

# **TDSQL-C for MySQL**

## **Database Audit**

### **Product Documentation**



## Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

## Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

## Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

---

# Contents

## Database Audit

- Overview

- Viewing Audit Instance List

- Enabling Audit Service

- Viewing Audit Logs

- Post-Event Alarm Configuration

- Modifying Audit Rule

- Modifying Audit Service

- Disabling Audit Service

- Audit Rule Template

  - Viewing Rule Template List

  - Creating Rule Template

  - Modifying Rule Template

  - Deleting Rule Template

- Viewing Audit Task

- Authorizing Sub-User to Use Database Audit

# Database Audit

## Overview

Last updated : 2023-12-12 10:58:22

Database audit is a professional, efficient, and comprehensive database audit service independently developed by Tencent Cloud for monitoring database security in real time. It can record the activities of TencentDB instances in real time, manage the compliance of database operations with fine-grained audit, and alarm risky database behaviors. TDSQL-C for MySQL provides database audit capabilities to help you record accesses to databases and executions of SQL statements, so you can manage risks and improve the database security. In addition, it allows you to customize frequent and infrequent access storage types to greatly reduce the costs of database audit.

The database audit function supports post-event alarms and configuration of alarm policies for events at a high, medium and low risks. The audit logs that match these policies can send alarm notifications to the bound users. At the same time, Users can view the alarm history, manage the alarm policy (toggle alarm switch on/off)) and mute alarms in the Tencent Cloud Observability Platform to help enterprises timely receive related alarm notifications and pinpoint the audit logs that trigger problems.

## Use Cases

Database audit offers a compliance audit basis for enterprises to pass CCP Level 3 and other industry-specific audits. Database audit helps enterprises record, analyze, and track database security incidents such as maloperations. Database audit improves the efficiency and accuracy in various database scenarios such as performance optimization and fault locating.

## Billing

Database audit is billed by the stored log size for every clock-hour, and usage duration shorter than one hour will be calculated as one hour.

For detailed pricing, see [Database Audit Billing Overview](#).

## Supported Versions

Database audit in TDSQL-C for MySQL currently supports MySQL 5.7 and 8.0.

## Strengths

Database audit in TDSQL-C for MySQL has a rich set of features, including full audit, rule-based audit, frequent/infrequent access storage, and long-term audit log retention. It has the following strengths:

### **Data integrity during collection**

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

### **Data reliability during collection**

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

### **Data tampering protection**

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

### **Data integrity during transfer**

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

### **Data integrity during storage**

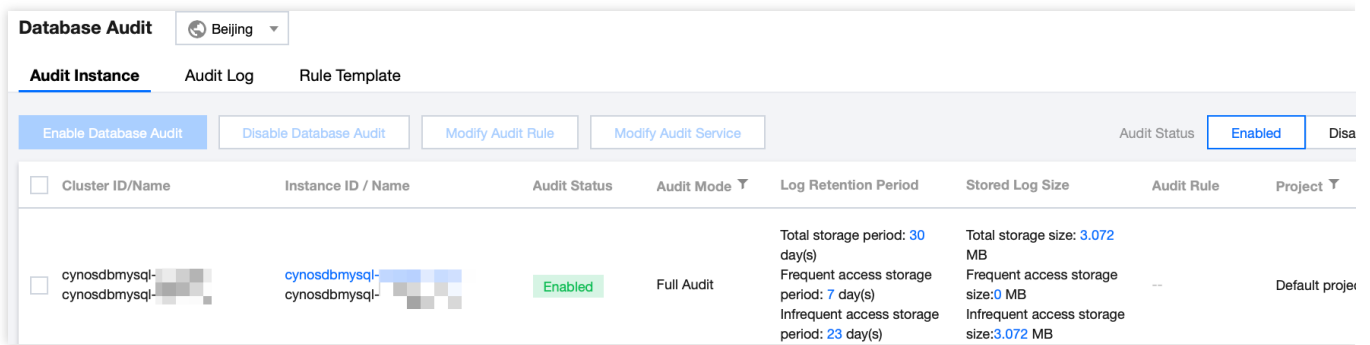
The database audit system encrypts the stored audit log files, so that only users with the encryption certificate access can view audit logs. This effectively prevents internal data leaks caused by plaintext storage and data thefts by high-privileged users, fundamentally eliminating the risks of audit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

# Viewing Audit Instance List

Last updated : 2024-06-07 14:42:22

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



## Audit instance list tab



## Viewing the audit instance list

1. Log in to the [TDSQL-C for MySQL console](#).
2. On the left sidebar, click **Database Audit**.
3. You will go to the **Database Audit > Audit Instance** tab by default.
4. On the **Audit Instance** tab, you can view the list of tools (for quickly filtering clusters/instances, refreshing the tab, and downloading the list information), feature operations, and instance list fields.

### Tool list

Tool	Description
Filter	You can select resource attributes such as instance ID, instance name, cluster ID, cluster name, tag key, and tag in the search box above the audit instance list to filter resources. Separate multiple keywords by vertical bar.
Refresh	You can click  to refresh the data in the audit instance list.
Download	You can click 

to download the information of the filtered audit instances as a .csv file. The list fields in the file include instance ID, instance name, audit status, audit rule, total storage period, frequent access storage period, infrequent access storage period, total storage size, frequent access storage size, infrequent access storage size, project, tag, and remarks.

### Relevant feature operations

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

### Fields in the audit instance list

Field	Description
Cluster ID/Name	ID/Name information of all clusters in a region.
Instance ID/Name	ID/Name information of all read-write instances in a cluster.
Audit Status	Display the enabled or disabled status of the audit service, and support filtering and displaying the clusters/instances in the corresponding status.
Audit Mode	Currently configured audit rules of the audit-enabled instances including <b>Full Audit</b> and <b>Rule-Based Audit</b> , which support a single type of rules displayed by drop-down filtration.
Log Retention	Total, frequent access, and infrequent access storage periods in days for audit-enabled clusters/instances.

Period	
Stored Log Size	Total, frequent access, and infrequent access storage sizes in MB for audit-enabled clusters/instances.
Audit Rule	It displays the number of audit rule templates bound to the instance. The ID and the name of each rule template can be seen when the mouse pointer points to the audit rule field of the corresponding instance. The detailed rule information of that template can be viewed by clicking on a specific rule template, including Basic info, Parameter Settings, and Modification Record.
Project	Projects of clusters/instances to help you categorize and manage resources easily. You can use the drop-down list to filter clusters/instances by a specific project.
Tag (key:value)	Tag information of clusters/instances.
Enabling Time	The time accurate down to the second when the audit service is enabled for clusters/instances.
Operation	Available operations when the audit service is enabled: View Audit Log More (Modify Audit Rule, Modify Audit Service, Disable) Available operations when the audit service is disabled: Enable Database Audit



# Enabling Audit Service

Last updated : 2024-06-18 09:37:17

TDSQL-C for MySQL provides database audit capabilities to help you record accesses to databases and executions of SQL statements, so you can manage risks and improve the database security. This document describes how to enable the audit service in the console.

## Prerequisite

You have created a cluster. For more information, see [Creating Cluster](#).

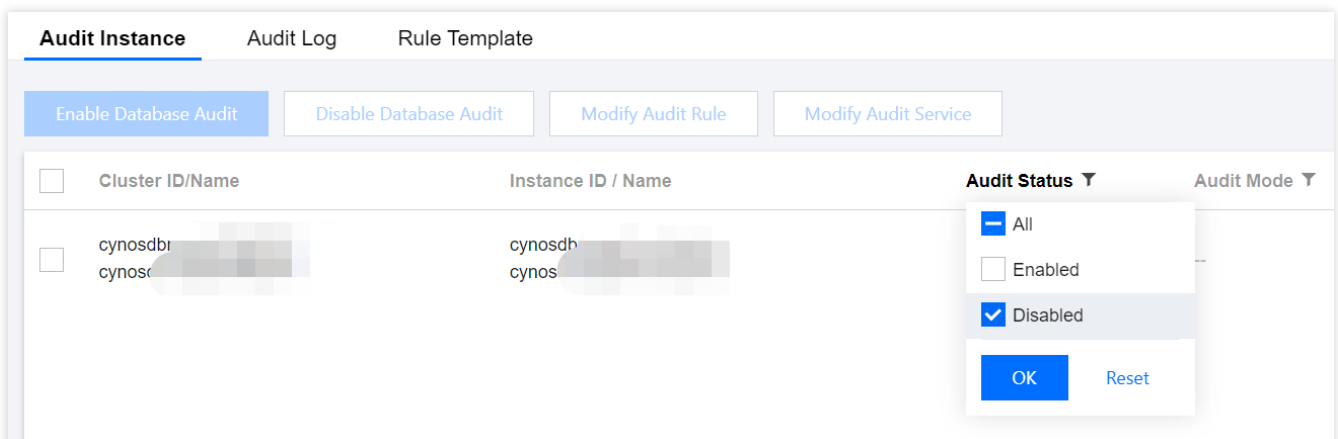
To utilize the rule-based audit capability, please [submit a service ticket](#).

The event alarm function is currently only available in Beijing, Shanghai, Guangzhou, Chengdu, and Singapore. To use it, please [submit a service ticket](#).

For instances belonging to **Full Audit**, if it is necessary to set risk levels and alarm policies for audit logs, please [submit a service ticket](#).

