TencentDB for MySQL

SQL Insight (Database Audit)

Copyright Notice

Trademark Notice

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

SQL Insight (Database Audit)
SQL Insight (Database Audit) Introduction

Last updated: 2026-04-29 17:50:01

SQL Insight (Database Audit) is a professional, efficient, comprehensive, and real-time database security auditing product independently developed by Tencent Cloud. This feature can record TencentDB activities in real time, perform fine-grained auditing for compliance management of database operations, and alarm on risky behaviors encountered by databases. TencentDB for MySQL provides SQL Insight (Database Audit) capability, which records database access and SQL statement execution to help enterprises control risks and improve the data security level. It also supports customizing frequent and infrequent access storage types, significantly reducing the feature usage costs.
The feature supports post-event alerts and allows configuring alarm policies for high, medium, and low risk level events. Audit logs triggered by policies can send alarm notifications to bound users. While also enabling viewing alarm history, alarm policy management (alarm switch), and alarm suppression in TCOP to help enterprises promptly obtain relevant alerts and pinpoint audit logs that trigger issues.

Use Cases

- **Address audit risk**
  - Incomplete audit logs make it difficult to trace and locate security incidents.
  - It fails to meet the explicit requirements in the National Standard for Classified Protection of Cybersecurity (Level 3).
  - It fails to meet the requirements specified in industry information security compliance documents.
- **Address management risks**
  - Misoperations, non-compliant operations, and overstepped operations by technical personnel compromise the secure operation of business systems.
  - Misoperations, malicious operations, and tampering by third-party development and maintenance personnel.
  - Super admin permissions are excessive and cannot be audited or monitored.
- **Address technical pain points**
  - SQL injection in the database system, maliciously retrieving database table information.
  - A surge in database requests not caused by slow logs makes it difficult to quickly locate the issue.

Billing

Billing is based on the storage volume of audit logs using a pay-as-you-go model. Each billing cycle is one hour, and any partial hour consumed is billed as a full hour.
For specific product pricing, see SQL Insight (Database Audit) billing details.

Supported Versions and Architecture

- The feature currently supports database kernel versions MySQL 5.6 20180122 and later, MySQL 5.7 20190429 and later, and MySQL 8.0 20210330 and later.
- The feature supports two-node, three-node, and cloud disk edition instance architectures, with read-only instances also supported.
- Instances of MySQL 5.5, single-node (cloud disk) architecture, read-only analysis engines, and two-node economical editions do not support this feature.

Advantages

Full Audit

Database Audit comprehensively records database access and SQL statement execution, meeting user auditing requirements to the greatest extent and enhancing database security.

Rule audit

Setting audit rules for attributes such as client IP address, username, and database name to record database access and SQL statement execution based on customized audit rules.

Efficient Audit

Unlike bypass audit modes, TencentDB records operations via database kernel plugins for more accurate auditing.

Long-Term Retention

Users are supported to store logs long-term based on business needs to meet compliance requirements.

Architectural Features

Adopting a multi-point deployment architecture to ensure service availability. Implementing streaming log recording to prevent tampering. Utilizing multi-replica storage to guarantee data reliability.

Data Security

- **Data Collection Integrity**

SQL Insight (Database Audit) for TencentDB for MySQL is implemented through MySQL kernel plugins, serving as a native and critical step in MySQL's SQL statement execution process. Each SQL statement undergoes a complete lifecycle: connection, parsing, analysis, rewriting, optimization, execution, result return, auditing, and connection release. When SQL Insight (Database Audit) is enabled and a connection is established to TencentDB for MySQL servers, every SQL statement is audited during execution. Therefore, if auditing fails, the SQL statement execution is unsuccessful. Conversely, if an SQL statement executes successfully, it is always audited. Even failed SQL executions are recorded along with failure reasons. Additionally, all login attempts—successful or not—are logged. The SQL request connection is only released after auditing completes, thus ensuring the integrity of audit data collection.

- **Data Collection Reliability**

  SQL Insight (Database Audit) for TencentDB for MySQL captures data synchronously from MySQL's own execution layer, rather than asynchronously via a bypass. Consequently, the audited SQL statements remain synchronized and consistent in real time with the SQL statements executed by TencentDB for MySQL. This mechanism prevents data capture errors and ensures the reliability of the audit data collection.
- **Data Tamper-Proofing**

  The audit control system incorporates behavior monitoring mechanisms. When vulnerabilities are exploited for attacks, vulnerability scanning captures relevant session information in real time and triggers alarms to monitor intrusion behaviors. When audit data is accessed, all operations are fully recorded in access logs, identifying which users accessed data from which source IP addresses at what time to promptly detect high-risk access operations. For operators, permission control is implemented through account and role authentication, granting different read/write permissions to personnel with different roles to prevent account sharing. When high-risk operations occur, real-time tamper alarms are triggered to promptly detect, trace, analyze, and block such activities.
- **Data Transmission Integrity**

  After audit data is collected, during processing at the transmission link layer, the data undergoes steps such as CRC (Cyclic Redundancy Check), globally unique message ID, link MQ redundancy, and Flink stream processing, and is verified from multiple dimensions and angles to ensure data integrity during transmission.
- **Data Storage Integrity**

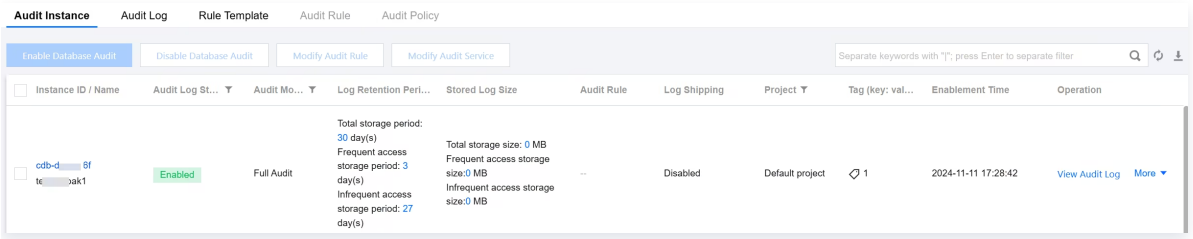
  On the data storage side, the SQL Insight (Database Audit) system encrypts audit log files to ensure data security. Only users with access rights to the encryption certificates can view the audit logs. This mechanism effectively prevents data internal leaks caused by plaintext storage and data theft by high-privilege users, thereby preventing audit data leaks at the source and ensuring the integrity of data storage.

Viewing Audit Instance List

Last updated: 2026-04-29 17:44:18

This document introduces how to view the SQL Insight (Database Audit) audit instance list, and the field information you can view and the related operations you can perform on the audit instance list page.

The audit instance list page displays



Viewing the Audit Instance List

1. Log in to the TencentDB for MySQL console.
2. Click **SQL Insight (Database Audit)** in the left sidebar.
3. The redirect page defaults to **Database Audit** > **Audit Instance**.
4. On the audit instance page, you can: view the tool list (quickly filter instances, refresh the audit instance page, download audit instance list information), view related feature operations, and view instance list field information.

Tool List

Tool	Description
Filter	In the search box above the audit instance list, you can select resource attributes (Instance ID, Instance Name, Tag Key, Tag) to filter, with multiple keywords separated by vertical bars and multiple filter tags separated by the Enter key.
Refreshing	Click to refresh the audit instance list data.

Download	Click ⬇ to download the filtered audit instance list information to your local device in ".csv" format.

Related Feature Operations

Audit Status	Function	Description
The audit service has been enabled.	Disable Audit Service	You can disable the audit service, and batch disabling is supported. For details, refer to Disable the Audit Service.
	Modify Audit Rule	You can modify audit rules, and batch modification is supported. For details, refer to Modifying Audit Rules.
	Modify Audit Service	You can modify the content of the audit service (audit retention period, high/low frequency storage period), and batch modification is supported. For details, refer to Modifying the Audit Service.
	View Audit Log	You can query historical audit log records. For details, refer to View Audit Logs.
	Configure Log Shipping	Audit logs can be shipped to CLS, Ckafka, and COS. For details, refer to log shipping.
The audit service is not enabled.	Enabe Database Audit	You can enable the audit service, and batch enabling is supported. For details, refer to enabling the audit service.

Audit Instance List Field Information

Field	Description
Instance ID/Name	Displays the instance ID/name information for all instances within a specific region.

Audit Log Storage Status	Displays whether audit log storage is enabled or disabled. You can use the options at the top of the list to filter and display instances in the corresponding status.
Audit Mode	Displays the currently configured audit rules: full audit or rule audit for the corresponding instance when the audit service is enabled, and supports filtering via a dropdown to display a single rule.
Log Retention Period	Displays the total storage duration (days), high-frequency storage duration (days), and low-frequency storage duration (days) for the corresponding instance when the audit service is enabled.
Stored Log Size	Displays the total storage volume (MB), high-frequency storage volume (MB), and low-frequency storage volume (MB) for the corresponding instance when the audit service is enabled.
Audit Rule	Displays the number of audit rule templates bound to the instance. When you hover over the audit rule field of the corresponding instance, you can view the ID and name of each rule template. Click a specific rule template to view its details, including basic information, parameter settings, and modification history.
Log Shipping	Displays the log shipping status of instances. • Disabled: Log shipping is not configured. • CKafka: Log shipping to CKafka is configured. • CLS: Log shipping to CLS is configured. • COS: Log shipping to COS is configured.
Project	Displays the associated project of the corresponding instance, enabling easy categorization and management of resources. Supports filtering instances under the desired project via a dropdown.
Tag (key:value)	Displays the tag information of instances.
Enablement Time	Displays the time when the audit service is enabled for the corresponding instance, down to the second.
Operation	Operations for which the audit service is enabled: • View Audit Log. • More (Modify Audit Rule, Modify Audit Service, Configure Log Shipping, and Disable Audit Service). Operations for which the audit service is not enabled: • Enabe Database Audit.

Enabling Audit Service

Last updated: 2026-04-29 17:41:24

Tencent Cloud provides SQL Insight (Database Audit) capability for TencentDB for MySQL, recording database access and SQL statement execution, helping enterprises perform risk control and improve data security levels.

Prerequisites

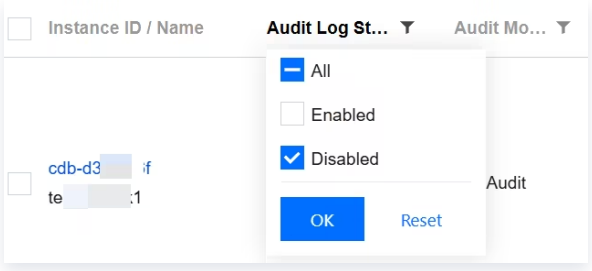
You have created a MySQL instance.

Supported Versions and Architecture

- The feature currently supports database kernel versions MySQL 5.6 20180122 and later, MySQL 5.7 20190429 and later, and MySQL 8.0 20210330 and later.
- The feature supports two-node, three-node, and cloud disk edition instance architectures, with read-only instances also supported.
- Instances of MySQL 5.5, single-node (cloud disk) architecture, read-only analysis engines, and two-node economical editions do not support this feature.

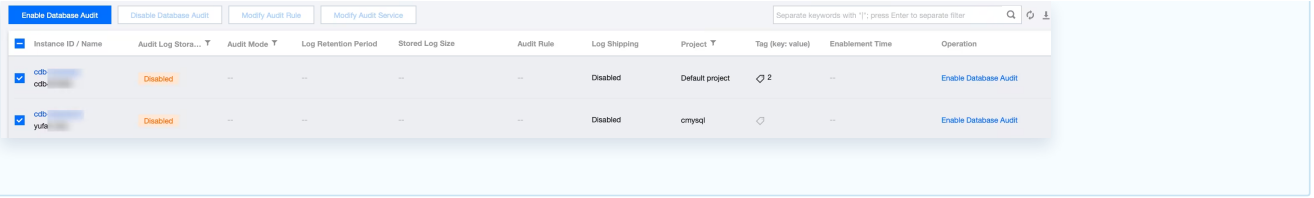
Operation Steps

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a region at the top, click the **Audit Log Storage Status** field on the **Audit Instance** page, and select **Disabled** to filter instances with the audit service disabled.



4. In the audit instance list, locate the target instance (you can also quickly find it by filtering resource attributes in the search box), and click **Enable Database Audit** in its **Operation** column.

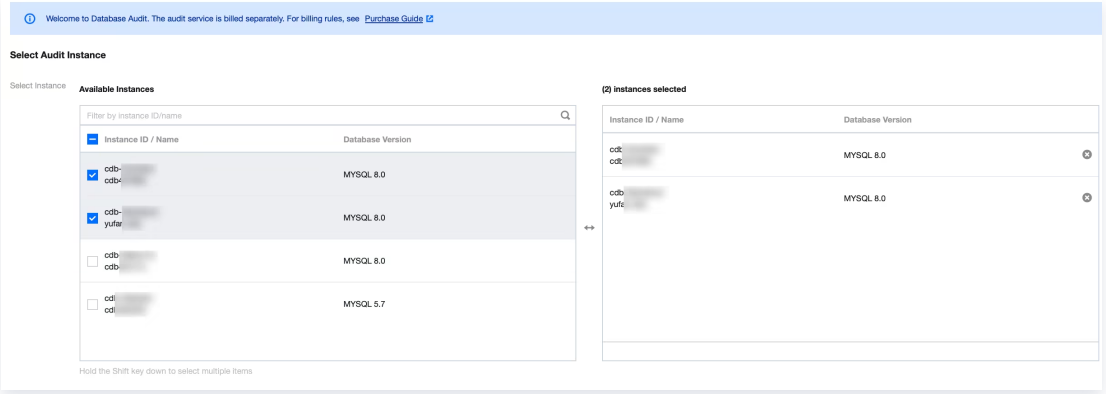
> **Note:**
> Batch enabling of the audit service is supported. On the Audit Instance page, select multiple target instances and click **Enable Database Audit** at the top to go to the settings page.



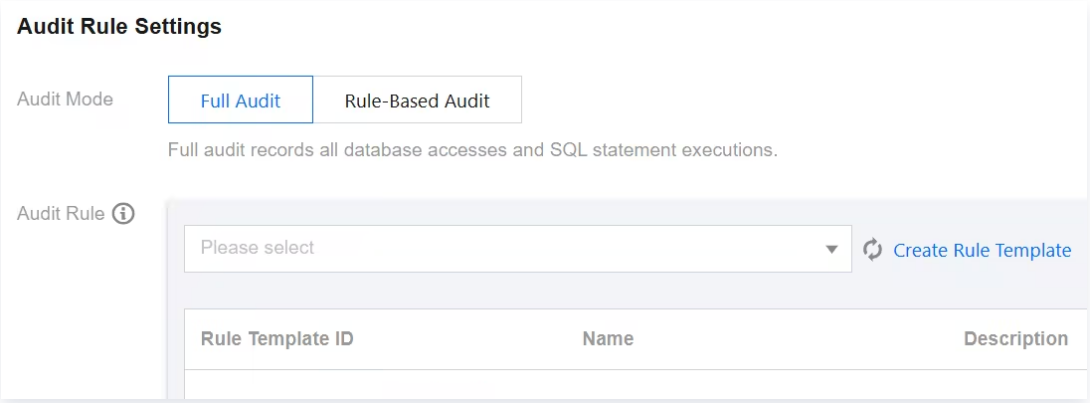
5. On the page for enabling the audit service, sequentially complete the audit instance selection, audit type settings, audit service settings, and advanced performance analysis settings. Read and select the Tencent Cloud Service Agreement, then click **OK**.

5.1 **Select Audit Instance**

Under the audit instance selection item, the system automatically selects the instance chosen in **Step 4** by default. It also supports modifying the target instance in this window (selecting other instances or multiple instances). You can also quickly locate the target instance in the search box by **Instance ID/Name**. After completing the instance selection, go to the audit rule settings.



5.2 **Audit Rule Settings**



In the audit type settings, you need to select either **Full Audit** or **Rule-Based Audit**. A detailed comparison between the two is provided in the following table.

Parameter	Description
Full	Comprehensively records all access to the database and SQL statement

Audit	execution.
Rule-Based Audit	Rule audit records access to the database and SQL statement execution based on customized audit rules. **Note:** Instances that have had CDS enabled cannot enable rule audit.

- When the audit type is set to Full Audit, proceed as follows.
  You can select an existing template from the rule templates or choose to create a new rule template. For detailed steps on creating a new template, refer to Create New Rule Template.
  After the rule template settings are completed, proceed to the audit service settings step.

  Note:
  - You can apply up to 5 rule templates, and different rule templates are in an "OR" relationship.
  - Rule templates are applied to instances with the audit type set to "Full Audit". They are only used to set the risk level and alarm policy for audit logs that match the rules in the template. Audit logs that do not match the rules are still retained.

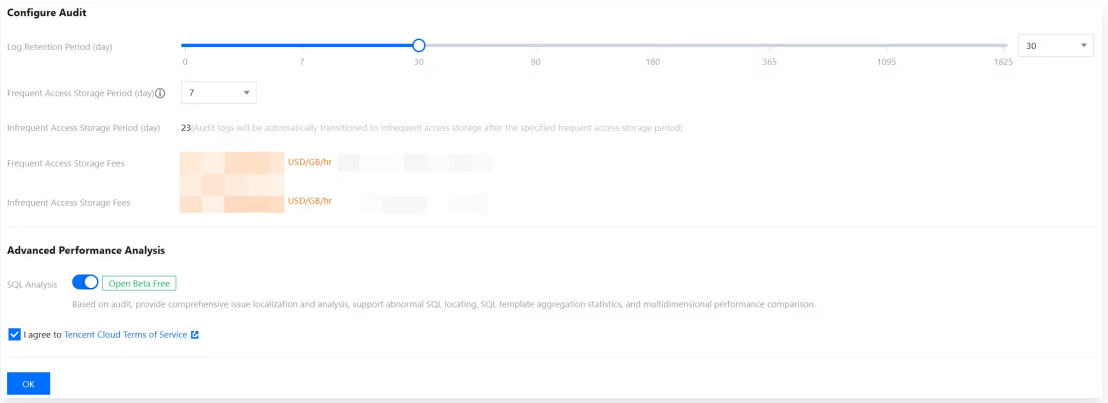
- When the audit type is set to Rule-Based Audit, you can select an existing rule template from the rule templates or create a new one. If you select an existing rule template, you can directly proceed to the audit service settings. If no suitable template is available, you can create a new rule template and refresh the list to select it. For detailed steps, refer to Create New Rule Template.

