	View Details
Redis	Redis	JAVA	Redis method call details	View Details
Url	Url	JAVA	URL monitoring	View 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: 1024 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.

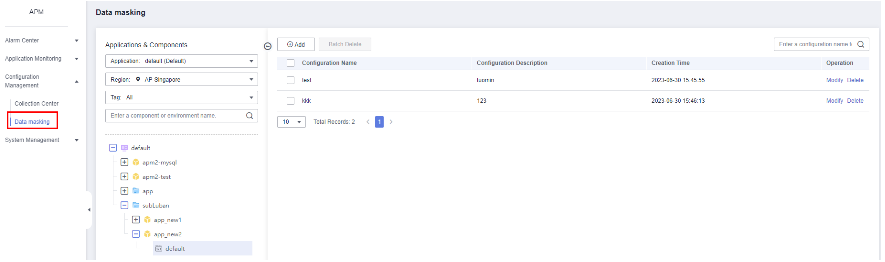
Querying a Data Masking Configuration

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 Querying a data masking configuration



Data masking

Application: default (Default)

Region: AP-Singapore

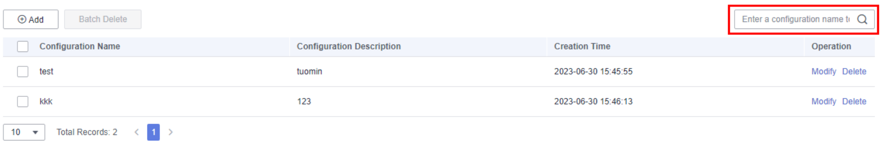
Tag: All

Configuration Name	Configuration Description	Creation Time	Operation
test	tuomin	2023-06-30 15:45:55	Modify Delete
kkk	123	2023-06-30 15:46:13	Modify Delete

Total Records: 2

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

Figure 12-3 Searching for a configuration



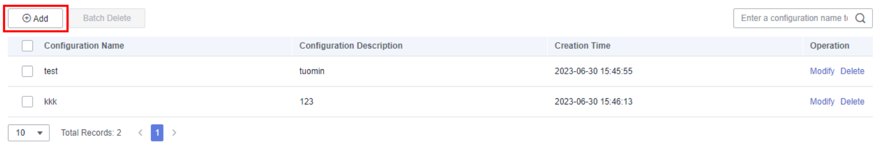
	Configuration Name	Configuration Description	Creation Time	Operation
□	test	tuomin	2023-06-30 15:45:55	Modify Delete
□	kkk	123	2023-06-30 15:46:13	Modify Delete

----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.

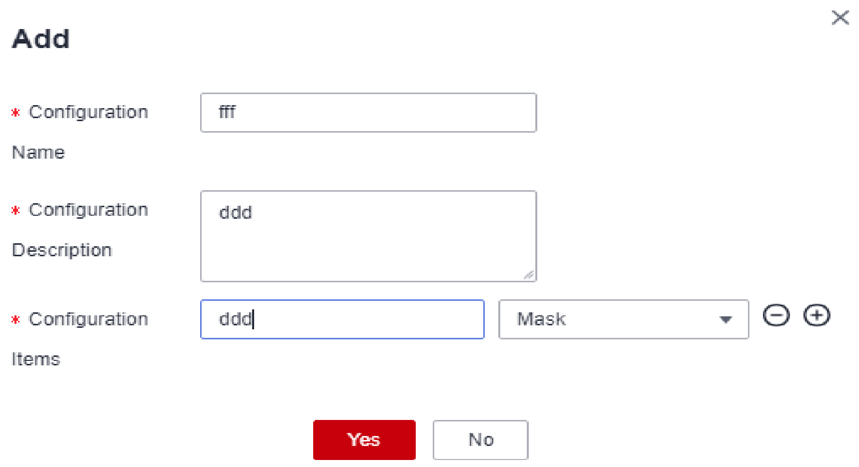
Figure 12-4 Add a data masking configuration



	Configuration Name	Configuration Description	Creation Time	Operation
□	test	tuomin	2023-06-30 15:45:55	Modify Delete
□	kkk	123	2023-06-30 15:46:13	Modify Delete

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

Figure 12-5 Adding a configuration



* Configuration Name: fff

* Configuration Description: ddd

* Configuration Items: ddd | Mask

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.

Parameter	Description
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. ● This parameter is mandatory. The options in the drop-down list are **Token** (replace the content with a globally unique random character string) and **Mask** (replace the content with asterisks (*)). You can also perform fuzzy search. **Mask** is displayed by default. ● 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 making. ● 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**.