## Directions

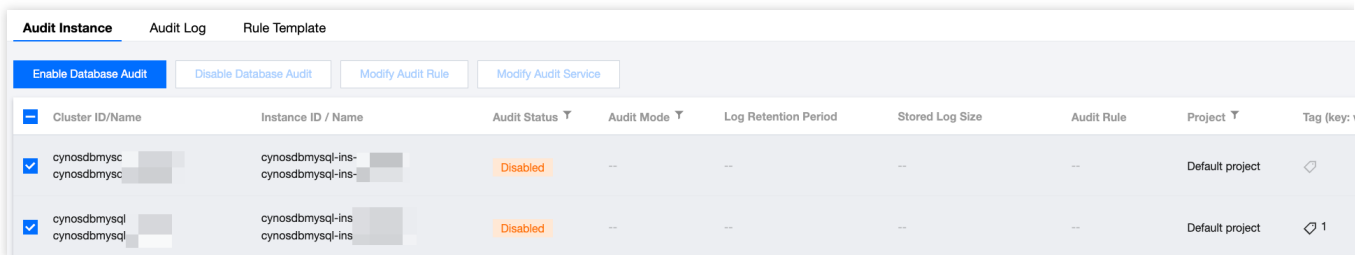
1. Log in to the [TDSQL-C for MySQL console](#).
2. On the left sidebar, click **Database Audit**.
3. After selecting a region at the top, click on **Audit Status** on the **Audit Instance** page, and select the **Disabled** option to filter instances that have not enabled audit.



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

**Note:**

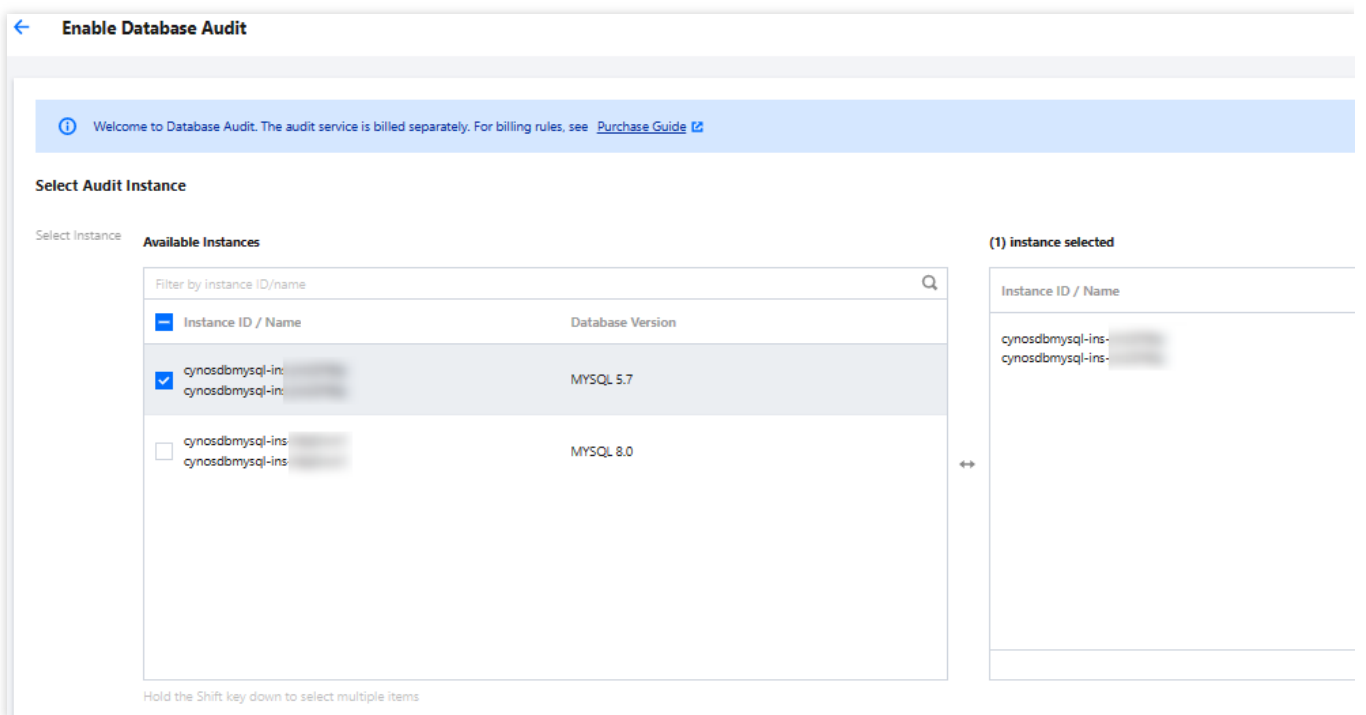
You can batch enable the audit service for multiple target instances by selecting them in the audit instance list and clicking **Enable Database Audit** above the list.



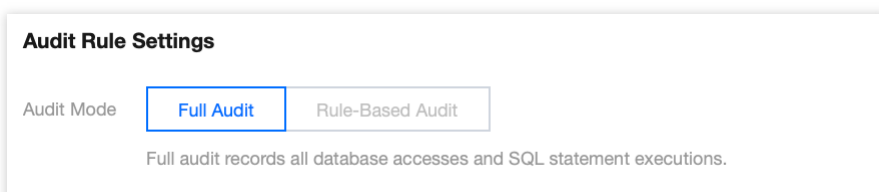
5. On the **Enable Database Audit** page, configure **Select Audit Instance**, **Audit Rule Settings**, **Configure Audit**, read and indicate your consent to the **Tencent Cloud Terms of Service**, and click **OK**.

### 5.1 Audit instance selection

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



### 5.2 Audit rule settings



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

Parameter	Description

Full Audit	Full audit records all database accesses and SQL statement executions.
Rule-Based Audit	Rule-based audit records the access to the database and the execution of SQL statements based on the customized audit rules.

When the audit mode is set to **Full Audit**, there are two actual operational scenarios in the console, for which you may refer to the corresponding procedures.

Scenario 1: Risk level and alarm capability without applying for the use of full audit

Scenario 2: Risk level and alarm capability after applying for the use of full audit

Upon setting the audit mode to **Full Audit**, you may directly proceed to the [audit service settings](#) step.

5.2.1 Select the existing template from the rule template or choose to create a rule template. For more information, please refer to [Create Rule Template](#).

5.2.2 Upon completion of the rule template setting, proceed to the [Audit Service Setup](#) step.

Note:

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

The rule template is designed for instances of **Full Audit mode**, and is only used for setting risk levels and alarm policies for audit logs that match the rule content of the template. Audit logs that do not match the rule content are still retained.

When the audit mode is set to **Rule-Based Audit**, you may select an existing rule template from the rule template or create a rule template. If an existing rule template from the rule template is chosen, you can directly proceed to the audit service settings. If there is no suitable rule templates in the rule template, you can refresh after creating a rule template, and then select the created one. For more information, please refer to [create rule template](#).

**Note:**

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

The rule template is designed for instances of **Rule-Based Audit** mode. It is used for log retention and risk level and alarm policy settings of the audit logs that match the template rule content. Audit logs that do not match the rule content are no longer retained.

5.3

### Audit service settings

In the **Configure audit** section, set the audit log retention period as well as frequent and infrequent access storage periods, read and indicate your content to the Tencent Cloud Terms of Service, and click **OK**.

**Configure Audit**

Log Retention Period (day) 0      7      30      90      180      365

Frequent Access Storage Period (day)

Infrequent Access Storage Period (day) **23**(Audit logs will be automatically migrated to infrequent access storage after the specified frequent access storage period)

Frequent Access Storage Fees ██████████ USD/GB/hr

Infrequent Access Storage Fees ██████████ USD/GB/hr

I agree to [Tencent Cloud Terms of Service](#)

OK

Parameter	Description
Log Retention Period	The audit log retention period in days, which can be 7, 30, 90, 180, 365, 1,095, or 1,825 days.
Frequent Access Storage Period	Frequent access storage has the best query performance as it uses ultra high-performance storage media. Audit data is initially stored in frequent access storage for the time period specified here, after which it is automatically migrated to infrequent access storage. These two storage types only differ in performance but both support auditing. For example, if the log retention period is set to 30 days, and frequent access storage period is set to 7 days, then the infrequent access storage period will be 23 days by default.

# Viewing Audit Logs

Last updated : 2024-10-25 10:19:02

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

## Note:

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

The unit of the audit log field "Execution Time" in the console and downloaded audit log files has been unified to milliseconds.

The unit of the audit log field "CPU Time" in the console and downloaded audit log files has been unified to microseconds.

The unit of the "Timestamp" field in the audit log files has been updated to display millisecond-level timing.

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

After enabling database audit, the storage regions of audit log files for instances in Tianjin, Taipei (China), and Shenzhen are different. Refer to the table below for the corresponding storage regions.

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

## Prerequisite

You have enabled audit service. For more information, see [Enabling Audit Service](#).

## Viewing Audit Logs

### Note:

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

1. Log in to the [TDSQL-C for MySQL console](#).
2. Click **Database Audit** on the left sidebar.

3. After selecting a **region** at the top, click on **Audit Status** on the **Audit Instance** page, and select the **Enabled** option to filter instances that have enabled audit.
4. Find the target instance in the audit instance list, or search for it by resource attribute in the search box, and click **View Audit Log** in the **Operation** column to enter the **Audit Log** tab and view logs.

### Tool list

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

In the **time box**, the last 1 hour is selected by default. You can quickly select another time period (last 3 hours, last 24 hours, or last 7 days), or enter a custom time period, to view relevant audit logs within the chosen time period.

**Note:**

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

In the **search box**, select the search items (such as SQL Details, Client IP, Database Account, Database Name, Error Code, SQL Type, Risk Level, Execution Time (ms), Lock Wait Time (µs), IO Wait Time (µs), Transaction Duration (µs), CPU Time (µs), Audit Rule, Thread ID, Transaction ID, Scanned Rows, Affected Rows, Returned Rows, etc.) for search. This allows you to view relevant audit results. Multiple keywords are separated by line break.