  Note:
  - You can apply up to 5 rule templates, and different rule templates are in an "OR" relationship.
  - Rule templates are applied to instances with the audit type set to "Rule Audit". They are used to retain audit logs that match the rules in the template, set risk levels, and configure alarm policies. Audit logs that do not match the rules will not be retained.

5.3 Configure Audit

Under the audit service settings, you need to configure the audit log retention period and

high/low-frequency storage duration, read and select the Tencent Cloud Service Agreement, then click **OK** to enable the audit service.



Parameter	Description
Log Retention Period	Set the retention period for audit logs. Unit: days. Supported values are 7, 30, 90, 180, 365, 1095, and 1825 days.
Frequent Access Storage Period	Frequent Access Storage Period represents ultra-high-performance storage medium with excellent query performance. Unit: days. After the storage duration is set, audit data within the specified period will be stored in high-frequency storage. Data beyond this duration will automatically move to low-frequency storage. Both storage types support identical audit capabilities, differing only in performance. For example: if the log retention period is set to 30 days and high-frequency storage duration to 7 days, the low-frequency storage duration defaults to 23 days.

5.4 Advanced Performance Analysis

SQL Analysis: DBbrain provides comprehensive problem identification and analysis capabilities based on SQL Insight (Database Audit), supporting abnormal SQL identification, SQL template aggregation statistics, and multi-dimensional performance comparison. This option is enabled by default but can be manually disabled, indicating that the SQL analysis capability is not enabled.

> **Note:**
> The SQL analysis feature is currently in open beta and is available for a free trial. Once the beta phase concludes, TencentDB for DBbrain will officially introduce a commercial billing plan. You can refer to the official announcement for specific pricing details at that time. For more details about SQL analysis, see SQL Analysis (MySQL).

Viewing Audit Log

Last updated: 2026-04-29 15:03:35

This document introduces how to view the audit logs of SQL Insight (Database Audit) and the fields in the related audit log list.

Note:

- If the audit mode is rule-based audit, log parsing errors may occur when an SQL statement contains non-ASCII binary characters or special characters. Log parsing is normal if the audit mode is full audit.
- When the SQL length exceeds 32KB, the SQL statements recorded in the log may be truncated, and truncated logs may cause abnormal parsing.
- SQL statements executed via functions or stored procedures will not be recorded in audit logs.
- On July 12, 2023, a new version of the audit log page was released. The audit log search field "Scanned Rows" is a newly added field. For existing audit logs prior to this date, the data for this field will be displayed as "-", and in downloaded files and via API, it will be displayed as "-1".
- Uniformly changed the unit of the audit log field Execution Time to microseconds in both the console and downloaded audit log files.
- The unit of the audit log field "CPU Time" has been uniformly changed to microseconds in both the console and downloaded audit log files.
- Added the display of the millisecond-level time for the unit of the Timestamp field in audit log files.
- When audit logs are searched, the character used to separate multiple search terms has been changed from **comma** to **newline**.
- After SQL Insight (Database Audit) is enabled, the storage regions for audit log files vary for instances in Tianjin, Taipei (China), and Shenzhen. The corresponding storage regions can be found in the table below.

Instance region	Audit Log Storage Region
Tianjin	Beijing
Taipei (China)	Hong Kong (China)
Shenzhen	Guangzhou

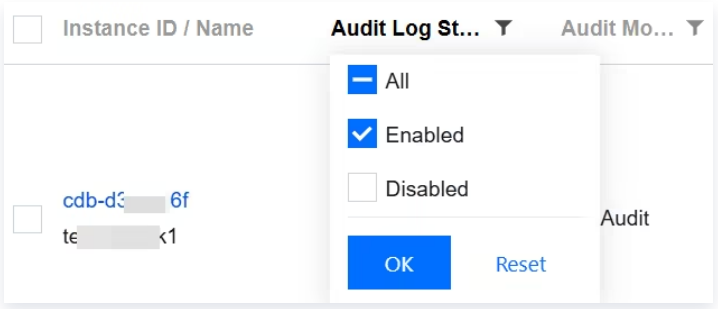
Prerequisites

Already enabling the audit service.

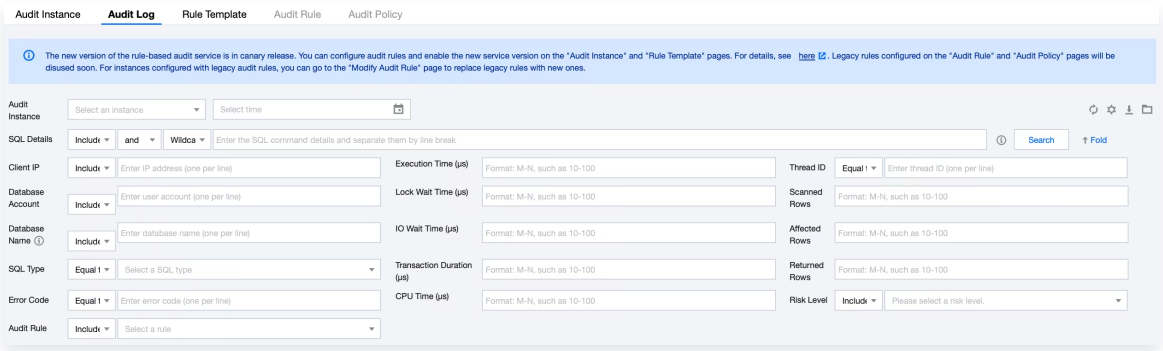
Viewing Audit Logs

> **Note:**
> Audit logs are displayed with millisecond precision, allowing for more accurate SQL sorting and troubleshooting.

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a **region** at the top. On the **Audit Instance** page, click **Audit Log Storage Status** and select the **Enabled** option to filter for instances with the audit service enabled.



4. In the **Audit Instance** list, locate the **target instance** (you can also use the search box to filter by resource attributes for quick search). Click **View Audit Log** in the Operation column to go to the **Audit Log** page and view the corresponding logs.



Tool List

Tool	Description
Refreshing	Click to refresh the audit log list.
Customize List Fields	Click to select fields you want to display in the list.

Download	Click to generate a log file. In the pop-up window, you can select the **log fields** to be included in the downloaded file. Available options are **All fields** and **Interaction with custom list fields**. If you select **Interaction with custom list fields**, the downloaded log file will only contain the fields displayed in the list, and the field order will be the same as that in the list.
File List	Click to access the **Audit Log List**. You can query the information and download address of files that have been generated or are being generated. You can copy the download address to download a file and obtain the complete SQL audit logs. • Currently, only Tencent Cloud private network addresses are provided for downloading log files. You can download files via a Tencent Cloud CVM instance in the same region. (For example, to download the audit logs of a database instance in the Beijing region, use a CVM instance in the Beijing region.) • Log files are valid for 24 hours. You should download them promptly. • The number of log files for each database instance should not exceed 30. You need to delete the log files after download. • If the displayed status is Failed, there may be too many logs. You can narrow the time range to download log files in batches.

Filtering and Search Conditions

- In the **audit instance filter box**, you can select and switch to other audit instances where the audit service is enabled.
- In the **time box**, the default selection is Last 1 hour. You can quickly select other time ranges (Last 3 hours, Last 24 hours, Last 7 days) or customize a time period to view relevant audit logs within the selected timeframe.

> **Note:**
> The time period for search supports selecting any time period with available data. A maximum of the top 60,000 matching records will be displayed.

- In the **Search Box**, select search items (such as SQL details, client IP, user account, database name, Table Name, SQL type, error code, execution time (μs), lock wait time (μs), IO wait time (ns), transaction duration (μs), CPU time (μs), risk level, thread ID, transaction ID, scanned rows, affected rows, returned rows, audit rules, etc.) to view relevant audit results. Separate multiple keywords with line breaks.

Search Item	Matching Items	Description

SQL Details	Include – Or – Tokenize	**Rule Description** • Enter SQL command details. Separate multiple keywords with line breaks. • The matching items in the SQL Command Details search box are divided into three levels: the first level sets positive/negative matching modes (Contains, Does Not Contain); the second level defines logical relationships between keywords (OR, AND); the third level configures the matching mode for each keyword (Tokenized, Wildcard). **⚠ Note:** • The search for SQL command details is case-insensitive. • Supports two types of positive/negative matching modes: "Contains" and "Does Not Contain". • Keywords support two types of logical matching: "OR" and "AND". "OR" represents a union relationship between different keywords, while "AND" represents an intersection relationship. • Each keyword supports two matching modes: "Tokenized" and "Wildcard". "Tokenized" indicates that each keyword in the SQL command details requires exact matching, while "Wildcard" indicates that each keyword can be matched with fuzzy logic. **Example Description** Assume the SQL command details are: SELECT * FROM test_db1 join test_db2 LIMIT 1; • In the "Contains (Tokenized)" search mode, you can search using tokenized keywords such as "SELECT", "select * from", "*", "SELECT * FROM test_db1 join test_db2 LIMIT 1;", and "from Test_DB1". However, you cannot search using wildcard keywords like "SEL", "sel", or "test". • In the "Contains (Wildcard)" search mode, you can search using wildcard keywords such as "SEL", "sel", "test", and "DB".
	Include – AND – Segmentation	
	Exclude – AND – Segmentation	
	Include – OR – Wildcard	
	Include – AND – Wildcard	

	Exclude – AND – Wildcard	• In the "Contains (AND)" search mode, multiple keywords are combined with an "AND" relationship. For example, entering keywords such as "SELECT" and "test_db" will query all SQL commands containing both "SELECT" and "test_db". • In the "Contains (OR)" search mode, multiple keywords are combined with an "OR" relationship. For example, entering "test_db1" or "test_db2" will query all SQL commands containing either "test_db1" or "test_db2".
Client IP	Include Exclude Equal to Not equal to	Enter the client IP addresses, separating multiple keywords with line breaks. IP addresses support using * as a wildcard for filtering. For example, searching for Client IP address: 9.223.23.2* will match all IP addresses starting with 9.223.23.2.
User Account	Include Exclude Equal to Not equal to	Enter user account(s), separating multiple keywords with line breaks.
Database Name	Include Exclude Equal to Not equal to	Enter database name(s), separating multiple keywords with line breaks. **Note:** The search for database names is case-insensitive.
Table Name	Equal to Not equal to	Enter table name(s). The search for table names follows these rules: • Case-insensitive. • The search format is DbName.TableName. For example: If the database test_db contains a table named test_table and you want to search for this table, you need to enter: Table name equals test_db.test_table. **Note:** • A maximum of 64 table names can be stored. • The field "Table Name" is directly supported in MySQL 5.7 20240331 and later versions, as well as MySQL 8.0 20240930 and later versions.

		Other versions do not support this field. You can upgrade to supported versions if needed.
SQL Type	Equal to Not equal to	Select an SQL type from the drop-down list. Available types: ALTER, CHANGEUSER, CREATE, DELETE, DROP, EXECUTE, INSERT, LOGOUT, OTHER, REPLACE, SELECT, SET, UPDATE, and PREPARE. Multiple types can be selected at the same time. **Note:** The SQL type "PREPARE" is supported only in MySQL 5.7 20230115 and later versions, as well as MySQL 8.0 20221215 and later versions. You can upgrade to supported versions if needed.
Error Code	Equal to Not equal to	Enter error code(s), separating multiple keywords with line breaks.
Execution time (μs)	Interval Format	Enter the execution time in the format M-N, such as 10-100 or 20-200.
Lock wait time (μs)	Interval Format	Enter the lock wait time in the format M-N, such as 10-100 or 20-200.
IO wait time (ns)	Interval Format	Enter the I/O wait time in the format M-N, such as 10-100 or 20-200.
Transaction duration (μs)	Interval Format	Enter the transaction duration in the format M-N, such as 10-100 or 20-200.
CPU time (μs)	Interval Format	Enter the CPU time in the format M-N, such as 10-100 or 20-200.
Risk Level	Include Not included	• Select Low, Medium, or High risk to filter audit logs that match the risk level settings of rule templates. • Leaving the input blank is also supported, which filters existing audit logs without a Risk Level Tag.
Thread ID	Equal to Not equal to	Enter Thread ID, with multiple keywords separated by line breaks.

Transaction ID	Equal to Not equal to	Enter Transaction ID, with multiple keywords separated by line breaks. **Note:** • For the field "Transaction ID", support is available in MySQL 5.7 version 20240331 and above, and MySQL 8.0 version 20230630 and above. Other versions do not support this feature. To enable support, please upgrade to a supported version. • Transaction IDs are generated only after INSERT, UPDATE, or DELETE operations are performed within explicit transactions. Implicit transactions do not have Transaction IDs.
Number of scanned rows	Interval Format	Enter the number of rows scanned, in the format M-N, such as 10-100 or 20-200.
Number of affected rows	Interval Format	Enter the number of affected rows, in the format M-N, 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. **Note:** The "Number of Rows Returned" field indicates the specific number of rows returned by SQL execution, primarily used for impact assessment of SELECT-type SQL statements.
Audit Rule	Include Exclude	• Displays the template ID and name for each rule template in the selected region. You can filter audit logs to show only those that match a specific rule template. • Supports leaving the input blank, which filters audit logs historically stored without audit rule tags and full audit logs that did not trigger any rules. • Supports searching audit rules by rule template ID and rule template name.

		• Supports simultaneously selecting multiple rule templates.

Audit Field

The audit logs of TencentDB for MySQL support the following fields.

No.	Field Name	Supported Kernel Version	Field Description
1	Time	MySQL 5.6 ⩾ 20180122 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	Records the start time of the operation (SQL execution).
2	Risk Level	–	Indicates the risk level of the operation, categorized as Low Risk, Medium Risk, or High Risk. For full audit logs that do not trigger any audit rules, the risk level will be displayed as "–".
3	Client IP	MySQL 5.6 ⩾ 20180122 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	The IP address of the client that initiates the database operation.
4	Database Name	MySQL 5.6 ⩾ 20180122 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	The name of the database involved in the operation.
5	Table Name	MySQL 5.6 not supported MySQL 5.7 ⩾ 20240331 MySQL 8.0 ⩾ 20230630	The specific names of the tables involved in the operation (if any). The system is limited to recording a maximum of 64 table names. **Note:** After the recycle bin feature is enabled, the table name field will record the database tables of

			__cdb_recycle_bin__ in the CloudAudit logs for truncate or drop operations.
6	User Account	MySQL 5.6 ⩾ 20180122 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	User account performing the operation.
7	SQL Type	MySQL 5.6 ⩾ 20180122 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	Type of SQL statement, such as SELECT, INSERT, UPDATE, DELETE.
8	SQL Details	MySQL 5.6 ⩾ 20180122 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	Executed SQL Command Text.
9	Error Code	MySQL 5.6 ⩾ 20180122 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	When an error occurs during SQL statement execution, an error code is generated. The error code is an integer value that identifies the specific error type, with 0 indicating success.
10	Thread ID	MySQL 5.6 ⩾ 20190930 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	Each client connected to the database has a unique thread ID. This ID is used to identify which client performed a specific operation.
11	Transaction ID	MySQL 5.6 not supported MySQL 5.7 ⩾ 20240331 MySQL 8.0 ⩾ 20230630	In transactional storage engines (such as InnoDB), each transaction has a unique transaction ID. This ID is used to identify a specific transaction.

12	Scanned Rows	MySQL 5.6 ⩾ 20190930 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	The number of rows scanned by the database when a query is executed. This number helps you assess the efficiency of the query.
13	Returned Rows	MySQL 5.6 ⩾ 20190930 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	The number of rows returned by the query result. This number helps you understand the size of the result set.
14	Affected Rows	MySQL 5.6 ⩾ 20180122 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	The number of rows actually affected when modification operations are performed (such as INSERT, UPDATE, DELETE) on a data table. This number helps you understand the extent of the operation's impact.
15	Execution Time (μs)	MySQL 5.6 ⩾ 20180122 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	The time taken for an SQL statement to execute from start to finish, measured in microseconds. This number helps you assess the performance of the query.
16	CPU Time (μs)	MySQL 5.6 ⩾ 20190930 MySQL 5.7 ⩾ 20190830 MySQL 8.0 ⩾ 20210330	The time consumed by the execution of an SQL statement on the CPU, measured in microseconds. This number helps you understand the CPU usage of the query.
17	Lock Wait Time (μs)	MySQL 5.6 ⩾ 20190930 MySQL 5.7 ⩾ 20190830 MySQL 8.0 ⩾ 20210330	Lock wait time (in microseconds). This number helps you understand the lock contention of the query.
18	IO Wait Time (ns)	MySQL 5.6 ⩾ 20190930 MySQL 5.7 ⩾ 20190830	I/O wait time (measured in nanoseconds). This metric helps you understand the I/O performance of the query.

		MySQL 8.0 ⩾ 20210330	
19	Transaction Duration (μs)	MySQL 5.6 ⩾ 20190930 MySQL 5.7 ⩾ 20190830 MySQL 8.0 ⩾ 20210330	The total time taken for a transaction from initiation to commit or rollback, measured in microseconds. This number helps you assess the performance of the transaction.
20	Policy Name	MySQL 5.6 ⩾ 20180122 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	This field is no longer used for rule-based audit in new versions.
21	Audit Rule	MySQL 5.6 ⩾ 20180122 MySQL 5.7 ⩾ 20190430 MySQL 8.0 ⩾ 20210330	• Indicates which rule template this audit log entry is triggered by. Clicking on the corresponding rule template displays detailed rule information, including basic information, parameter settings, and modification history. • For historical audit logs, the audit rule value is displayed as "-". • For comprehensive audit logs that do not match any rules, the audit rule value is displayed as "-".
22	Client Port	MySQL 5.7 ⩾ 20240331 MySQL 8.0 ⩾ 20240930	The port number of the client that initiates database operations.

