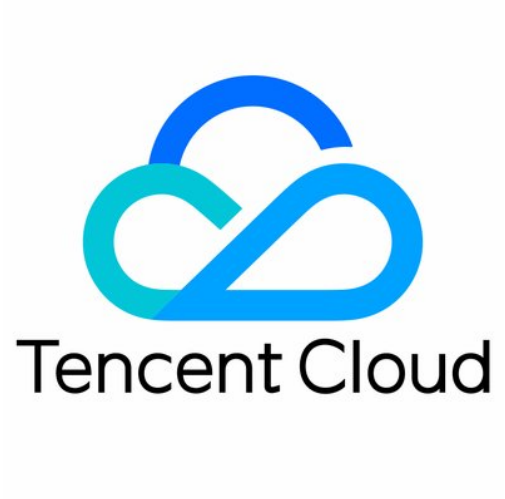
TencentDB for MySQL

Database Audit

Product Documentation



Contents

Database Audit
- Overview
- Viewing Audit Instance List
- Enabling Audit Service
- Viewing Audit Log
- Configuring Post-Event Alarms
- Modifying Audit Rule
- Modifying Audit Services
- Disabling Audit Service
- Audit Rule Template
  - Viewing Rule Template List
  - Creating Rule Template
  - Modifying Rule Template
  - Deleting Rule Template
- SQL Audit Rule (Legacy)
- Viewing Audit Task
- Authorizing Sub-User to Use Database Audit

Database Audit Overview

Last updated：2023-11-28 19:16:36

Database audit is a professional, efficient, and comprehensive database audit service independently developed by Tencent Cloud for monitoring database security in real time. It can record the activities of TencentDB instances in real time, manage the compliance of database operations with fine-grained audit, and alert risky database behaviors.
TencentDB for MySQL provides database audit capabilities to help you record accesses to databases and executions of SQL statements, so you can manage risks and improve the database security. In addition, it allows you to customize frequent and infrequent access storage types to greatly reduce the costs of database audit.
The database auditing feature supports post-event alerts, allowing for the configuration of high, medium, and low risk event alert strategies. Audit logs that match these strategies can send alert notifications to associated users. Concurrently, within Tencent Cloud's observable platform, one can view alert history, manage alert strategies (including alert toggles), and suppress alerts. This aids enterprises in promptly receiving relevant alert notifications and accurately pinpointing the audit logs that triggered the issue.

Use Cases

Audit risks
Difficulty in tracing and locating security breaches due to incomplete audit logs.
Inability to meet the requirements defined by China's Cybersecurity Classified Protection Certification (Level 3).
Inability to meet the requirements defined by industry-specific information security compliance documents.
Administrative risks
Business system security risks caused by faulty, non-compliant, and unauthorized operations of technical personnel.
Faulty and malicious operations and tampering by third-party development and maintenance personnel.
Excessive permissions granted to the super admin, which cannot be audited and monitored.
Technical challenges
Database system SQL injections that maliciously pull data from databases and tables.
Inability to troubleshoot the sudden increase of database requests that are not slow queries.

Product Billing

Database audit is billed by the stored log size for every clock-hour, and usage duration shorter than one hour will be calculated as one hour.
For detailed pricing, see Database Audit Billing Overview.

Supported Versions

TencentDB for MySQL audit is supported for two-node and three-node instances on MySQL 5.6 20180101 or above, MySQL 5.7 20190429 or above, and MySQL 8.0 20210330 or above.

Advantages

Full audit

Database Audit fully records the accesses to databases and executions of SQL statements to meet your audit requirements and ensure database security as much as possible.

Rule-based audit

Rule-based audit records access requests to the database and SQL statement executions according to the custom audit rule.

Efficient audit

Different from non-embedded audit mode, Database Audit records TencentDB operations through the embedded database kernel plugin, which makes the records more accurate.

Long-term retention

Database Audit allows you to retain logs persistently according to your business needs to meet regulatory compliance requirements.

Architecture characteristics

Database audit adopts the multi-point deployment architecture to guarantee the service availability. It records logs in a streaming manner to prevent tampering and retains them in multiple copies to ensure the data reliability.

Data Security

Data integrity during collection

Database audit in TencentDB for MySQL is implemented based on the kernel plugin of MySQL. The execution of each SQL statement will undergo a complete process from connection, parsing, analysis, rewrite, and optimization to execution, return, audit, and release. After database audit is enabled and connected to the TencentDB for MySQL server, each SQL statement will be audited during execution. If audit fails, the statement was not executed successfully. If a statement is executed successfully, it will definitely be successfully audited. A SQL request connection will be released only after audit, which guarantees the integrity of the collected data.

Data reliability during collection

Database audit in TencentDB for MySQL captures data synchronously from MySQL's own execution layer instead of capturing data asynchronously. Therefore, the audited SQL statements and the SQL statements executed in TencentDB for MySQL are synced in real time and consistent with each other. This ensures that the captured data is always correct, guaranteeing the reliability of the collected data.

Data tampering protection

The audit control system has a behavior monitoring mechanism. When someone exploits a vulnerability to launch attacks, vulnerability scan can monitor intrusions in real time by capturing relevant session information and sending alarms. When someone manipulates the audit data, all access requests will be logged for you to check which user accesses the data from which source IP address and thus discover high-risk access operations in time. The database audit service also supports account/role-based authentication, so that different data read/write permissions can be granted to users with different roles, which solves problems caused by account sharing. When someone performs a high-risk operation, a tampering alarm will be triggered in real time for prompt risk discovery, analysis, tracking, and prevention.

Data integrity during transfer

When audit data is processed at the transfer linkage layer after being collected, it will be verified in multiple dimensions, including cyclic redundancy check (CRC), globally unique ID check, linkage MQ redundancy check, and Flink-based stream processing, guaranteeing the data integrity during transfer.

Data integrity during storage

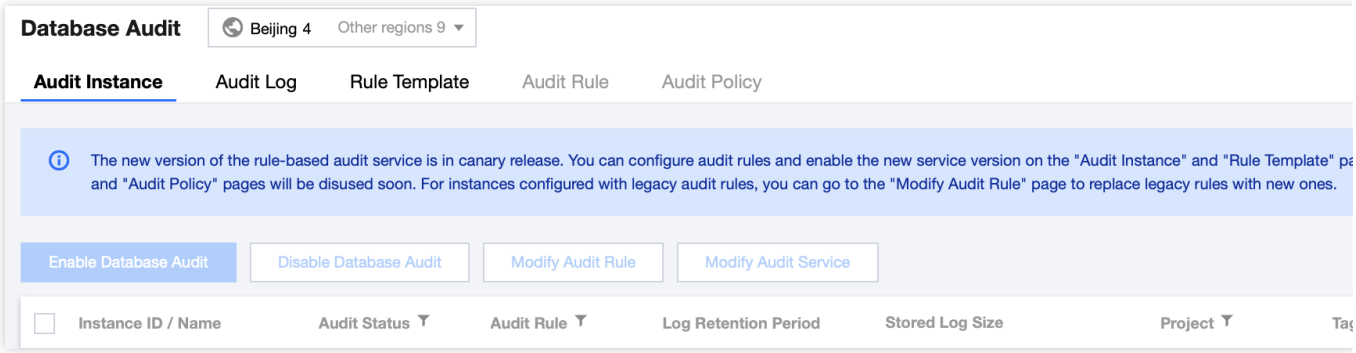
The database audit system encrypts the stored audit log files, so that only users with the encryption certificate access can view audit logs. This effectively prevents internal data leaks caused by plaintext storage and data thefts by high-privileged users, fundamentally eliminating the risks of audit the data leakage and guaranteeing the integrity of the stored data.

Viewing Audit Instance List

Last updated：2023-11-28 19:21:28

This document describes how to view the audit instance list as well as fields and executable operations in the list.

Audit instance list tab



Viewing the audit instance list

1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, click **Database Audit**.
3. You will be redirected to the **Database Audit** > **Audit Instance** tab by default.
4. On the **Audit Instance** tab, you can view the list of tools (for quickly filtering instances, refreshing the tab, and downloading the list information), feature operations, and instance list fields.

Tool list

Tool	Description
Filter	You can select resource attributes such as instance ID/name, tag key, and tag in the search box above the audit instance list to filter resources. Separate multiple keywords by vertical bar "
Refresh	You can click to refresh the data in the audit instance list.
Download	You can click to download the information of the filtered audit instances as a .csv file. The list fields in the file include instance ID/name, audit status, audit rule, total storage period, frequent access storage

	period, infrequent access storage period, total storage size, frequent access storage size, infrequent access storage size, project, tag, enablement time, and remarks.

Relevant feature operations

Audit Status	Feature	Description
The audit service is enabled.	Disable Database Audit	You can (batch) disable the audit service as instructed in Disabling Audit Service.
	Modify Audit Rule	You can (batch) modify audit rules as instructed in Modifying Audit Rule.
	Modify Audit Service	You can (batch) modify the audit service items such as audit log retention period and frequent/infrequent access storage periods as instructed in Modifying Audit Service.
	View Audit Log	You can query historical audit logs as instructed in Viewing Audit Log.
The audit service is disabled	Enable Database Audit	You can (batch) enable the audit service as instructed in Enabling Audit Service.

Fields in the audit instance list

Field	Description
Instance ID/Name	ID/Name information of all instances in a region.
Audit Status	Audit enablement or disablement status. You can select **Enabled** or **Disabled** to filter instances in the corresponding status.
Audit Rule	The audit rule (full audit or rule-based audit) configured for audit-enabled instances. You can use the drop-down list to filter instances by a specific rule.
Log Retention Period	Total storage period and frequent/infrequent access storage periods in days for audit-enabled instances.
Stored Log Size	Total storage size and frequent/infrequent access storage sizes in MB for audit-enabled clusters/instances.
Audit Regulations	The display enumerates the quantity of audit rule templates associated with the instance.

	When the cursor hovers over the audit rule field of the corresponding instance, you can view the ID and name of each rule template. By clicking on a specific rule template, you can delve into the detailed rule information of that template, which includes basic information, parameter configurations, and modification history.
Project	Projects of instances to help you categorize and manage resources easily. You can use the drop-down list to filter instances by a specific project.
Tag (key:value)	Tag information of instances
Enablement Time	The time accurate down to the second when the audit service is enabled for instances.
Operation	Available operations when the audit service is enabled: View Audit Log More (Modify Audit Rule, Modify Audit Service, Disable) Available operations when the audit service is disabled: Enable Database Audit

Enabling Audit Service

Last updated：2024-08-19 15:19:52

Tencent Cloud provides database audit capabilities for TencentDB for MySQL, which can record accesses to databases and executions of SQL statements to help you manage risks and improve the database security.

Note:

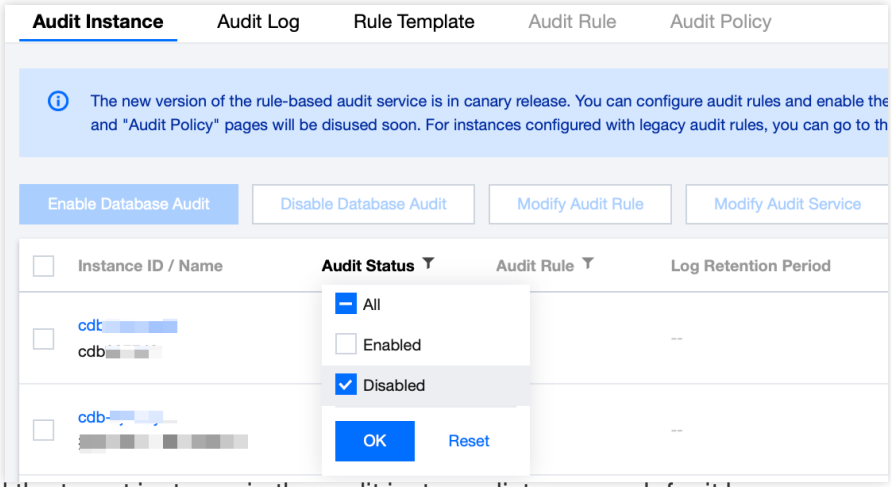
TencentDB for MySQL supports database audit feature in the following versions: MySQL 5.6 20180101 and later, MySQL 5.7 20190429 and later, MySQL 8.0 20210330 and later on two-node and three-node architectures. MySQL 5.5 and TencentDB for MySQL on single-node and cluster edition architectures do not support database audit feature.

Prerequisite

You have created a MySQL instance. For more information, see Creating MySQL Instance.

Directions

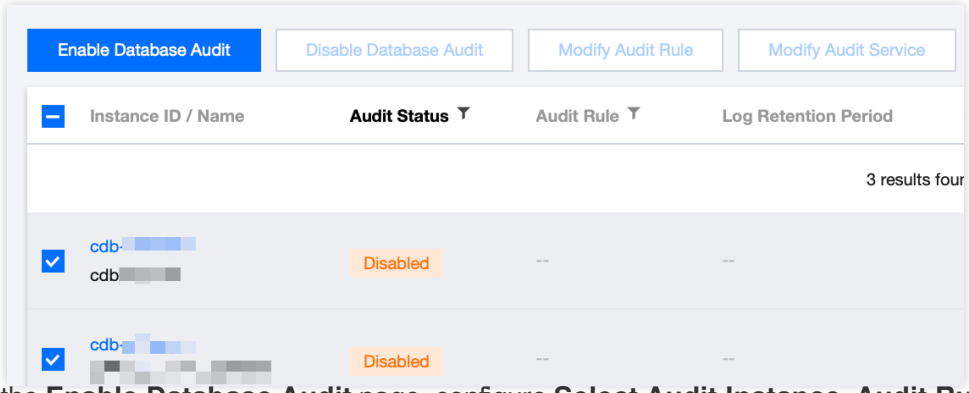
1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, click **Database Audit**.
3. Select a region at the top, click the **Audit Instance** tab, and click **Disabled** to filter audit-disabled instances.



4. Find the target instance in the audit instance list, or search for it by resource attribute in the search box, and click **Enable Database Audit** in the **Operation** column.

Note:

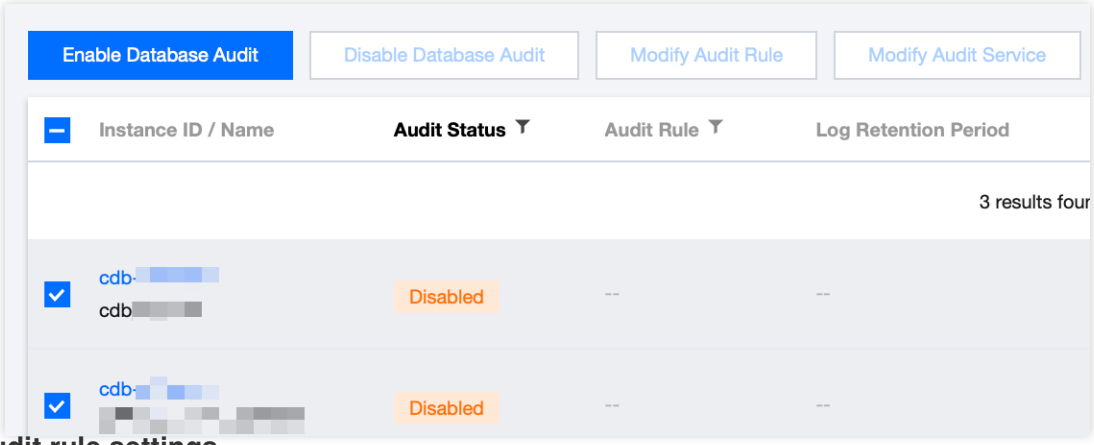
You can batch enable the audit service for multiple target instances by selecting them in the audit instance list and clicking **Enable Database Audit** above the list.



5. On the **Enable Database Audit** page, configure **Select Audit Instance**, **Audit Rule Settings**, **Configure Audit**, read and indicate your consent to the **Tencent Cloud Terms of Service**, and click **OK**.

5.1 **Audit instance selection**

In the **Select Audit Instance** section, all instances selected in **step 4** are selected by default. You can select other or more target instances in this window or search for target instances by instance ID/name in the search box. Then, set the audit rule.



5.2 **Audit rule settings**

In the **Audit Rule Settings** section, select **Full Audit** or **Rule-Based Audit**. Their differences are as detailed below:

Parameter	Description
Full audit	Full audit records all database accesses and SQL statement executions.
Rule-based audit	Rule auditing will chronicle the access to the database and the execution of SQL statements, in accordance with the bespoke audit rules.

When the audit type is set to full audit

, there are two actual operational scenarios in the console, for which you may refer to the corresponding procedures. Choose from existing rule templates or decide to create a new rule template. For detailed steps on creating a new template, please refer to Creating Rule Templates.

After completing the rule template configuration, proceed to the Audit Service Configuration step.

Note:

You may apply up to five rule templates, and the relationship between different rule templates is of 'or' nature.

The rule templates are intended for instances with 'Full Audit' type, serving the sole purpose of assigning risk levels and alert policies to audit logs that match the rules of the template. The audit logs that do not match the rules will still be preserved.

If you select **Rule-Based Audit**, you need to select **Create rule** or **Select from rule templates**. If you select an existing rule from rule templates, you can directly configure audit. If there are no appropriate rule templates, you can create a new one, refresh the page, and select it. For detailed directions, see Creating Rule Template.

Note:

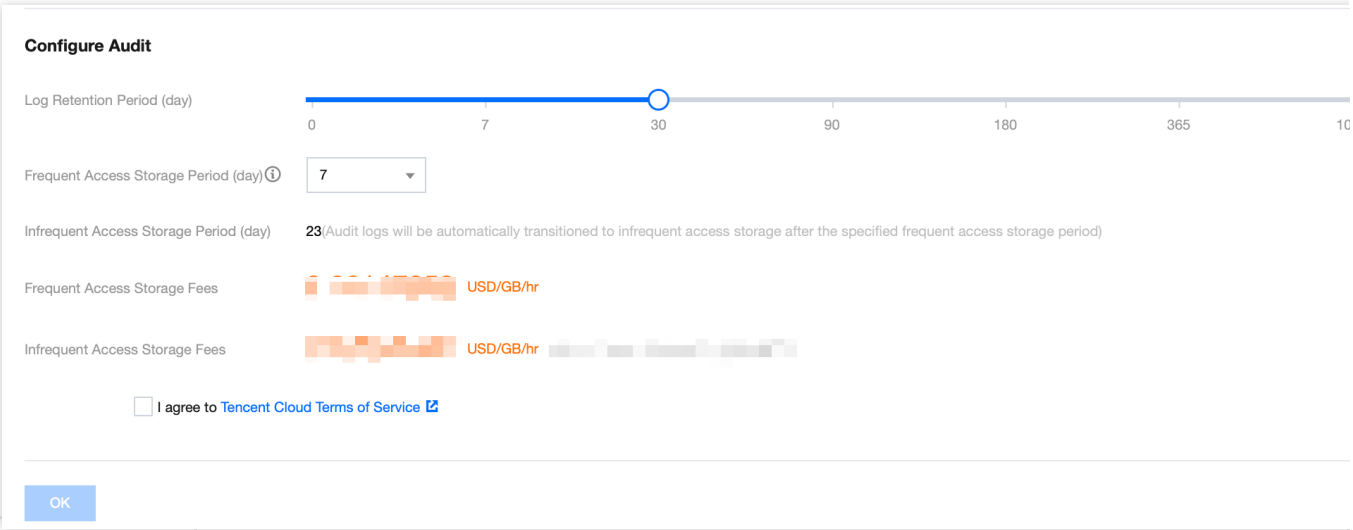
You may apply up to five rule templates, with the relationship between different rule templates being "or".

Rule templates are targeted at instances with the audit type of "rule audit". They are used for retaining audit logs that hit the template rules, setting risk levels, and establishing alarm strategies. Audit logs that do not hit the rule content are no longer retained.