Search Item	Operator	Description
SQL Details	Include-OR-Segment	<p><b>Rule Description</b></p> <p>Enter the details of the SQL command and separate multiple keywords by line break.</p> <p>The match items in the SQL command details search box are divided into three levels. The first level sets the forward and reverse matching modes (Include, Exclude); the second level sets the logical relationship between keywords (OR, AND); the third level sets each keyword matching mode (Segment, Wildcard).</p> <p><b>Note:</b></p> <p>The search of SQL command details is case-insensitive. Include and Exclude match modes are supported.</p>
	Include-AND-Segment	
	Exclude-AND-Segment	

	<p>Include-OR-Wildcard</p> <p>Include-AND-Wildcard</p> <p>Exclude-AND-Wildcard</p>	<p>Keywords support "OR" and "AND" logical match. "OR" means a "union" relationship between different keywords, and "AND" means an "intersection" relationship between different keywords.</p> <p>Each keyword supports two match modes: "segment" and "wildcard".</p> <p>"Segment" means that each keyword in the SQL command details needs to be accurately matched, and "wildcard" means that fuzzy match is supported for each keyword in the SQL command details.</p> <p><b>Example</b></p> <p>For example, if the SQL command details are <code>SELECT * FROM test_db1 join test_db2 LIMIT 1; ,</code></p> <p>In the "Include (segment)" search mode, you can search by segment keywords such as "SELECT", "select from", "", "SELECT * FROM test_db LIMIT 1;", "from Test_DB". However, you can't search by wildcard keywords such as "SEL", "sel", and "test".</p> <p>In the "Include (wildcard)" search mode, you can't search by wildcard keywords such as "SEL", "sel", "test", and "DB".</p> <p>In the "Include (AND)" search mode, multiple keywords are in an "AND" relationship, which means you can query all SQL commands containing "SELECT" and "test_db" by entering keywords such as "SELECT" and "test_db".</p> <p>In the "Include (OR)" search mode, multiple keywords are in an "OR" relationship, which means you can query all SQL commands containing "test_db1" and "test_db2" by entering keywords such as "test_db1" and "test_db2".</p>
Client IP	<p>Include</p> <p>Exclude</p> <p>Equal to</p> <p>Not equal to</p>	<p>You can filter client IP addresses by using the wildcard "" and separate them by line break. For example, if you enter "client IP: 9.223.23.2", IP addresses that start with "9.223.23.2" will be searched.</p>
User Account	<p>Include</p> <p>Exclude</p> <p>Equal to</p> <p>Not equal to</p>	<p>Enter a user account and separate multiple keywords by line break.</p>
Database Name	<p>Include</p> <p>Exclude</p> <p>Equal to</p> <p>Not equal to</p>	<p>Enter a database name and separate multiple keywords by line break.</p> <p><b>Note:</b></p> <p>The search of database name is case-insensitive.</p>
Error Code	<p>Equal to</p> <p>Not equal to</p>	<p>Enter an error code and separate multiple keywords by line break.</p>

SQL Type	Equal to Not equal to	Pull down the list to select a SQL type (ALTER, CHANGEUSER, CREATE, DELETE, DROP, EXECUTE, INSERT, LOGOUT, OTHER, REPLACE, SELECT, SET, UPDATE). You can select multiple types.
Risk Level	Include Exclude	Select low, medium, or high risk to filter the audit logs that meet the risk level settings of the rule template. It also supports empty inputs, which indicate filtering the audit logs without risk level tags in the historical inventory.
Execution Time (ms)	Range format	Enter an execution time in the format of M-N, such as 10-100 or 20-200.
Lock Wait Time (μs)	Range format	Enter a lock wait time in the format of M-N, such as 10-100 or 20-200.
IO Wait Time (μs)	Range format	Enter an IO wait time in the format of M-N, such as 10-100 or 20-200.
Transaction Duration (μs)	Range format	Enter a transaction duration in the format of M-N, such as 10-100 or 20-200.
CPU Time (μs)	Range format	Enter a CPU time in the format of M-N, such as 10-100 or 20-200.
Audit Rule	Include Exclude	Display the template IDs and names of all rule templates in a specific region. You can filter the audit logs meeting a specific rule template. Supports empty inputs, which indicate filtering the audit logs without audit rule tags and the full audit logs not meeting rules in the historical inventory. Supports searching for audit rules by rule template ID and rule template name. Supports choosing multiple rule templates simultaneously.
Thread ID	Equal to Not equal to	Enter a thread ID and separate multiple keywords by line break.
Transaction ID	Equal to Not equal to	Enter a transaction ID and separate multiple keywords by line break. <b>Note :</b> Only the kernel minor version 2.1.11 and later versions of TDSQL-C for MySQL 5.7 support the <b>Transaction ID</b> field, which is not supported by TDSQL-C for MySQL 8.0.
Scanned Rows	Range format	Enter a range of scanned rows in the format of M-N, such as 10-100 or 20-200.
Affected Rows	Range format	Enter a range of affected rows in the format of M-N, such as 10-100 or 20-200.



Returned Rows	Range format	Enter a range of returned rows returned in the format of M-N, such as 10-100 or 20-200.
---------------	--------------	---

## Log list

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

Time ↕	Risk Level ▼	Client IP	Database Name	Database Account	SQL Type	SQL Details	Thread ID	Return
No data yet								

## Audit Fields

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

Audit Instance	Audit Log	Rule Template
Audit Instance	cynosdbmysql-	cynosdbmysql-
	Select time	Resource Usage ⓘ

### Note:

Currently, you can download audit log files of a database instance only at the Tencent Cloud private network address by using a CVM instance in the same region. For example, to download the audit logs of database instances in Beijing region, download them with a CVM instance in Beijing.

Log files are valid for 24 hours. Download them promptly.

Up to 30 log files can be retained for one database instance. Delete files promptly after download.

If the status is `Failed`, there may be too many logs. You can download them in batches by narrowing down the time range.

No.	Field	Remarks
1	Time	The exact timestamp when an operation is performed.
2	Risk Level	The risk level of an operation, categorized as low risk, medium risk, and high risk. For full audit, the risk level of logs that do not meet any audit rules will be displayed as "-".
3	Client IP	IP address of the client initiating a database operation.
4	Database Name	Name of the database involved in an operation.
5	User Account	User account executing an operation.

6	SQL Type	Type of SQL statements, such as SELECT, INSERT, UPDATE, and DELETE.
7	SQL Details	The specific SQL command text being executed.
8	Error Code	When an error occurs during the execution of an SQL statement, an error code is generated. The error code is an integer used to identify a specific error type, with 0 indicating success.
9	Thread ID	Unique thread ID for each client connected to a database, which is used to identify which client executed a specific operation.
10	Transaction ID	Unique ID for each transaction in the storage engine that supports transactions (such as InnoDB), which is used to identify a specific transaction.
11	Scanned Rows	The number of rows scanned in a database during query execution, which can help you understand the query efficiency.
12	Returned Rows	The number of rows returned in the query results, which can help you understand the result set size.
13	Affected Rows	The number of rows actually affected when a modification operation (such as INSERT, UPDATE, or DELETE) is performed on a data table, which can help you understand the impact scope of the operation.
14	Execution Time (ms)	The time from starting execution of an SQL statement to finishing it, in milliseconds. This field can help you understand the query performance.
15	CPU Time ( $\mu$ s)	The time spent executing SQL statement on the CPU, in microseconds. This field can help you understand the CPU usage during the query.
16	Lock Wait Time ( $\mu$ s)	The time spent waiting to acquire the database lock, in microseconds. This field can help you understand the lock contention situation of the query.
17	IO Wait Time ( $\mu$ s)	The waiting spent waiting for an I/O operation to complete, in microseconds. This field can help you understand the I/O performance of the query.
18	Transaction Duration ( $\mu$ s)	The total time consumed for a transaction from start to submission or rollback, in microseconds. This field can help you

		understand the performance of the transaction.
19	Audit Rule	<p>It displays the rule template that the audit log meets. Upon clicking the corresponding rule template, the details of the rule template will be displayed, including the basic information, the parameter settings, and the modification record.</p> <p>The value of the audit rule for the audit logs in the historical inventory is displayed as "-".</p> <p>The value of the audit rule for the audit logs that don't meet rules is displayed as "-".</p>

## Relationship Between SQL Statement Type and SQL Statement Mapping Object

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

		SQLCOM_ALTER_TABLESPACE, SQLCOM_ALTER_SERVER, SQLCOM_ALTER_EVENT, SQLCOM_ALTER_USER, SQLCOM_ALTER_INSTANCE, SQLCOM_ALTER_USER_DEFAULT_ROLE, SQLCOM_ALTER_RESOURCE_GROUP
8	REPLACE	SQLCOM_REPLACE, SQLCOM_REPLACE_SELECT
9	SET	SQLCOM_SET_OPTION, SQLCOM_RESET, SQLCOM_SET_PASSWORD, SQLCOM_SET_ROLE, SQLCOM_SET_RESOURCE_GROUP
10	EXECUTE	SQLCOM_EXECUTE
11	LOGIN	Database login behavior, which is not constrained by audit rules and is recorded by default.
12	LOGOUT	Database logout behavior, which is not constrained by audit rules and is recorded by default.
13	CHANGEUSER	User change behavior, which is not constrained by audit rules and is recorded by default.

# Post-Event Alarm Configuration

Last updated : 2023-12-12 14:41:21

Event alarms related to the database audit function have been connected to the Tencent Cloud Observability Platform and the EventBridge (EB). If you set risk level alarms in the rule template and select **Send alarm notification**, the audit logs matching the rule template will trigger alarm notifications to the bound users. At the same time, on the Tencent Cloud Observability Platform, You can also view alarm history, manage alarm policies (toggle alarm switch on/off) and mute alarms. Configuring event alarms for database audit helps you obtain risk alarms in time and pinpoint problematic audit logs quickly.

This document describes how to configure event alarms by using Tencent Cloud Observability Platform (TCOP) and EB for an instance with database audit enabled.

## Prerequisites

You have enabled the audit service. For more information, see [Enabling Audit Service](#).