SQL Statement Types and Mapped Objects Relationship

No.	SQL Statement Type	SQL Statement Mapping Object
0	OTHER	All SQL statement types except those listed below.
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. This behavior is not constrained by audit rules and is recorded by default.
12	LOGOUT	Database logout. This behavior is not constrained by audit rules and is recorded by default.
13	CHANGEUSER	User modification behavior. This behavior is not constrained by audit rules and is recorded by default.
14	PREPARE	-

Log Shipping

Last updated: 2026-04-29 14:53:37

TencentDB for MySQL's SQL Insight (Database Audit) provides the log shipping feature. Through log shipping, it can collect audit logs from TencentDB for MySQL instances and ship them to CLS (Cloud Log Service) for centralized management and analysis. It also supports shipping to Ckafka message queues. After shipping, you can perform real-time stream computing on logs in the Ckafka message queue console. It also supports shipping to COS object storage for archive storage of log data. This document describes how to configure the log shipping feature for SQL Insight (Database Audit) via the console.

Prerequisites

If you need to ship to CLS, the prerequisites are as follows.:

- Before using this feature, make sure you have activated CLS.
- Already enabling the audit service.
- The instance status is Running.

If you need to ship logs to TDMQ for CKafka, the prerequisites are as follows:

- The CKafka instance has been purchased.
- A routing policy has been added for CKafka instances.
- Already enabling the audit service.
- The instance status is Running.

Prerequisites for shipping logs to COS:

- Before using this feature, make sure you have activated COS.
- Already enabling the audit service.
- The instance status is Running.

Supported Versions and Architecture

- MySQL 5.6 20180101 and later versions.
- MySQL 5.7 20190429 and later versions.
- MySQL 8.0 20210330 and later versions.
- Instance architectures include two-node, three-node, and cloud disk versions.

Billing Overview for Log Shipping

- The feature of shipping SQL Insight (Database Audit) logs to CLS for TencentDB for MySQL involves the third-party independently billed cloud product CLS. For billing standards, see CLS > Billing Overview.

- The feature of shipping SQL Insight (Database Audit) logs to Ckafka message queue for TencentDB for MySQL involves the third-party independently billed cloud product Ckafka message queue. For billing standards, see Ckafka Billing Overview.
- The feature of shipping SQL Insight (Database Audit) logs to COS object storage for TencentDB for MySQL involves the third-party independently billed cloud product COS object storage. For billing standards, see Billing Overview.
- After the SQL Insight (Database Audit) log shipping feature is enabled for TencentDB for MySQL, traffic fees will be incurred based on the volume of shipped logs. For details, see the table below.

> **Note:**
> After the log shipping feature is enabled, traffic fees are incurred. However, regardless of whether you enable one or more log shipping paths (CLS, CKafka, or COS), the system only charges traffic fees incurred by this feature as a whole.

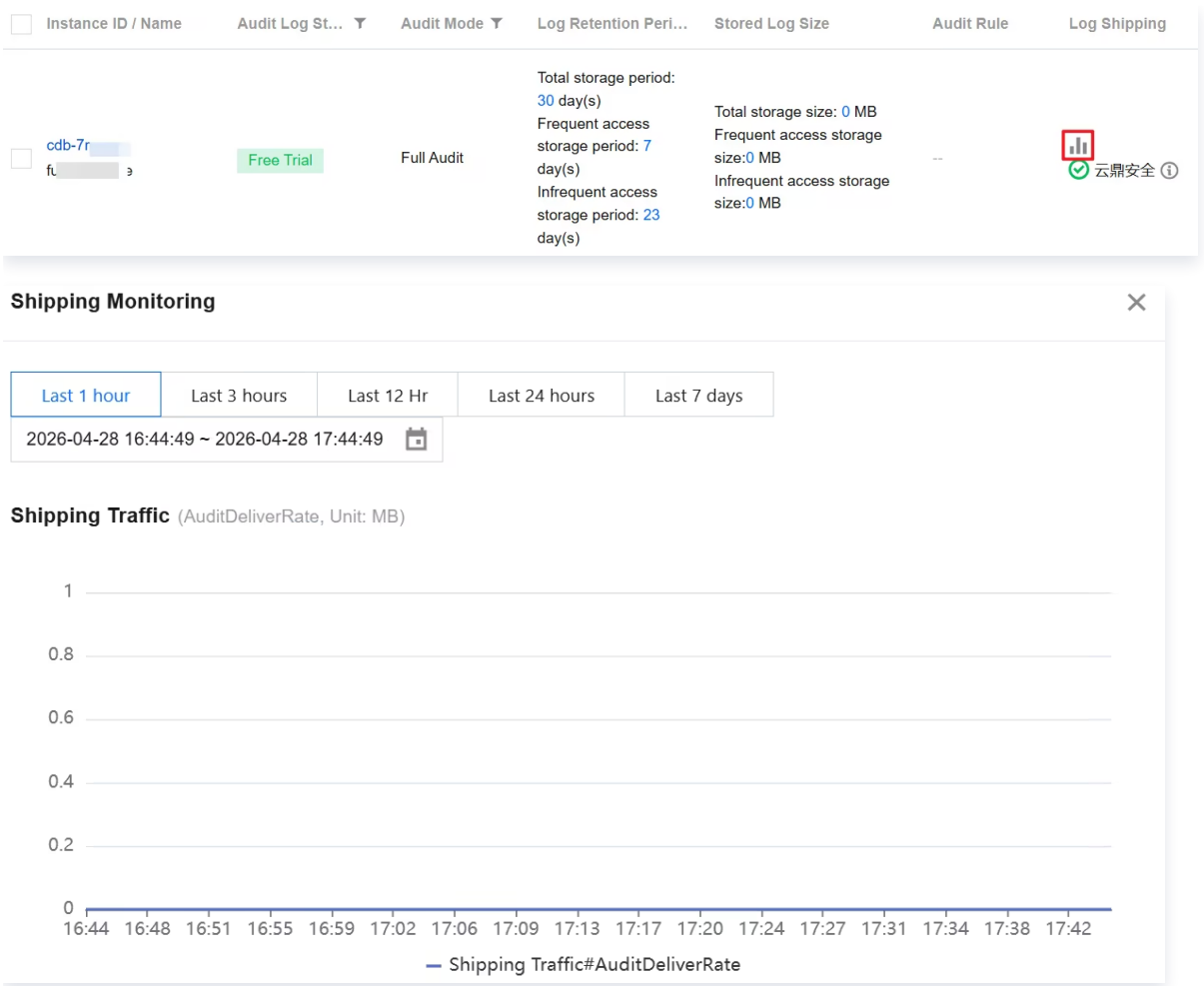
Billable Item: Audit Log Traffic	
Chinese mainland regions (CNY/GB)	Hong Kong (China), other countries and regions (CNY/GB)
0.4	0.6

Description of Log Shipping Traffic Monitoring

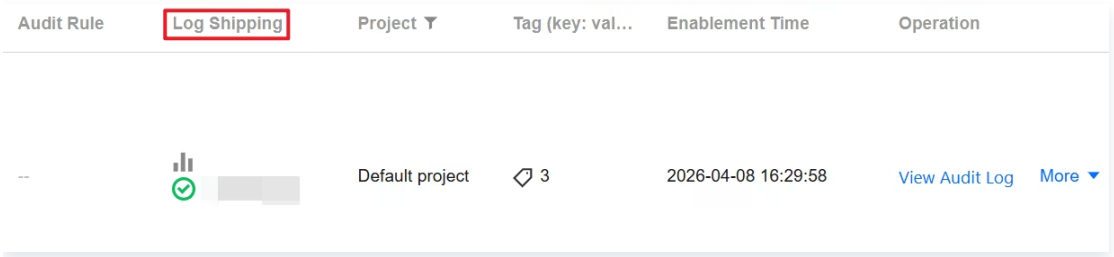
After enabling the log shipping, you can learn about the real-time shipping traffic generated by log shipping through the monitoring feature.

Monitoring Metric Name	Callable Metric Name	Unit	Description
Shipping traffic	AuditDeliverRate	MB	Shipping traffic generated by the log shipping

You can find instances with the log shipping feature enabled in Audit Instance List. Under the **Log Shipping** field, you can click the monitoring icon to view the monitoring status of the shipping traffic.



Description of Log Shipping Status



As shown above, on the SQL Insight (Database Audit) page of TencentDB for MySQL, the audit log shipping status of instances is displayed under the **Log Shipping** column. The descriptions of each shipping status are as follows.

- **Ckafka**: Indicates that the SQL Insight (Database Audit) feature of the current instance has enabled log shipping to the Ckafka message queue.
- **CLS**: Indicates that the SQL Insight (Database Audit) feature of the current instance has enabled log shipping to CLS.
- **COS**: Indicates that the SQL Insight (Database Audit) feature of the current instance has enabled log shipping to COS.
- **Disabled**: Indicates that the SQL Insight (Database Audit) feature of the current instance has not been configured for log shipping.

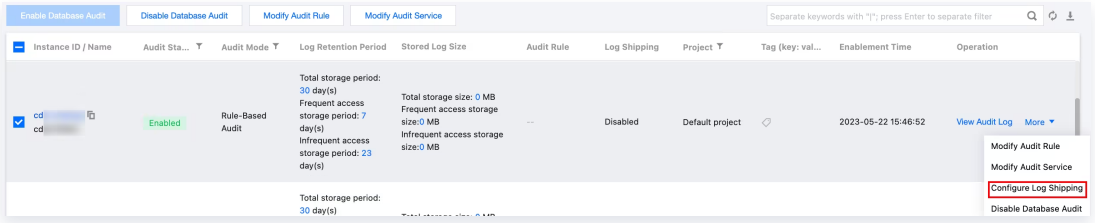
Related Documentation

For relevant procedures on shipping audit logs to CLS, Ckafka message queues, and COS, refer to the guides on the following pages.

Operations Related to Shipping to CLS

Enabling Log Shipping to CLS

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a region at the top. On the **Audit Instance** page, click **Audit Log Storage Status**, and select the **Enabled** option to filter instances with audit enabled.
4. Find the target instance in the audit instance list (or search for the instance by resource attributes in the search box), and choose **More** > **Configure Log Shipping** in the **Operation** column.



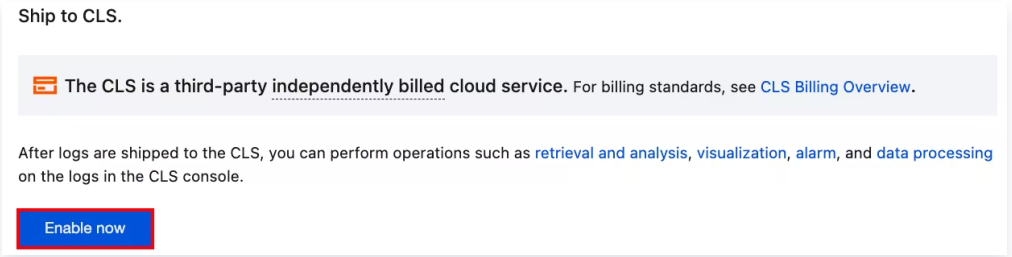
5. (Skip this step if CLS has already been activated.) Click **go to activate** in the pop-up sidebar to activate CLS.
6. (Skip this step if CLS has already been activated.) Return to the console after activation and click **Activation Completed** in the pop-up window for activation confirmation.

> **Note:**
> During the activation process, the system will verify whether activation is successful. If the system prompts that activation has failed, wait for a while and try again.

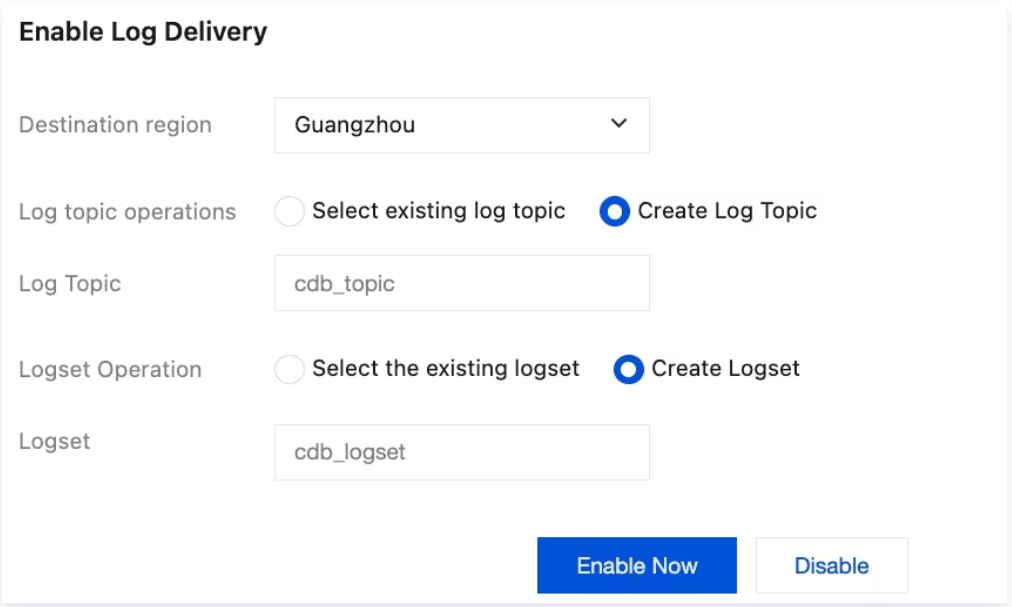
7. (Skip this step if COS has already been authorized.) In the sidebar, click **Go to Authorization**. Then, in the **Service Authorization** pop-up window, click **Grant**.

> **Note:**
> During the authorization process, the system will verify whether the service role authorization is successful. If the system prompts that authorization has failed, wait for a while and try again.

8. Click **Enable Now** in the **Ship to CLS** area in the sidebar.



9. Complete the following configurations in the pop-up window and click **Enable Now**.



Parameter	Description
Destination region	Select the region for log shipping. If CLS supports the region where the database instance resides, this item will default to the instance region (you may select other available regions). If CLS does not support the database instance region, you can select other regions supported by CLS.
Log topic operations	It supports selecting an existing topic or creating one.
Select existing log topic	If the log topic is set to select an existing topic, you need to further select the existing logsets and log topics. • Logset: Logsets classify log topics to facilitate log topic management. You can filter existing logsets in the search box. • Log topic: A log topic is the basic unit for collecting, storing, retrieving, and analyzing log data. You can filter log topics of the selected logset in the search box.

	Note: Log topics that can be selected in this step should be those created with the Create Log Topic option selected for log topic operations when enabling log shipping in the console. Log topics created in the CLS console cannot be selected.
Create Log Topic	If the log topic is set to create a log topic, you need to further customize the log topic and then assign it to an existing logset or a created logset. • Log topic: A log topic is the basic unit for collecting, storing, retrieving, and analyzing log data. You need to create a log topic. • Select the existing logset: The log topic to be created will be added to an existing logset. If you select this option, you can filter existing logsets in the search box. • Create logset: The log topic to be created will be added to a newly created logset. If you select this option, you need to create a logset.

Viewing Log Shipping to CLS

After the SQL Insight (Database Audit) feature of shipping logs to CLS is enabled for an instance, you can view the current log shipping status to CLS (view the logset and log topic for log shipping).

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a region at the top. On the **Audit Instance** page, find the target instance (or search for the instance by resource attributes in the search box), and choose **More** > **Configure Log Shipping** in the **Operation** column.
4. In the pop-up sidebar, view the current log shipping information.
5. Click the logset name, log topic name, or Search & Analysis to jump to the CLS console to view the details of log shipping.

Disabling Log Shipping to CLS

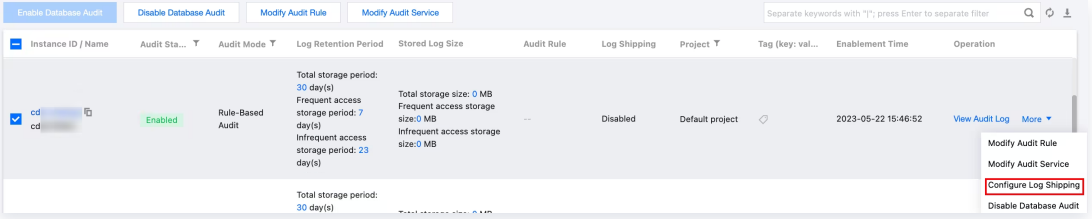
Note:
After log shipping is disabled, the shipping of audit logs for the current instance will stop. Note that only the shipping of new logs will be stopped. Existing logs will continue to be stored in the log topic until expiration, during which storage fees will continue to be incurred. To delete the log topic, go to log topic management to delete it.

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a region at the top. On the **Audit Instance** page, find the target instance (or search for the instance by resource attributes in the search box), and choose **More** > **Configure Log Shipping** in the **Operation** column.
4. Click **Disable Shipping** in the upper right corner of the **Shipping to CLS Log** area in the pop-up sidebar.
5. Read the precautions in the pop-up window, select **Disable**, and click **OK**.

Shipping to TDMQ for CKafka

Enabling Log Shipping to TDMQ for CKafka

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a region at the top. On the **Audit Instance** page, click **Audit Log Storage Status**, and select the **Enabled** option to filter instances with audit enabled.
4. Find the target instance in the audit instance list (or search for the instance by resource attributes in the search box), and choose **More** > **Configure Log Shipping** in the **Operation** column.



