

# **TDSQL for MySQL**

## **Operation Guide (InnoDB)**

### **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

## Operation Guide (InnoDB)

### Instance Management

- Renaming Database Instance
- Specifying Project for Instance
- Isolating/Restoring/Terminating Instances
- Adjusting Deployed Node
- Changing Instance Specification
- Restarting Instance

### Disaster Recovery Read-Only Instance

### Changing Networks

### Account Management

- Creating Account
- Modifying Account Permissions
- Cloning Account
- Configuring Read/Write Separation
- Resetting Account Password
- Deleting Account

### Security Management

#### Access Management

- Overview
- Policy Structure
- Resource-level Permissions Supported
- Console Examples
- CAM-enabled Operations

#### Security Group Configuration

#### Transparent Data Encryption (TDE)

### Slow Query Analysis

### Backup and Rollback

- Backup Mode
- Downloading Backup File
- Backup Encryption
- Rolling Back Database

### Data Migration

### Database Audit

- Enabling Database Audit

Viewing Audit Logs

Modifying Log Retention Period

# Operation Guide (InnoDB)

## Instance Management

### Renaming Database Instance

Last updated : 2024-01-06 17:33:30

This document describes how to rename a database instance in the [TDSQL console](#).

#### Note:

Renaming an instance does not change the private IP of the database or affect database connections.

After the instance is renamed, its project and network remain unchanged.

If an instance is in another task flow (such as upgrade or initialization), it cannot be renamed.

## Directions

1. Log in to the [TDSQL console](#), locate an instance in the instance list, and click the



icon next to its name. You can also click an instance name/ID in the instance list to access the instance details page, and click the



icon next to the instance name in the **Basic Info** section.

2. In the pop-up window, modify the instance name and click **OK**.

#### Note:

An instance cannot be renamed to an existing database instance name.

### Modify instance name ✕

Instance Name \*  ✔

It can contain up to 60 letters, digits, or symbols (-\_).

# Specifying Project for Instance

Last updated : 2024-01-06 17:33:30

This document describes how to assign an instance to different projects for management in the [TDSQL console](#). In Tencent Cloud, project is defined as a method for assigning resources among teams. You can use a project to assign different resources to different teams based on your organizational structure.

Read-only instances and disaster recovery instances are the associated instances of the source instance and should be in the same project as the source instance.

Assigning and reassigning TencentDB instances will not affect the services provided by the instances.

You need to specify a project to which a new instance belongs when purchasing it. The default project will be used if you don't specify one.

## Directions

1. Log in to the [TDSQL console](#), click an instance name in the instance list to enter the instance details page, and click the



icon after **Project**.

### Basic Info

Instance Name	<input type="text" value=""/> <a href="#">Copy</a>
Instance ID	<input type="text" value=""/> <a href="#">Copy</a>
Status	Running
Instance Type	Source Instance
Instance Version	Standard Edition (1 source, 1 replica)
Region	South China(Guangzhou)
Private Network Address	<input type="text" value=""/> <a href="#">Security Group</a>
Private Port	<input type="text" value=""/> <a href="#">Copy</a>
Public Network Address	<a href="#">Enable</a>
Network	<a href="#">luke-test - luke-test=sub</a> <a href="#">Change Network</a>
Project	DEFAULT PROJECT <a href="#">Copy</a>
Character Set	UTF8MB4 <a href="#">Copy</a>
Tag	-- <a href="#">Copy</a>

2. In the pop-up window, select the project and click **OK**.



### Assign to Project ✕

You need to bind the security group again after the database migration. Click to view [Operation Guide](#)

You have selected **1 instance in total**. [View Details](#) ▾

Project Name	Description
<input checked="" type="radio"/> DEFAULT PROJECT	DEFAULT PROJECT

# Isolating/Restoring/Terminating Instances

Last updated : 2024-01-06 17:33:30

## Isolating Instances

An instance can be isolated when you no longer use it. Once isolated, the instance can neither be used nor accessed (but is not eliminated yet), and will be moved to the recycle bin, where you can restore or eliminate it or it will be automatically eliminated when it expires. Even though the instance is isolated, the space occupied by its resources is not freed, and it still has the most basic data replicas.

You can log in to the [console](#), select the pay-as-you-go instance in the instance list, click **Terminate/Return** to return it manually. After the instance is returned, it is in the **Isolated** status and will be retained for 3 days, during which it cannot be accessed. To restore it, you can do so in the recycle bin list.

After an instance is returned, once its status changes to "isolated", no fees related to it will be incurred.