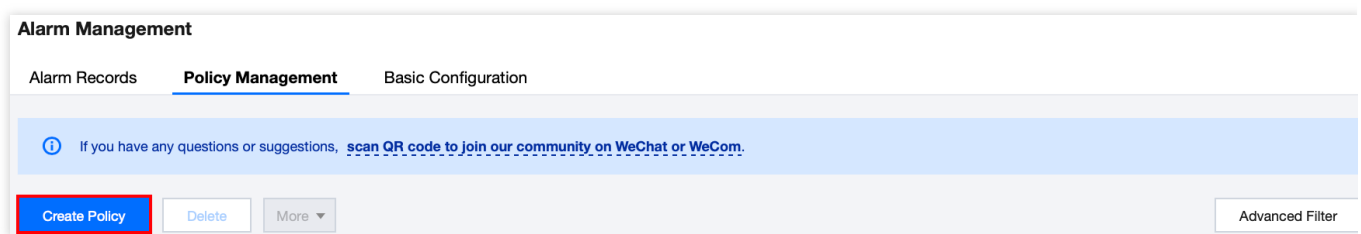
You have [submitted a ticket](#) to apply for the event alarm function (this function can only be applied for instances deployed in Beijing, Shanghai, Guangzhou, Chengdu, and Singapore).

You have [submitted a ticket](#) to apply for the rule audit function.

## Configuring Event Alarms through TCOP

### Creating an Alarm Policy

1. Log in to the [TCOP console](#) and choose **Alarm Management** > **Policy Management** on the left navigation bar.
2. On the **Alarm Policy List** page, click **Create Policy**.



3. On the policy creation page, finish the setting for **Basic info**, **Configure Alarm Rule**, and **Configure Alarm notification**.

**Policy Type:** Choose **Cloud Database** > **TDSQL-C** > **MySQL**.

**Alarm Object:** You can find the object instance to be associated by selecting the region where the object is or searching for the instance ID of the object.

**Trigger Condition:** You can find event alarm, click **Add Event**, add alarm events of **AuditLowRisk**, **AuditMediumRisk**, or **AuditHighRisk** based on the risk level for which the alarm is needed.

**Configure Alarm Notification:** You can select a notification template or create one below. Each alarm policy can be bound to at most three notification templates. For more information about the Customizd Notification Template, please see [Creating Notification Template](#).

Selecting a preset template

### Select notification template

You have selected 1 notification template, and 2 more can be selected.

Search for notification template

	Notification Template Name	Included Operations
<input checked="" type="checkbox"/>	Preset [blurred]	Recipient: 1
<input type="checkbox"/>	[blurred]	Recipient: 1
<input type="checkbox"/>	[blurred]	Recipient: 1

Total items: 3 20 ▼ / page

OK
Cancel

Creating a template

### Create Notification Template

#### Basic Info

Template Name

Notification Type  Alarm Trigger  Alarm Recovery

Notification Language

Tag   ×

[+ Add](#) [Tag Clipboard](#)

**Notifications** (Fill in at least one item)

User Notification You can add a user only for receiving messages.

Recipient Object  ↻

Notification Cycle  Mon  Tue  Wed  Thu  Fri  Sat  Sun

Notification Period  🕒 ℹ️

Receiving Channel  Email  SMS

[Add User Notification](#)

API Callback ℹ️ [Add API Callback](#)

ℹ️ It supports pushing to the WeCom group robot [Try Now](#) [🔗](#)

Ship to CLS  Enable ℹ️

[Complete](#)

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

## Associating Alarm Objects

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

1. On the [alarm policy list](#), click the **Policy Name** to enter the alarm policy management page.

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

## Viewing Alarm Records, Managing Alarm Policies (Alarm Switch), and Silencing Alarm

You can view the alarm history of the relevant events or manage alarm policies and create alarm silence through [TCOP](#). You can refer to the following guidelines for the corresponding operation.

[Viewing Alarm Records](#)

[Alarm Switch](#)

[Alarm Silencing](#)

## Configuring Event Alarms via EB

### Step 1: Activating the EB service

Tencent Cloud EB implements permission management through Cloud Access Management (CAM). CAM is a permission and access management service provided by Tencent Cloud, which is mainly used to help customers securely manage the access rights of resources under Tencent Cloud accounts. Users can create, manage and destroy users (groups) through CAM, and use identity management and policy management to control the rights of other users to use Tencent Cloud resources. Before using the EB, you need to enable the service on the product page. For details about how to activate the root account and how to authorize sub-accounts to use the service, see [Activating EB](#).

### Step 2: Configure event alarms related to TDSQL-C MySQL database audit

After the EB service is enabled, you need to select an event source access mode. Currently, monitoring events generated through TDSQL-C MySQL version database audit can be used as event sources to access the EB.

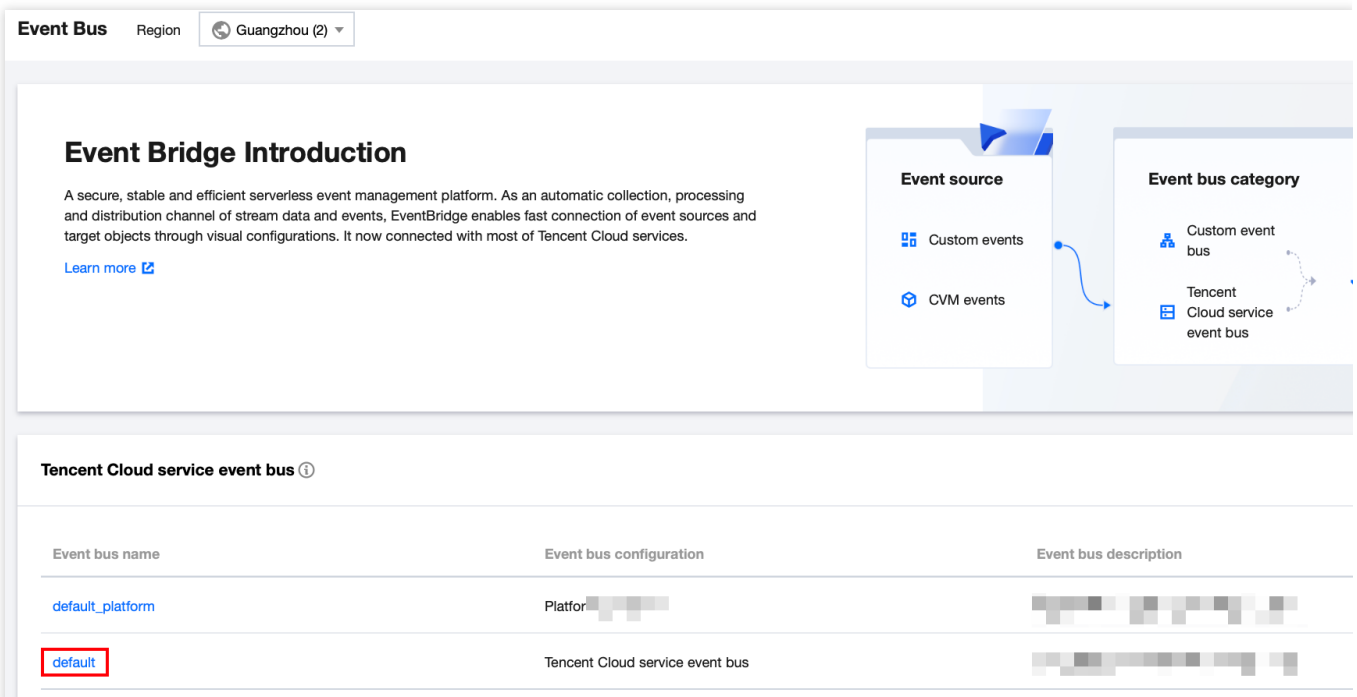
#### Note:

All operation and maintenance events such as alarms and audits generated by TDSQL-C MySQL version will be delivered to the cloud service event set. The delivery is the default delivery and cannot be changed or edited.

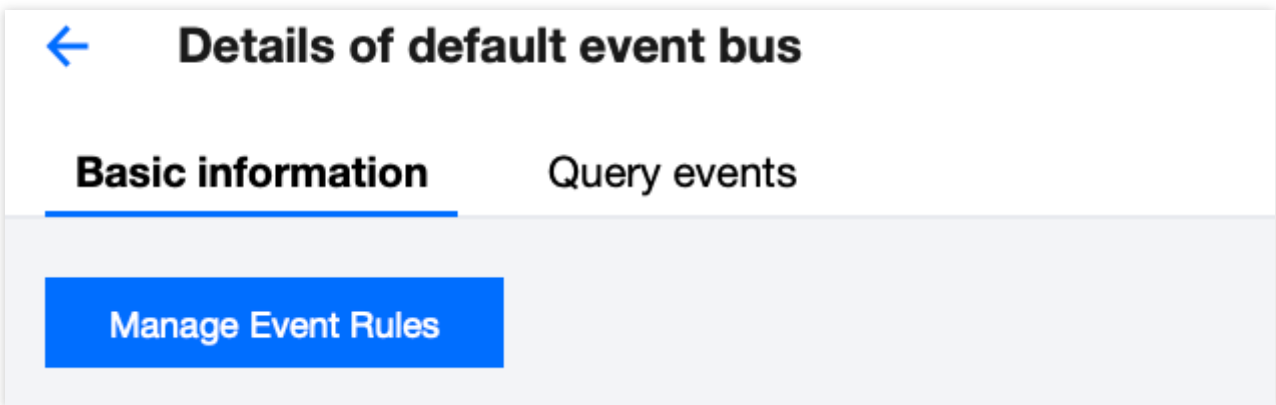
After opening Tencent Cloud Event Bus service, the default cloud service event set will be automatically created for you in Guangzhou region, and the alarm events (monitoring events and audit events) generated by TDSQL-C MySQL version will be automatically delivered to the default cloud service event set.