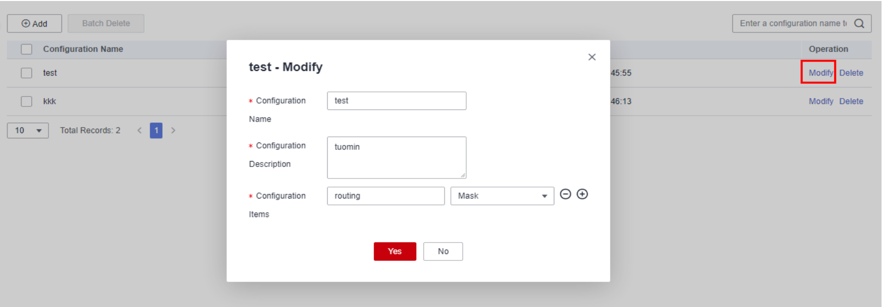
----End

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 information.

Figure 12-6 Going to the modification page



test - Modify

* Configuration Name: test

* Configuration Description: tuomin

* Configuration Items: routing, Mask

	Configuration Name		Operation
□	test	45:55	Modify Delete
□	kkk	46:13	Modify Delete

Step 3 Click **Yes**.

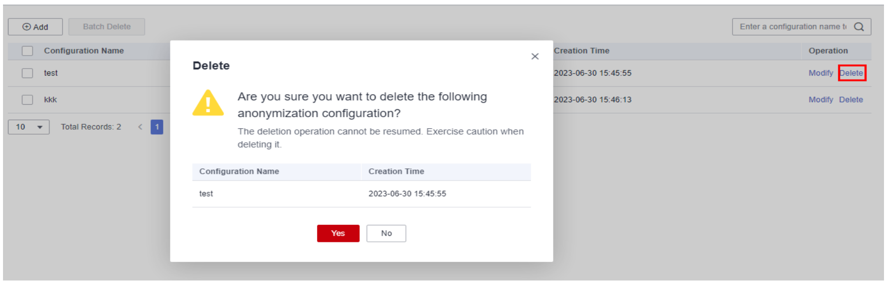
----End

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.

Figure 12-7 Deleting a data masking configuration



□	Configuration Name	Creation Time	Operation
□	test	2023-06-30 15:45:55	Modify Delete
□	kkk	2023-06-30 15:46:13	Modify Delete

Delete

Are you sure you want to delete the following anonymization configuration?

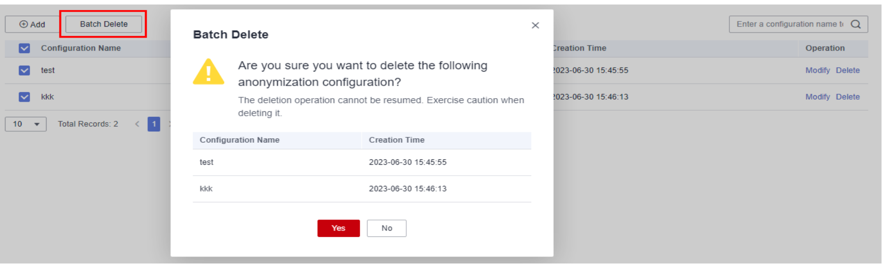
The deletion operation cannot be resumed. Exercise caution when deleting it.

Configuration Name	Creation Time
test	2023-06-30 15:45:55

Yes No

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.

Figure 12-8 Deleting configurations in batches



☑	Configuration Name	Creation Time	Operation
☑	test	2023-06-30 15:45:55	Modify Delete
☑	kkk	2023-06-30 15:46:13	Modify Delete

Batch Delete

Are you sure you want to delete the following anonymization configuration?

The deletion operation cannot be resumed. Exercise caution when deleting it.

Configuration Name	Creation Time
test	2023-06-30 15:45:55
kkk	2023-06-30 15:46:13

Yes No

----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. AK is used together with SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct.

Precautions

Each access key consists of a pair of AK/SK and has unlimited validity. Each user can create up to two access keys. They have the same permissions but are independent from each other. Periodically change your access keys and keep them secure to prevent data leakage. To change an access key, delete the old one and add a new one.

NOTE

By default, the SK is stored in plaintext in the **apm.config** file. APM also provides an encryption and decryption mechanism to meet higher security requirements.

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

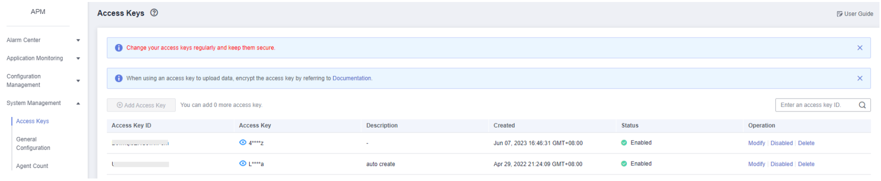
Step 1 Log in to the management console.