5.3

Audit service settings

In the **Configure Audit** section, set **Log Retention Period**, **Frequent Access Storage Period**, and **Infrequent Access Storage Period**, read and indicate your content to the **Tencent Cloud Terms of Service**, and click **OK**.



Parameter	Description
Log Retention Period	The audit log retention period in days, which can be 7, 30, 90, 180, 365, 1,095, or 1,825 days.
Frequent Access Storage Period	Frequent access storage has the best query performance as it uses ultra-high-performance storage media. Audit data is initially stored in frequent access storage for the time period specified here, after which it is automatically transitioned to infrequent access storage. These two storage types only differ in performance but both support auditing. For

	example, if the log retention period is set to 30 days, and frequent access storage period is set to 7 days, then the infrequent access storage period will be 23 days by default.

Viewing Audit Log

Last updated：2024-08-16 11:14:03

This document describes how to view database audit logs and their list field.

Note:

A new version of the audit log page was released on July 12, 2023. The new version added a new audit log search field "Scanned Rows". For existing audit logs before this release date, the data in this field will be displayed as "-", and the corresponding downloaded files and APIs will be displayed as "-1".

The unit of the execution time which is the audit log field has been uniformly adjusted to millisecond in both the console and the downloaded audit log files.

The unit of the CPU time which is the audit log field has been uniformly adjusted to microsecond in both the console and the downloaded audit log files.

The unit of the timestamp field in the audit log files has been enhanced to display time with the unit being millisecond.

When searching audit logs, the character used to separate multiple search items is changed from **comma** to **line break**.

After database audit is enabled, instances in the regions of Tianjin, Taipei (China), and Shenzhen will have different audit log storage regions in CFS. Please refer to the table below for the corresponding storage regions.

Instance Region	Audit log storage region
Tianjin	Beijing
Taipei (China)	Hong Kong (China)
Shenzhen	Guangzhou

Prerequisite

You have enabled the audit service. For more information, see Enabling Audit Service.

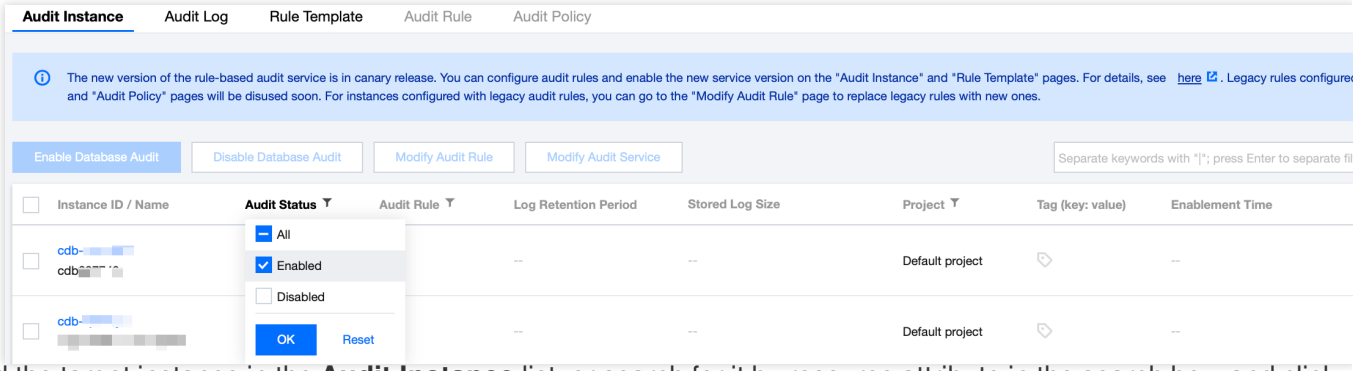
Viewing Audit Log

Note:

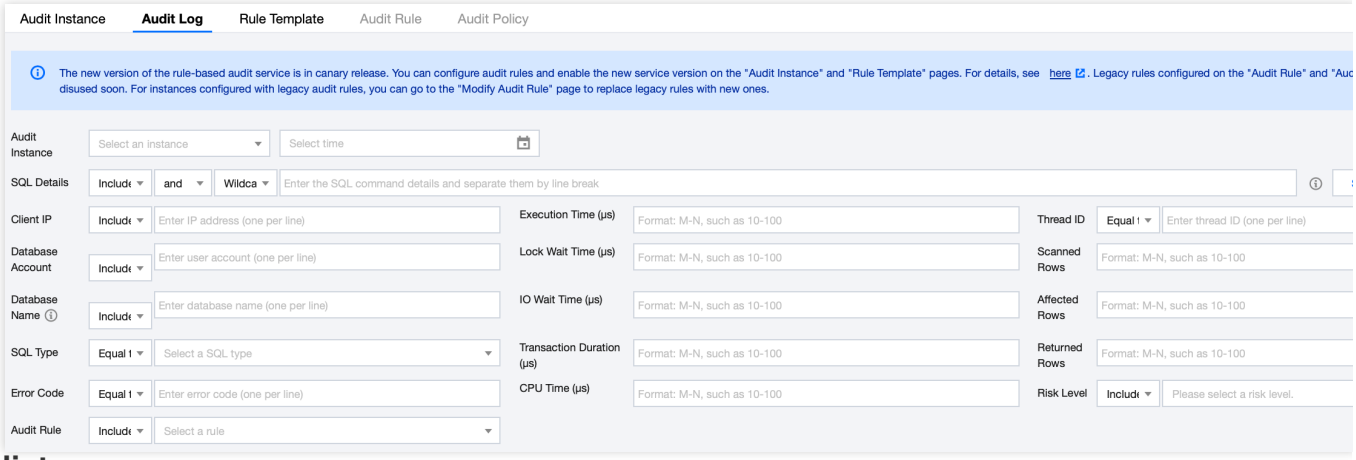
The audit log display time is down to milliseconds, facilitating more precise sorting and problem analysis of SQL commands.

1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, click **Database Audit**.

3. Select **Region** at the top, click **Audit Instance** tab, click **Audit Status**, and click **Enabled** to filter the audit-enabled instances.



4. Find the target instance in the **Audit Instance** list, or search for it by resource attribute in the search box, and click **View Audit Log** in the **Operation** column to enter the **Audit Log** tab and view logs.



Tool list

In the **audit instance filter box**, you can choose to switch to other audit instances that have enabled the audit service.

In the **Time Frame**, the default selection is Nearly 1 Hour. Other time periods (Last 3 Hours, Last 24 Hours, Last 7 Days) can be quickly selected. It also supports for custom time range to view audit logs within the selected time period.

Note:

You can select any time period with data for search. Up to the first 60,000 eligible records can be displayed.

In the **search box**, select search items (SQL details, client IP, user account, database name, Table Name, SQL type, error code, execution time (μs), lock wait time (μs), IO wait time (μs), transaction duration (μs), CPU time (μs), risk level, thread ID, transaction ID, scanned rows, affected rows, returned rows, audit rules, etc.) to search, and you can view relevant audit results. Multiple search items are separated by line break.

Search Item	Match Item	Description
SQL Command Details	Include - Or - Tokenize	**Rule Description**

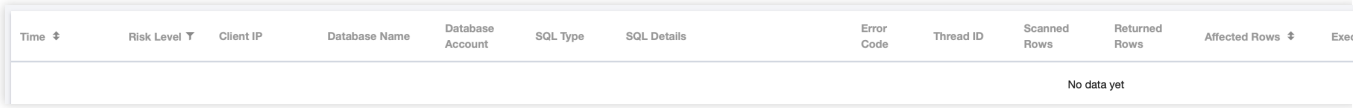
	Include - AND - Segmentation Exclude - AND - Segmentation Include - OR - Wildcard Include - AND - Wildcard Exclude - AND - Wildcard	Enter SQL Command Details, separating multiple keywords with line breaks. The SQL Command Details search box matches on three levels: The first level sets the match mode (inclusive or exclusive); The second level sets the logical relationship between keywords (OR, AND); The third level sets the match mode for each keyword (tokenization, wildcard). **Note:** SQL Command Details search is case-insensitive. Supports two match modes: "Inclusive" and "Exclusive". Keywords support two logical matches, "OR" and "AND". "OR" represents a "union" relationship between different keywords, while "AND" represents an "intersection" relationship. Each keyword supports "tokenization" and "wildcard" match modes. "Tokenization" means each keyword in the SQL Command Details needs to be exactly matched, while "wildcard" means each keyword in the SQL Command Details can be fuzzily matched. **Example Description** Assume the SQL Command Details are as follows: SELECT * FROM test_db1 JOIN test_db2 LIMIT 1; Under the "Inclusive (Tokenization)" search mode, you can search using tokenized keywords such as "SELECT", "select * from", "*", "SELECT * FROM test_db1 join test_db2 LIMIT 1;", "from Test_DB1", etc. However, wildcard keywords such as "SEL", "sel", "test", etc., cannot be used for search. Under the "Inclusive (Wildcard)" search mode, you can perform searches using wildcard keywords like "SEL", "sel", "test", and "DB". Under the "Inclusive (AND)" search mode, there is an "AND" relationship between multiple keywords. That is to say, entering keywords such as "SELECT", "test_db" will retrieve all SQL commands that include both "SELECT" and "test_db". Under the "Inclusive (OR)" search mode, there exists an "OR" relationship between multiple keywords. In other words, inputting "test_db1" or "test_db2" will yield all SQL commands that either include "test_db1" or "test_db2".
Client IP	Include Exclude Equal to Not equal to	Enter the client IP, separate multiple keywords with a new line; IP addresses can be filtered using * as a condition. For example, searching client IP: 9.223.23.2* will match IP addresses beginning with 9.223.23.2.
User Account	Include Exclude Equal to Not equal to	Enter the user account, separating multiple keywords with a new line.
Database Name	Include	Enter the database name, separating multiple keywords with a new line.

	Exclude Equal to Not equal to	**Note:** The database name search is case-insensitive.
Table Name	Equal to Not equal to	Input the table name, and the table name search are described as follows: Case-insensitive. The search format is DbName.TableName. For example: If the database test_db contains the table test_table, to search for table test_table, you need to input: the table name equals to test_db.test_table. **Note:** A maximum of 64 table names can be recorded. Only MySQL 8.0.30 20230630 and later versions support the "Table Name" field. If you require activation, submit a ticket to obtain a solution.
SQL Type	Equal to Not equal to	Select from the drop-down list the SQL types (ALTER, CHANGEUSER, CREATE, DELETE, DROP, EXECUTE, INSERT, LOGOUT, OTHER, REPLACE, SELECT, SET, UPDATE). Multiple selections are allowed.
Error Code	Equal to Not equal to	Enter the error code. Separate multiple keywords with a line break.
Execution time (Millisecond)	Interval Format	Enter the execution time in the format of M-N, such as 10-100 or 20-200.
Lock wait time (μs)	Interval Format	Enter the lock wait time in the format of M-N, such as 10-100 or 20-200.
IO wait time (μs)	Interval Format	Enter the IO wait time in the format of M-N, like 10-100 or 20-200.
Transaction duration (μs)	Interval Format	Enter the transaction duration in the format of M-N, like 10-100 or 20-200.
CPU time (μs)	Interval Format	Input the CPU time in the format M-N, for example, 10-100 or 20-200.
Risk Level	Include Exclude	Select low risk, medium risk, or high risk to filter the audit logs set by the risk level of the matched rule template. Support is also available for blank inputs, which means filtering audit logs without a risk level TAG from historical data.
Thread ID	Equal to Not equal to	Enter the Thread ID, separate multiple keywords using a line break.
Transaction ID	Equal to	Enter the transaction ID, and use a line break to separate multiple

	Not equal to	keywords. **Note：** Only MySQL 8.0.30 20230630 and later versions support the "Transaction ID" field.
Number of scanned rows	Interval Format	Enter the number of lines to be scanned in an M-N format, for example, 10-100 or 20-200.
Number of affected rows	Interval Format	Enter the number of affected rows in an M-N format, such as 10-100 or 20-200.
Number of returned rows	Interval Format	Enter the number of rows returned in the format M-N, such as 10-100 or 20-200.
Audit Rule	Include Exclude	Displays the Template ID and Template Name of all rule templates in a certain region. You can filter out the audit logs that match this rule template. It accepts blank input, indicative of filtering out audit logs without any audit rule TAG from historical data, and the full audit logs that did not hit any rules. Enables search operations based on Rule Template ID and Rule Template Name for audit rules. Allows selection of multiple rule templates at the same time.

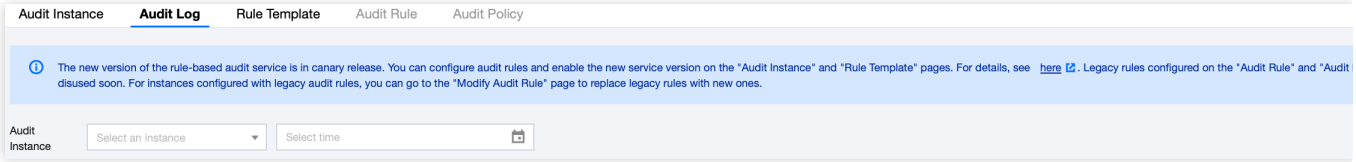
Log list

The **Returned Rows** field represents the specific number of rows returned by executing the SQL command, which is mainly used to determine the impact of `SELECT` commands.



Audit Fields

The following fields are supported in TencentDB for MySQL audit logs. On the **Audit Log** tab, click the download icon in the upper right corner. After download, click the file list icon. On the page redirected to, copy the download address and access it to get the complete SQL audit logs.



Note:

Currently, you can download audit log files of a database instance only at the Tencent Cloud private network address by using a CVM instance in the same region. For example, to download the audit logs of database instances in Beijing region, download them with a CVM instance in Beijing.
Log files are valid for 24 hours. Download them promptly.
Up to 30 log files can be retained for one database instance. Delete files promptly after download.
If the status is `Failed`, there may be too many logs. You can download them in batches by narrowing down the time range.

No.	Field	Remarks	
1	Time	-	
2	Risk Level	Divided into low risk, medium risk, and high risk. For comprehensive audit, logs that do not hit the audit rules will have their risk level displayed as "-".	
3	Client IP	-	
4	Database Name	-	
5	Table Name	A maximum of 64 table names can be recorded.	
6	User Account	-	
7	SQL Type	-	
8	SQL Details	-	
9	Error Code	`0` means success	
10	Thread ID	-	
11	Transaction ID	-	
12	Scanned Rows	-	
13	Returned Rows	-	
14	Affected Rows	-	
15	Execution Time (Millisecond)	-	
16	CPU Time (μs)	-	
17	Lock Wait Time (μs)	-	
18	IO Wait Time (μs)	-	

19	Transaction Duration (μs)	-	
20	Policy Name	-	
21	Audit Rule	This displays the rule template that the audit log has hit. By clicking on the corresponding rule template, you can see the specific details of the rule template, including basic information, parameter settings, and modification history. For historical audit logs, the value of the audit rule is displayed as "-". For full audit logs that haven't hit any rules, the value of the audit rule will be displayed as "-".	

Relationship Between SQL Statement Type and SQL Statement Mapping Object

No.	SQL Statement Type	SQL Statement Mapping Object
0	OTHER	All other SQL statement types except the following
1	SELECT	SQLCOM_SELECT
2	INSERT	SQLCOM_INSERT, SQLCOM_INSERT_SELECT
3	UPDATE	SQLCOM_UPDATE, SQLCOM_UPDATE_MULTI
4	DELETE	SQLCOM_DELETE, SQLCOM_DELETE_MULTI, SQLCOM_TRUNCATE
5	CREATE	SQLCOM_CREATE_TABLE, SQLCOM_CREATE_INDEX, SQLCOM_CREATE_DB, SQLCOM_CREATE_FUNCTION, SQLCOM_CREATE_USER, SQLCOM_CREATE_PROCEDURE, SQLCOM_CREATE_SPFUNCTION, SQLCOM_CREATE_VIEW, SQLCOM_CREATE_TRIGGER, SQLCOM_CREATE_SERVER, SQLCOM_CREATE_EVENT, SQLCOM_CREATE_ROLE, SQLCOM_CREATE_RESOURCE_GROUP, SQLCOM_CREATE_SRS
6	DROP	SQLCOM_DROP_TABLE, SQLCOM_DROP_INDEX, SQLCOM_DROP_DB, SQLCOM_DROP_FUNCTION, SQLCOM_DROP_USER, SQLCOM_DROP_PROCEDURE, SQLCOM_DROP_VIEW, SQLCOM_DROP_TRIGGER, SQLCOM_DROP_SERVER,

		SQLCOM_DROP_EVENT, SQLCOM_DROP_ROLE, SQLCOM_DROP_RESOURCE_GROUP, SQLCOM_DROP_SRS
7	ALTER	SQLCOM_ALTER_TABLE, SQLCOM_ALTER_DB, SQLCOM_ALTER_PROCEDURE, SQLCOM_ALTER_FUNCTION, SQLCOM_ALTER_TABLESPACE, SQLCOM_ALTER_SERVER, SQLCOM_ALTER_EVENT, SQLCOM_ALTER_USER, SQLCOM_ALTER_INSTANCE, SQLCOM_ALTER_USER_DEFAULT_ROLE, SQLCOM_ALTER_RESOURCE_GROUP
8	REPLACE	SQLCOM_REPLACE, SQLCOM_REPLACE_SELECT
9	SET	SQLCOM_SET_OPTION, SQLCOM_RESET, SQLCOM_SET_PASSWORD, SQLCOM_SET_ROLE, SQLCOM_SET_RESOURCE_GROUP
10	EXECUTE	SQLCOM_EXECUTE
11	LOGIN	Database login is not subject to audit rules.
12	LOGOUT	Database logout is not subject to audit rules.
13	CHANGEUSER	User change is not subject to audit rules.

Configuring Post-Event Alarms

Last updated：2024-08-16 11:10:02

Event alarms related to the database audit function have been integrated into TCOP and EB. If you have configured **Risk Level** and select **Send alarm notification** in your rule template, audit logs matching the rule template will trigger an alarm notification to the bound users. On the Tencent Cloud Observability Platform (TCOP), users can also view the alarm history, manage alarm policies (alarm switch), and shield alarms. Configuring event alarms for database audit can assist users in promptly receiving risk warnings and swiftly pinpointing problematic audit logs. This document describes how to configure event alarms for instances that have database audit enabled from TCOP and EB.

Prerequisites

You have enabled the audit service. For more information, see Enabling Audit Service.

Configuring Event Alarms through TCOP

Creating an Alarm Policy

1. Log in to the TCOP console and select **Alarm Configuration** > **Alarm Policy** > **Policy Management** on the left sidebar.
2. On the policy management page, click **Create Policy**.