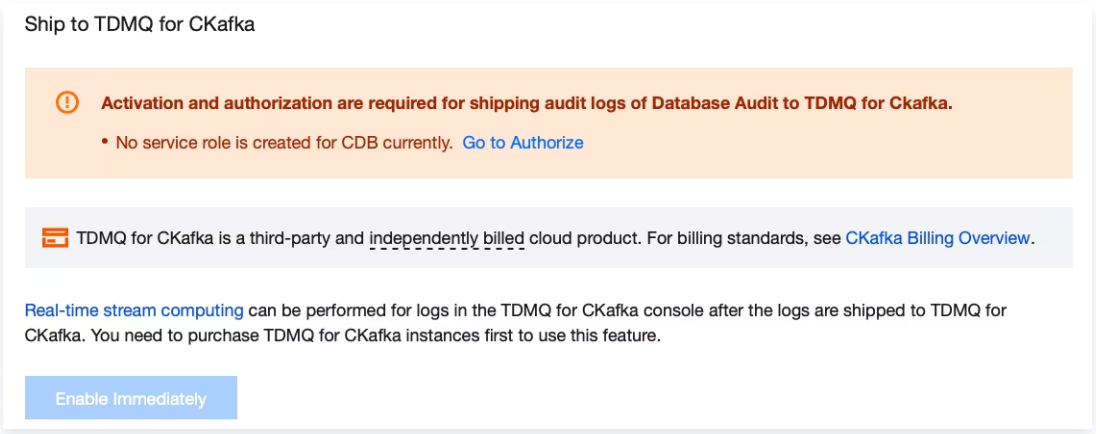
5. (Skip this step if CKafka has already been activated.) Click **go to activate** in the pop-up sidebar to activate CKafka.
6. (Skip this step if CLS has already been activated.) Return to the console after activation and click **Activation Completed** in the pop-up window for activation confirmation.

> **Note:**
> During the activation process, the system will verify whether activation is successful. If the system prompts that activation has failed, wait for a while and try again.

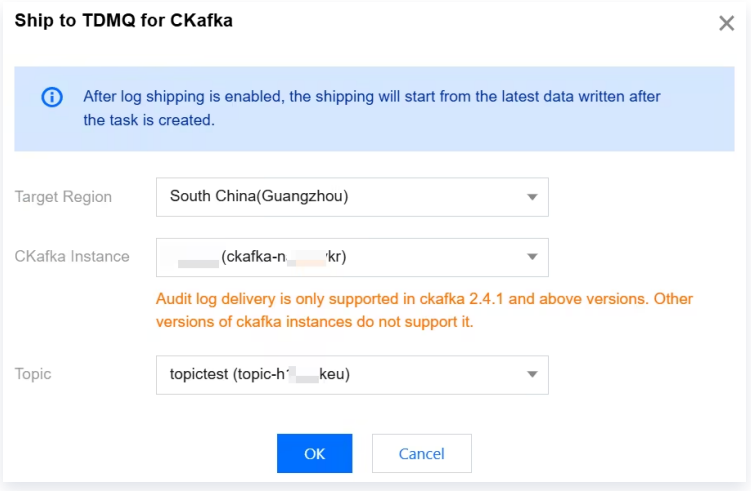
7. (Skip this step if COS has already been authorized.) In the sidebar, click **Go to Authorization**. Then, in the **Service Authorization** pop-up window, click **Grant**.

> **Note:**
> During the authorization process, the system will verify whether the service role authorization is successful. If the system prompts that the authorization fails, you can try authorization again later.

8. Click **Enable immediately** in the **Ship to TDMQ for Ckafka** area in the pop-up sidebar.



9. In the Shipping to Ckafka Message Queue pop-up window, complete the following configurations and click **OK**.



Parameter	Description
Target Region	Select the region for log shipping. If the region where the database instance is located is supported on the TDMQ for CKafka, the location of the instance will be selected by default. You can also choose other available regions; if the region where the database instance is located is not supported on the TDMQ for CKafka, you can choose other regions supported by the TDMQ for CKafka.
CKafka Instance	Select a CKafka instance in the target region.

	Note: Note: Audit log shipping is supported only in CKafka 2.4.1 and later versions. CKafka instances of other versions do not support it.
Topic	Select a topic to ship. If there is no available topic, you can also create one. For operations, view Creating Topic.

Viewing Log Shipping to TDMQ for CKafka

After log shipping to the Ckafka message queue is enabled for the SQL Insight (Database Audit) feature of the instance, you can view the current shipping status to the Ckafka message queue (including the Ckafka instance, Ckafka Topic ID/name, region, and creation time).

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a region at the top. On the **Audit Instance** page, find the target instance (or search for the instance by resource attributes in the search box), and choose **More** > **Configure Log Shipping** in the **Operation** column.
4. In the pop-up sidebar, view the current log shipping information.
5. Click the CKafka instance ID, CKafka topic ID/name, and Message Query button to view instance details and query messages in the CKafka console.

Modifying Shipping

After log shipping to the Ckafka message queue is enabled for the SQL Insight (Database Audit) feature of the instance, if you need to change the destination Ckafka instance, region, or topic (Ckafka Topic ID/name), refer to the following operations.

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a region at the top. On the **Audit Instance** page, find the target instance (or search for the instance by resource attributes in the search box), and choose **More** > **Configure Log Shipping** in the **Operation** column.
4. Click **Modify Shipping** in the upper right corner of the **Ship to TDMQ for Ckafka** area in the pop-up sidebar.
5. Select another CKafka instance, region, or topic (CKafka topic ID/name) in the pop-up window and click **OK**.

Disabling Log Shipping to TDMQ for CKafka

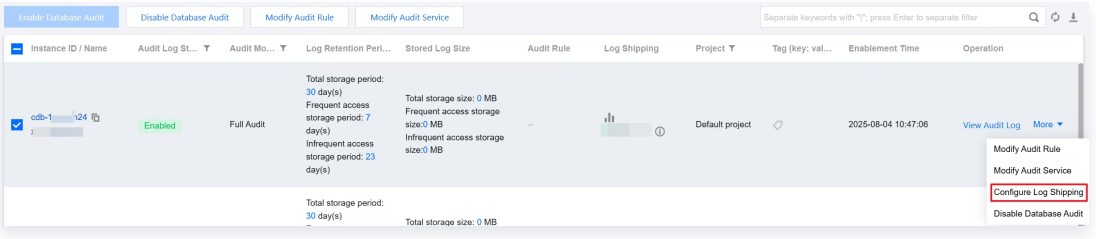
> **Note:**
> After log shipping is disabled, the audit logs of the current instance will no longer be shipped. Note: Only new logs will stop being shipped; existing logs will remain stored in the CKafka message queue until expiration, during which storage fees will continue to incur. To delete messages, go to the CKafka console for configuration.

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a region at the top. On the **Audit Instance** page, find the target instance (or search for the instance by resource attributes in the search box), and choose **More** > **Configure Log Shipping** in the **Operation** column.
4. Click **Disable Shipping** in the upper right corner of **Ship to TDMQ for Ckafka** area in the pop-up sidebar.
5. Read the notes in the pop-up window, select **Disable**, and click **OK**.

Operations About Shipping to COS

Enabling Log Shipping to COS

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a region at the top. On the **Audit Instance** page, click **Audit Log Storage Status**, and select the **Enabled** option to filter instances with audit enabled.
4. Find the target instance in the audit instance list (or search for the instance by resource attributes in the search box), and choose **More** > **Configure Log Shipping** in the **Operation** column.

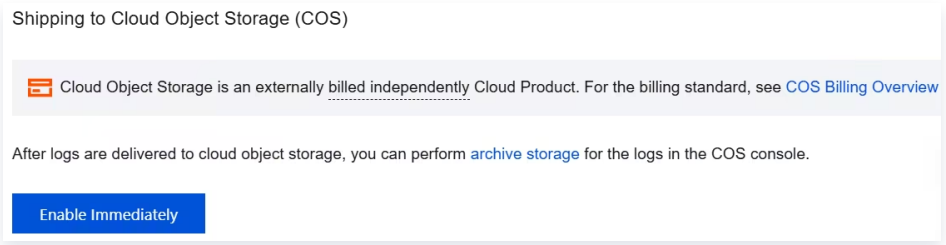


5. (Skip this step if COS has already been authorized.) In the sidebar, click **Go to Authorization**. Then, in the **Service Authorization** pop-up window, click **Grant**.

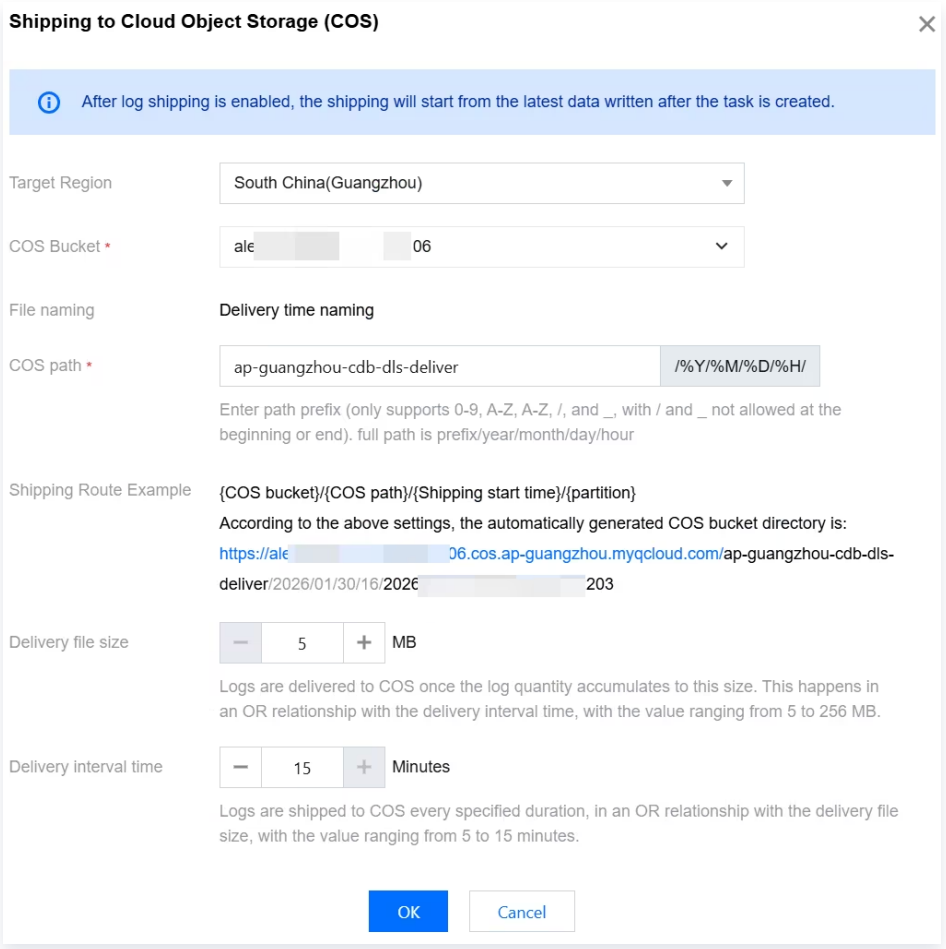
> **Note:**
> During the authorization process, the system will verify whether the service role authorization is successful. If the system prompts that the authorization fails, you

can try authorization again later.

6. In the pop-up sidebar, click **Enable Immediately** below **Shipping to Cloud Object Storage (COS)**.



7. In the Shipping to COS pop-up window, complete the following configurations, and click **OK**.



Parameter	Description
Target Region	Select the region for log shipping. If the region where the database instance resides is supported by COS, this field defaults to that region. You can also choose another available region. If the region where the database instance resides is not supported by COS, you can select another region supported by COS.

COS Bucket	Select an existing COS bucket. The dropdown list supports quick search. If no COS bucket exists, you can select Create Bucket in the dropdown list. If you have not activated COS, the system guides you to activate it during the bucket creation process before you can proceed to complete the bucket creation operation.
File naming	Name the shipping file. By default, the file is named based on the shipping time.
COS Path	Enter a COS path prefix here (Only 0–9, A–Z, a–z, /, and _ are allowed. The / and _ characters cannot be used at the beginning or end of the prefix). Complete path format: prefix/year/month/day/hour. This is the address within your COS bucket where shipped audit log files will be stored.
Shipping Route Example	Automatically generate a COS bucket directory based on the settings of the previous field. You can know the set COS bucket directory as displayed by this field.
Delivery file size	Set the shipping file size in MB. It is used together with the shipping interval. If any of the conditions are met, the file is compressed and shipped to COS according to the corresponding rule. Default value: 5. Value range: 5 to 256. For example, you set the size to 256 MB and the interval to 15 minutes. If the file size reaches 256 MB in 5 minutes, the file size condition is met, which triggers a shipping task.
Delivery interval time	Specify the interval to trigger a shipping task in minutes. It is used together with the file size. If any of the conditions are met, the file is compressed and shipped to COS according to the corresponding rule. Default value: 15. Value range: 5 to 15. For example, you set the size to 256 MB and the interval to 15 minutes. If the file size is only 200 MB after 15 minutes, the shipping interval is met, which triggers a shipping task.

Viewing Log Shipping to COS

After database audit log shipping to COS is enabled for an instance, you can view the current information on log shipping to COS (such as the COS bucket, region, and creation time for log shipping).

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a region at the top. On the **Audit Instance** page, find the target instance (or search for the instance by resource attributes in the search box), and choose **More** > **Configure Log Shipping** in the **Operation** column.

4. In the pop-up sidebar, view the current log shipping information.
5. Click the COS bucket name to navigate to the file list details page of the corresponding bucket. Click **Archive Storage** to navigate to the COS console and view the stored shipping file.

Modifying Shipping

After SQL Insight (Database Audit) log shipping to COS is enabled for an instance, you can refer to the following steps to modify the shipping configuration.

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a region at the top. On the **Audit Instance** page, find the target instance (or search for the instance by resource attributes in the search box), and choose **More** > **Configure Log Shipping** in the **Operation** column.
4. In the pop-up sidebar, click **Modify Delivery** on the right of **Shipping to Cloud Object Storage (COS)**.
5. In the Shipping to COS pop-up window, re-select the required configurations, and click **OK**.

Disabling Log Shipping to COS

> **Note:**
> After log shipping is disabled, the delivery of audit logs for the current instance will stop. Note that only new log deliveries will be stopped; existing logs will remain in COS until they expire. Storage fees will continue to accrue during this period. To delete logs, go to the COS console for configuration.

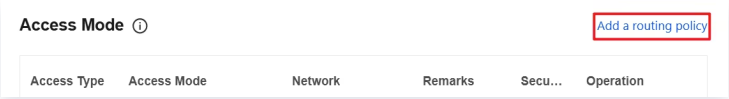
1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a region at the top. On the **Audit Instance** page, find the target instance (or search for the instance by resource attributes in the search box), and choose **More** > **Configure Log Shipping** in the **Operation** column.
4. In the pop-up sidebar, click **Disable Delivery** on the right of **Shipping to Cloud Object Storage (COS)**.
5. Read the notes in the pop-up window, select **Disable**, and click **OK**.

Appendix 1: Adding a Routing Policy

If you need to ship audit logs to Ckafka, you must first add a routing policy under the Ckafka instance. Otherwise, an error may occur when log shipping is configured: "Ckafka does not

support the PLAINTEXT access method for environment routing". The procedure is as follows.

1. Log in to the CKafka console.
2. Click Instance List in the left sidebar and click the ID/name of the target instance to go to the basic information page.
3. On the basic instance information page, click **Add a routing policy** in the Access Method module.

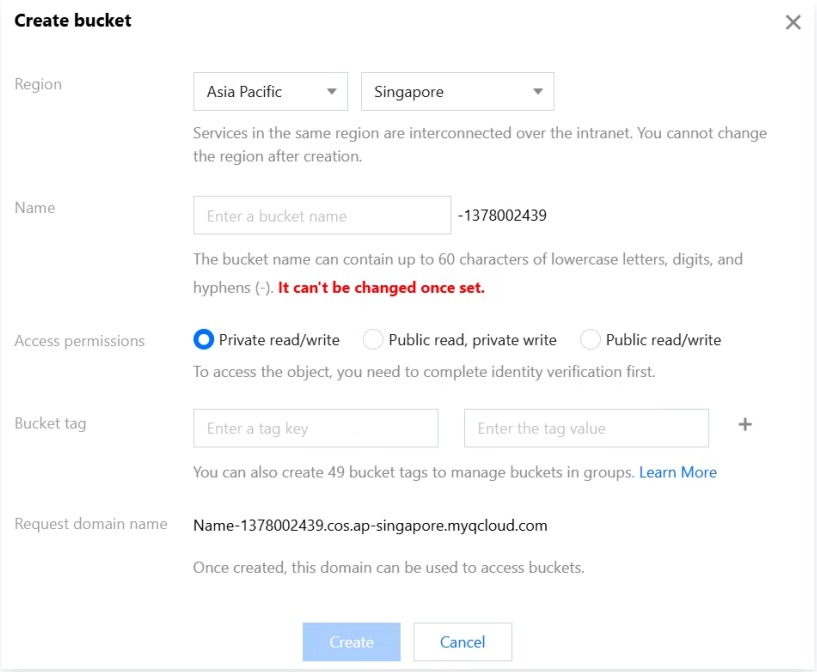


4. In the pop-up window, select **Support Environment** for the routing type, choose **PLAINTEXT** for the access method, and click **Submit**.

Appendix 2: Creating a Bucket

When enabling log shipping to COS, you need to select a COS bucket. If no COS bucket exists, you can follow the steps below to create a bucket and then select it.

1. Click **Create Bucket** in the dropdown list.
2. In the pop-up window, complete the following configurations, and click **Create**.



Parameter	Description
Region	Select a region of the bucket. You should select a COS region corresponding to the physical region where your business is mainly located for communication with other Tencent Cloud services in the same region via the private network. **The region cannot be modified after creation.**

Name	Enter a custom bucket name. Only lowercase letters, digits, and hyphens (-) are supported. The total number of characters in the domain name cannot exceed 60. **The bucket name cannot be modified once set.**
Access permissions	Select the access permission. By default, a bucket is provided with three access permissions: private read/write, public read/private write, and public read/write. The permission can be modified after setting. For details, see ACL.
Bucket tag	Bucket tags are used as identifiers for bucket management. You can set tags for buckets to facilitate group-based bucket management. For details, see Setting Bucket Tags.
Request domain name	This field displays the request domain name after the settings are completed. You can use this domain name to access the bucket.