1. Log in to the [EB Console](#).
2. Select the **Guangzhou** region at the top.
3. Click on the **default** EB under Tencent Cloud service EB.

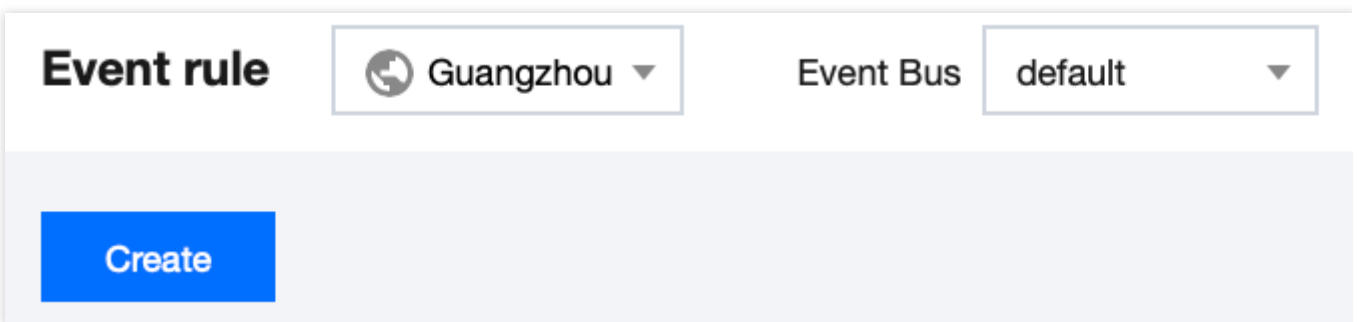




4. On the details page of the default EB, click **Manage Event Rules**.



5. Click **Create** on the skip page.



6. After finishing the following configuration on the **Create Event Rule** page, click **Next**.

Parameter	Description
Rule name	Enter the rule name. It should contain 2-60 characters in the form of letters, digits, underscores, and hyphens. It must start with a letter and end with a digit or a letter.

Rule description	Fill in the rule description including digits, English and Chinese characters, and commonly used punctuation, not exceeding 200 characters.
Tag	Decide whether to enable tag. Once enabled, you can add tags to this event rule.
Data conversion	Event data conversion can help you easily and simply process the event content. For example, you can extract and parse fields from an event and reassemble them before delivering them to the event target.
Event sample	Provide an example of the event structure for reference in configuring event matching rules. You can find the target template under event sample for reference.
Rule pattern	Both a template and a custom event are supported, but it is recommended to use a template here.
Tencent Cloud Service	Please choose TDSQL-C MySQL version.
Event type	Select the required and event type of database audit related alarms ( <b>AuditLowRisk</b> , <b>AuditMediumRisk</b> or <b>AuditHighRisk</b> ).
Test match rule	Choose the event type template selected in the event example, then click on <b>Test match rule</b> . If test match rule passes, you can proceed to the next step.

**Note:**

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

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

This indicates that only events originated from TDSQL-C MySQL version with the instance ID being ins-xxx can be pushed through rule matching. Other events will be discarded and will be unable to reach the user.

Multiple resources can also be matched:

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

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



**Create event rule**



Rule pattern



Delivery target

### Delivery target

Trigger method \*

Notification message ⓘ ▾

Message template \*

Monitoring alert template  General notification

Alert content \*

Chinese  English

Notification method \*

publishing channel ▾

#### publishing channel

Recipients \*

User ▾

Notification period \*

09:30:00 ~ 23:30:00 ⌚

Delivery method \*



Email  SMS  Phone  Message center

Add

Enable event rules now

[Back](#)[Complete](#)

Parameter	Description
Trigger method	Select <b>Notification message</b> .
Message template	Support for selecting <b>Monitoring alert template</b> or <b>General notification template</b> .
Alert content	Support <b>Chinese</b> or <b>English</b> .
Notification method	Support for selecting <b>API callback</b> , <b>channel push</b> , or <b>all the methods</b> . The following settings will use <b>channel push</b> as an example.
Recipients	Select a recipient user or user group.
Notification period	Custom <b>Notification period</b> .
Delivery method	Select <b>Delivery method</b> . <b>SMS</b> is limited to 500 characters. <b>Phone</b> is limited to 350 characters. too long events (may be caused by too long instance name and other reasons) will not be pushed. You are advised to configure multiple channels.

**Note:**

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

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

# Modifying Audit Rule

Last updated : 2024-06-07 15:43:57

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

## Prerequisites

You have enabled the audit service as instructed in [Enabling Audit Service](#).

## Feature overview

The audit rule can be changed from full audit to rule-based audit or vice versa.

After the audit rule is modified, the modification will be applied to the selected instance.

The modification of audit rules includes the modification of audit type and rule template.

## Modifying the audit rule for one instance

1. Log in to the [TDSQL-C for MySQL console](#).
2. Click **Database Audit** on the left sidebar.
3. After selecting a **region** at the top, click on **Audit Status** on the **Audit Instance** page, and select the **Enabled** option to filter instances that have enabled audit.
4. Find the target cluster/instance in the audit instance list, or search for it by resource attribute in the search box, and select **More > Modify Audit Rule** in the **Operation** column.

Cluster ID/Name	Instance ID / Name	Audit Status	Audit Mode	Log Retention Period	Stored Log Size	Audit Rule	Project
<input type="checkbox"/> cynosdbm- cynosdbm	<input type="checkbox"/> cynosdbmysql- cynosdbmysql	Enabled	Full Audit	Total storage period: 30 day(s) Frequent access storage period: 7 day(s) Infrequent access storage period: 23 day(s)	Total storage size: 3.072 MB Frequent access storage size: 0 MB Infrequent access storage size: 3.072 MB	--	Default projec

5. Under the Modify Audit Rule window, complete the necessary alterations (Audit Type or Audit Rule), then click **Confirm**.

**Before**

Cluster ID/Name	Instance ID / Name	Audit Mode
cynosdbmysql- cynosdbmysql-	cynosdbmysql- cynosdbmysql-	Full Audit

**After**

Audit Mode

Full audit records all database accesses and SQL statement executions.

## Batch modifying the audit rule

### Note:

The audit rule can be changed from full audit to rule-based audit or vice versa.

After the audit rule is modified, the modification will be applied to the selected instance.

The modification of audit rules includes the modification of audit type and rule template.

1. Log in to the [TDSQL-C for MySQL console](#).
2. Click **Database Audit** on the left sidebar.
3. After selecting a **region** at the top, click on **Audit Status** on the **Audit Instance** page, and select the **Enabled** option to filter instances that have enabled audit.
4. Find the target clusters/instances in the audit instance list, or search for them by resource attribute in the search box, and select them. Then, click **Modify Audit Rule** above the list.

**Audit Instance**    Audit Log    Rule Template

Audit Status

<input checked="" type="checkbox"/>	Cluster ID/Name	Instance ID / Name	Audit Status	Audit Mode	Log Retention Period	Stored Log Size	Audit Rule	Project
<input checked="" type="checkbox"/>	cynosdbmysql- cynosdbmysql-	cynosdbmysql- cynosdbmysql-	Enabled	Full Audit	Total storage period: 30 day(s) Frequent access storage period: 7 day(s) Infrequent access storage period: 23 day(s)	Total storage size: 3.072 MB Frequent access storage size: 0 MB Infrequent access storage size: 3.072 MB	--	Default projec

5. Under the **Modify Audit Rule** window, complete the necessary modifications (Audit Type or Audit Rule), then click **OK**.

# Modifying Audit Service

Last updated : 2024-06-18 09:39:07

This document describes how to modify the audit service in 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, expired logs will be cleared immediately.

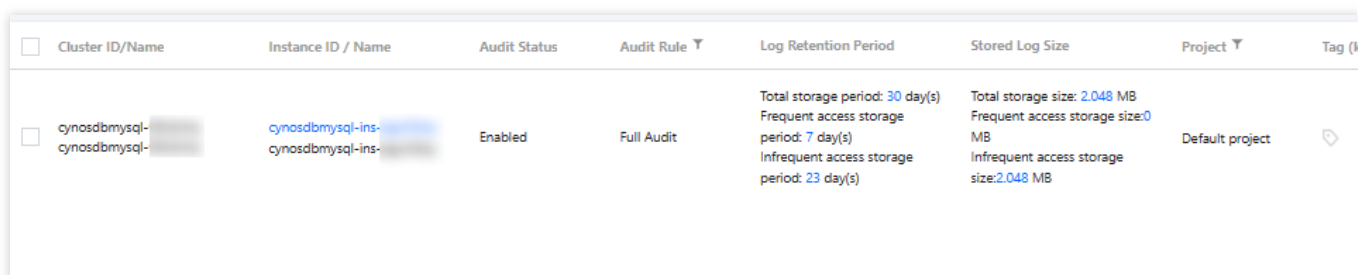
If the data of the last n days is set to be stored in frequent access storage, older data will be automatically transitioned to infrequent access storage. After the frequent access storage period is extended, the audit data that falls in the extension period will be automatically migrated back from infrequent access storage to frequent access storage.

## Prerequisites

You have enabled the audit service as instructed in [Enabling Audit Service](#).

## Modifying the audit service for one instance

1. Log in to the [TDSQL-C for MySQL console](#).
2. Click **Database Audit** on the left sidebar.
3. After selecting a **region** at the top, click on **Audit Status** on the **Audit Instance** page, and select the **Enabled** option to filter instances that have enabled audit.
4. Find the target instance in the audit instance list, or search for it by resource attribute in the search box, and select **More > Modify Audit Service** in the **Operation** column.