3. On the policy creation page, finalize the setup for basic information, alarm rules, and alarm notifications.

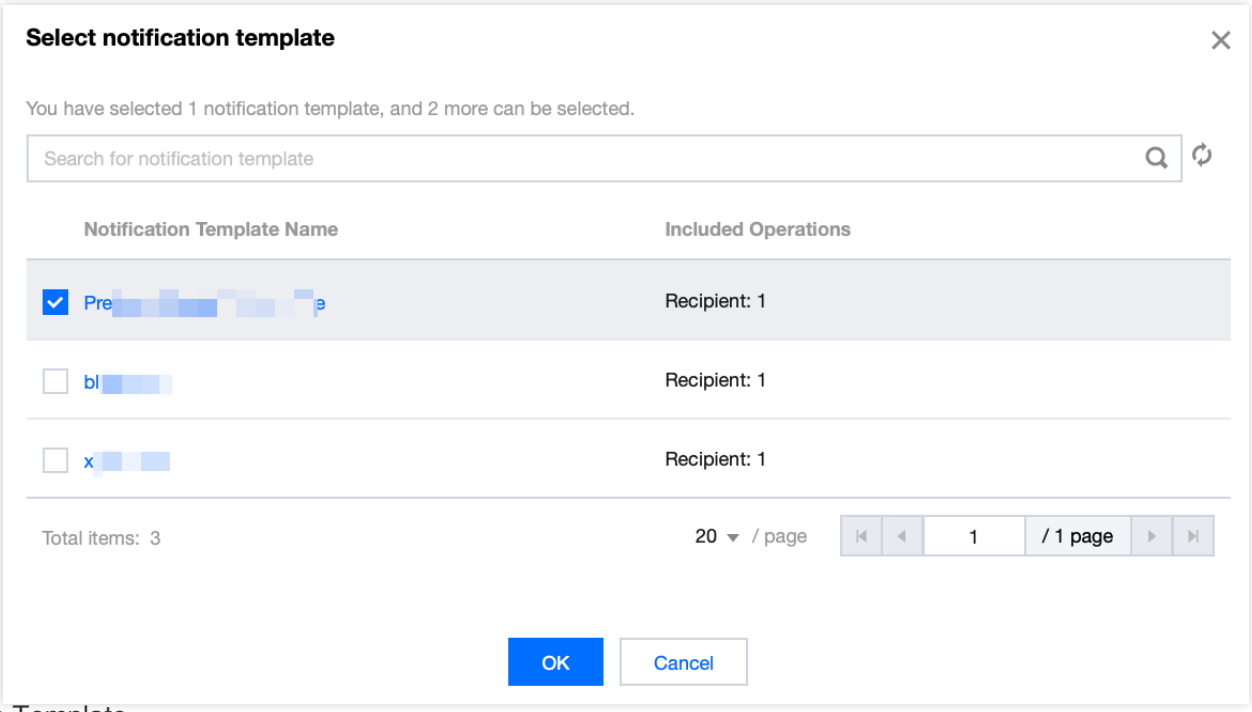
Policy Type: Select **CDB** > **MySQL** > **MASTER**.

Alarm Object: The object instance to be associated can be found by selecting the region where the object is located or searching for the instance ID of the object.

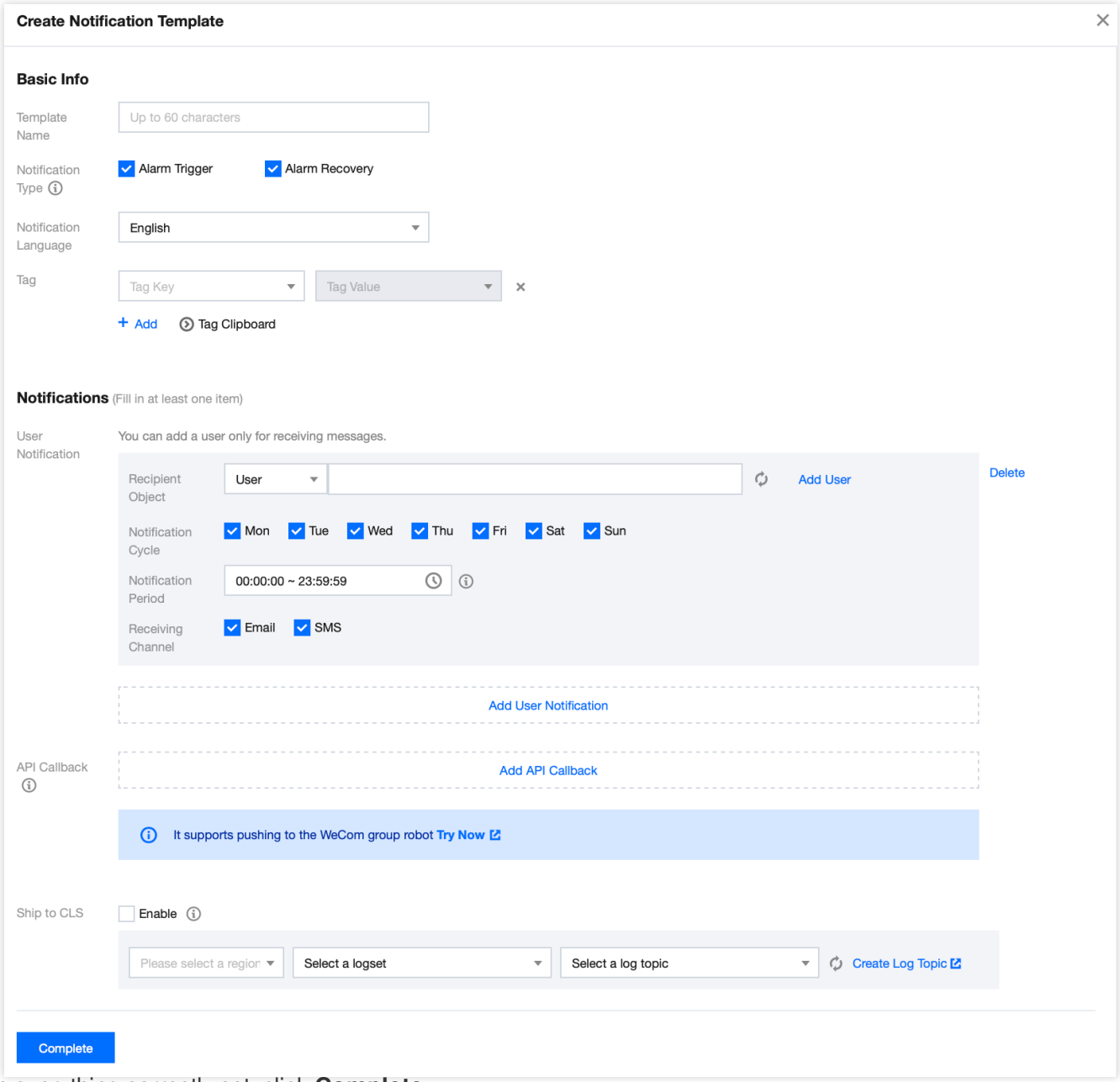
Trigger Condition: Locate "Event Alarm", click **Add Event**, add alarm events **AuditLowRisk**, **AuditMediumRisk**, or **AuditHighRisk** based on the actual risk level for which the alarm is needed.

Configure Alarm Notification: You can select a preset or custom notification template. Each alarm policy can be bound to three notification templates at most. For more information, see Creating Notification Template.

Select Template



Create Template



4. With everything correctly set, click **Complete**.

Associating Alarm Objects

After creating an alarm policy, you can associate it with other alarm objects (those instances which are consistent with the policy). When instances match the rule content in the rule template and have the added risk level, and the alarm policy of the rule template is set to **send alarm**, the generated audit logs will trigger an alarm notification.

1. On the alarm policy list, click the **Policy Name** to enter the alarm policy management page.
2. On the alarm policy management page, click **Add Object** in the **Alarm Object** column.
3. In the pop-up dialog box, select the alarm objects to be associated with, and click **OK**.

Viewing Alarm Records, Managing Alarm Policies (Alarm On-Off), and Silencing Alarms

You can view relevant event alarm histories or manage alarm policies and create silencing alarm through TCOP. For relevant operations, see the following guidelines:

Viewing Alarm Records

Alarm On-Off

Silencing Alarms

Configuring Event Alarms through EB

Step 1: Activating the EB Service

Tencent Cloud EB utilizes Cloud Access Management (CAM) for its permissions management. CAM is a service provided by Tencent Cloud meant to aid users in securely managing the access permissions of resources within their Tencent Cloud accounts. Users can use CAM to create, manage, and terminate users (groups) and employ identity and policy management to govern other user's access to Tencent Cloud resources. To use the EB EventBridge, you must first activate the service on the product page. For information on how to activate this service for your root account and delegate authorization to sub-accounts, see Activating EB.

Step 2: Configuring Event Alarms Related to TencentDB for MySQL Database Audit

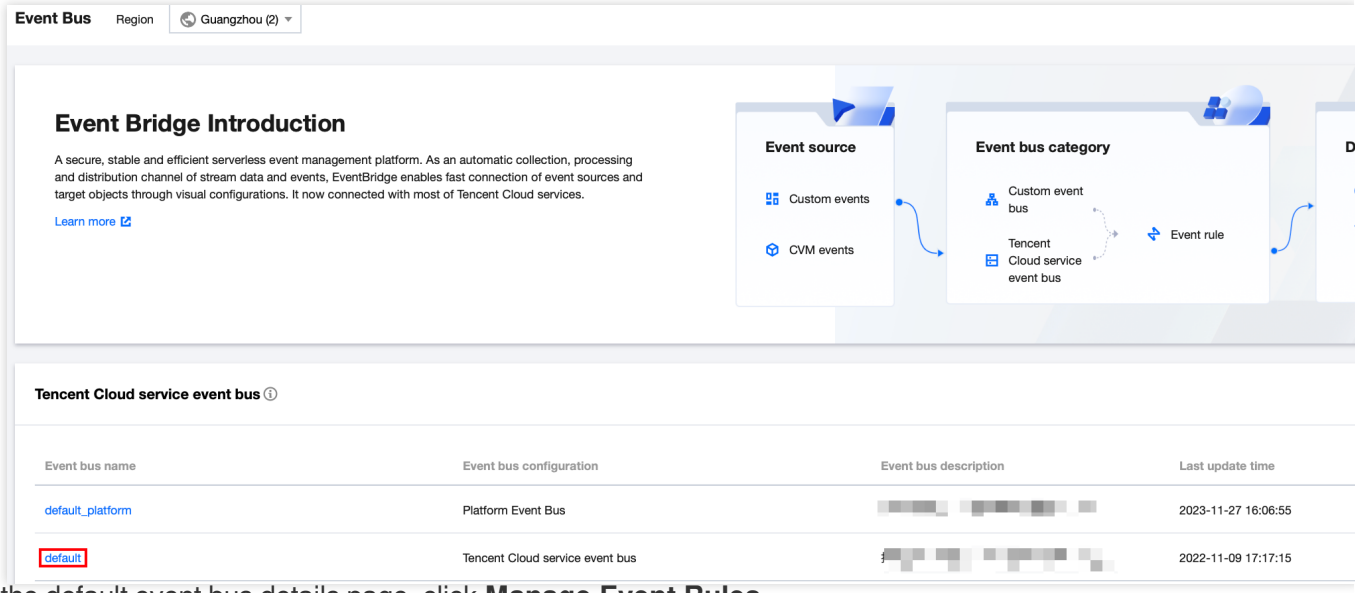
After activating the EB service, you need to select the types of event sources to connect to EB. Currently, you can select monitoring events generated by TencentDB for MySQL database audit as the event source to connect to EB.

Note:

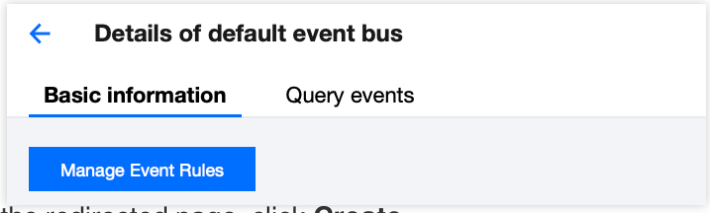
All operational events such as alarms and audits generated by TencentDB for MySQL will be delivered to the **Tencent Cloud service event bus** by default. This process cannot be altered or edited.

Upon activation of Tencent Cloud EB service, a default Tencent Cloud service event bus is automatically created in the **Guangzhou** region. Alarm events (monitoring and auditing events) generated by TencentDB for MySQL will then be automatically delivered to it.

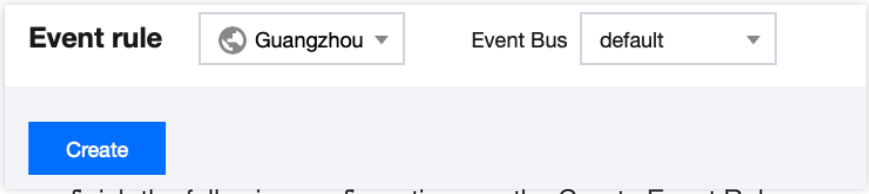
1. Log in to the EB Console.
2. Select the **Guangzhou** region at the top.
3. Click on the **default** event bus under Tencent Cloud service event bus.



4. On the default event bus details page, click **Manage Event Rules**.



5. On the redirected page, click **Create**.



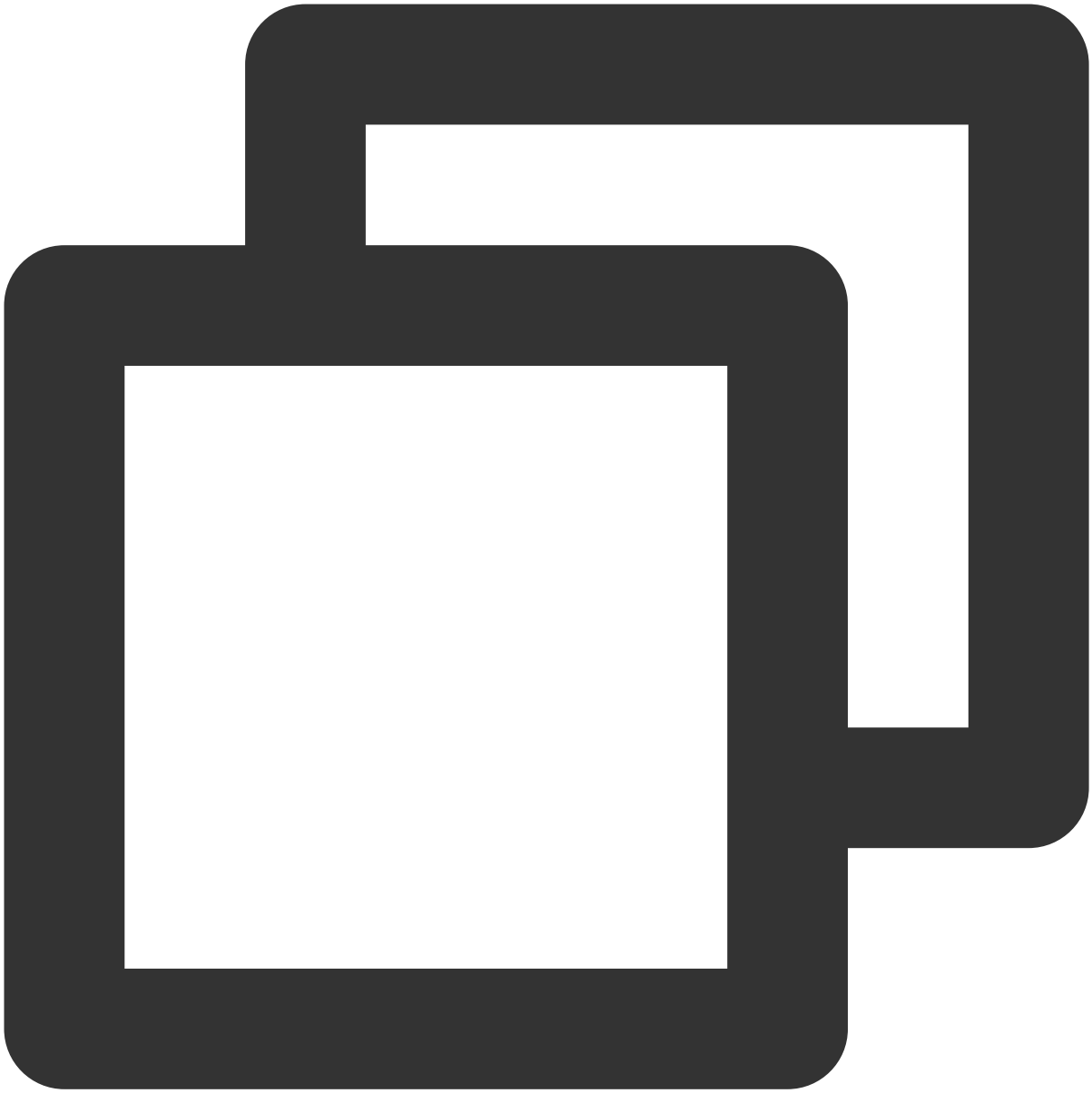
6. After you finish the following configurations on the Create Event Rule page, click **Next**.

Parameter	Description
Rule name	Enter the rule name. It should contain 2-60 characters in the form of letters, digits, underscores, and hyphens. It must start with a letter and end with a digit or a letter.
Rule description	Provide rule description using digits, English and Chinese characters, and commonly used punctuation, not exceeding 200 characters.
Tag	Decide whether to enable the Tag. Once it is enabled, you can add Tags to this event rule.
Data conversion	Event data conversion facilitates easy processing of event content. For example, you can extract, parse, and remap fields in events before delivering them to the event target.
Event sample	An event structure sample is provided for your reference for event matching rule setting-up. You can locate the target template under event examples as a reference point.

Rule pattern	Both form template and custom events are supported, but form template is recommended.
Tencent Cloud service	Choose TencentDB for MySQL.
Event Type	Select the required event types related to database audit alarms (AuditLowRisk, AuditMediumRisk, AuditHighRisk)
Test match rule	Choose the event type template selected in the event example, and then click on test matching rules. If the test passes, proceed to the next step.