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



Change your access keys regularly and keep them secure.

When using an access key to upload data, encrypt the access key by referring to Documentation.

You can add 0 more access key.

Enter an access key ID.

Access Key ID	Access Key	Description	Created	Status	Operation
[redacted]	4****z	-	Jun 07, 2023 16:46:31 GMT+08:00	Enabled	Modify | Disabled | Delete
[redacted]	L****a	auto create	Apr 29, 2022 21:24:09 GMT+08:00	Enabled	Modify | Disabled | Delete

Step 5 Add an access key description and click **OK** 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 the access key, click **Enable** in the row that contains the access key. On the page that is displayed, click **Yes**.

----End

13.2 General Configuration

General Configuration: You can set the maximum number of rows for data collection, set a slow request threshold, and specify whether to stop collecting data through bytecode instrumentation.

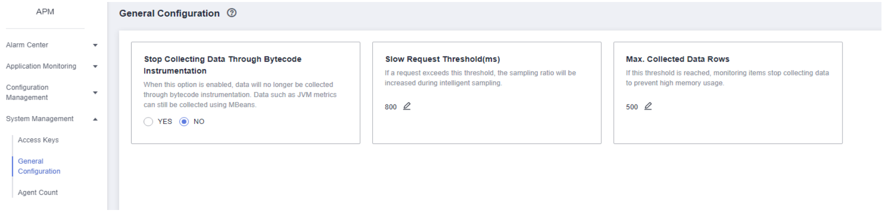
Step 1 Log in to the management console.

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

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

You can set the maximum number of rows of data to collect, set a slow request threshold, and specify whether to stop collecting data through bytecode instrumentation.

Figure 13-2 Modifying general configuration



General Configuration

Stop Collecting Data Through Bytecode Instrumentation
When this option is enabled, data will no longer be collected through bytecode instrumentation. Data such as JVM metrics can still be collected using MBeans.
○ YES ● NO

Slow Request Threshold(ms)
If a request exceeds this threshold, the sampling ratio will be increased during intelligent sampling.
800

Max. Collected Data Rows
If this threshold is reached, monitoring items stop collecting data to prevent high memory usage.
500

----End

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.

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**.

- **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

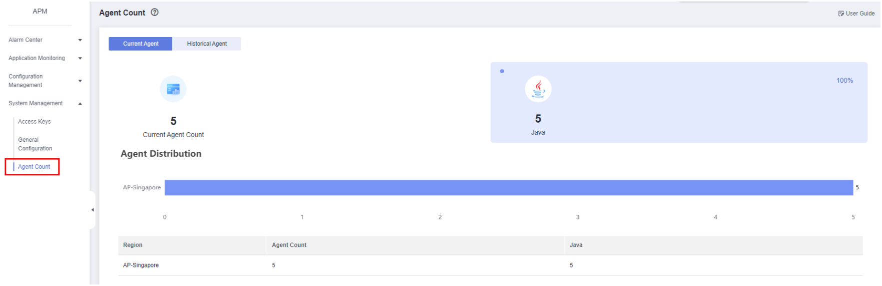
Checking the Number of Agents Used by an Application

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.

Figure 13-3 Agent counting



Region	Agent Count	Java
AP-Singapore	5	5

- **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

APM uses enterprise project management to control users' access to APM resources. After creating an IAM user group for an employee using your cloud account, you can create an enterprise project on the Enterprise Management console and grant permissions to the user group in the enterprise project, realizing personnel authorization and permissions control. With enterprise project management, you can centrally manage resources in different regions by enterprise project and configure user groups with different permissions for each enterprise project.

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**).

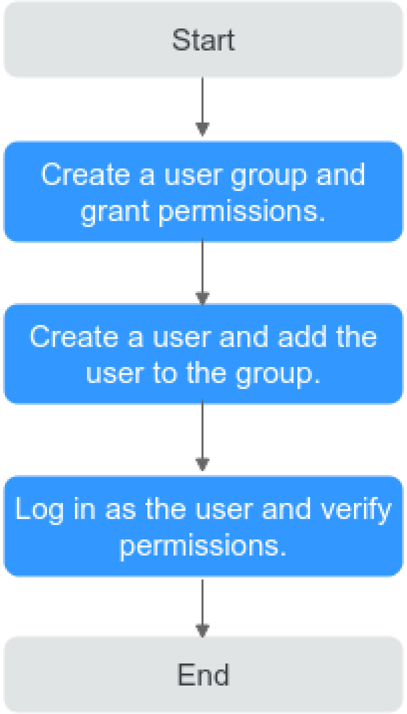
Prerequisite

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


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

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
2023-07-20	This issue is the first official release.