References

Related CLS documents are as follows.:

- Logset
- Managing Log Topics
- Dashboard
- Data Processing
- Search and Analysis

Related documents of TDMQ for CKafka are as follows:

Querying Messages

Relevant COS documents:

- Querying Buckets
- Clearing Buckets
- Deleting Buckets
- ACL

Configuring Post-Event Alarms

Last updated: 2026-05-12 17:03:00

Event alarms related to the SQL Insights (Database Audit) feature have been integrated with TCOP and Event Bus. If you configure risk-level alarms in a rule template and choose to send alarms, audit logs that match that rule template will trigger alarm notifications to bound users. In TCOP, users can also view alarm history, manage alarm policies (alarm switch), and configure alarm blocking. Configuring event alarms for SQL Insights (Database Audit) helps users obtain risk alarms promptly and quickly locate problematic audit logs.
This document describes how to configure event alarms for instances with the audit service enabled from Tencent Cloud Observability Platform (TCOP) and Event Bridge.

Prerequisites

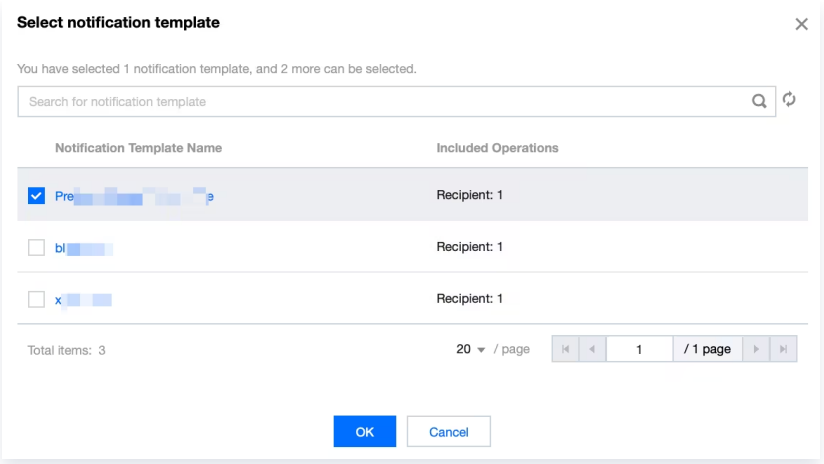
Already enabling the audit service.

Configuring Event Alarms via TCOP

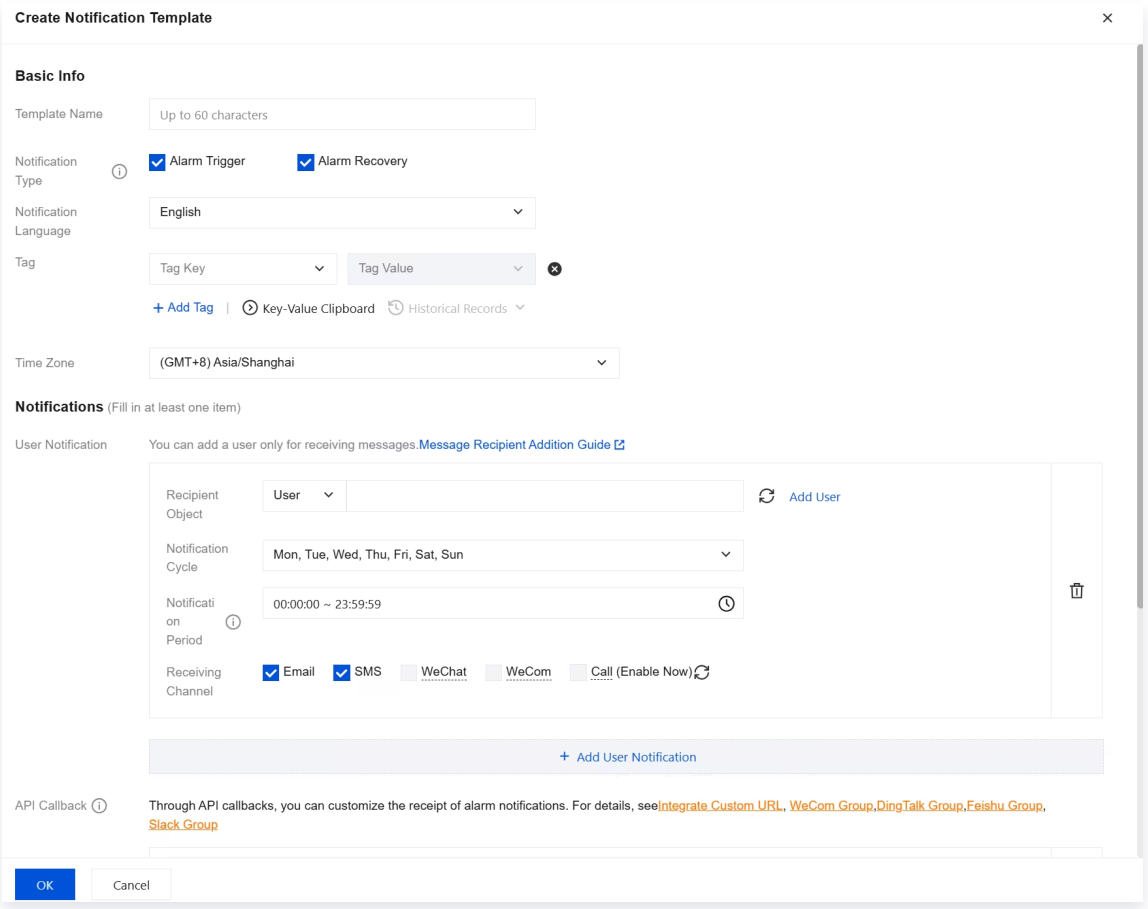
Creating an Alarm Policy

1. Log in to the TCOP console, and choose **Alarm Management** > **Alarm Configuration** in the left sidebar.
2. On the alarm policy list page, click **Create Policy**.
3. On the policy creation page, complete the settings for basic information, alarm rules, and alarm notifications.

- **Policy Type**: choose **CDB** > **MySQL** > **MASTER**.
- **Alarm Object**: You can locate the object instance to be associated by selecting the region where the object resides or searching for the instance ID of the object.
- **Trigger Condition**: Find the event alarm, click **Add Event**, and add alarm events for **AuditLowRisk**, **AuditMediumRisk**, or **AuditHighRisk** based on the actual risk level for which you need to alarm.
- **Configure Alarm Notification**: You can select either system preset notification templates or custom notification templates. Each alarm policy can be bound to up to three notification templates. For custom templates, see Create Notification Template.
  - Select a system preset template.



- Create a template.



4. After confirmation, click **OK**.

Associating an Alarm Object

After creating an alarm policy, you can also associate other alarm objects with it (instances consistent with this alarm policy). When rules in the rule template are triggered, and the risk level matches the added level, and the alarm policy of the rule template is set to **send alarm** for the instance, the generated audit logs will send alarm notifications.

1. On the Alarm Policy List Page, click the **Policy Name** to go to the Alarm Policy Management Page.

2. On the **Alarm Object** section of the alarm policy management page, click **Add Object**.
3. In the pop-up dialog box, select the alarm object to be associated with, and click **OK** to associate the alarm object.

View Alarm History, Manage Alarm Policies (Alarm Switch), and Mute Alarms

You can use TCOP to view related event alarm history, manage alarm policies, and create alarm muting. For related operations, refer to the following guidance:

- View alarm history
- Alarm Enable/Disable
- Alarm Muting

Configure Event Alarms via Event Bus

Step 1: Enable Event Bus

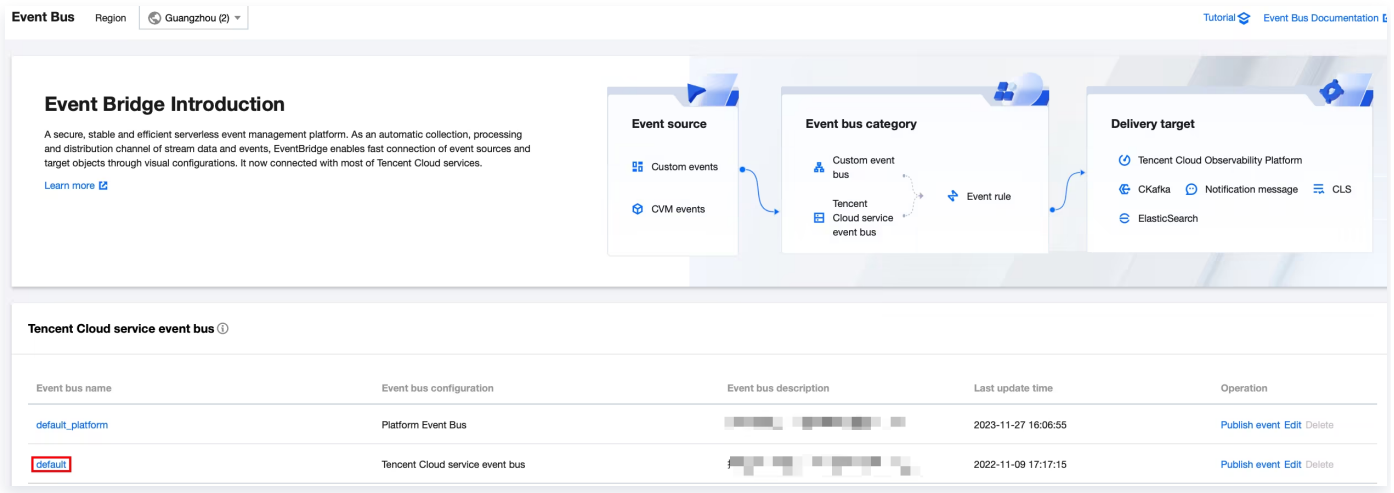
Tencent Cloud EventBridge implements permission management through Cloud Access Management (CAM). CAM is a permission and access management service provided by Tencent Cloud, primarily designed to help customers securely manage access permissions to resources under their Tencent Cloud accounts. Users can create, manage, and delete users (groups) through CAM, and control other users' permissions to use Tencent Cloud resources via identity management and policy management. Before using EventBridge, you need to activate the service on the product page. For activation methods for the primary account and granting sub-accounts permission to use this service, see Activating EventBridge.

Step 2: Configuring Event Alarms for TencentDB for MySQL SQL Insight (Database Audit)

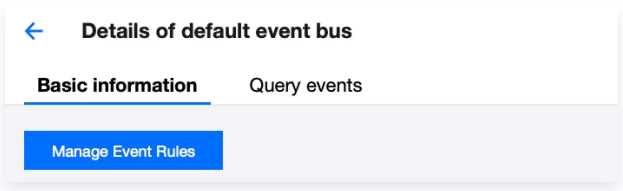
After the EventBridge service is enabled, you need to select an event source connection method. Currently, monitoring events generated by TencentDB for MySQL SQL Insight (Database Audit) are supported as event sources for connecting to EventBridge.

> ⚠ **Note:**
> - For alarm, audit, and other Ops events generated by TencentDB for MySQL, they are all delivered to the **Tencent Cloud service event bus**. This delivery is the default and cannot be changed or edited.
> - After Tencent Cloud EventBridge service is enabled, a default cloud service event set will be automatically created for you in the **Guangzhou region**. Alarm events (monitoring events and audit events) generated by TencentDB for MySQL will be automatically delivered to it.

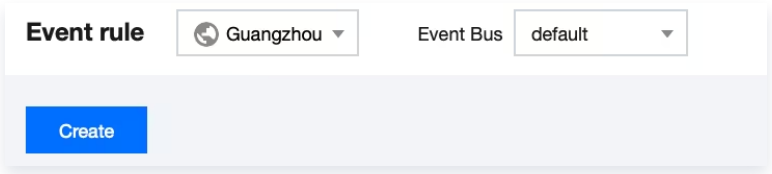
1. Log in to the EventBridge console.
2. Select **Guangzhou** as the region above.
3. Click the **default** event bus under Cloud Service Event Bus.



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



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



6. On the Create Event Rule page, complete the following configurations and click **Next**.

Parameter	Description
Rule name	Fill in the rule name, which can only contain letters, numbers, underscores, and hyphens. It must start with a letter and end with a letter or number, with a length of 2–60 characters.
Rule description	Fill in the rule description, which can only contain numbers, Chinese/English letters, and common punctuation marks, with a maximum of 200 characters.
Tag	Customize whether to enable Tags. After enabling, you can add Tags to this event rule.

Data conversion	Event data transformation helps you easily perform simple processing on event content. For example, you can extract, parse, and remap fields from events before delivering them to event targets.
Event sample	An example event structure is provided as a reference for configuring event matching rules. You can find the target template under event examples for reference.
Event Mode	Supports form mode and custom events. It is recommended to use form mode here for greater efficiency.
Tencent Cloud service	Select TencentDB for MySQL
Event Type	Select the required event types for SQL Insight (Database Audit) related alarms (Database Audit Low Risk, Database Audit Medium Risk, Database Audit High Risk).
Test match rule	Select the event type template from the event examples, then click Test matching rules. If the test passes, you can proceed to the next step.

Note:

If you need to receive event alarms from specified instances, configure it as follows:

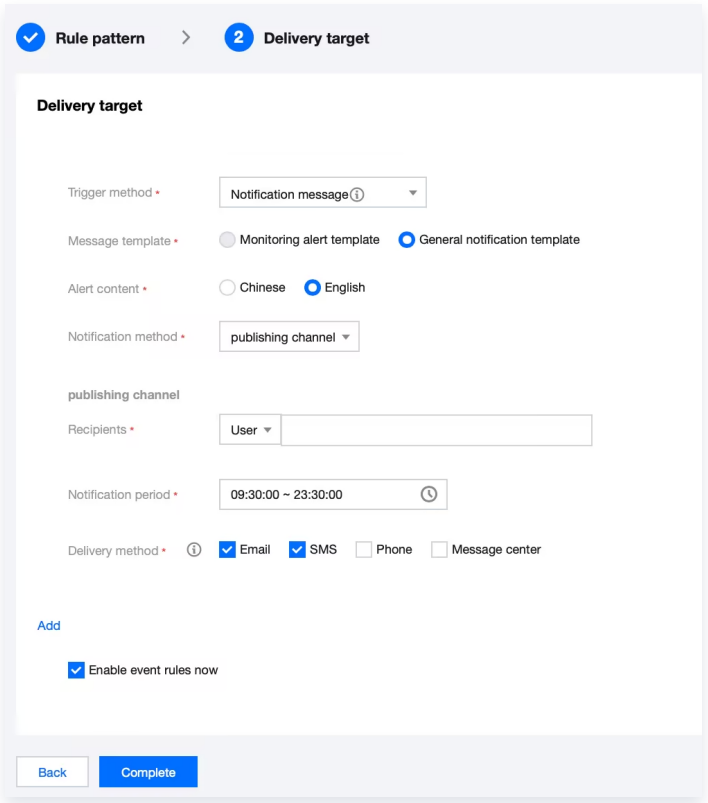
```
{
  "source":"cdb.cloud.tencent",
  "subject":"ins-xxxxxx"
}
```

This indicates that only events from TencentDB for MySQL with instance id ins-xxx can be pushed through rule matching; other events will be discarded and cannot reach users.

You can also use array mode to match multiple resources:

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

7. On the Event Target tab, complete the following configuration, select **Enable event rules now**, and click **Complete**.



Parameter	Description
Trigger method	Select Message Push.
Message template	Supports selecting a monitoring alarm template or a general notification template.
Alarm content	Supports selecting Chinese or English.
Notification method	Supports selecting API callback, channel push, or both. Here, channel push is selected as an example for subsequent configuration steps.
Recipients	Select recipient users or user groups.
Notification period	Custom Notification Time Period

Receive method	Select receiving channels. SMS is limited to 500 characters, and phone is limited to 350 characters. Events that are too long (possibly due to long instance names or other reasons) will not be pushed. It is recommended to configure multiple channels simultaneously.

Note:
If you need to configure multiple event targets, click **Add** to set them up.

8. After creation, you can query and manage this event rule in the event rule list.

Modifying Audit Rule

Last updated: 2026-05-11 19:38:04

This document introduces the operations related to modifying audit rules via the console.

Prerequisites

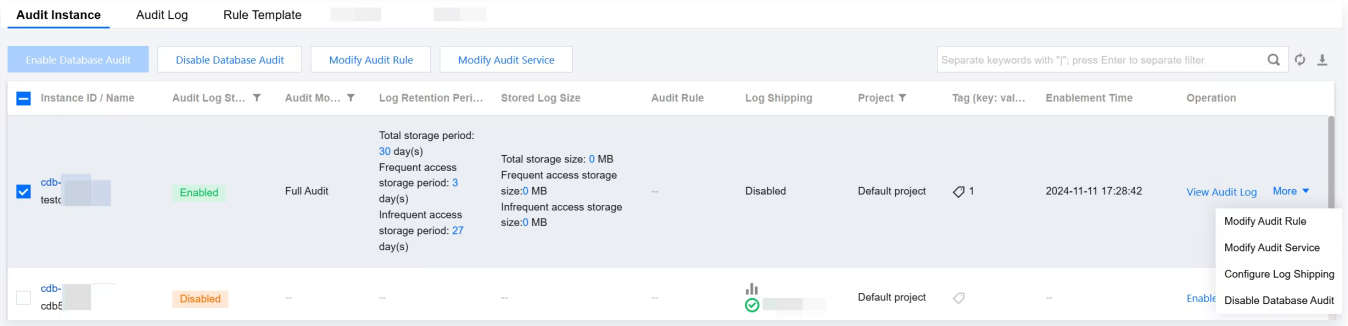
Already enabling the audit service.