Note:

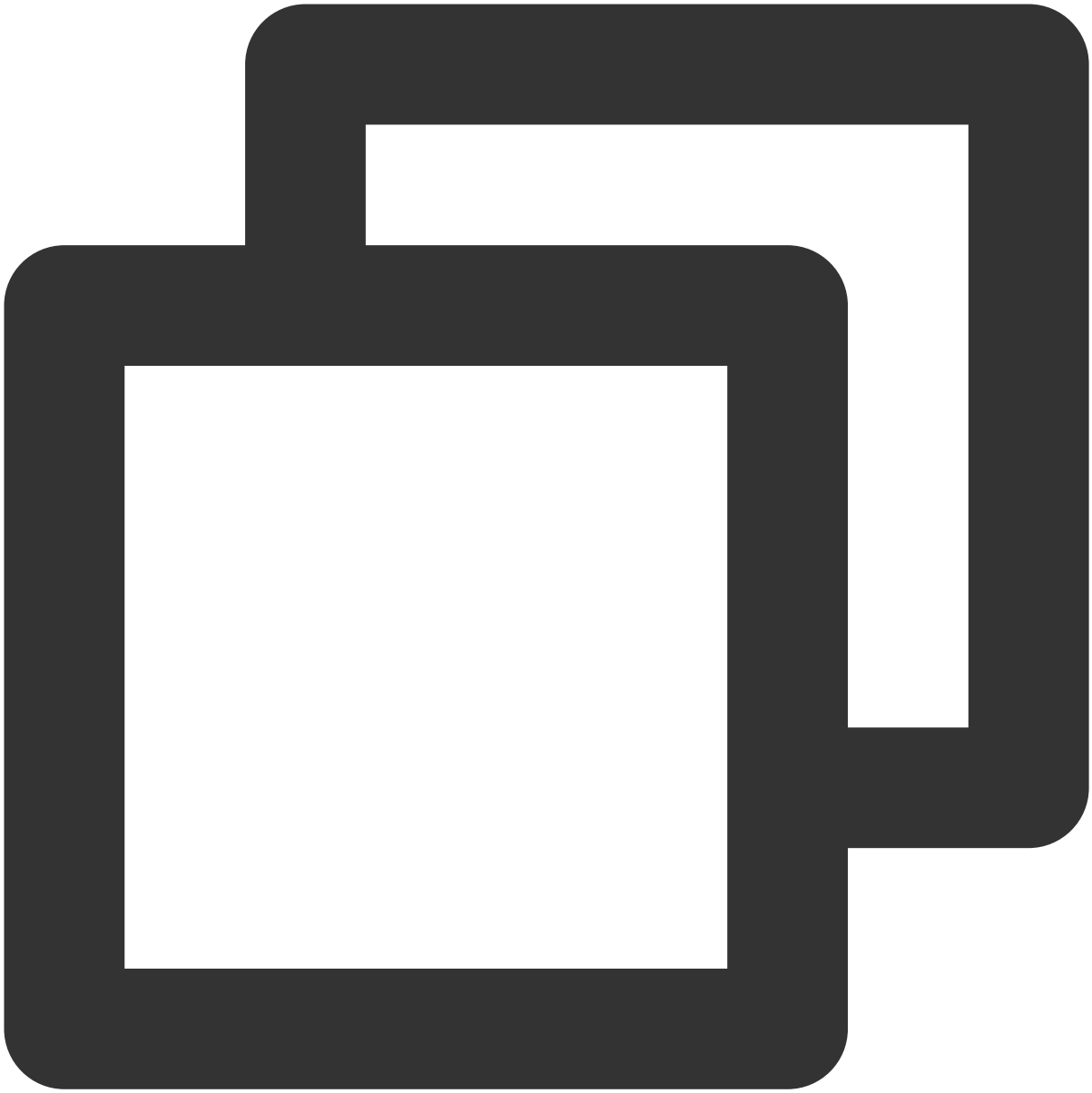
To receive event alarms from specified instances, the rule configuration is as follows:



```
{
  "source":"cdb.cloud.tencent",
  "subject":"ins-xxxxxx"
}
```

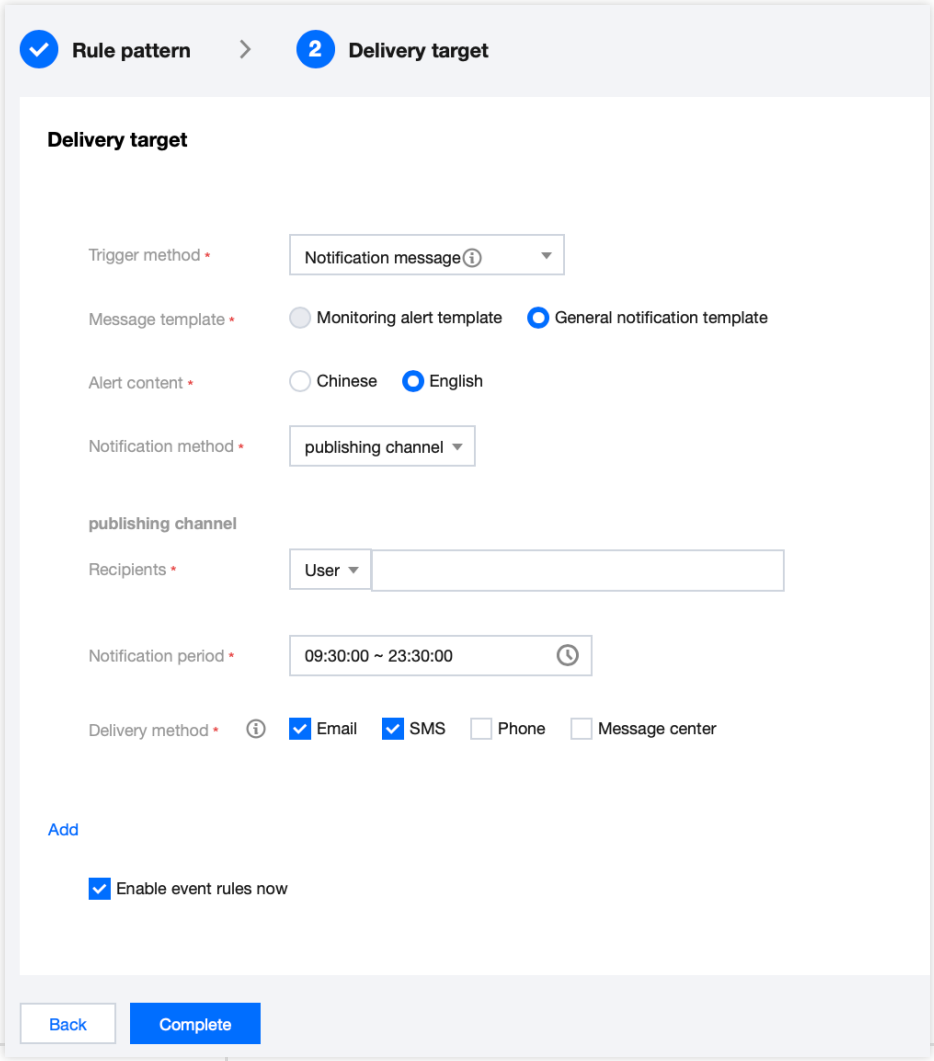
This signifies that only events originating from TencentDB for MySQL with the instance ID of ins-XXX can be disseminated through rule matching. Other events will be discarded and will not reach the user.

An array mode can also be used to match multiple resources:



```
{
  "source":"cdb.cloud.tencent",
  "subject":["ins-xxxxxx","ins-xxxxxx"]
}
```

7. In the event target tab, complete the following configurations, check **Enable event rules now**, and click **Complete**.



Parameter	Description
Trigger method	Choose message notification.
Message template	Support for selecting either a monitoring alarm template or a general notification template.
Alarm content	Support for selecting either Chinese or English.
Notification method	Support for selecting API callback, publishing channel, or all methods. The following settings will use publishing channel as an example.
Recipients	Select a recipient user or user group.
Notification period	Customize the notification period.
Receive method	Select the receive channel. An SMS message is limited to 500 characters, and a phone message is limited to 350 characters. Events with excessively long descriptions (possibly due to causes such as overly lengthy instance names) will not be pushed. You are advised to configure multiple channels concurrently.

Note:

If you need to configure multiple event targets, feel free to click on **Add**.

8. After the event rule is created, you can locate and manage it in the event rule list.

Modifying Audit Rule

Last updated：2024-07-22 13:05:45

This document describes how to modify the audit rule in the console.

Prerequisite

You have enabled the audit service. For more information, see Enabling Audit Service.

Note

The audit rule can be changed from full audit to rule-based audit or vice versa.
After the audit rule is modified, the modification will be applied to the selected instance.
You're allowed to modify the rule type, parameter field, operator, and characteristic string for an audit rule. You can add or remove the items but must keep at least one of them. For detailed directions, see Enabling Audit Service > Set the audit rule.

Modifying the audit rule for one instance

1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, click **Database Audit**.
3. Select **Region** at the top, click the **Audit Instance** tab, and click **Enabled** to filter audit-enabled instances.
4. Find the target instance in the audit instance list, or search for it by resource attribute in the search box, and select **More** > **Modify Audit Rule** in the **Operation** column.
5. In the **Modify Audit Rule** window, modify the audit rule and click **OK**.

Batch modifying the audit rule

Note:
The audit rule can be changed from full audit to rule-based audit or vice versa.
After the audit rule is modified, the modification will be applied to the selected instance.
You're allowed to modify the rule type, parameter field, operator, and characteristic string for an audit rule. You can add or remove the items but must keep at least one of them. For detailed directions, see Enabling Audit Service > Set the audit rule.

1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, click **Database Audit**.
3. Select **Region** at the top, click the **Audit Instance** tab, and click **Enabled** to filter audit-enabled instances.
4. Find the target instances in the audit instance list, or search for them by resource attribute in the search box. Then, click **Modify Audit Rule** above the list.
5. In the **Modify Audit Rule** window, modify the audit rule and click **OK**.

Note:

The **Batch Modify Audit Rule** window displays the audit rules both before and after the modification to make comparisons easier. The new rules will be applied to the selected instances. Therefore, proceed with caution.

Modifying Audit Services

Last updated：2023-12-06 15:06:08

This document describes the procedure of modifying the audit service on the console.

Note：

If you choose to extend the log retention period, the change will be enforced immediately. If you choose to shorten the log retention period, logs that have exceeded their storage period will be cleaned immediately.

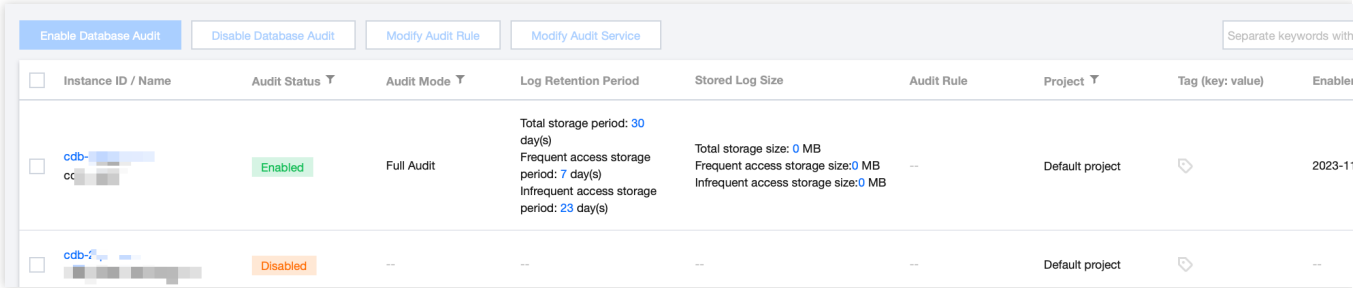
If you configure that data in recent n days is stored in the frequent access storage, data exceeding the n days threshold will be automatically reallocated to the infrequent access storage. As the duration of frequent access storage extends, audit data compliant with the retention duration will be automatically migrated from infrequent to frequent access storage.

Prerequisites

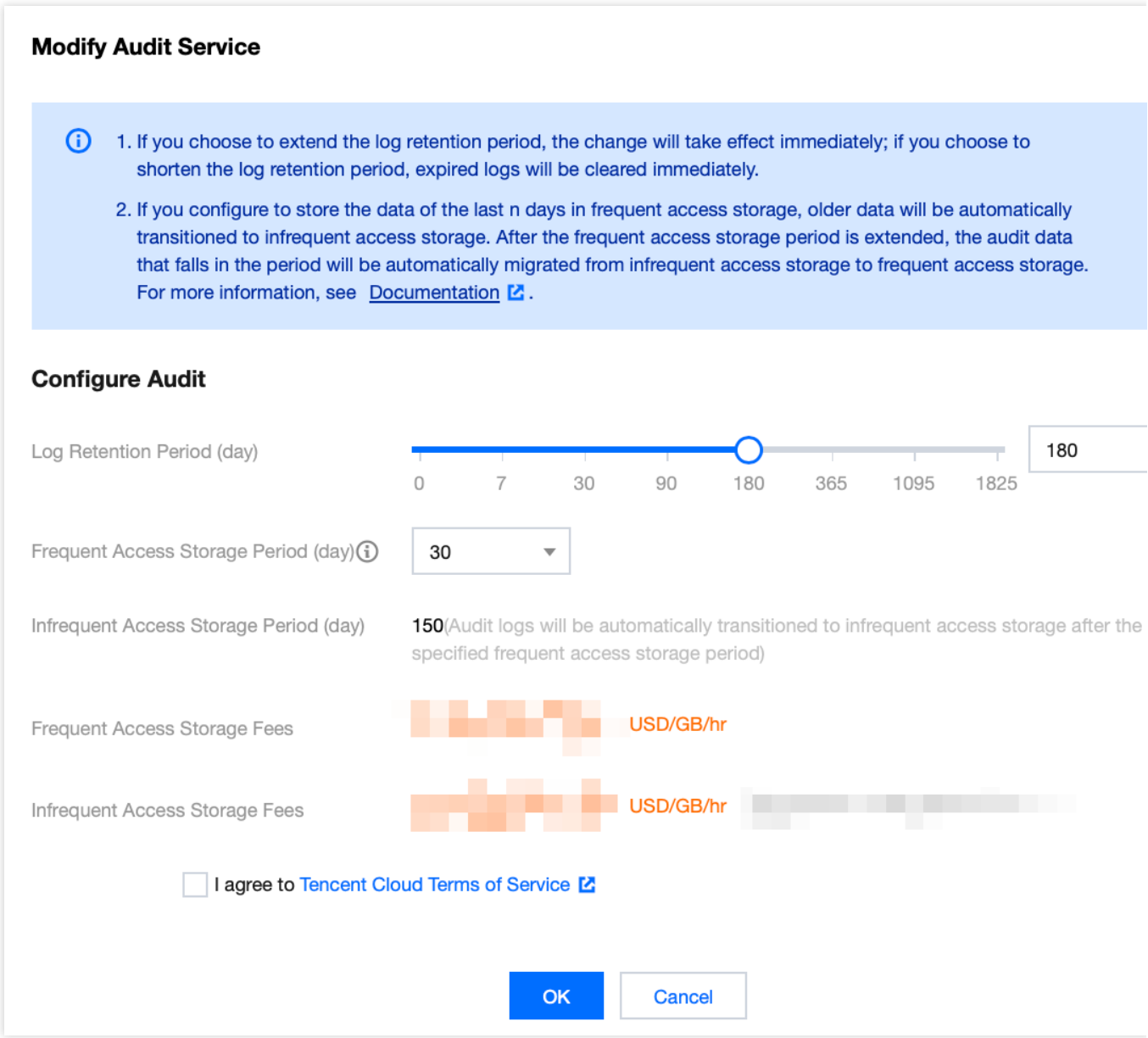
You have enabled the audit service. For more information, see Enabling Audit Service.

Modifying the Audit Service of one Individual Instance

1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, choose **Database Audit**.
3. After selecting the desired **Region** at the top, proceed to the **Audit Instances** page, and then click **Audit Status** and select the **Enabled** option to filter the instances with audit enabled.
4. Locate the target instance in the **Audit Instances** list (or you can quickly find it by filtering resource attributes in the search box), and in the **Operation** column, select **More** > **Modify Audit Service**.

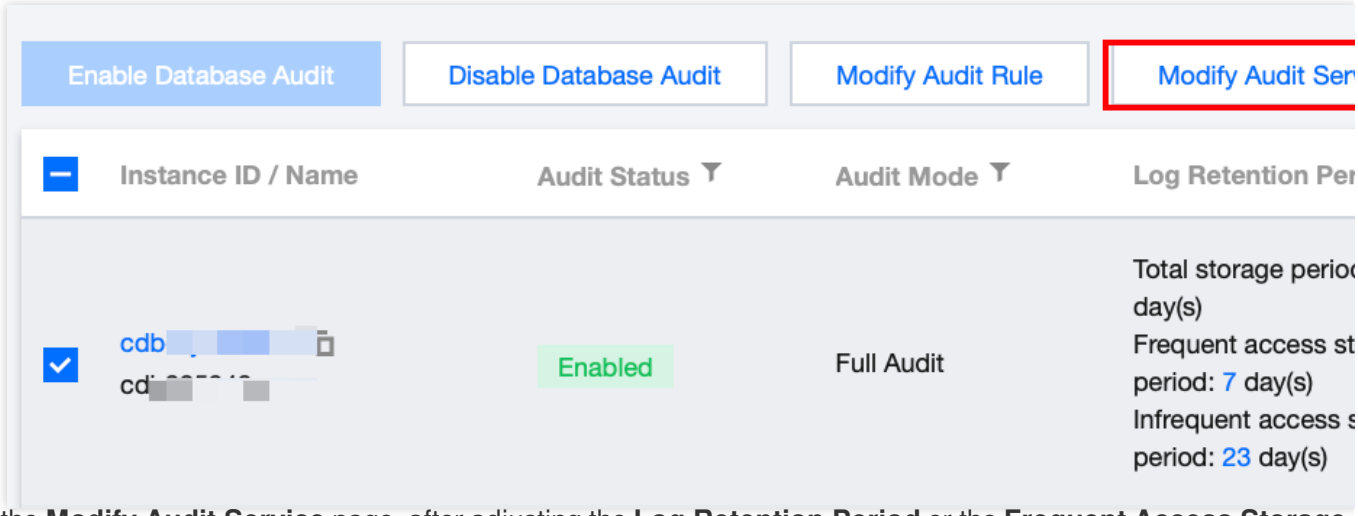


5. On the **Modify Audit Service** page, after adjusting the **Log Retention Period** or the **Frequent Access Storage Period**, click **OK**.



Modifying Audit Services in Batches

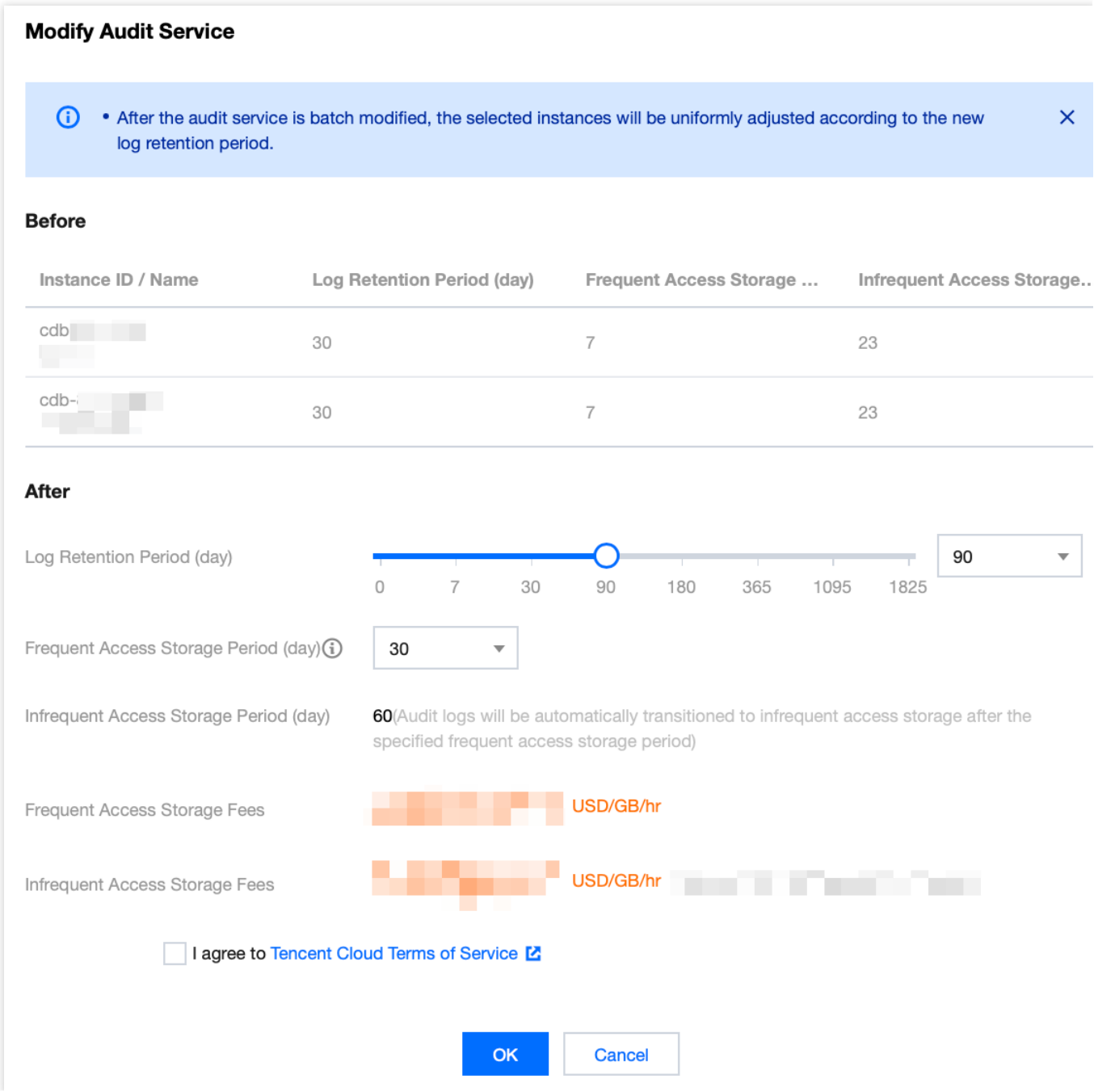
1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, choose **Database Audit**.
3. After selecting a **Region** at the top, click on **Audit Status** and select **Enabled** on the **Audit Instances** page to filter instances without active audit process.
4. Find the target instances in the **Audit Instance** list, or expediently locate them using resource attribute filters in the search bar. On the **Audit Instance** page, select multiple target instances, and then click **Modify Audit Service** located above the list.