<input type="checkbox"/>	Cluster ID/Name	Instance ID / Name	Audit Status	Audit Rule	Log Retention Period	Stored Log Size	Project	Tag
<input type="checkbox"/>	cynosdbmysql- cynosdbmysql-	cynosdbmysql-ins- cynosdbmysql-ins-	Enabled	Full Audit	Total storage period: 30 day(s) Frequent access storage period: 7 day(s) Infrequent access storage period: 23 day(s)	Total storage size: 2.048 MB Frequent access storage size:0 MB Infrequent access storage size:2.048 MB	Default project	

5. In the **Modify Audit Service** window, modify the log retention period or frequent access storage period and click **OK**.

### Modify Audit Service ✕

**1.** If you choose to extend the log retention period, the change will take effect immediately; if you choose to shorten the log retention period, expired logs will be cleared immediately.

**2.** If you configure to store the data of the last n days in frequent access storage, older data will be automatically migrated to infrequent access storage. After the frequent access storage period is extended, the audit data that falls in the period will be automatically migrated from infrequent access storage to frequent access storage. For more information, see [Documentation](#).

#### Configure Audit

Log Retention Period (day) 180 ▼

Frequent Access Storage Period (day) 30 ▼

Infrequent Access Storage Period (day) 150 (Audit logs will be automatically migrated to infrequent access storage after the specified frequent access storage period)

Frequent Access Storage Fees USD/GB/hr

Infrequent Access Storage Fees USD/GB/hr

I agree to [Tencent Cloud Terms of Service](#)

OK Cancel

## Batch modifying the audit service

1. Log in to the [TDSQL-C for MySQL console](#).
2. Click **Database Audit** on the left sidebar.
3. After selecting a **region** at the top, click on **Audit Status** on the **Audit Instance** page, and select the **Enabled** option to filter instances that have enabled audit.
4. Find the target instances in the audit instance list, or search for them by resource attribute in the search box, and select them. Then, click **Modify Audit Service** above the list.

Audit Instance		Rule Template	Audit Log				Audit Status	Di
<span style="background-color: #007bff; color: white; padding: 2px 5px;">Enable Database Audit</span> <span style="background-color: #f0f0f0; padding: 2px 5px; margin-left: 5px;">Disable Database Audit</span> <span style="background-color: #f0f0f0; padding: 2px 5px; margin-left: 5px;">Modify Audit Rule</span> <span style="border: 2px solid red; padding: 2px 5px; margin-left: 5px;">Modify Audit Service</span>							Enabled	
<input checked="" type="checkbox"/>	Cluster ID/Name	Instance ID / Name	Audit Status	Audit Rule	Log Retention Period	Stored Log Size	Project	Tag
<input checked="" type="checkbox"/>	cynosdbmysql- cynosdbmysql-	cynosdbmysql-ins-e cynosdbmysql-ins-e	Enabled	Full Audit	Total storage period: 30 day(s) Frequent access storage period: 7 day(s) infrequent access storage period: 23 day(s)	Total storage size: 2,048 MB Frequent access storage size: 0 MB Infrequent access storage size: 2,048 MB	Default project	

5. In the **Modify Audit Service** window, modify the log retention period or frequent access storage period and click **OK**.



**Note:**

The **Modify Audit Service** window displays the log retention periods both before and after the modification to make comparisons easier. The new log retention period will be applied to the selected instances. Therefore, proceed with caution.

**Modify Audit Service**
✕

i
• After the audit service is batch modified, the selected instances will be uniformly adjusted according to the new log retention period.
✕

**Before**

Instance ID / Name	Log Retention Period (day)	Frequent Access Storage ...	Infrequent Access Storage...
cynosdbmysql-ins- cynosdbmysql-ins-	30	7	23
cynosdbmysql-ins-fr cynosdbmysql-ins-fr	30	7	23

**After**

Log Retention Period (day)

30

Frequent Access Storage Period (day) i

7

Infrequent Access Storage Period (day)

**23**(Audit logs will be automatically transitioned to infrequent access storage after the specified frequent access storage period)

Frequent Access Storage Fees

Infrequent Access Storage Fees

I agree to [Tencent Cloud Terms of Service](#)

OK

Cancel

# Disabling Audit Service

Last updated : 2024-06-18 09:40:53

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

## Note :

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

## Prerequisites

You have [enabled audit in TDSQL-C for MySQL](#).

## Directions

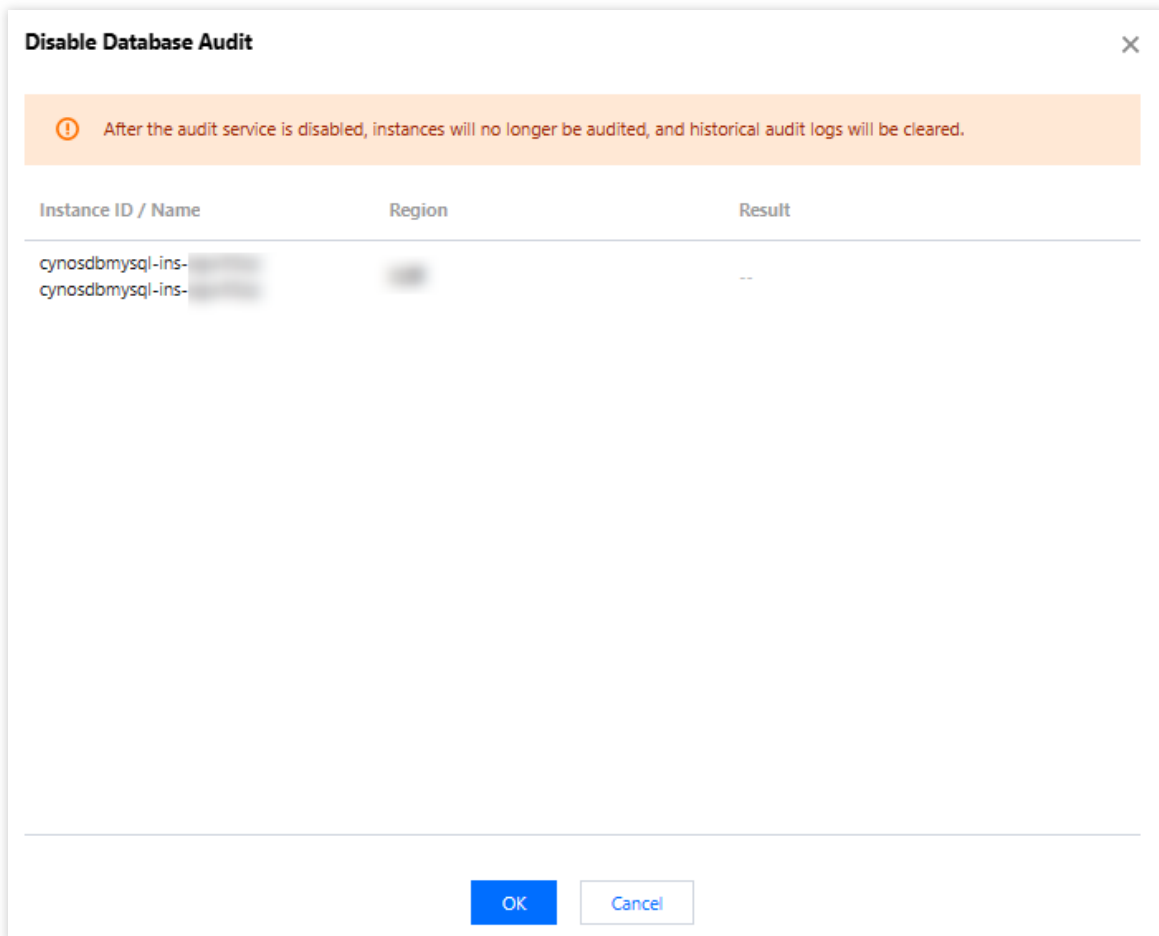
1. Log in to the [TDSQL-C for MySQL console](#).
2. On the left sidebar, select **Database Audit**.
3. After selecting a **region** at the top, click on **Audit Status** on the **Audit Instance** page, and select the **Enabled** option to filter instances that have enabled audit.
4. Find the target instance in the audit instance list, or search for it by resource attribute in the search box, and select **More > Disable** in the **Operation** column.

<input type="checkbox"/>	Cluster ID/Name	Instance ID / Name	Audit Status	Audit Rule <span>▼</span>	Log Retention Period	Stored Log Size	Project <span>▼</span>	Tag
<input type="checkbox"/>	cynosdbmysql- cynosdbmysql-	cynosdbmysql-ins- cynosdbmysql-ins-	Enabled	Full Audit	Total storage period: 30 day(s) Frequent access storage period: 7 day(s) Infrequent access storage period: 23 day(s)	Total storage size: 2,048 MB Frequent access storage size:0 MB Infrequent access storage size:2,048 MB	Default project	

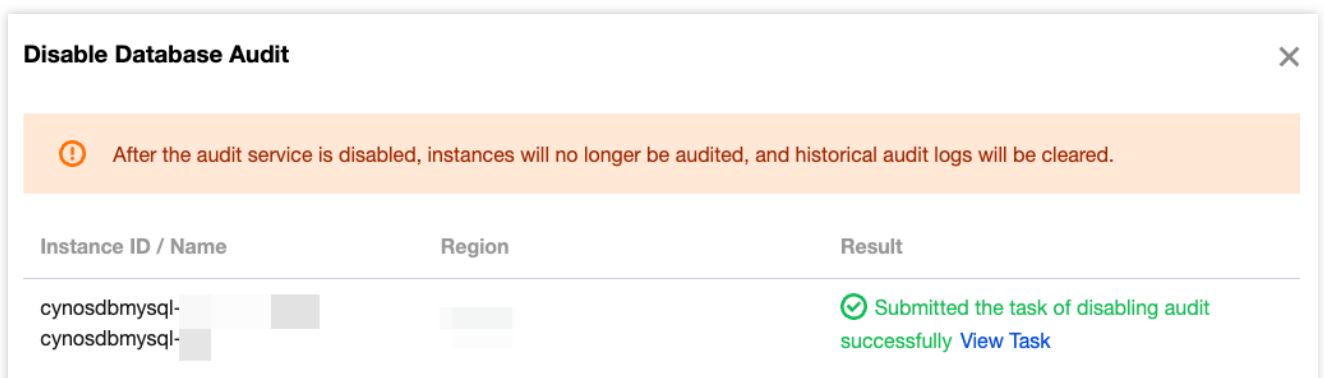
## Note:

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

5. In the **Disable Database Audit** window, confirm that everything is correct and click **OK**.



6. After confirmation, the disablement result will be displayed in the result column. You can click **View Task** to enter the task list and view the details.



