Database Audit

Getting Started

Product Documentation

Contents

Getting Started
Enabling TencentDB for MySQL Audit

Last updated：2024-09-06 12:10:52

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

Note:

Database Audit currently supports TencentDB for MySQL 5.6, 5.7, and 8.0 (two-node and three-node) instances but not TencentDB for MySQL 5.5 or single-node instances.

Creating Audit Rule

1. Log in to the TencentDB for MySQL console, select **Database Audit** on the left sidebar, select a region at the top, and click the **Audit Rule** tab.
2. On the **Audit Rule** tab, click **Create Rule**.
3. On the **Create Audit Rule** page, enter the rule name and description and click **Next**.
4. On the **Set Parameters** page, select the required audit mode and parameters and click **Save**.

Note:

After the rule is created successfully, it must be associated with an audit policy before it can take effect.

For use instructions of SQL audit rules, see SQL Audit Rule.

Enabling SQL Audit Service

1. Log in to the TencentDB for MySQL console, select **Database Audit** on the left sidebar, select a region at the top, click the **Audit Instance** tab, and click **Disabled** to filter instances whose audit is disabled.
2. On the **Audit Instance** tab, click the ID of the target instance to enter the enablement page, indicate your consent to the agreement, and click **Next**.
3. On the **Configure SQL Audit** page, select the audit log retention period and click **Next**.

Note:

You can select 7 days, 30 days, 3 months, 6 months, 1 year, 3 years, or 5 years as the audit log retention period. You can also modify it in the console after enabling audit. For more information, see Modifying Log Retention Period.

In order to meet the security compliance requirements for the retention period of SQL logs, we recommend you select 180 days or above.

4. On the **Create a Policy** page, set the policy name, select a created audit rule, and click **Create a Policy**.

Creating Audit Policy

1. Log in to the TencentDB for MySQL console, select **Database Audit** on the left sidebar, select a region at the top, and click the **Audit Policy** tab.
2. On the **Audit Policy** tab, click **Create Policy**.
3. In the pop-up window, set the policy name, select a created audit rule, and click **OK**.

Viewing Audit Log

After enabling audit, you can view SQL audit logs on the **Audit Log** tab. For more information, see Viewing Audit Log.

Enabling TDSQL-C for MySQL Audit

Last updated：2024-09-06 12:09:40

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

Enabling SQL Audit Service

1. Log in to the TDSQL-C for MySQL console, select **Database Audit** on the left sidebar, select a region at the top, click the **Audit Instance** tab, and click **Disabled** to filter instances whose audit is disabled.
2. On the **Audit Instance** tab, click the ID of the target instance to enter the enablement page, select a log retention period, and click **Enable**.

Note:

You can select 7 days, 30 days, 3 months, 6 months, 1 year, 3 years, or 5 years as the audit log retention period. You can also modify it in the console after enabling audit. For more information, see Modifying Log Retention Period.
In order to meet the security compliance requirements for the retention period of SQL logs, we recommend you select 180 days or above.

Viewing Audit Log

After enabling audit, you can view SQL audit logs on the **Audit Log** tab. For more information, see Viewing Audit Log.

Enabling TencentDB for MongoDB Audit

Last updated：2024-09-06 12:12:19

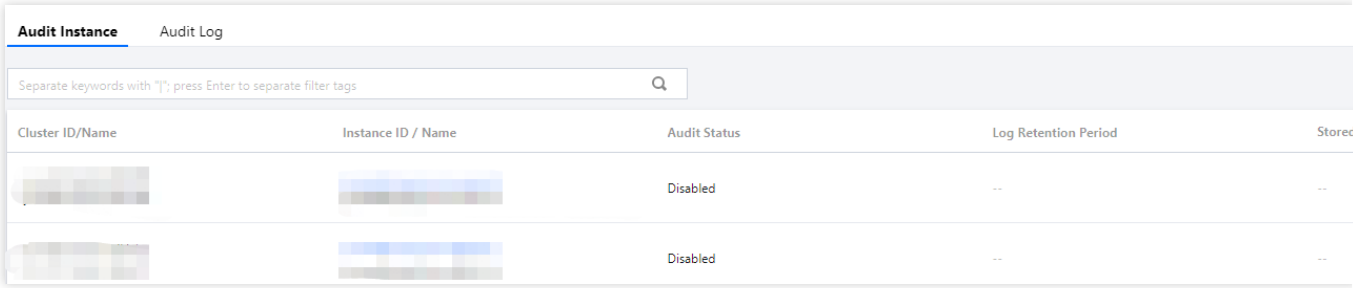
Tencent Cloud provides database audit capabilities for TencentDB for MongoDB, which can record accesses to databases and executions of SQL statements to help you manage risks and improve the database security.

Note:

Database Audit currently supports TencentDB for MongoDB 4.0.

Enabling SQL Audit Service

1. Log in to the TencentDB for MongoDB console, select **Database Audit** on the left sidebar, select a region at the top, click the **Audit Instance** tab, and click **Disabled** to filter instances whose audit is disabled.



Note:

Alternatively, in **Audit Instance** on the **Audit Log** tab, directly search for instances whose audit is disabled and then enable audit.

2. On the **Audit Instance** tab, click the ID of the target instance to enter the enablement page, select a log retention period, and click **Enable**.

Note:

After audit is enabled for TencentDB for MongoDB, the rule is full audit.

You can select 7 days, 30 days, 3 months, 6 months, 1 year, 3 years, or 5 years as the audit log retention period. You can also modify it in the console after enabling audit. For more information, see Modifying Log Retention Period.

In order to meet the security compliance requirements for the retention period of SQL logs, we recommend you select 180 days or above.

Viewing Audit Log

After enabling audit, you can view SQL audit logs on the **Audit Log** tab. For more information, see Viewing Audit Log.

SQL Audit Rule

Last updated：2023-12-21 17:17:05

Rule Content

The following types are supported:
Client IP, database account, and database name. Supported operators are **include and exclude**.
The full audit rule is a special rule, and all statements will be audited after it is enabled.

Rule Operation

The different fields in each rule add the conditions; that is, the relationship between field and condition is "AND" (&&).
The relationship between rules is "OR" (||).
You can specify one or more audit rules for an instance, and as long as any one of them is met, the instance should be audited. For example, if rule A specifies that only operations of user1 with an execution time >= 1 second need to be audited, and rule B audits the statements of user1 with an execution time < 1 second, then all statements of user1 need to be audited eventually.

Rule Description

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

Database name description

If a statement is of the following table object type:

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

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

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

Then, "db1" and "db2" will be used as the target database for rule judgment. If the rule is configured to audit "db1", "db1" will be audited, and if the rule is configured to audit "db3", "db3" will not be audited.
For statements not of the above table object type, the currently used database will be used as the target database for

rule judgment. For example, if the currently used database is "db1", and the executed statement is `show databases` , then "db1" will be used as the target database for judgment. If the rule is configured to audit "db1", "db1" will be audited.

Notes

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.