5. On the **Modify Audit Service** page, after adjusting the **Log Retention Period** or the **Frequent Access Storage Period**, click **OK**.

Note：

For ease of comparison, the Batch Modify Audit Service page will display the log retention period both before and after modification. After the adjustment, the selected instances will collectively begin to adapt to the new log retention period. Therefore, ensure the modifications are accurate before proceeding.



Disabling Audit Service

Last updated：2024-07-22 13:06:08

This document describes how to disable the audit service in the console.

Note:

After the audit service is disabled, instances will no longer be audited, and historical audit logs will be cleared.

Prerequisite

You have enabled the audit service. For more information, see Enabling Audit Service.

Directions

1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, click **Database Audit**.
3. Select **Region** at the top, click **Audit Instance** tab, click **Audit Status**, and click **Enabled** to filter the audit-enabled instances.
4. Find the target instance in the **Audit Instance** list, or search for it by resource attribute in the search box, and select **More** > **Disable** in the **Operation** column.

Note:

You can batch disable the audit service for multiple target instances by selecting them in the audit instance list and clicking **Disable Database Audit** above the list.

5. In the **Disable Database Audit** window, confirm that everything is correct and click **OK**.
6. After confirmation, the disablement result will be displayed in the result column. You can click **View Task** to enter the task list and view the details.

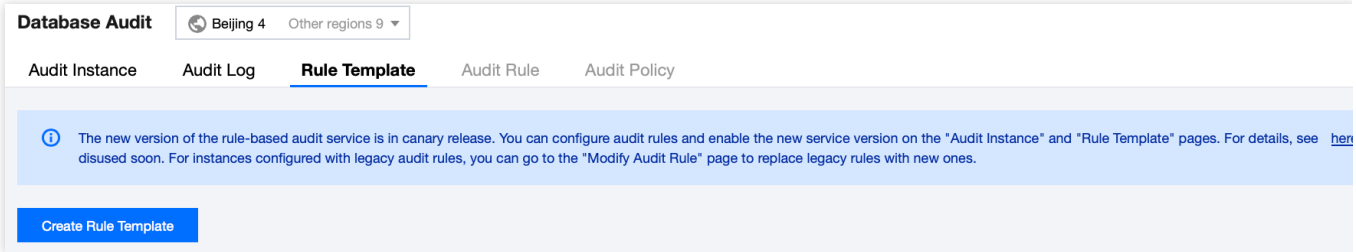
Audit Rule Template
Viewing Rule Template List

Last updated：2023-11-28 19:36:51

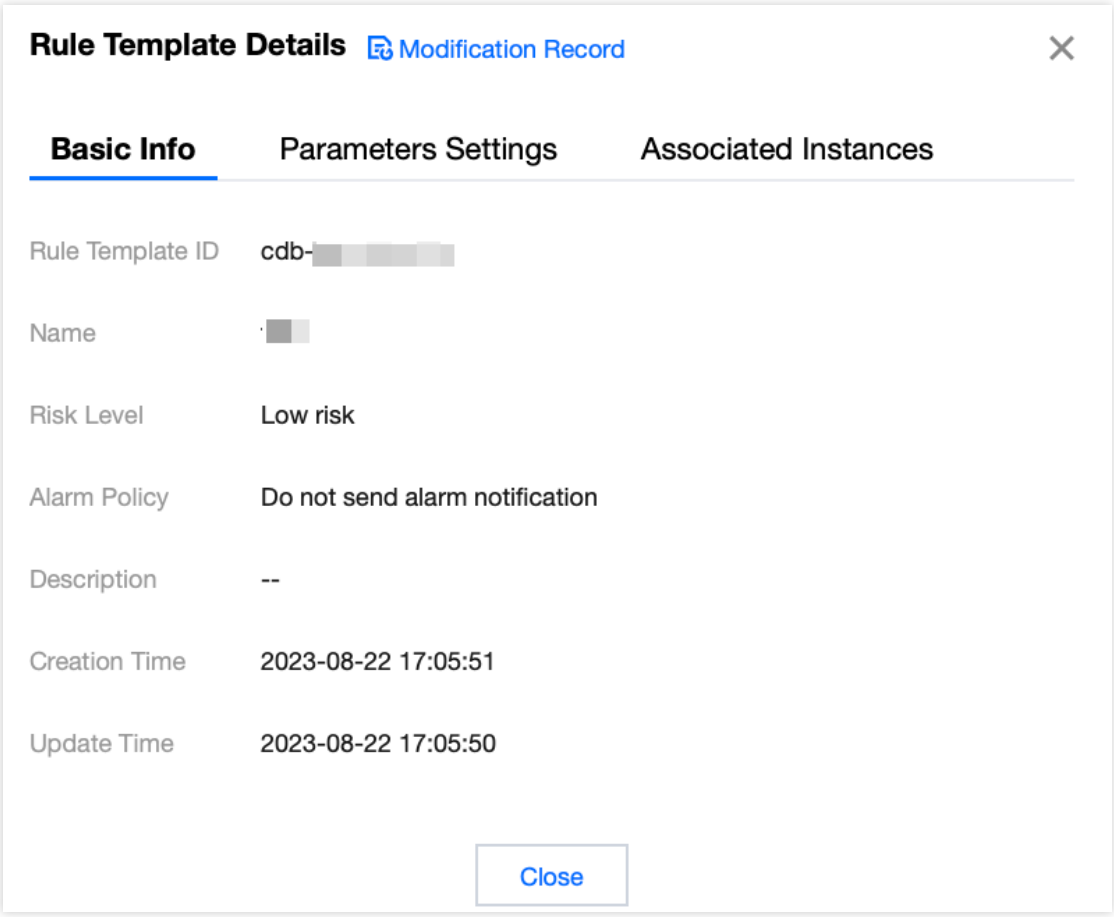
This document describes how to view the rule template list in the console.

Viewing the rule template list and template details

1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, click **Database Audit**.
3. Select a **region** and click **Rule Template**.



4. Find the target rule template in the **rule template** list, or search for it by resource attribute in the search box, and click **Details** in the **Operation** column.
5. In the pop-up window, you can switch to view **Basic Information**, **Parameter Settings**, **Associated Instances**, and **Modification History** of the rule template.



Tool list

Tool	Description
Search box	You can click to filter rule templates by resource attributes such as ID and name. Separate multiple keywords by vertical bar "
Revision History	Click to navigate to the Revision History page where you can globally view the history of any changes made to the rule templates in a specific region.
Refresh	You can click to refresh the list.

Template list fields

Field	Description
Rule Template ID	ID of the rule template.
Name	Name of the rule template.
Associated Instances	Displays the number of instances associated with the respective rule template. Clicking on the number of instances reveals detailed information about the associated instances, including Instance ID, audit types, and more.
Risk Level	Displays the risk level (low, medium, high) of the respective rule template and supports filtering.
Alarm Policy	Displays the alarm policy (No Alarm, Send Alarm) of the corresponding rule template and supports filtering.
Description	Remarks of the rule template.
Creation Time	Creation time of the rule template in the format of year-month-day hour:minute:second.
Operation	Details, where you can view the **Basic Information**, **Parameter Settings**, **Associated Instances**, and **Modification History** of the rule template. Edit, where you can modify the content of the rule template. Delete, to remove the rule template.

Relevant operations

Creating Rule Template

Modifying Rule Template

Deleting Rule Template

Creating Rule Template

Last updated：2024-08-16 11:08:24

This document describes how to create a rule template in the console.

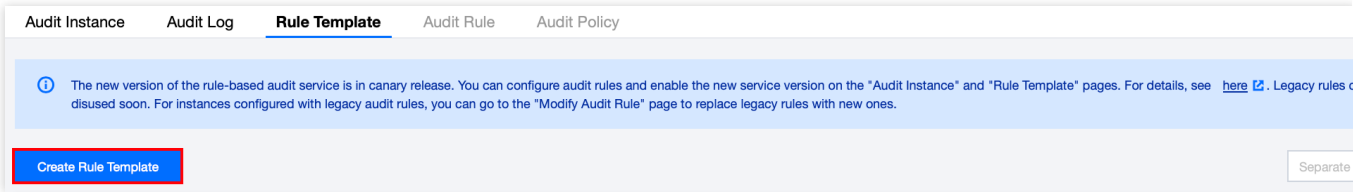
Note:

Starting from September 202325, the relationship between rule templates and audit instances has transitioned from **initialization** to **strong association**. Alterations to the rule template content will **synchronously impact** the audit rules applied to the instances bound to the said rule template.

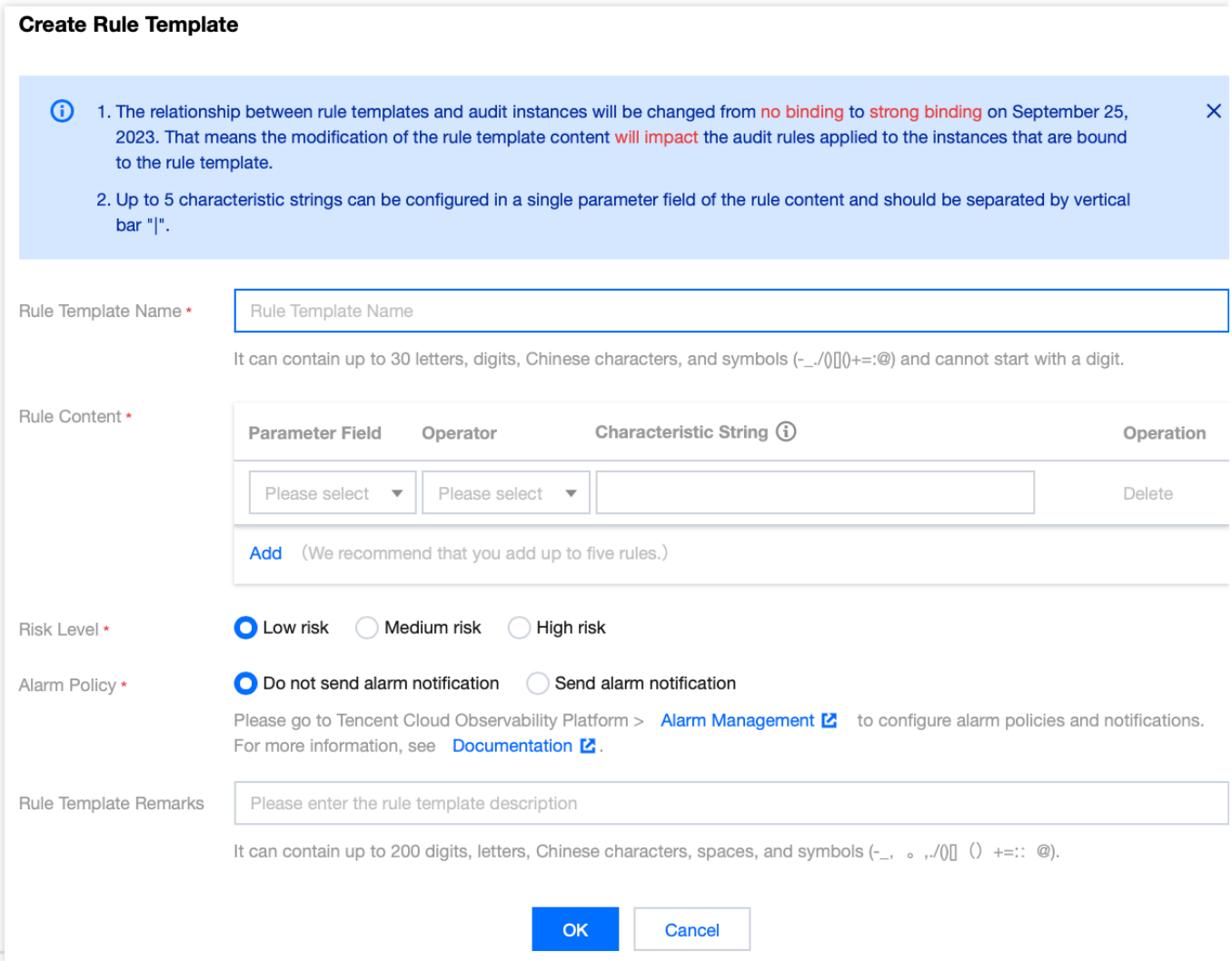
A rule template allows up to 5 characteristic strings for a single parameter field, with each string being separated by vertical bar "|".

Directions

1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, click **Database Audit**.
3. Select **Region** and click **Rule Template**.
4. In the template list, click **Create Rule Template**.



5. In the **Create Rule Template** window, set the following configuration items and click **OK**.



Parameter	Description
Rule Template Name	This field can contain up to 30 letters, digits, and symbols -_./()[] （） += ：:@ and cannot start with a digit.
Rule Content	This fields sets the rule content (parameter field, operator, characteristic string). For detailed instructions, see the Rule content details and examples. **Note:** Under the section of rule content, one can augment parameter fields by clicking on 'Add'. Within the operation column under the rule content, unnecessary parameter fields and conditions can be eliminated by clicking 'Delete'. However, at least one parameter field and condition must be retained.
Risk Level	Select a risk level for the newly created rule template, with options including low risk, medium risk, and high risk.
Alarm Policy	Choose an alarm policy for the newly created rule template, with options of either refraining from sending alarms or sending alarms. **Note:**

	Please go to TCOP->Alarm Management to set alarm rules and notifications. For detailed information, refer to Post-Event Alarm Configuration.
Rule Template Remarks	This field can contain up to 200 letters, digits, and symbols-_./()[]（）+=：:@ and cannot start with a digit.

Rule content details and examples

Note

You can configure one or multiple rules. Up to 5 rules can be configured.

Different rules are in **AND** relationship; that is, they need to be met at the same time.

Different characteristic strings in a rule are in **OR** relationship; that is, at least one of them needs to be met.

You can add only one operator for the same parameter field; for example, for the database name, the operator can be either **Include** or **Exclude**.

Parameter Field	Operator	Characteristic String
Client IP	Include, Exclude, Equal to, Not equal to, Regex	Up to five client IPs can be configured and should be separated by vertical bar "|". When the operator is **Regex**, only one characteristic string can be entered.
User Account	Include, Exclude, Equal to, Not equal to, Regex	Up to 5 user accounts can be configured, separated by English vertical bars. When the match type is regular expression, only one feature string is supported.
Database Name	Include, Exclude, Equal to, Not equal to, Regex	Up to five database names can be configured and should be separated by vertical bar "|". When the operator is **Regex**, only one characteristic string can be entered.
SQL Details	Include, Exclude	Up to five SQL commands can be configured and should be separated by vertical bar "|".
SQL Type	Equal to, Not equal to	Up to five SQL types can be selected. Valid options: ALTER, CHANGEUSER, CREATE, DELETE, DROP, EXECUTE, INSERT, LOGIN, LOGOUT, OTHER, REPLACE, SELECT, SET, UPDATE.
Affected Rows	Greater than, Less than	Select affected rows
Returned Rows	Greater than, Less than	Select returned rows

Scanned Rows	Greater than, Less than	Select scanned rows
Execution Time	Greater than, Less than	Select execution time, with the unit being millisecond.

Example: If the following rule content is set, the database name should include `a`, `b`, or `c`, and the client IP should include IP1, 2 or 3, then the audit logs filtered by the rule are those where the database name includes `a`, `b`, or `c` and the client IP includes IP1, 2, or 3.

Modifying Rule Template

Last updated：2024-08-16 11:06:28

This document describes how to modify a database audit rule template in the console.

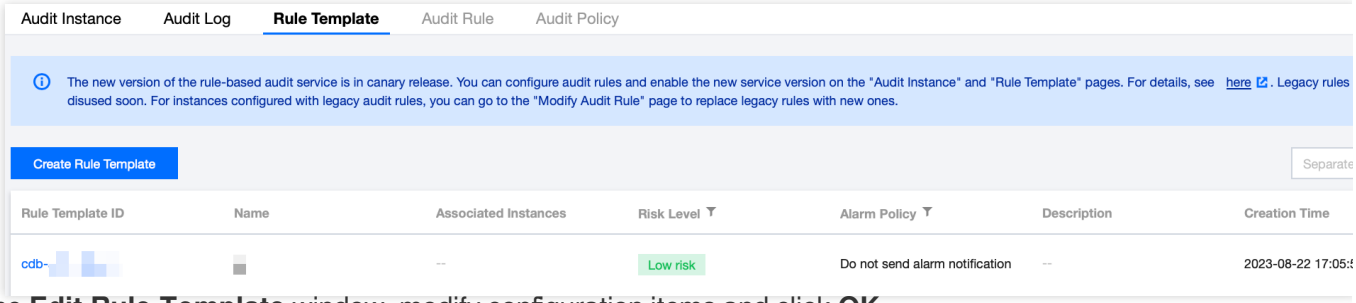
Note：

Starting from September 202325, the relationship between rule templates and audit instances has transitioned from **initialization** to **strong association**. Alterations to the rule template content will **synchronously impact** the audit rules applied to the instances bound to the said rule template.

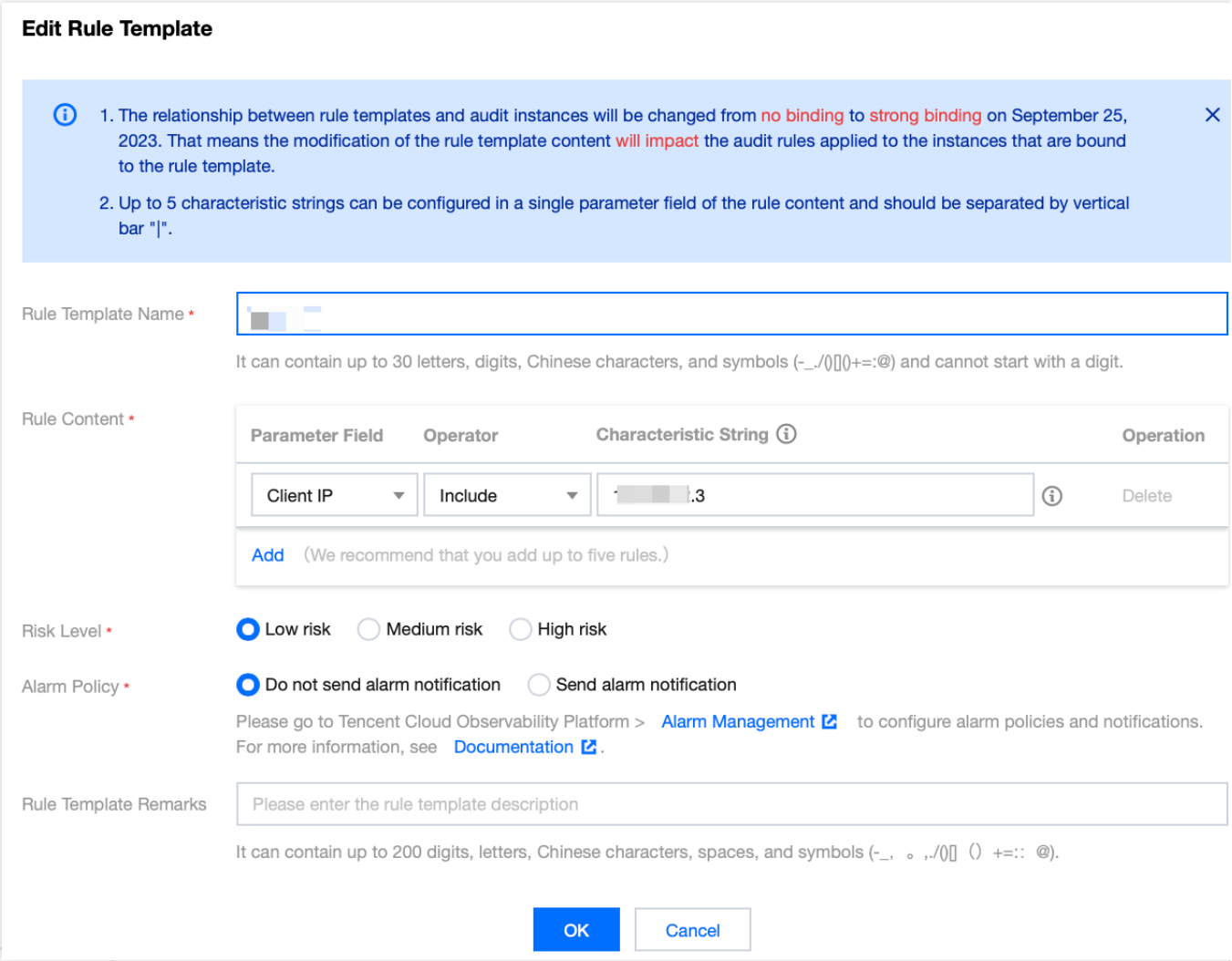
A rule template allows up to 5 characteristic strings for a single parameter field, with each string being separated by vertical bar "|".