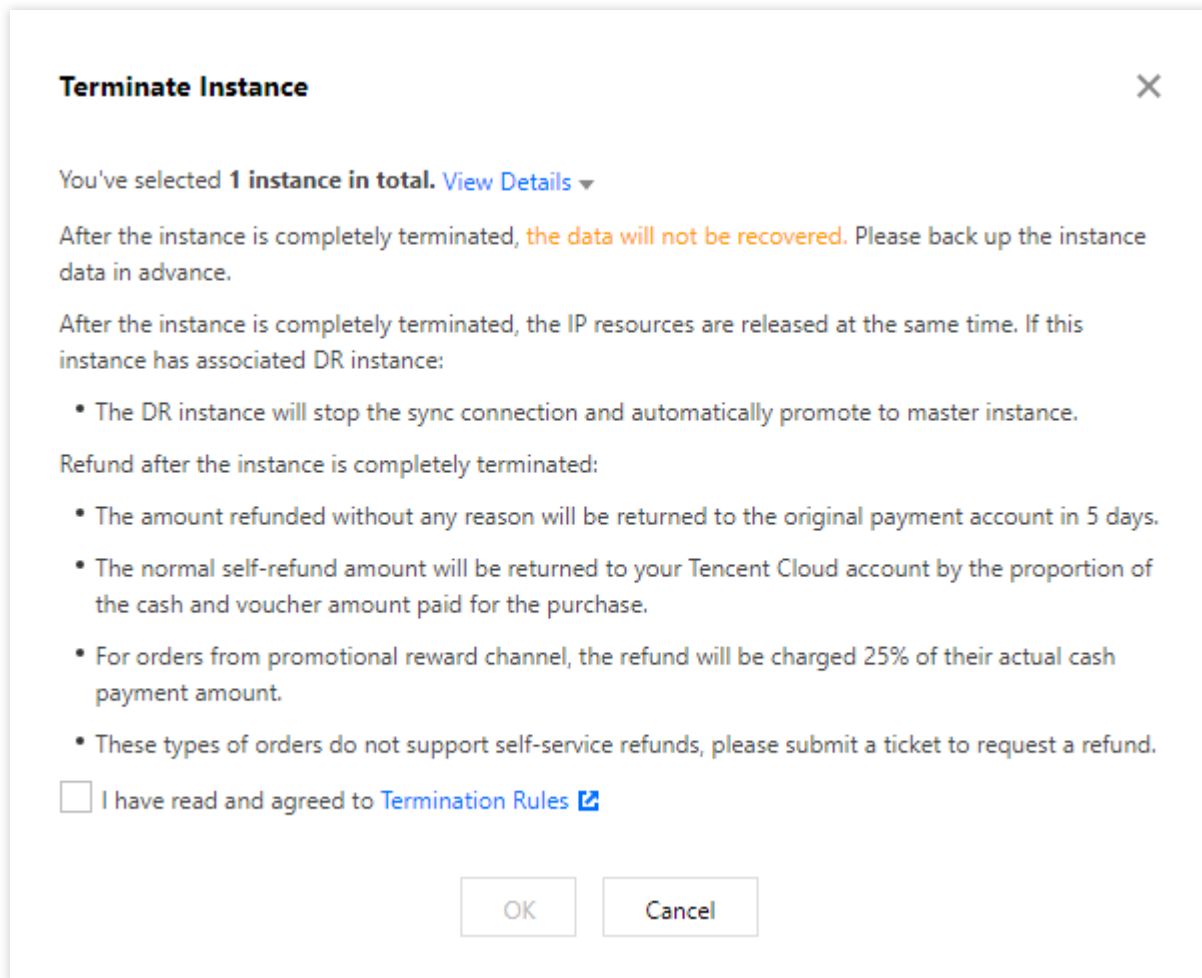
### Note:

After an instance is isolated, its IP will be released, and you may not get back the original IP after the instance is restored.

After an instance is isolated, you cannot upgrade it, modify its parameters, create or modify an account for it, roll it back, or rename it.

## Directions

1. Log in to the [TDSQL for MySQL console](#). In the instance list, select an instance, and click **More >** **Terminate/Return** at the top.
2. In the pop-up dialog box, indicate your consent and click **OK**.



Go to the recycle bin where the instance is in the "isolated" status.

## Restoring Instances

An isolated instance can be restored to its normal running status, which may take several minutes. The restored instance may have a new IP rather than the original IP before isolation.

### Directions

1. Log in to the [TDSQL for MySQL console](#), locate the instance in the recycle bin list, and click **Restore/Start up**.
2. In the pop-up dialog box, click **OK**.

## Terminating Instances

If you don't need an instance anymore, you can return it. Once returned, it is in the "isolated" status and moved to the recycle bin, where it will be automatically eliminated when it expires, or you can click **Eliminate Now** to completely terminate it.

## Notes

After an instance is eliminated, its data will not be recoverable. Please back up the data in advance.

After an instance is eliminated, its IP resources will be released simultaneously, and its disaster recovery instance will stop the sync connection and automatically promote to primary instance.