Feature Overview

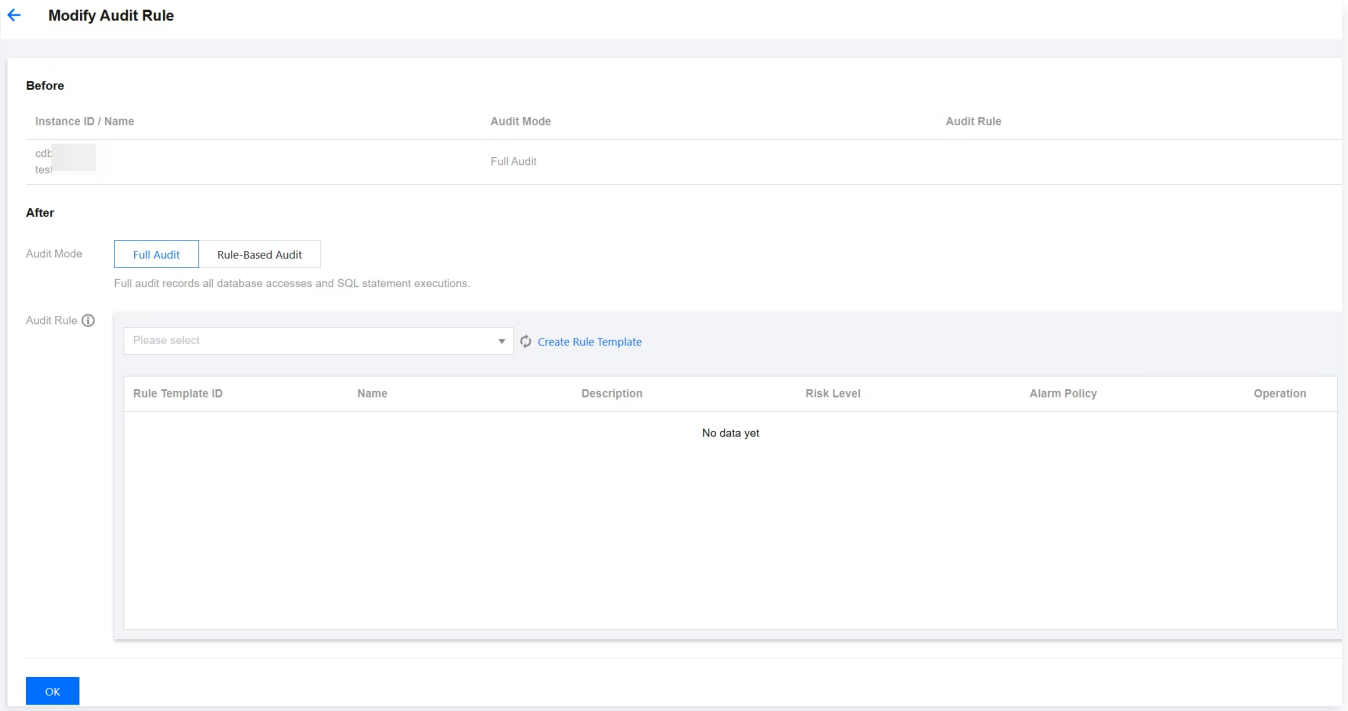
- Audit rules support switching from full audit to rule-based audit, and vice versa. Note that instances with CDS enabled cannot be configured for rule-based audit.
- After the audit rules are modified, the selected instances will be reconfigured according to the updated rules.
- Audit rule modifications include changes to the audit type and rule template.

Modifying Audit Rules for a Single Instance

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select **a region** at the top, click the **Audit Log Storage Status** field on the **Audit Instance** page, and select **Enabled** to filter instances with the audit service enabled.
4. Locate the target instance in the **Audit Instance** list (or quickly find it by filtering by resource attributes in the search box), and in its **Operation** column, choose **More** > **Modify Audit Rule**.



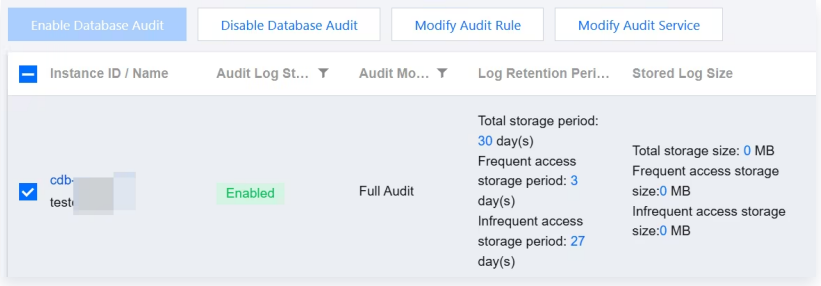
5. In the Modify Audit Rule window, make the desired changes (audit type or audit rules), and click **OK**.



Batch Modification of Audit Rules

> **Note:**
> After batch modification of audit rules, the audit rules for the selected instances will be uniformly adjusted according to the updated rules.

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select **a region** at the top, click the **Audit Log Storage Status** field on the **Audit Instance** page, and select **Enabled** to filter instances with the audit service enabled.
4. Locate the target instance in the **Audit Instance** list (or quickly find it by filtering by resource attributes in the search box), select multiple instances on the audit instance list page, and click **Modify Audit Rule** at the top.



5. In the Modify Audit Rule window, make the desired changes (audit type or audit rules), and click **OK**.

Modifying Audit Services

Last updated: 2026-05-11 19:34:32

This document introduces how to modify the audit service through the console.

Note:

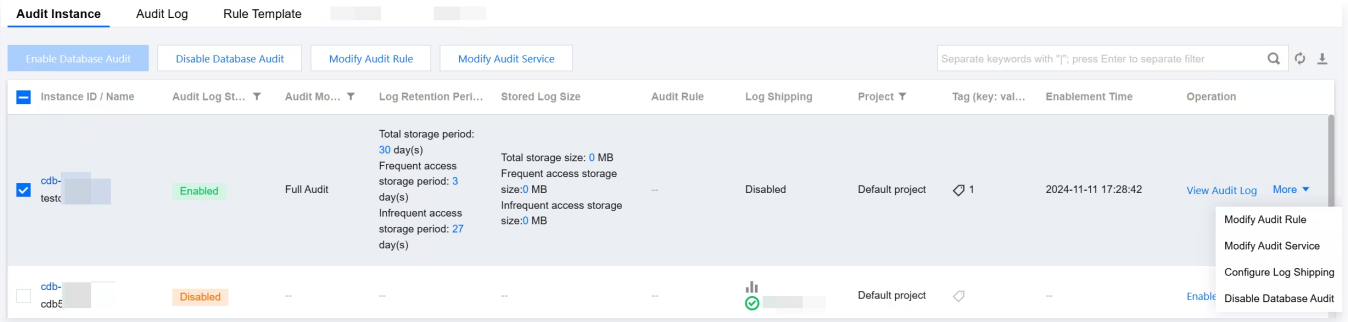
- If you choose to extend the log retention period, the change will take effect immediately. If you choose to shorten the log retention period, historical logs that exceed the new storage duration will be purged immediately.
- If you set data from the last n days to be stored in high-frequency storage, data older than the last n days will automatically be moved to low-frequency storage. After the high-frequency storage duration is extended, audit data that meets the retention period will automatically be migrated from low-frequency storage to high-frequency storage.
- SQL Analysis Option Description: DBbrain leverages the comprehensive problem identification and analysis capabilities provided by SQL Insight (formerly Database Audit) to support abnormal SQL identification, SQL template aggregation statistics, and multi-dimensional performance comparison. This option is enabled by default, supports manual disabling, and indicates that the SQL analysis capability is not enabled.

Prerequisites

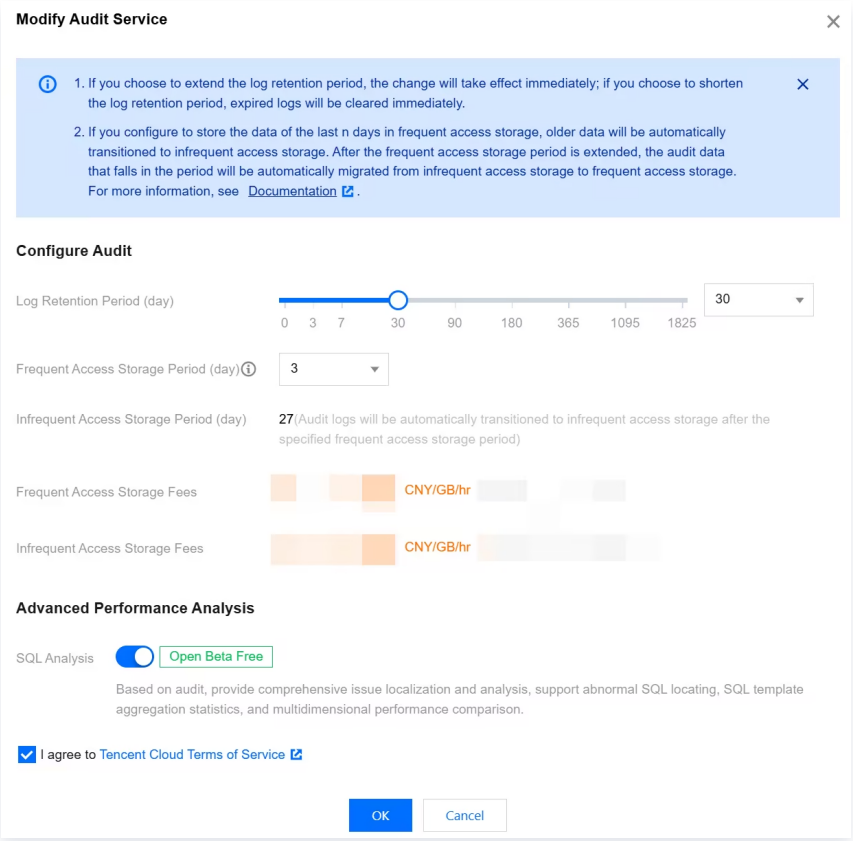
Already enabling the audit service.

Modify Audit Service For Single Instance

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a **region** at the top. On the **Audit Instance** page, click **Audit Log Storage Status** and select the **Enabled** option to filter for instances with the audit service enabled.
4. Locate the target instance in the **Audit Instance** list (you can also quickly find it by filtering with resource attributes in the search box), then choose **More** > **Modify Audit Service** in its **Operation** column.

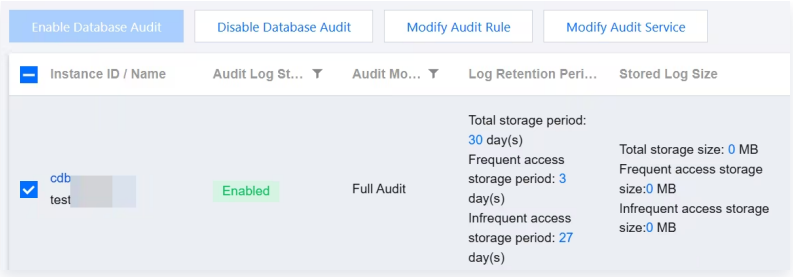


5. On the **Modify Audit Service** page, after modifying the **Log Retention Period** or **Frequent Access Storage Period**, click **OK**.



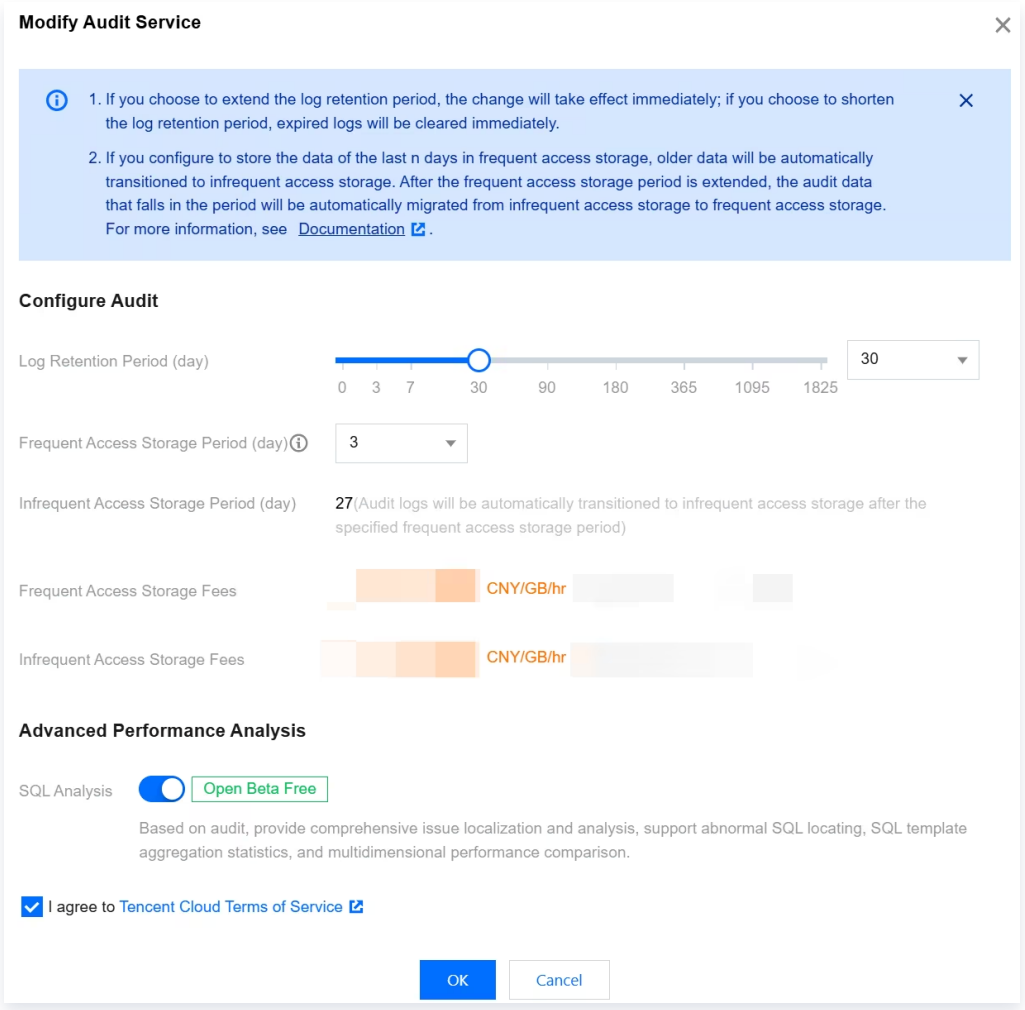
Batch Modification of Audit Service

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. After a **region** is selected at the top, on the **Audit Instance** page, click **Audit Log Storage Status** and select the **Enabled** option to filter out instances that do not have audit enabled.
4. Locate the target instance in the **Audit Instance** list (you can also quickly find it by filtering with resource attributes in the search box). On the **Audit Instance** list page, select multiple target instances, then click **Modify Audit Service** at the top.



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

> **Note:**
> For easy comparison, the batch modification audit service page displays the log retention period before and after modification. After modification, the selected instances will uniformly start adjusting to the new log retention period. Please confirm everything is correct before proceeding with the modification.



Disabling Audit Service

Last updated: 2026-05-11 19:30:12

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

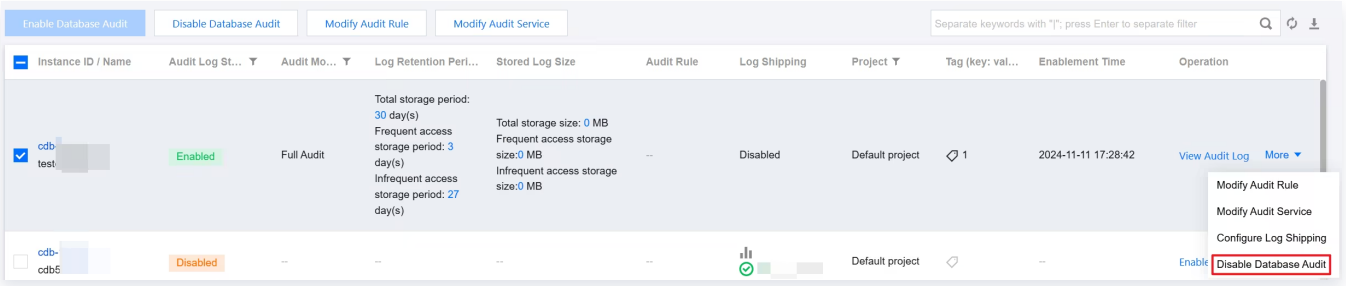
> **Note:**
> After the audit service is disabled, it will stop auditing instances and historical audit logs will be cleared. DBbrain's full-link analysis capability will also be unavailable.

Prerequisites

Already enabling the audit service.