Directions

1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, click **Database Audit**.
3. Select **Region** and click **Rule Template**.
4. Find the target rule template in the **rule template** list, or search for it by resource attribute in the search box, and click **Edit** in the **Operation** column.



5. In the **Edit Rule Template** window, modify configuration items and click **OK**.



Parameter	Description
Rule Template Name	This field can contain up to 30 letters, digits, and symbols -_./()[] （） += ：:@ and cannot start with a digit.
Rule Content	Specify the rule content, including parameters, matching types, and feature strings. For detailed descriptions and examples, see Rule Content Details and Examples . **Note:** You can click 'Add' under Rule Content to include additional parameter fields. You can click 'Delete' in the action column under Rule Content to remove unnecessary parameter fields and conditions, although at least one parameter field and condition must remain.
Risk Level	Choose a risk level for this rule template. Options include Low Risk, Medium Risk, and High Risk.
Alarm Policy	Choose an alarm policy for this rule template. Options include 'Do Not Send Alarms' and 'Send Alarms'. **Note:**

	Please go to TCOP->Alarm Management to set alarm rules and notifications. For detailed information, refer to Post-Event Alarm Configuration.
Rule Template Remarks	This field can contain up to 200 letters, digits, and symbols-_./()[]（）+=：:@ and cannot start with a digit.

Rule content details and examples

Note:

You can configure one or multiple rules. Up to 5 rules can be configured.

Different rules are in **AND** relationship; that is, they need to be met at the same time.

Different characteristic strings in a rule are in **OR** relationship; that is, at least one of them needs to be met.

You can add only one operator for the same parameter field; for example, for the database name, the operator can be either **Include** or **Exclude**.

Parameter Field	Operator	Characteristic String
Client IP	Include, Exclude, Equal to, Not equal to, Regex	Up to five client IPs can be configured and should be separated by vertical bar "|". When the operator is **Regex**, only one characteristic string can be entered.
User Account	Include, Exclude, Equal to, Not equal to, Regex	Up to 5 user accounts can be configured, separated by English vertical bars. When the match type is regular expression, only one feature string is supported.
Database Name	Include, Exclude, Equal to, Not equal to, Regex	Up to five database names can be configured and should be separated by vertical bar "|". When the operator is **Regex**, only one characteristic string can be entered.
SQL Details	Include, Exclude	Up to five SQL commands can be configured and should be separated by vertical bar "|".
SQL Type	Equal to, Not equal to	Up to five SQL types can be selected. Valid options: ALTER, CHANGEUSER, CREATE, DELETE, DROP, EXECUTE, INSERT, LOGIN, LOGOUT, OTHER, REPLACE, SELECT, SET, UPDATE.
Affected Rows	Greater than, Less than	Select affected rows.

Returned Rows	Greater than, Less than	Select returned rows.
Scanned Rows	Greater than, Less than	Select scanned rows.
Execution Time	Greater than, Less than	Select execution time, with the unit being millisecond.

Example: If the following rule content is set, the database name should include `a`, `b`, or `c`, and the client IP should include IP1, 2 or 3, then the audit logs filtered by the rule are those where the database name includes `a`, `b`, or `c` and the client IP includes IP1, 2, or 3.

Deleting Rule Template

Last updated：2023-11-28 20:01:25

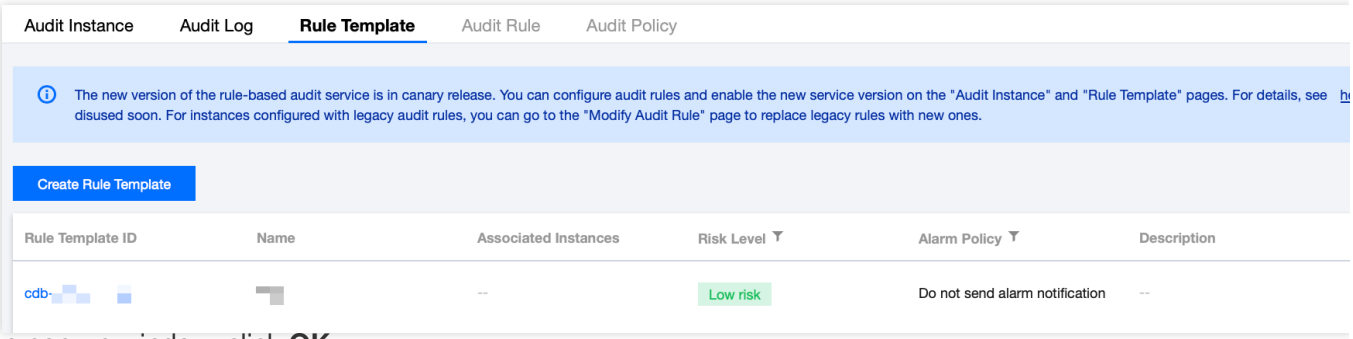
This document describes how to delete a database audit rule template in the console.

Note：

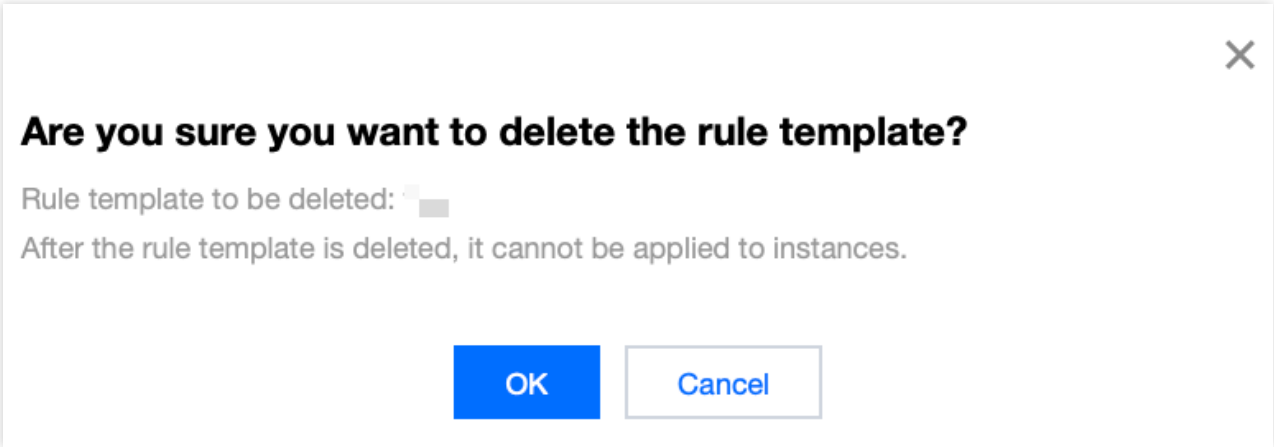
Should a rule template be associated with an instance, deletion is not supported. Only when a rule template is not bound to any instance can it be removed. Once a rule template is deleted, it can no longer be applied to instances.

Directions

1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, click **Database Audit**.
3. Select **Region** and click **Rule Template**.
4. Find the target rule template in the rule template list, or search for it by resource attribute in the search box, and click **Delete** in the **Operation** column.



5. In the pop-up window, click **OK**.



SQL Audit Rule (Legacy)

Last updated：2024-08-16 11:21:10

This document describes the TencentDB for MySQL audit rules.

Note:

The old version of audit rules and audit policies went offline on August 9, 2024. For instances that have previously enabled the old version of audit rules, their audit rules should be adjusted through modifying audit rules. After modification, audit and log storage will be performed for these instances in accordance with the new version of audit rules. For more details, refer to the announcement on the rule-based audit feature of database audit.

Rule Content

The following types are supported:

Client IP, database account, and database name. Supported operators are **Include**/ **Exclude**.

The full audit rule is a special rule, and all statements will be audited after it is enabled.

Rule Operation

The different fields in each rule add the conditions; that is, the relationship between field and condition is "AND" (&&). The relationship between rules is "OR" (||).

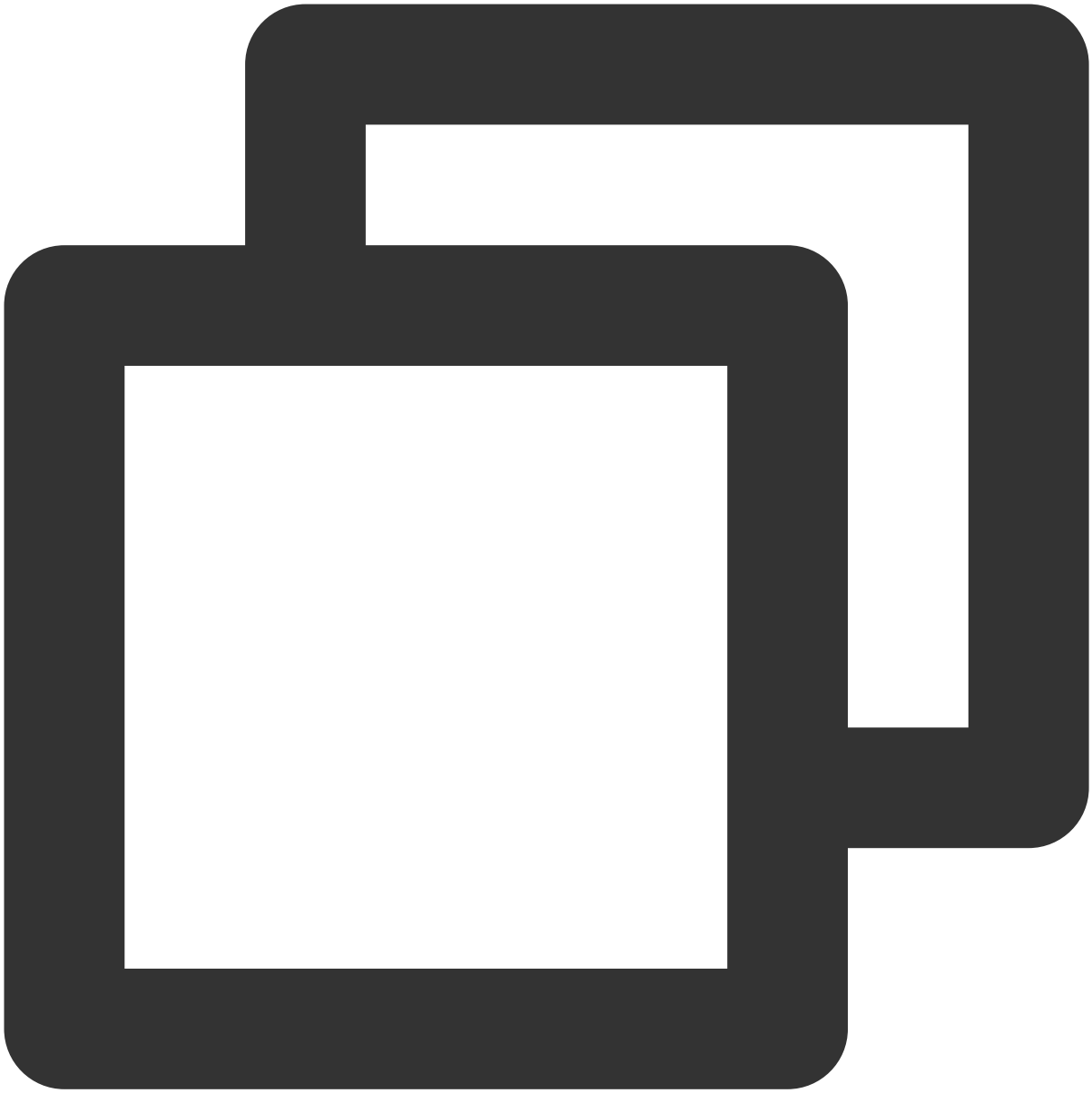
You can specify one or more audit rules for an instance, and as long as any one of them is met, the instance should be audited. For example, if rule A specifies that only operations of user1 with an execution time >= 1 second need to be audited, and rule B audits the statements of user1 with an execution time < 1 second, then all statements of user1 need to be audited eventually.

Rule Description

Client IP, database account, and database name support **Include**/**Exclude** operators, and only one operator can be set at a time.

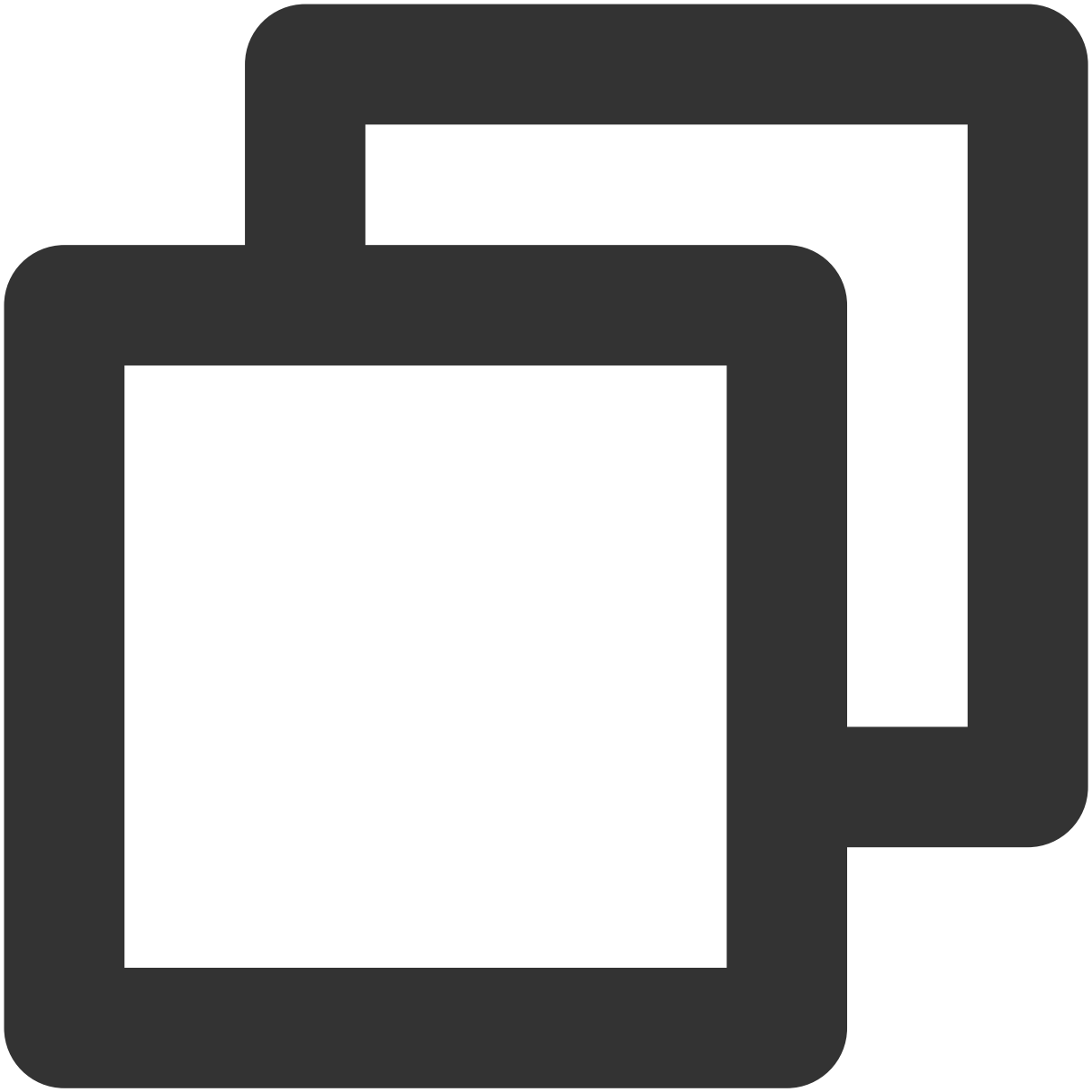
Database name description

If a statement is of the following table object type:



```
SQLCOM_SELECT, SQLCOM_CREATE_TABLE, SQLCOM_CREATE_INDEX, SQLCOM_ALTER_TABLE,
SQLCOM_UPDATE, SQLCOM_INSERT, SQLCOM_INSERT_SELECT, SQLCOM_DELETE, SQLCOM_TRUNCATE,
```

Then, for this type of operation, the name of the database actually manipulated by the statement shall prevail. For example, if the currently used database is "db3", and the statement is:



```
select *from db1.test,db2.test;
```

Then, "db1" and "db2" will be used as the target database for rule judgment. If the rule is configured to audit "db1", "db1" will be audited, and if the rule is configured to audit "db3", "db3" will not be audited.

For statements not of the above table object type, the currently used database will be used as the target database for rule judgment. For example, if the currently used database is "db1", and the executed statement is `show databases` , then "db1" will be used as the target database for judgment. If the rule is configured to audit "db1", "db1" will be audited.

Note

You can write only one value for "Include" and "Exclude" operator. If you write multiple values, they will be treated as a string, resulting in incorrect matching.

Viewing Audit Task

Last updated：2024-07-22 13:07:00

This document describes how to view the details and progress of an audit task in the console, such as enabling/disabling/modifying the audit service and modifying the audit rule.

Viewing Task Types

In the task list, you can view the following types of audit tasks: enabling/disabling/modifying the database audit service, modifying the audit rule, and modifying/deleting an audit rule template.

Viewing Audit Task

1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, click **Task List**.
3. Select **Region** at the top.
4. Directly find the target audit task in the **Task List** or search for it by keyword to view its details.

Searching by Keyword

In the task list, you can search for the target task by task ID and instance ID/name. Separate multiple keywords by vertical bar "|" and separate filter tags by carriage return.

Downloading Task Data

Click the

icon next to the search box to download the data on the current page or under the current search criteria.

Viewing Task Details

In the task list, find the target audit task and click **Task Details** in the **Operation** column.

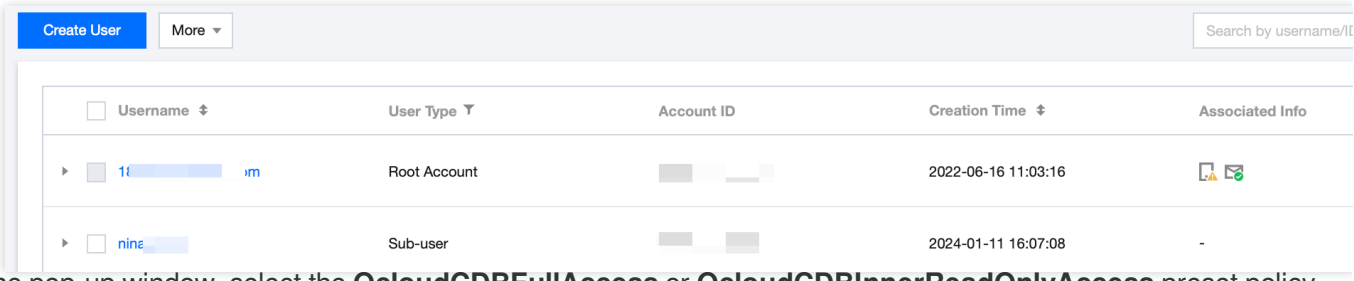
Authorizing Sub-User to Use Database Audit

Last updated：2024-02-18 11:34:11

By default, sub-users have no permission to use TencentDB for MySQL database audit. Therefore, you need to create policies to allow sub-users to use it.
If you don't need to manage sub-users' access to resources related to TencentDB for MySQL Database Audit, you can ignore this document.
Cloud Access Management (CAM) is a web-based Tencent Cloud service that helps you securely manage and control access permissions to your Tencent Cloud resources. Using CAM, you can create, manage, and terminate users (groups), and control the Tencent Cloud resources that can be used by the specified user through identity and policy management.
You can use CAM to bind a user or user group to a policy which allows or denies them access to specified resources to complete specified tasks.For more fundamental information regarding CAM policies, please refer to Policy Syntax.