# Audit Rule Template

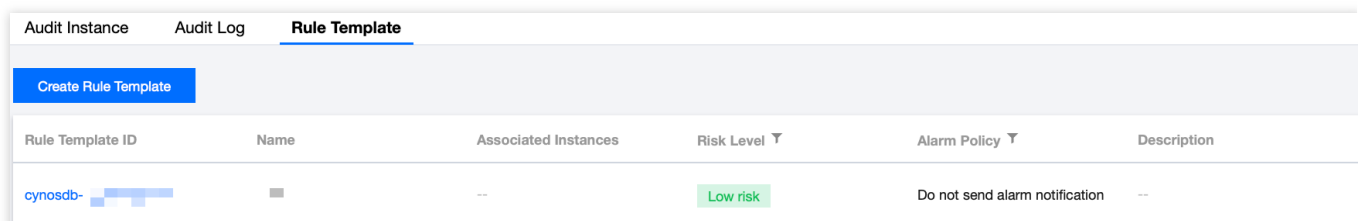
## Viewing Rule Template List

Last updated : 2023-12-12 14:33:03

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

## Viewing the rule template list and template details

1. Log in to the [TDSQL-C for MySQL console](#).
2. Select **Database Audit on** the left sidebar.
3. Click **Rule Template** after selecting **Region**.



Rule Template ID	Name	Associated Instances	Risk Level ▾	Alarm Policy ▾	Description
cynosdb- [redacted]	[redacted]	--	Low risk	Do not send alarm notification	--



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. View **Basic Info**, **Parameter Settings**, **Associated Instances** and **Modification Record** of this rule template in the pop-up window.

**Rule Template Details** [Modification Record](#)

**Basic Info**


Parameters Settings



Associated Instances

Rule Template ID	cynosdb- 
Name	r 
Risk Level	Low risk
Alarm Policy	Do not send alarm notification
Description	--
Creation Time	2023-11-29 18:44:23
Update Time	2023-11-29 18:44:22

Close

## Tool list

Tool	Description
Search box	You can click  to filter rule templates by resource attributes such as ID and name. Separate multiple keywords by the vertical bar " ".
Modification	You can click

Record	 <p>to switch to the <b>Modification Record</b> page, where you can globally view the modification history of rule templates of a certain region.</p>
Refresh	<p>You can click</p>  <p>to refresh the list.</p>

## Template list fields

Field	Description
Rule Template ID	ID of the rule template.
Name	Name of the rule template.
Risk Level	Risk level ( <b>Low risk</b> , <b>Medium risk</b> or <b>High risk</b> ) of the corresponding rule template, which supports filtration.
Alarm Policy	Alarm policy ( <b>Do not send alarm notification</b> or <b>Send alarm notification</b> ) of the corresponding rule template, which supports filtration.
Associated Instances	The number of instances bound to the corresponding rule template. Click the number of instances to show the detailed information about the associated instances, including the instance ID, audit type, and so forth.
Description	Remarks of the rule template.
Creation Time	Creation time of the rule template in the format of year-month-day hour:minute:second.
Update Time	The latest update time for the corresponding rule template.
Operation	<p><b>Details:</b> One can peruse the <b>fundamental details</b> of the rule template, <b>parameter configurations</b>, <b>associated instances</b>, and <b>modification history</b>.</p> <p><b>Modify:</b> You can modify the rule template.</p> <p><b>Delete:</b> You can delete the rule template.</p>

## Relevant operations

[Creating Rule Template](#)

[Modifying Rule Template](#)

[Deleting Rule Template](#)

# Creating Rule Template

Last updated : 2024-06-07 16:05:38

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

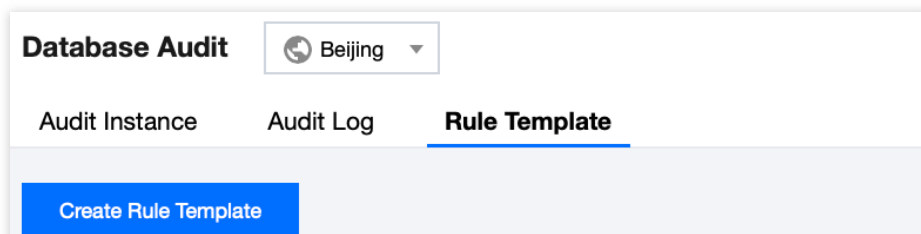
## Note:

As of September 25, 2023, the relationship between rule templates and audit instances has been adjusted from **initialization** to **strong association**. Any modification to the content of a rule template **will synchronously impact** the audit rule applied to instances that are bound to the rule template.

The same field of rule content can be configured with a maximum of 5 characteristic strings. And each string is separated by vertical bar"|".

## Directions

1. Log in to the [TDSQL-C for MySQL console](#).
2. On the left sidebar, click **Database Audit**.
3. Select **Region** and click **Rule Template**.
4. In the template list, click **Create Rule Template**.



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



### Create Rule Template

- 1. The relationship between rule templates and audit instances will be changed from **no binding** to **strong binding** on September 2023. That means the modification of the rule template content **will impact** the audit rules applied to the instances that are bound to the rule template.
- 2. Up to 5 characteristic strings can be configured in a single parameter field of the rule content and should be separated by vertical bar "|".

Rule Template Name \*

It can contain up to 30 letters, digits, Chinese characters, and symbols (-\_./()+=:@) and cannot start with a digit.

Rule Content \*

Parameter Field	Operator	Characteristic String ⓘ
<input type="text" value="Please select"/>	<input type="text" value="Please select"/>	<input type="text"/>

[Add](#) (We recommend that you add up to five rules.)

Risk Level \*  Low risk  Medium risk  High risk

Alarm Policy \*  Do not send alarm notification  Send alarm notification

Please go to Tencent Cloud Observability Platform > [Alarm Management](#) to configure alarm policies and For more information, see [Documentation](#).

Rule Template Remarks

It can contain up to 200 digits, letters, Chinese characters, spaces, and symbols (-\_./() +=: @).

Parameter	Description
Rule Template Name	This field can contain up to 30 letters, digits, and symbols -_./() ( ) += ::@and cannot start with a digit.
Rule Content	This fields sets the rule content (parameter field, operator, characteristic string). For detailed instructions, see the following <a href="#">Rule content details and examples</a> . <b>Note:</b> Click <b>Add</b> to add parameter fields in rule content. Click <b>Delete</b> in the <b>Operation</b> column in rule content to remove the unnecessary parameter field and condition. Note that at least one parameter field and condition should be reserved.
Risk Level	Select a risk level for the created rule template, with options of <b>Low risk</b> , <b>Medium risk</b> , and <b>High risk</b> .

Alarm Policy	Select an alarm policy for the created rule template, with options of <b>Do not send alarm notification</b> or <b>Send alarm notification</b> . <b>Note:</b> Please proceed to <a href="#">Tencent Cloud Observability Platform &gt; Alarm Management</a> to configure alarm rules and notifications. For more information, please refer to <a href="#">Post-Event Alarm Configuration</a> .
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.

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

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

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

Parameter Field	Operator	Characteristic String
Client IP	Include, Exclude, Equal to, Not equal to, Regex	Up to 5 client IPs can be configured and should be separated by vertical bar " ".
Database Account	Include, Exclude, Equal to, Not equal to, Regex	Up to 5 usernames can be configured and should be separated by vertical bar " ".
Database Name	Include, Exclude, Equal to, Not equal to, Regex	Up to 5 database names can be configured and should be separated by vertical bar " ".
SQL Details	Include, Exclude	Up to five SQL commands can be configured and should be separated by vertical bar " ".
SQL Type	Equal to, Not equal to	Up to five SQL types can be selected. Valid options: ALTER, CHANGEUSER, CREATE, DELETE, DROP, EXECUTE, INSERT, LOGIN, LOGOUT, OTHER, REPLACE, SELECT, SET, UPDATE.
Affected Rows	Greater than, Less than	Select affected rows

Returned Rows	Greater than, Less than	Select returned rows
Scanned Rows	Greater than, Less than	Select scanned rows
Execution Time	Greater than, Less than	Select execution time 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 : 2024-06-07 16:09:14

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

## Note:

As of September 25, 2023, the relationship between rule templates and audit instances has been adjusted from **initialization** to **strong association**. Any modification to the content of a rule template **will synchronously impact** the audit rule applied to instances that are bound to the rule template.

The same field of rule content can be configured with a maximum of 5 characteristic strings. And each string is separated by vertical bar"|".

## Directions

1. Log in to the [TDSQL-C for MySQL console](#).
2. On the left sidebar, click **Database Audit**.
3. Select **Region** and click **Rule Template**.

Rule Template ID	Name	Associated Instances	Risk Level	Alarm Policy	Description	Operation
cynosdb-	r...	--	Low risk	Do not send alarm notification	--	20

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**.

### Edit Rule Template

- 1. The relationship between rule templates and audit instances will be changed from **no binding** to **strong binding** on September 25, 2023. That means the modification of the rule template content **will impact** the audit rules applied to the instances that are bound to the rule template.
- 2. Up to 5 characteristic strings can be configured in a single parameter field of the rule content and should be separated by vertical bar "|".