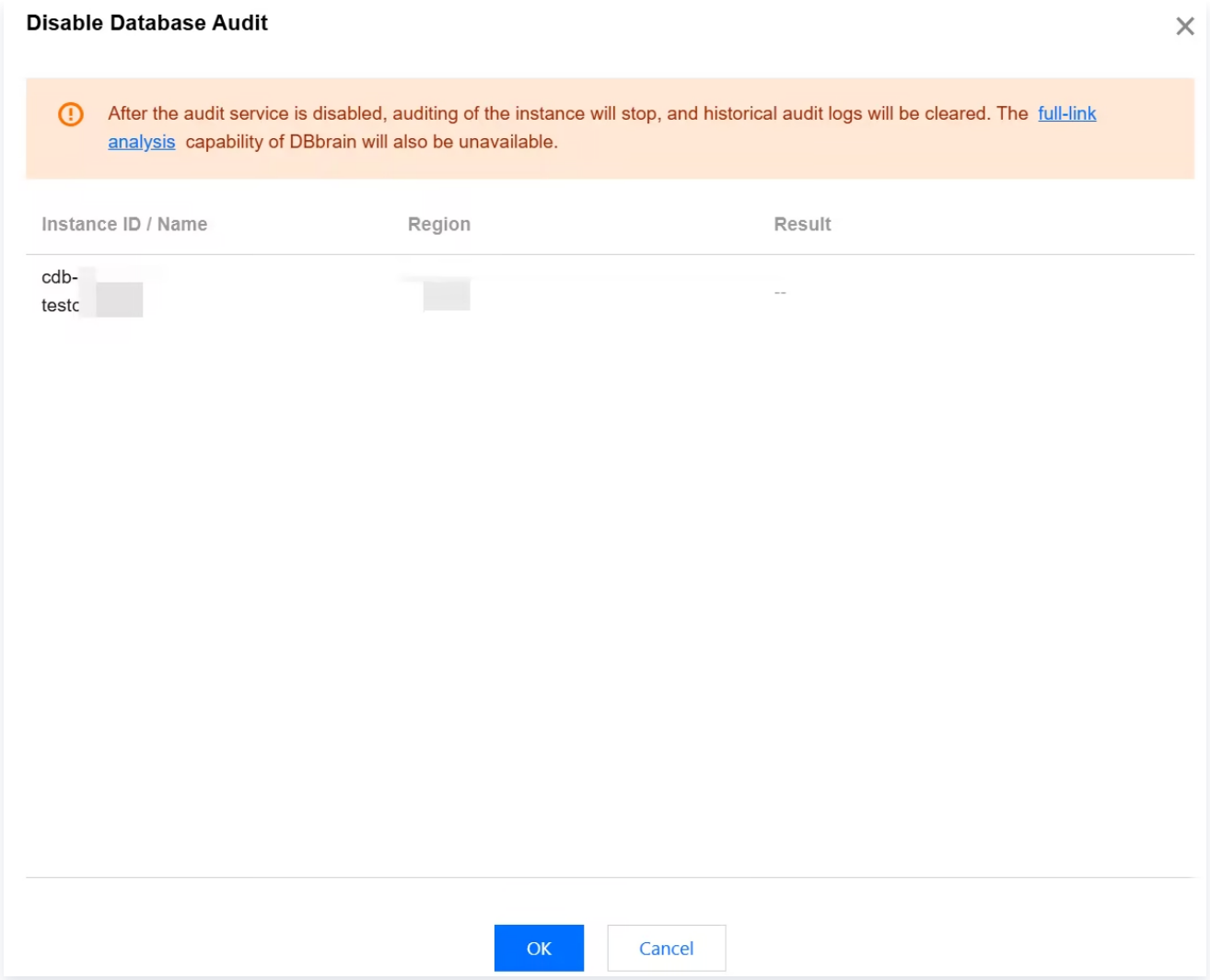
Operation Steps

1. Log in to the TencentDB for MySQL console.
2. Select **SQL Insight (Database Audit)** in the left sidebar.
3. Select a **region** at the top, then on the **Audit Instance** page, click the **Audit Log Storage Status** field and select the **Enabled** option to filter instances with the audit service enabled.
4. In the **Audit Instance** list, locate the target instance (you can also quickly find it by filtering by resource attributes in the search box), then in its **Operation** column, choose **More** > **Disable Database Audit**.



> **Note:**
> Supports batch disabling of the audit service. On the audit instance list page, select multiple target instances and click **Disable Database Audit** at the top.

5. In the **Disable Database Audit** window, click **OK** after verification.



6. After confirmation, the result prompt column will display the disable result. Click **View Task** to jump to the task list for details.

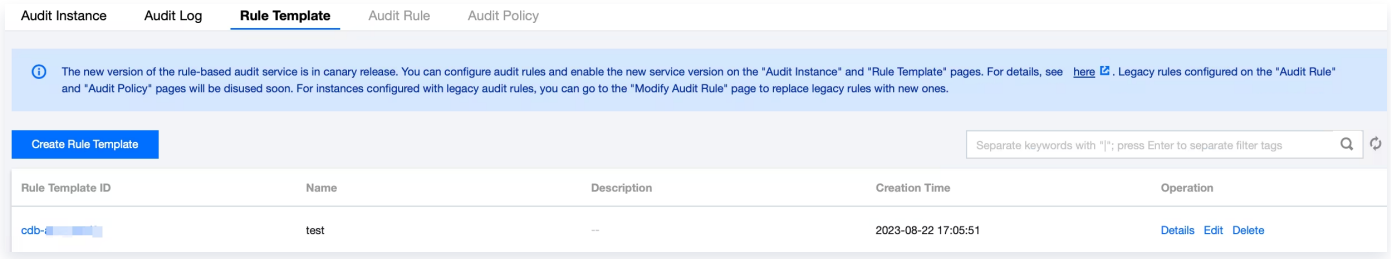
Audit Rule Template
Viewing Rule Template List

Last updated: 2023-09-01 16:37:54

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

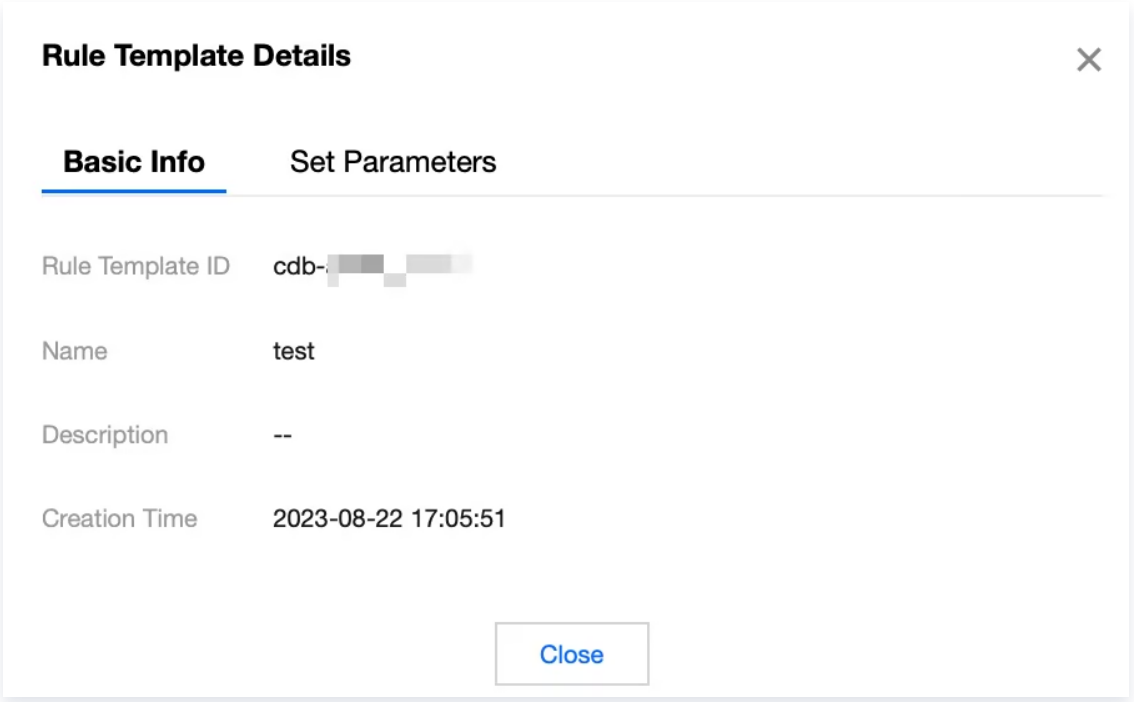
Viewing Rule Template List and Template Details

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

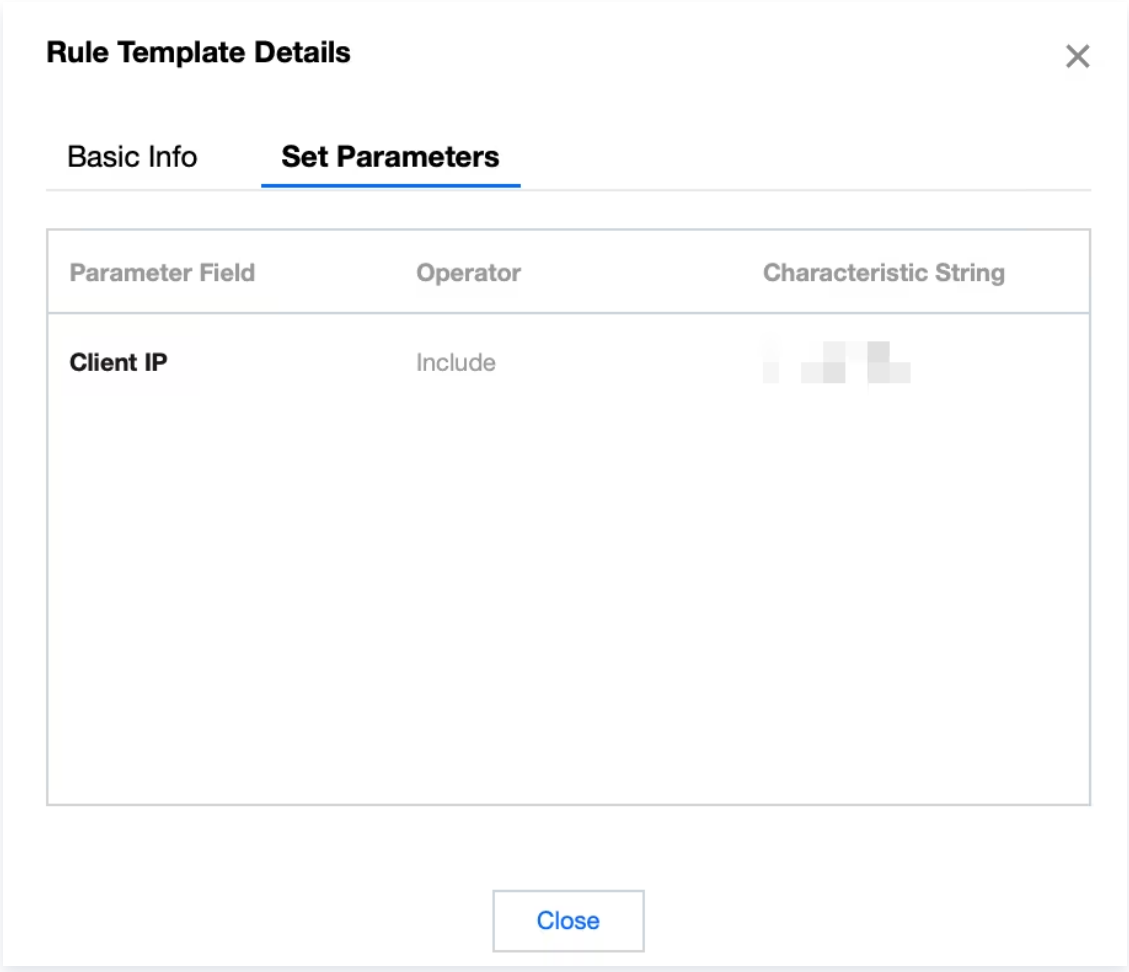


4. Find the target rule template in the **Rule Template** list, or search for it by resource attribute in the search box, and click **Details** in the **Operation** column.
5. In the pop-up window, you can switch the tabs to view the **Basic Info** and **Parameter Settings** of the rule template.

- **Basic Info** tab



- **Parameter Settings** tab



Tool List

Tool	Note
Search box	You can click to filter rule templates by resource attributes such as ID and name. Separate multiple keywords by vertical bar "|" and separate multiple filter tags by carriage return.
Refresh	You can click to refresh the list.

Template List Fields

Parameter	Note
Rule Template ID	ID of a created rule template
Name	Name of a created rule template

Description	Remarks of a created rule template
Creation time	Creation time of a rule template in the format of year-month-day hour:minute:second
Action	• Details: You can view the basic information and parameter settings of the rule template details. • Edit: You can modify the content of the rule template. • Delete: You can delete a rule template.

Related Actions

- Create Rule Template
- Modifying Rule Template
- Delete Rule Template

Creating Rule Template

Last updated: 2025-06-09 17:02:31

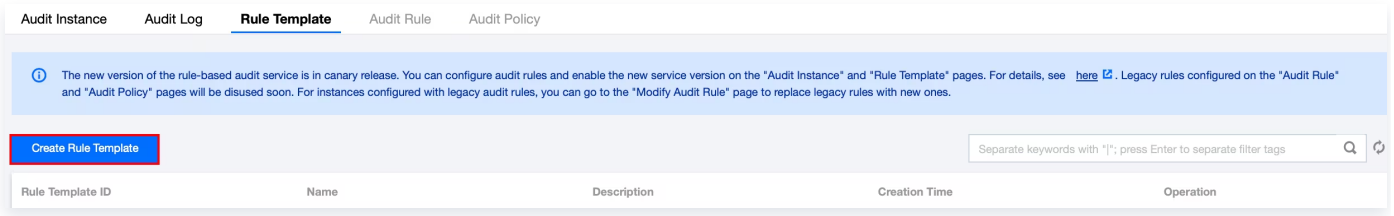
This document describes how to create a rule template in the console.

Note

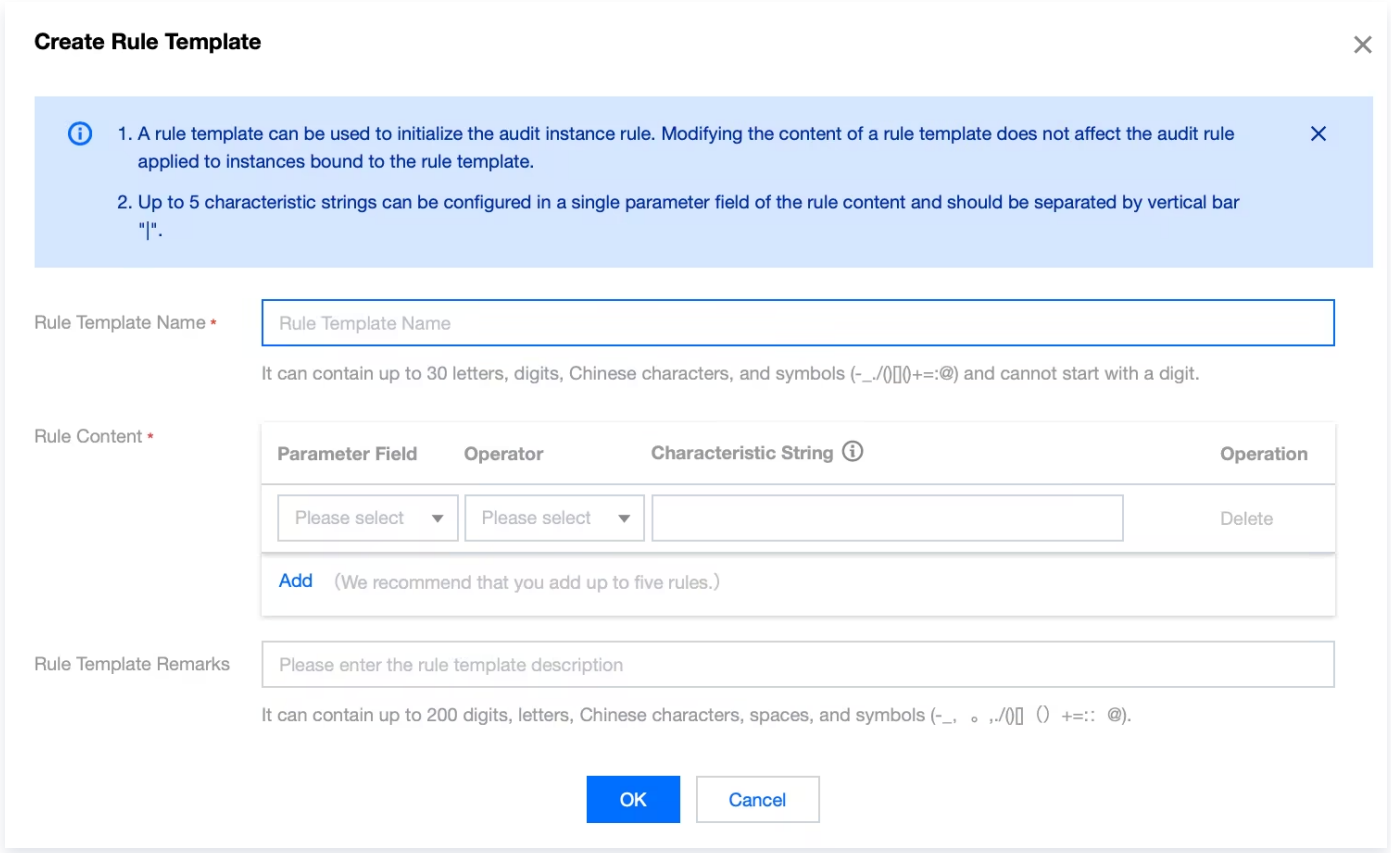
- A rule template can be used to initialize the audit rule for an instance. When a rule template is bound to an instance, the audit rules already applied to the instance remain effective even after the template is modified.
- A rule template allows up to 5 characteristic strings for a single parameter field, with each string being separated by vertical bar "|".

Instructions

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



Category	Note
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 following **Rule content details and examples**. **Note:** • In **Rule Content**, you can click **Add** to add up to 5 parameter fields. • You can click **Delete** in the **Operation** column to delete an unwanted parameter field and condition. However, you must retain at least one parameter field and condition.
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
The 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.
Username	Include, Exclude, Equal to, Not equal to, Regex	Up to five usernames can be configured and should be separated by vertical bar "|". When the operator is **Regex**, only one characteristic string can be entered.
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 "|". When the operator is **Regex**, only one characteristic string can be entered.
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 in microseconds

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: 2025-06-09 17:02:31

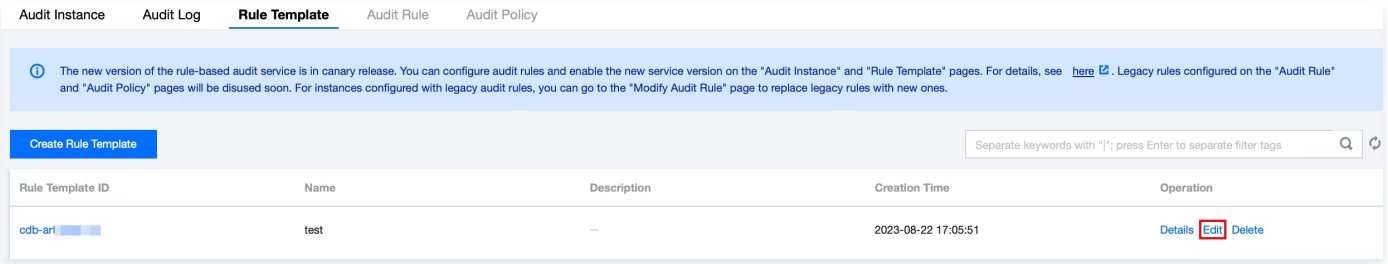
This document describes how to modify a database audit rule template in the console.