Authorizing Sub-User

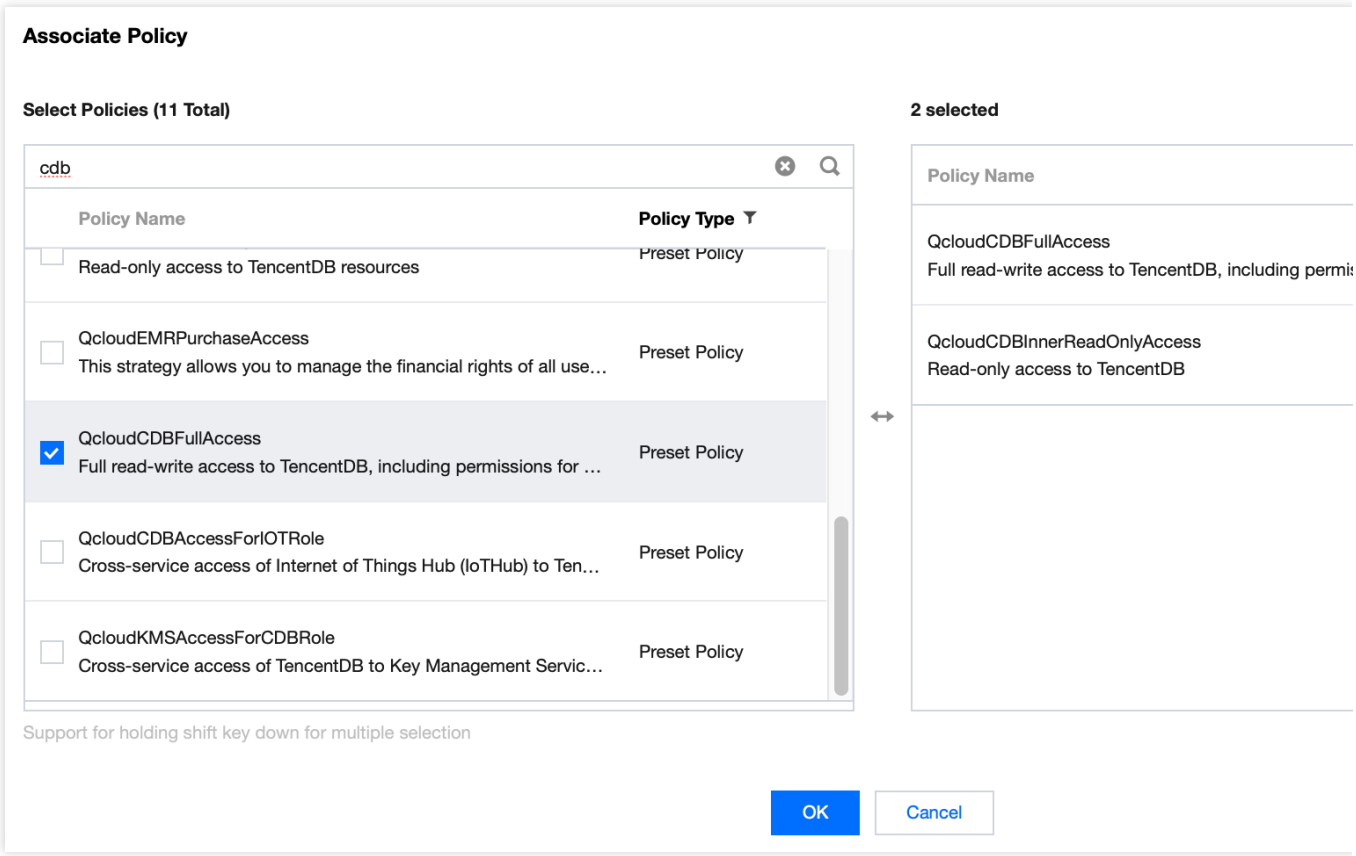
1. Log in to the CAM console with the root account, locate the target sub-user in the user list, and click **Authorize**.



2. In the pop-up window, select the **QcloudCDBFullAccess** or **QcloudCDBInnerReadOnlyAccess** preset policy and click **OK** to complete the authorization.

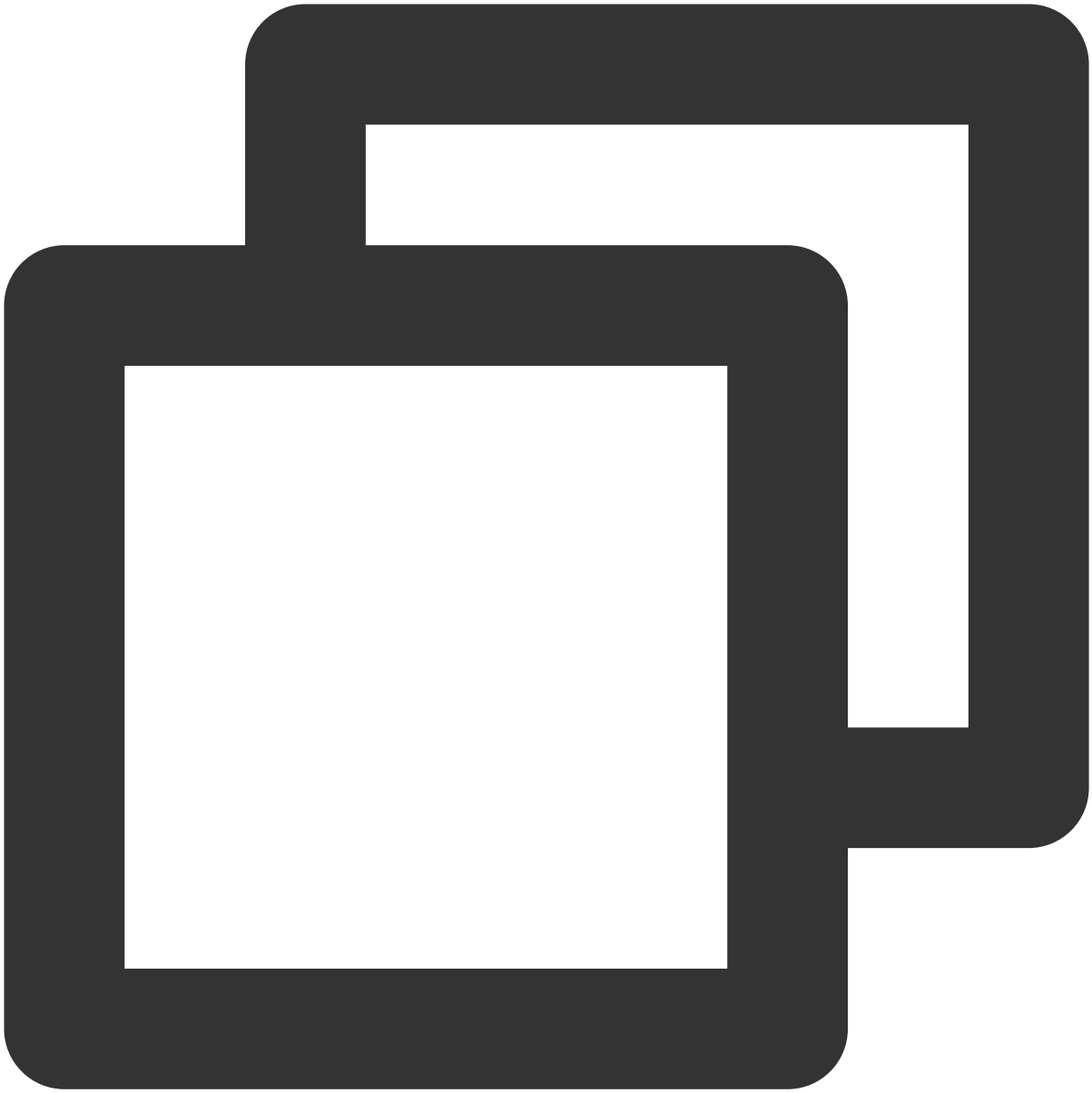
Note:

MySQL Database Audit is a module in TencentDB for MySQL, so the above two preset policies of TencentDB for MySQL already cover the permission policies required by it. If the sub-user only needs the permission to use this module, see Custom MySQL Database Audit Policy.



Policy Syntax

The CAM policy for MySQL Database Audit is described as follows:



```
{
        "version":"2.0",
        "statement":
        [
            {
                "effect":"effect",
                "action":["action"],
                "resource":["resource"]
            }
        ]
}
```

version is required. Currently, only the value "2.0" is allowed.

statement describes the details of one or more permissions. It contains a permission or permission set of multiple other elements such as `effect` , `action` , and `resource` . One policy has only one `statement` .

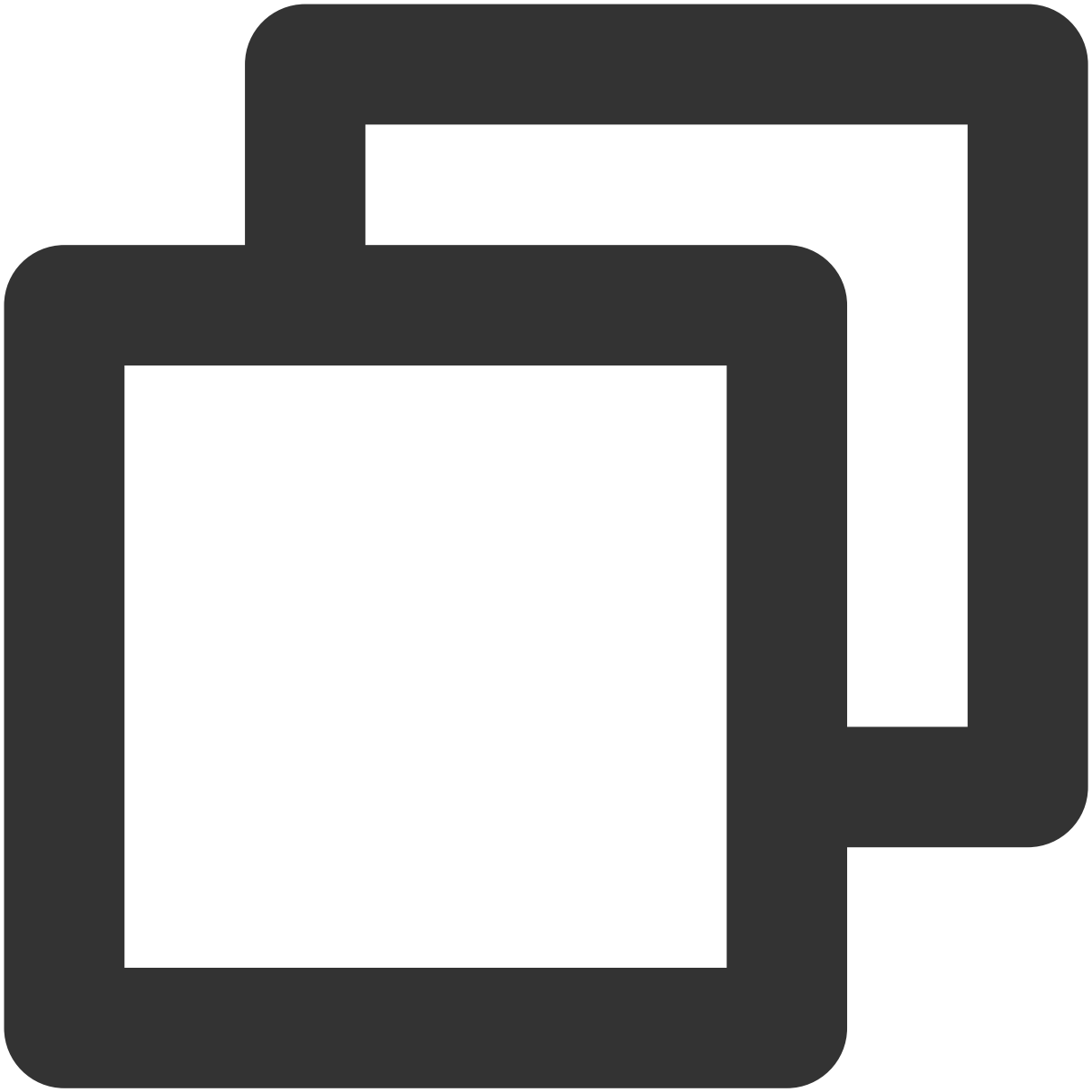
effect is required. It describes the result of a statement. The result can be "allow" or an "explicit deny".

action is required. It describes the allowed or denied action (operation). An operation can be an API (prefixed with "name") or a feature set (a set of specific APIs prefixed with "permid").

resource is required. It describes the details of authorization.

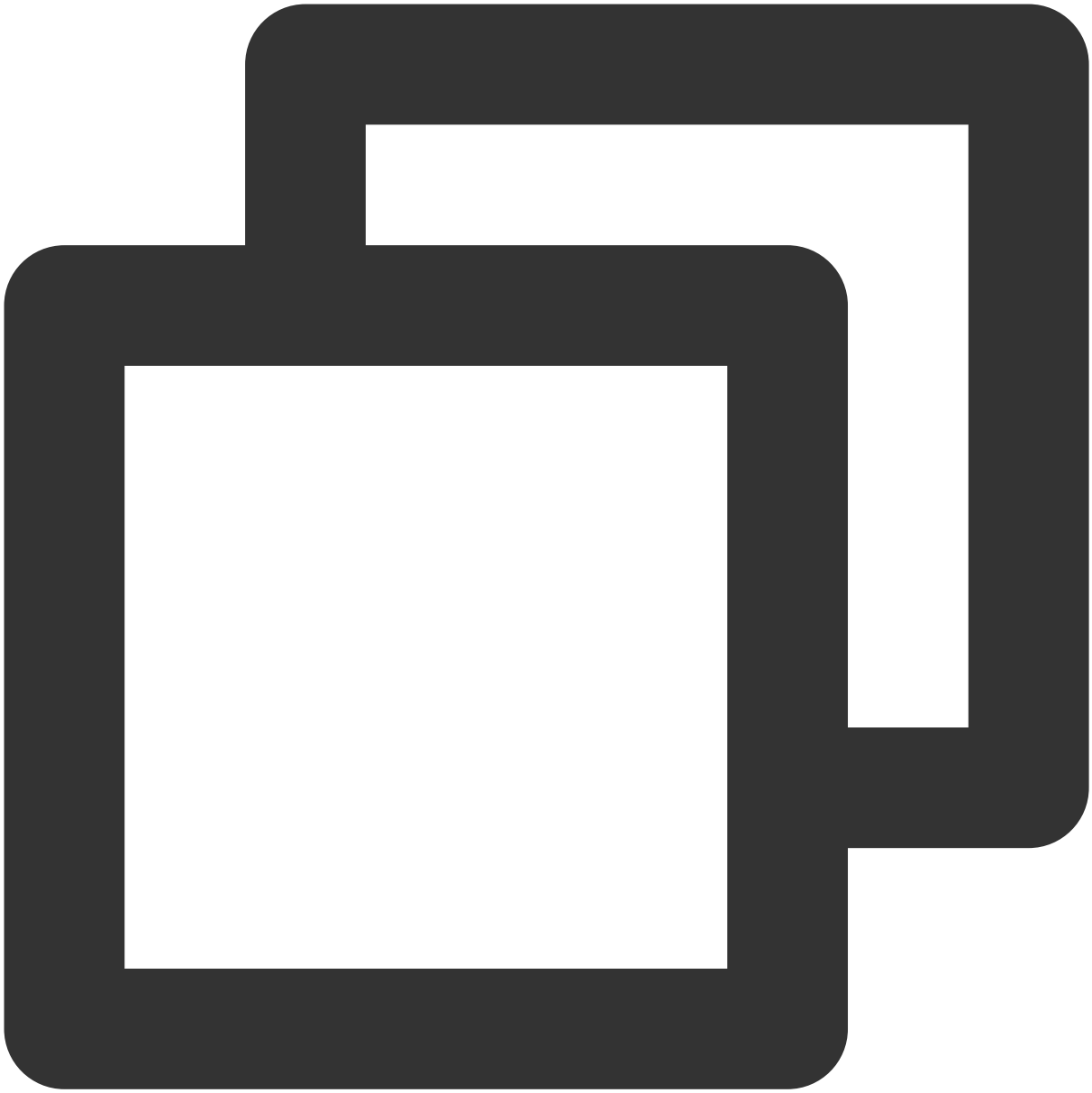
API Operation

In a CAM policy statement, you can specify any API operation from any service that supports CAM. APIs prefixed with `name/cdb:` should be used for Database Audit. To specify multiple operations in a single statement, separate them with commas as shown below:



```
"action":["name/cdb:action1","name/cdb:action2"]
```

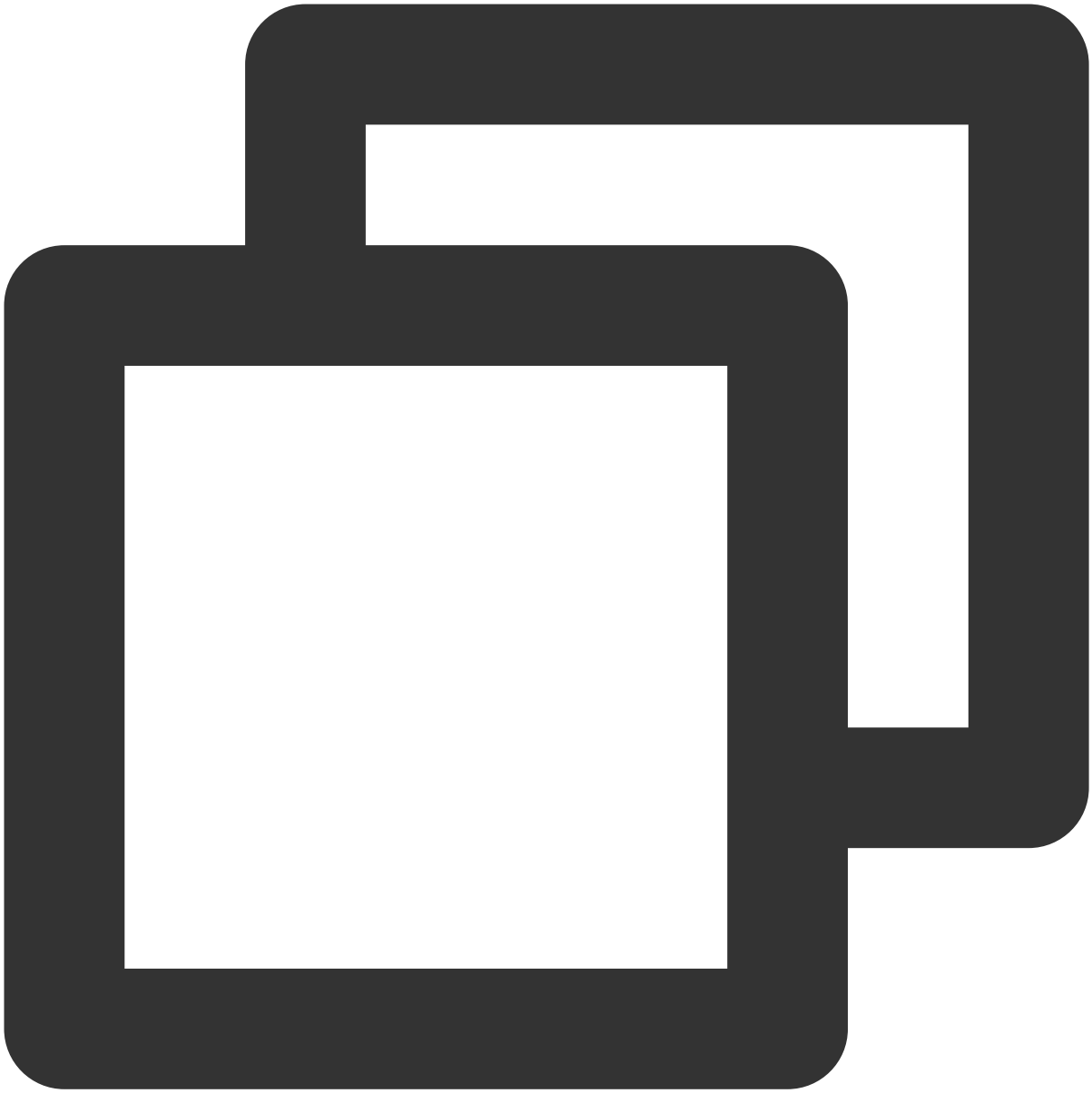
You can also specify multiple operations by using a wildcard. For example, you can specify all operations beginning with "Describe" in the name as shown below:



```
"action":["name/cdb:Describe*"]
```