Rule Template Name \*

It can contain up to 30 letters, digits, Chinese characters, and symbols (-\_./()+=:@) and cannot start with a digit.

Rule Content \*

Parameter Field	Operator	Characteristic String ⓘ	Operation
Client IP ▾	Include ▾	1 <input type="text"/>	ⓘ Delete
<a href="#">Add</a> (We recommend that you add up to five rules.)			

Risk Level \*  Low risk  Medium risk  High risk

Alarm Policy \*  Do not send alarm notification  Send alarm notification

Please go to Tencent Cloud Observability Platform > [Alarm Management](#) to configure alarm policies and notifications. For more information, see [Documentation](#).

Rule Template Remarks

Please enter the rule template description

It can contain up to 200 digits, letters, Chinese characters, spaces, and symbols (-\_ . ,/() () +=: @).

Parameter	Description
Rule Template Name	This field can contain up to 30 letters, digits, and symbols -_./()[] () += ::@, and cannot start with a digit.
Rule Content	This fields sets the rule content (parameter field, operator, characteristic string). For detailed instructions, see the following <a href="#">Rule content details and examples</a> . <b>Note:</b> Click <b>Add</b> to add parameter fields in rule content. Click <b>Delete</b> in the <b>Operation</b> column in rule content to remove the unnecessary parameter field and condition. Note that at least one parameter field and condition should be reserved.
Risk Level	Select the risk level for this rule template, with options of <b>Low risk</b> , <b>Medium risk</b> , and <b>High risk</b> .
Alarm Policy	Select an alarm strategy for this rule template, with options of <b>Do not send alarm notification</b> and <b>send alarm notification</b> . <b>Note:</b>

	Please proceed to <a href="#">Tencent Cloud's Observability Platform &gt; Alarm Management</a> to configure alarm rules and notifications. For more details, refer to <a href="#">Post-Event Alarm Configuration</a> .
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.

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

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

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

Parameter Field	Operator	Characteristic String
Client IP	Include, Exclude, Equal to, Not equal to, Regex	Up to 5 client IPs can be configured and should be separated by vertical bar " ".
Database Account	Include, Exclude, Equal to, Not equal to, Regex	Up to 5 usernames can be configured and should be separated by vertical bar " ".
Database Name	Include, Exclude, Equal to, Not equal to, Regex	Up to 5 database names can be configured and should be separated by vertical bar " ".
SQL Details	Include, Exclude	Up to five SQL commands can be configured and should be separated by vertical bar " ".
SQL Type	Equal to, Not equal to	Up to five SQL types can be selected. Valid options: ALTER, CHANGEUSER, CREATE, DELETE, DROP, EXECUTE, INSERT, LOGIN, LOGOUT, OTHER, REPLACE, SELECT, SET, UPDATE.
Affected Rows	Greater than, Less than	Select affected rows
Returned Rows	Greater than, Less than	Select returned rows

Scanned Rows	Greater than, Less than	Select scanned rows
Execution Time	Greater than, Less than	Select execution time 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 : 2023-12-12 15:03:38

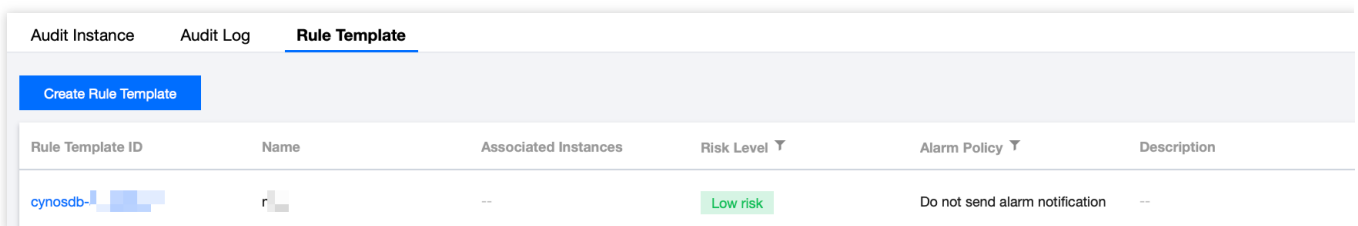
This document describes how to delete a database audit rule template in the console.

## Note:

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

## Directions

1. Log in to the [TDSQL-C for MySQL console](#).
2. On the left sidebar, click **Database Audit**.
3. Select **Region** and click **Rule Template**.



The screenshot shows the 'Rule Template' tab in the console. At the top, there are tabs for 'Audit Instance', 'Audit Log', and 'Rule Template'. Below the tabs is a 'Create Rule Template' button. A table lists the rule templates with columns: Rule Template ID, Name, Associated Instances, Risk Level, Alarm Policy, and Description. One row is visible with ID 'cynosdb-...', Name 'r...', Associated Instances '--', Risk Level 'Low risk', Alarm Policy 'Do not send alarm notification', and Description '--'.

Rule Template ID	Name	Associated Instances	Risk Level	Alarm Policy	Description
cynosdb-...	r...	--	Low risk	Do not send alarm notification	--

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**.

## Are you sure you want to delete the rule template?

Rule template to be deleted: nijne

After the rule template is deleted, it cannot be applied to instances.

OK

Cancel



# Viewing Audit Task

Last updated : 2023-02-23 11:06:12

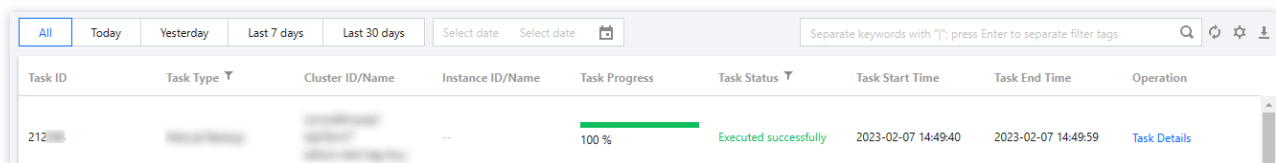
This document describes how to view the details and progress of an audit task in the console, such as enabling/disabling/modifying the audit service and modifying the audit rule.

## Task type

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 an audit task

1. Log in to the [TDSQL-C for MySQL console](#).
2. On the left sidebar, click **Task List**.
3. Select the region at the top.
4. Directly find or search for the target audit task by keyword to view its details.



The screenshot shows a table with the following columns: Task ID, Task Type, Cluster ID/Name, Instance ID/Name, Task Progress, Task Status, Task Start Time, Task End Time, and Operation. A single row is visible with a task ID of 212, a progress bar at 100%, and a status of 'Executed successfully'. The start and end times are both 2023-02-07 14:49:40. A 'Task Details' link is present in the Operation column.

Task ID	Task Type	Cluster ID/Name	Instance ID/Name	Task Progress	Task Status	Task Start Time	Task End Time	Operation
212				100 %	Executed successfully	2023-02-07 14:49:40	2023-02-07 14:49:59	<a href="#">Task Details</a>

## Searching by keyword

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

## Downloading the 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.

### Task Details - Manual Backup

Task ID: 21239

Cluster ID/Name: [blurred]

Instance ID/Name: --

Start Time: 2023-02-07 14:49:40

End Time: 2023-02-07 14:49:59

Task Progress: 100%

Task Status: Executed successfully

Task ID	Task Name	Task Status	Task Type
21239	Manual Backup	Executed successfully	Backup

Disable

# Authorizing Sub-User to Use Database Audit

Last updated : 2023-07-27 15:37:21

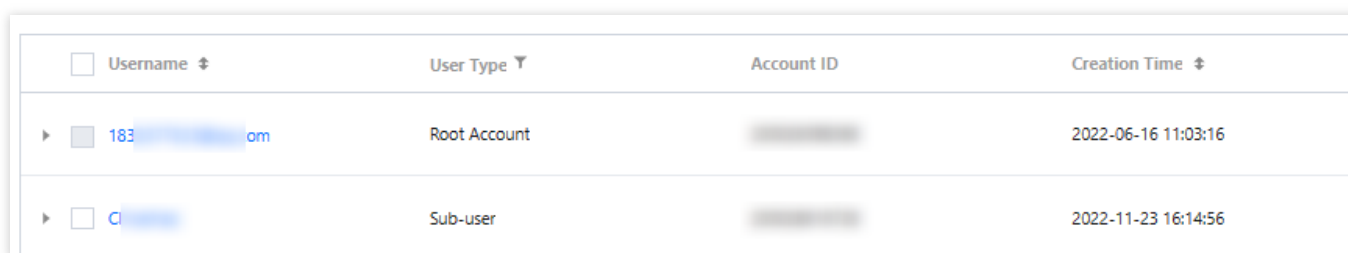
By default, sub-users have no permission to use database audit in TDSQL-C for MySQL. Therefore, you need to create policies if you want them to use it. If you don't need to manage sub-accounts' access to resources related to TDSQL-C for MySQL Database Audit, you can ignore this document.

[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](#).

## Directions

1. Log in to the [CAM console](#) as a root account, select the target sub-user in the user list, and click **Authorize**.



<input type="checkbox"/> Username ↕	User Type ∨	Account ID	Creation Time ↕
▶ <input type="checkbox"/> 183...om	Root Account	██████████	2022-06-16 11:03:16
▶ <input checked="" type="checkbox"/> Cl...	Sub-user	██████████	2022-11-23 16:14:56

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

### Associate Policy

Select Policies (2 Total)

tdsql-c	
Policy Name	Policy type
<input checked="" type="checkbox"/> QcloudCynosDBFullAccess Full read-write access to CynosDB	Preset Policy
<input checked="" type="checkbox"/> QcloudCynosDBReadOnlyAccess Read-only access to CynosDB	Preset Policy

2 selected

Policy Name	
QcloudCynosDBFullAccess Full read-write access to CynosDB	Pi
QcloudCynosDBReadOnlyAccess Read-only access to CynosDB	Pi

Support for holding shift key down for multiple selection