Note

- A rule template can be used to initialize the audit rule for an instance. When a rule template is bound to an instance, the audit rules already applied to the instance remain effective even after the template is modified.
- A rule template allows up to 5 characteristic strings for a single parameter field, with each string being separated by vertical bar "|".

Instructions

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

Category	Note
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 following Rule content details and examples introduce **Note:** • In **Rule Content**, you can click **Add** to add up to 5 parameter fields.

	• You can click **Delete** in the **Operation** column to delete an unwanted parameter field and condition. However, you must retain at least one parameter field and condition.
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
The 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.
Username	Include, Exclude, Equal to, Not equal to, Regex	Up to five usernames can be configured and should be separated by vertical bar "|". When the operator is **Regex**, only one characteristic string can be entered.
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 "|". When the operator is **Regex**, only one characteristic string can be entered.

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 in microseconds

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

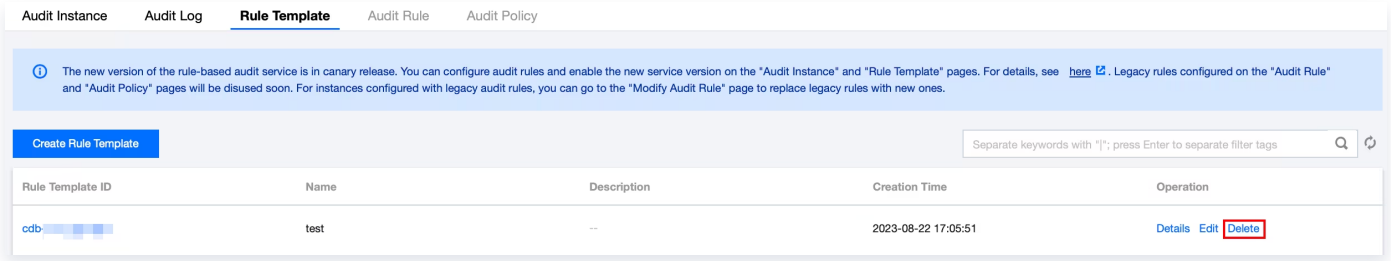
Last updated: 2023-09-01 16:47:10

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

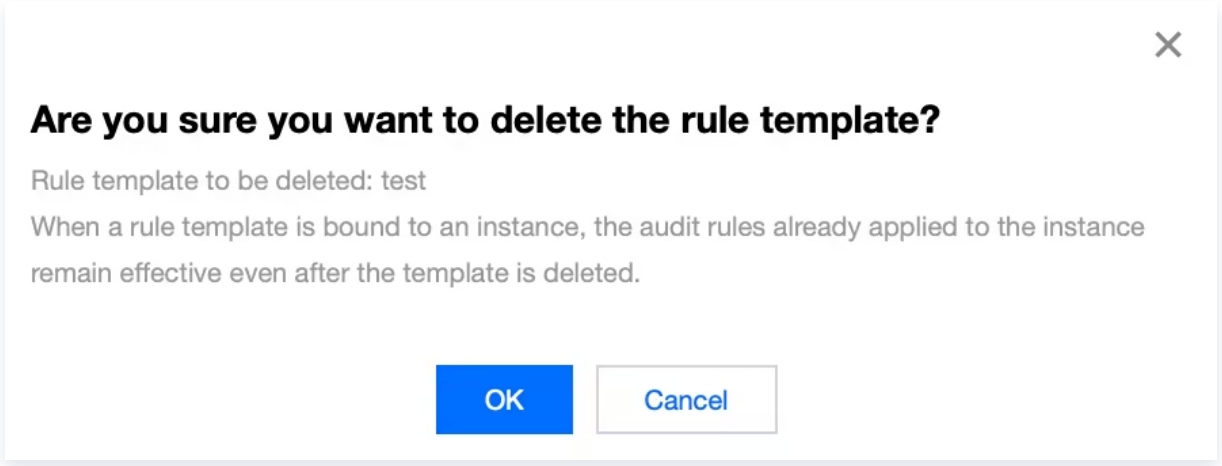
> **Note**
> When a rule template is bound to an instance, the audit rules already applied to the instance remain effective even after the template is deleted.

Instructions

1. Log in to the TencentDB for MySQL console.
2. On the left sidebar, select **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: 2023-09-01 16:47:30

This document describes the TencentDB for MySQL audit rules.

> **Note**
> The current audit rule capability is under reconstruction and does not support adding new rules.

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 matching

- 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, SQLCOM_DROP_TABLE
```

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: 2023-09-01 16:47:50

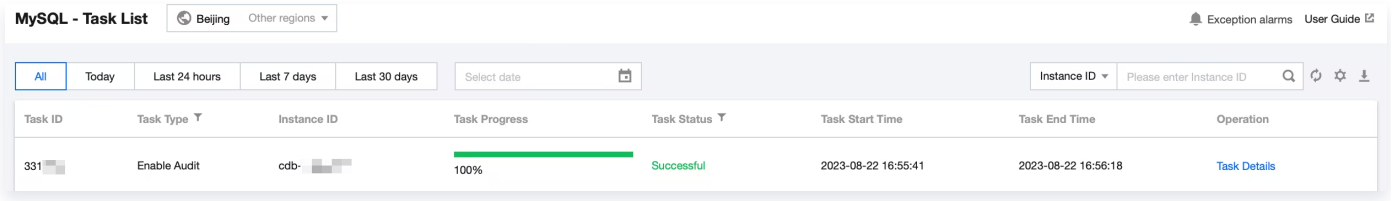
This document describes how to view the details and progress of an audit task in the console, such as enabling/disabling/modifying the audit service and modifying the audit rule.

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

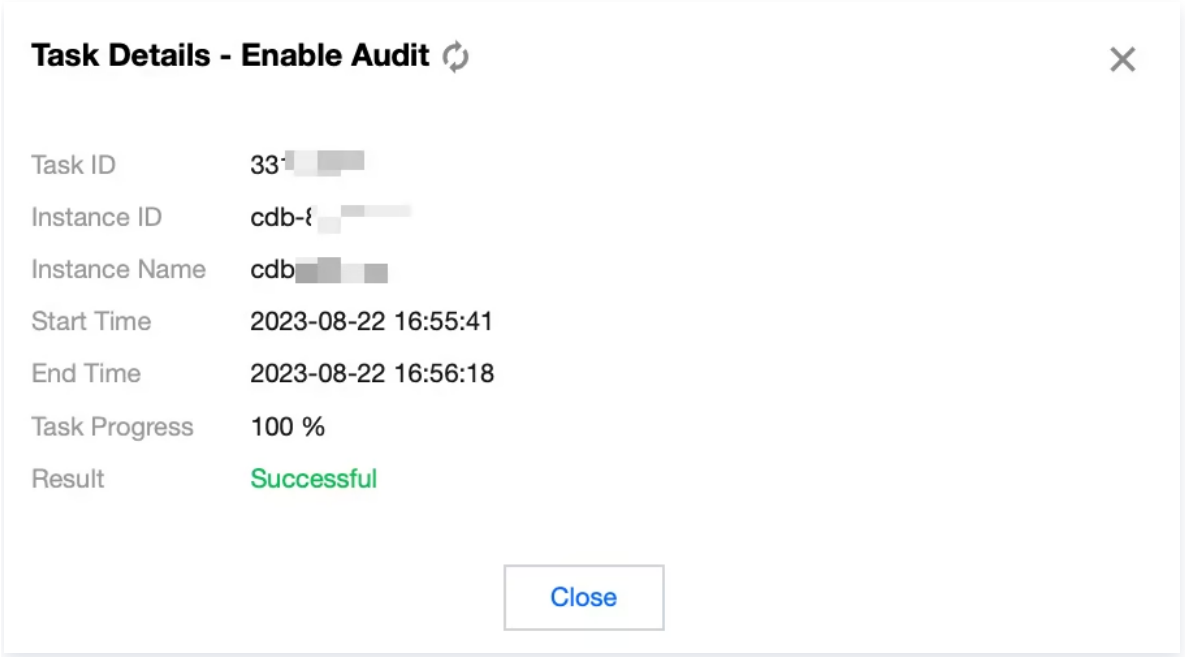
In the task list, you can search for the target task by task ID and instance ID/name. Separate multiple keywords by vertical bar "|" and separate filter tags by carriage return.

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.



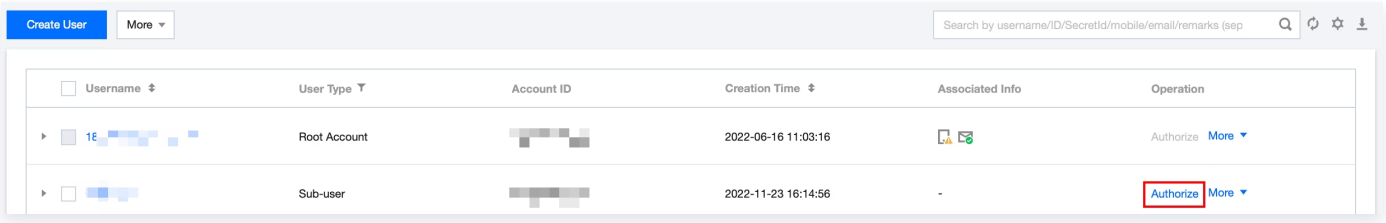
Authorizing Sub-User to Use Database Audit

Last updated: 2023-09-01 16:48:12

By default, sub-accounts have no permission to use TencentDB for MySQL Database Audit. Therefore, you need to create policies to allow sub-accounts to use it.
If you don't need to manage sub-accounts' 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.
When using CAM, you can associate a policy with a user or user group to allow or forbid them to use specified resources to complete specified tasks. For more information on CAM policies, see Syntax Logic.

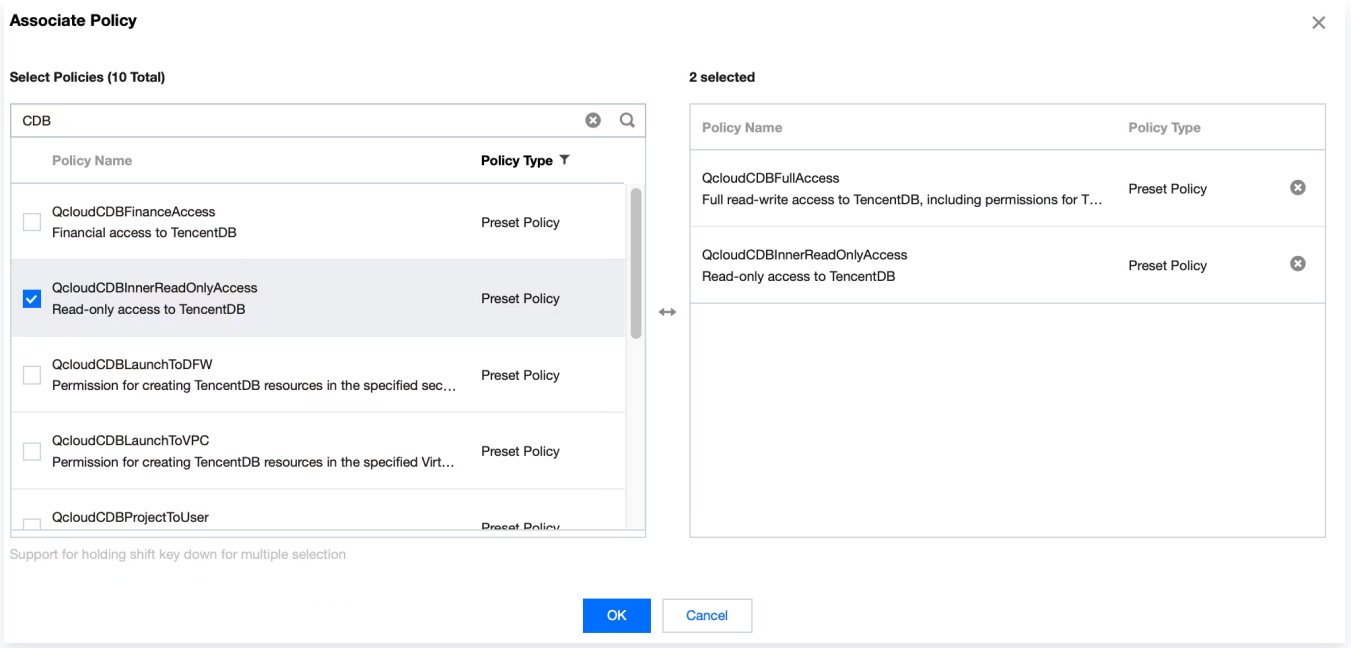
Authorizing Sub-User

1. Log in to the CAM console as a root account, select 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.

Configuring using API

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.

Sample:

```
 "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.

Sample

The following example only shows the usage of CAM. For the complete list of MySQL Database Audit APIs, see the API documentation.

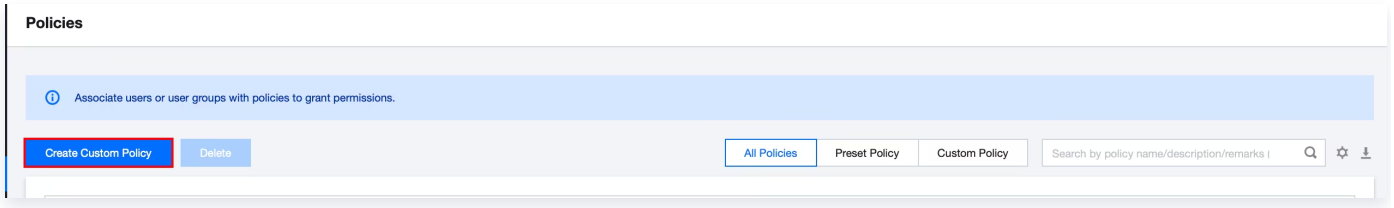
```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
```

```
            "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"
            ]
        }
    ]
}
```

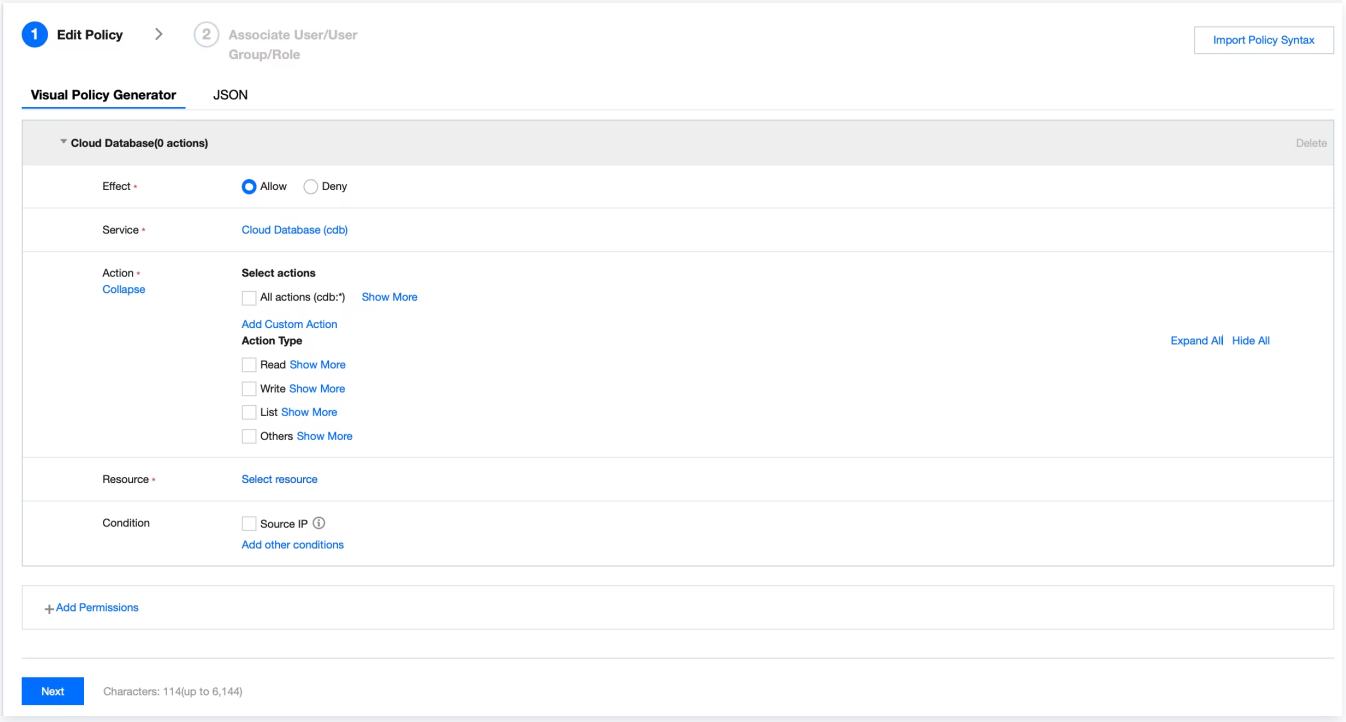
Customizing MySQL Database Audit Policy

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



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

- Service: Select **TencentDB for MySQL**.
- Action: Select all APIs of MySQL Database Audit. For more information, see the API documentation.
- Resource: See Resource Description Method. You can select all resources, indicating 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 **Associate User/User Group/Role** page, enter the **Policy Name** (such as `SQLAuditFullAccess`) as required and **Description**, and click **Complete**.
5. Return to the policy list and you can view the custom policy just created.