Resource Path

Resource paths are generally in the following format:



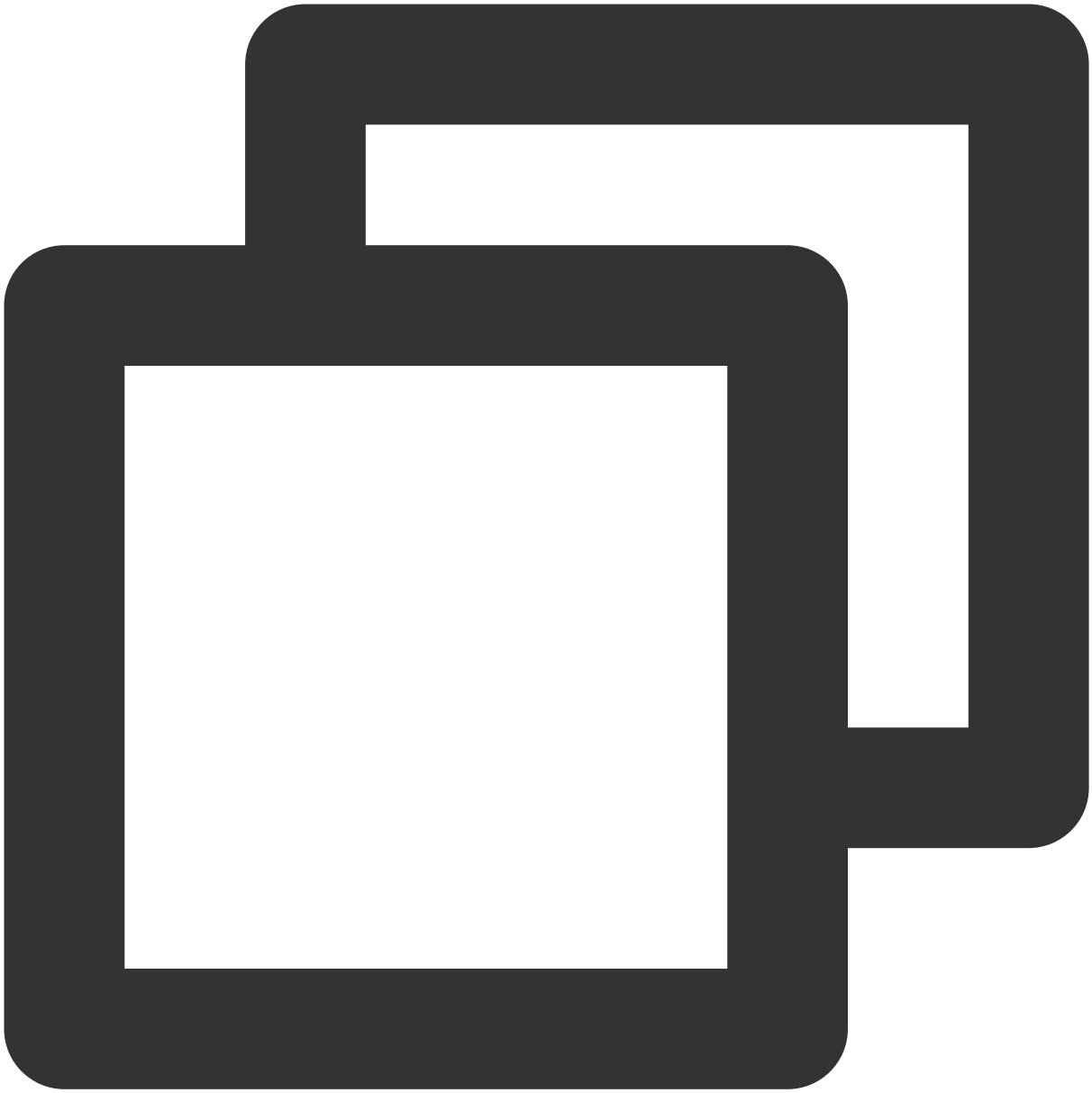
```
qcs::service_type::account:resource
```

service_type: Describes the product abbreviation, such as `cdb` here.

account: Describes the root account of the resource owner, such as `uin/326xxx46` .

resource: Describes the detailed resource information of the specific service. Each TencentDB for MySQL instance (instanceId) is a resource.

Below are examples:

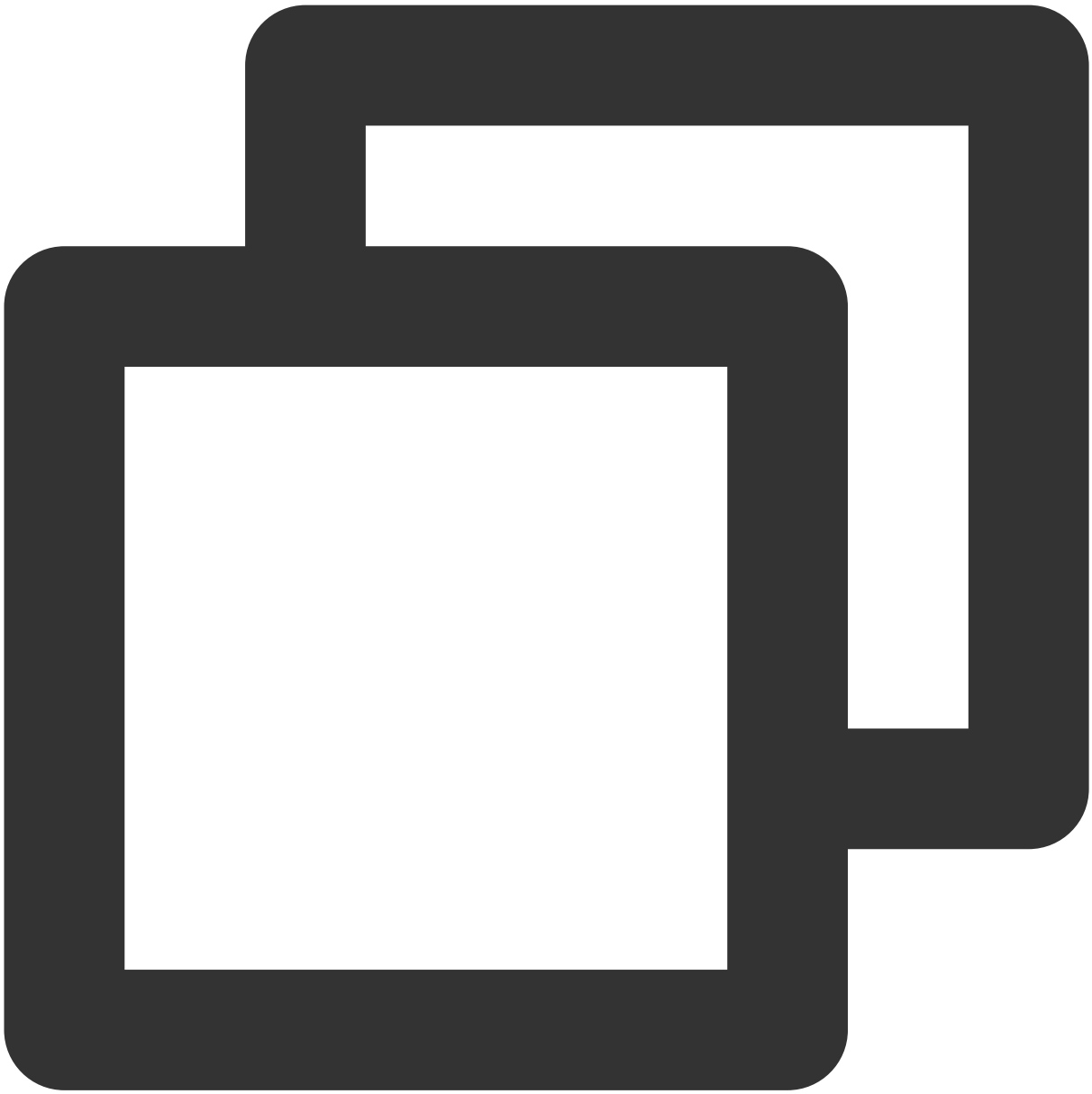


```
"resource": ["qcs::cdb::uin/326xxx46:instanceId/cdb-kf291vh3"]
```

Here, `cdb-kf291vh3` is the ID of the TencentDB for MySQL instance resource, i.e., the `resource` in the CAM policy statement.

Example

The following example only shows the usage of CAM,For a comprehensive API of MySQL database auditing, please refer to the API Documentation。



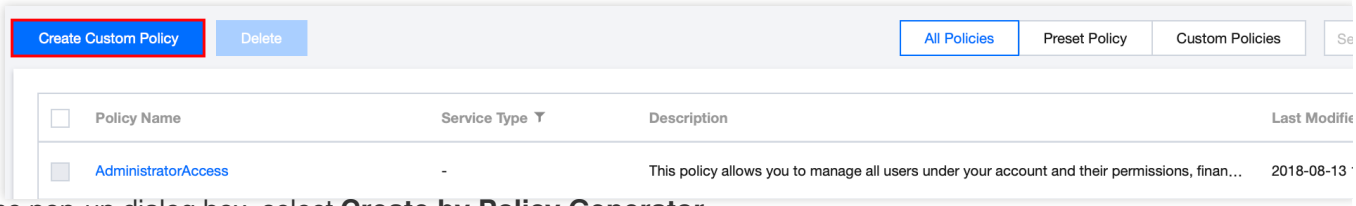
```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "name/cdb: DescribeAuditRules"
            ],
```

```
            "resource": [
                "*"
            ]
        },
        {
            "effect": "allow",
            "action":[
                "name/cdb: CreateAuditPolicy"
            ],
            "resource": [
                "*"
            ]
        },

        {
            "effect": "allow",
            "action":[
                "name/cdb: DescribeAuditLogFiles"
            ],
            "resource": [
                "qcs::cdb::uin/326xxx46:instanceId/cdb-kf291vh3"
            ]
        }
    ]
}
```

Custom MySQL Database Audit Policy

1. Log into the CAM console with the root account and click **Create Custom Policy** in the policy list.



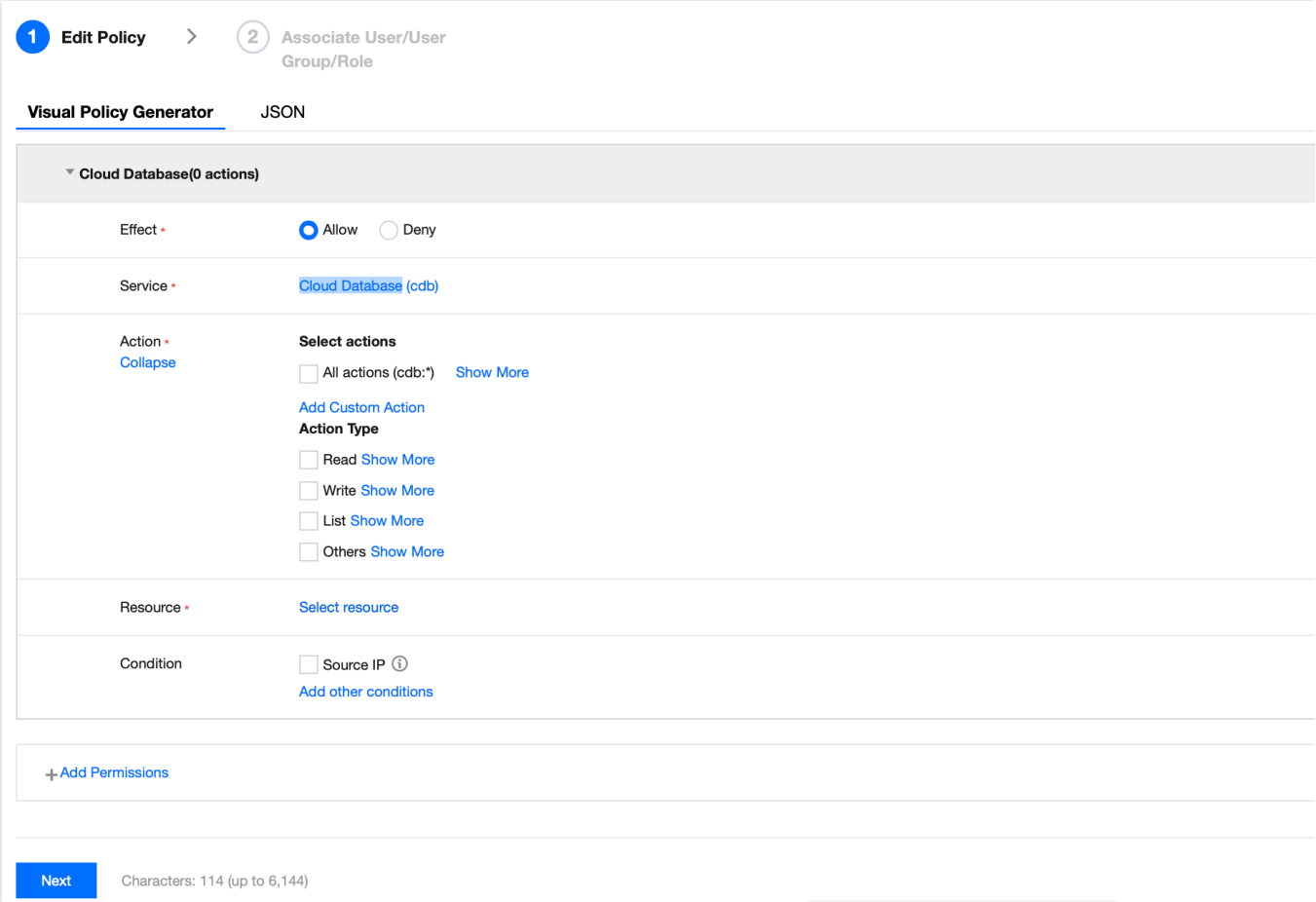
2. In the pop-up dialog box, select **Create by Policy Generator**.
3. On the Select Service and Action page, select configuration items, and click **Next**.

Effect: Select for either **Allow** or **Deny**. If Deny is selected, the user or user group will be unable to obtain authorization.

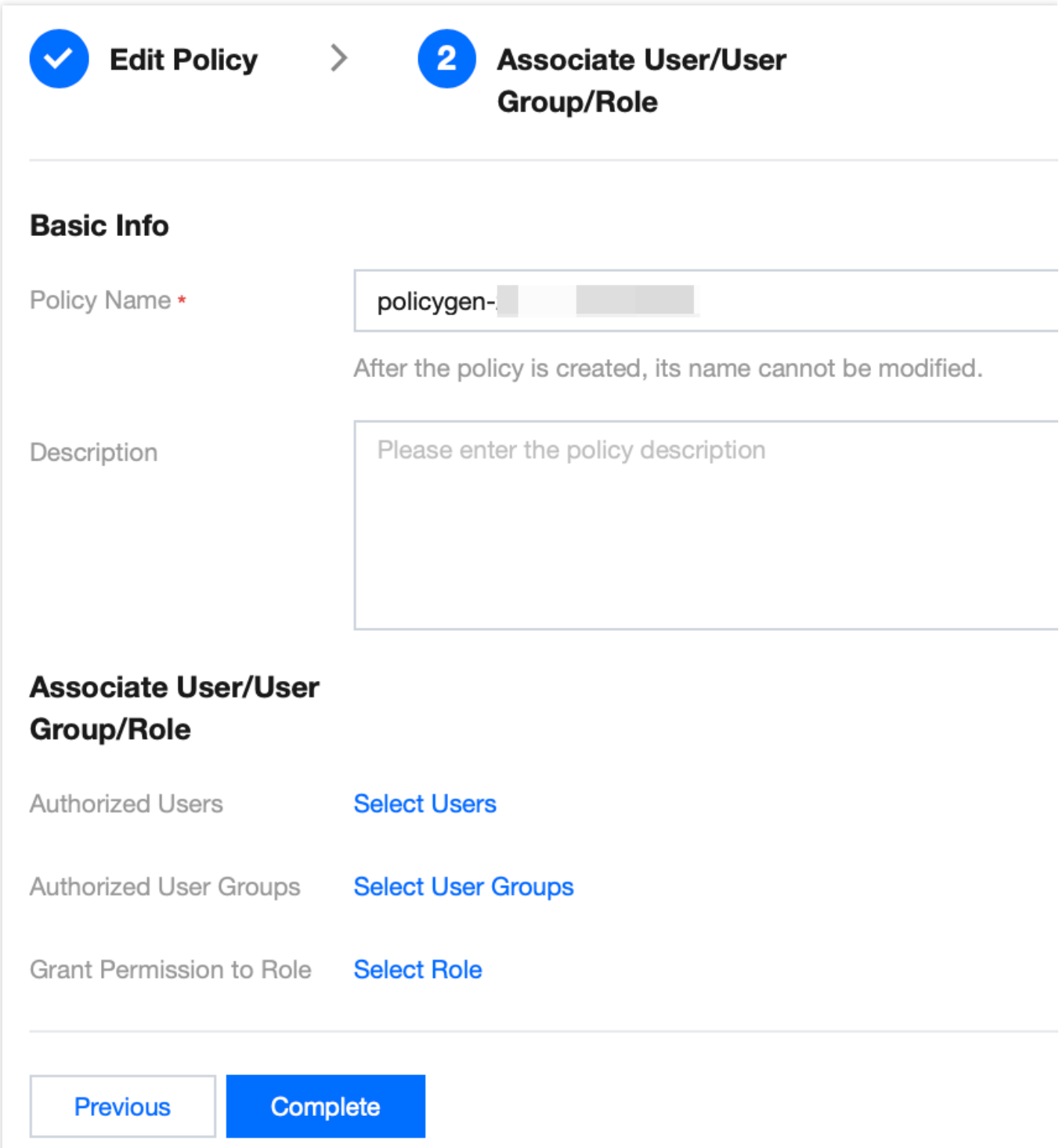
Service: Select **TencentDB for MySQL (cdb)**.

Action: Select all APIs of MySQL Database Audit. For more details, please refer to the API Documentation.

Resource: Please refer to the Resource Description Method. Selecting all resources indicates that the audit logs of all TencentDB for MySQL instances can be manipulated.
Condition (optional): Set the conditions that must be met for the authorization to take effect.



4. On the **Bind User/Group/Role** page, enter the **Policy Name** (such as `SQLAuditFullAccess`) and **Description** as required, then click **Complete**.



5. Return to the policy list and you can view the custom policy just created.