# Adjusting Deployed Node

Last updated : 2024-01-06 17:33:30

This document describes how to adjust deployed nodes in the TDSQL console. You can add replica nodes to enjoy cross-region replica support, reduce the execution pressure, and increase the read speed. You can also remove unnecessary replica nodes to save the redundant performance costs during idle hours.

## Note:

You can still use the old instance as usual during the adjustment.

The name, access IP, and access port of an instance will remain the same after the adjustment; however, the SQL passthrough ID (Setid) will change.

When the adjustment is completed, the database will be disconnected for several seconds. We recommend that you implement an automatic reconnection feature in your program.

During the adjustment, try avoiding operations such as modifying global parameters, instance name, or user password of the database.

## Adjusting the node deployment region

1. Log in to the [TDSQL console](#) and click the target instance ID in the instance list to enter the instance details page.
2. In **Availability Info** > **Deployment Mode** on the **Instance Details** page, click **Change Deployment Mode**.

### Availability Info [Source-Replica Switch](#)

Data Replication Mode	Strong sync (downgradable)
Replication Status	Sync
Deployment Mode	Multi-AZ (Guangzhou Zone 7, Guangzhou Zone 6, Guangzhou Zone 6) <a href="#">Change Deployment Mode</a>
Source AZ	Guangzhou Zone 7
Replica AZ	Guangzhou Zone 6, Guangzhou Zone 6
Nearby Access	Close

3. On the **Change Deployment Mode** page, select the target deployment mode, and select the regions of the source and replica nodes in the drop-down lists.

## Note:

**Target Deployment Mode:** You can select **Single-AZ** or **Multi-AZ**. In single-AZ mode, the region of replica nodes must be the same as that of the source node. In multi-AZ mode, replica nodes can be in any regions.

Instance Name		
Status	Running	
Network	luke-test - luke-test=sub	
Private Network Address		
Original Deployment Mode	Multi-AZ (Guangzhou Zone 6, Guangzhou Zone 7) (source AZ: Guangzhou Zone 7, replica AZ: Guangzhou Zone 6, Guangzhou Zone 6)	
Original Instance Edition	Standard Edition (1 source, 1 replica)	
Target Deployment Mode	<input checked="" type="radio"/> Single-AZ <input type="radio"/> Multi-AZ	
Source Node	Guangzhou Zone 7	
Replica Node	Guangzhou Zone 7	Delete
	<input type="button" value="Add Replica Node"/>	
Time Consumed	3hr0.160min <small>If the instance has high load or a lot of data writes, adjustment time will be prolonged to ensure its stable operation.</small>	
Specify Switch Time	<input checked="" type="checkbox"/>	
Set Switch Time	2023-02-28 04:22:28	<input type="button" value="Calendar"/> 15-minute deviation (Available switch time: 02-28 04:22:28 to 03-03 01:22:28)
	<input type="checkbox"/> If the switch failed, retry after 2 hours.	
Configuration Fees	362775.21USD/hour <small>Original Price: 848222.08 USD/hour</small> ( <a href="#">Instance</a> <a href="#">Billing Details</a> )	

## Adding/Removing replica nodes

1. Log in to the [TDSQL console](#) and click the target instance ID in the instance list to enter the instance details page.
2. In **Availability Info > Deployment Mode** on the **Instance Details** page, click **Change Deployment Mode**.

**Availability Info** [Source-Replica Switch](#)

Data Replication Mode	Strong sync (downgradable) 
Replication Status	Sync
Deployment Mode	Multi-AZ (Guangzhou Zone 7, Guangzhou Zone 6, Guangzhou Zone 6) <a href="#">Change Deployment Mode</a>
Source AZ	Guangzhou Zone 7
Replica AZ	Guangzhou Zone 6, Guangzhou Zone 6
Nearby Access 	Close 

3. On the **Change Deployment Mode** page, click **Add Replica Node** to add up to five replica nodes.

**Note:**

**Delete:** Click it to remove existing replica nodes. If there is only one replica node, it cannot be removed.

**Scheduled switch:** You can choose to switch the database to its new configuration at a specified time, which is usually during off-peak hours and must be within 72 hours.

Generally, the switch time has a deviation of about 15 minutes, as there may be high amounts of write requests to large transactions, which will affect the data sync progress. In this case, the system will first guarantee sync between the new and old instances instead of performing the scheduled switch.

To ensure a successful switch, you can select the option for retry upon failure, and the system will try switching again two hours after a switch failure.

Instance Name [blurred]

Status **Running**

Network [luke-test - luke-test=sub](#)

Private Network Address [blurred]

Original Deployment Mode **Multi-AZ (Guangzhou Zone 6, Guangzhou Zone 7)** (source AZ: Guangzhou Zone 7, replica AZ: Guangzhou Zone 6, Guangzhou Zone 6)

Original Instance Edition **Standard Edition (1 source, 1 replica)**

Target Deployment Mode

Source Node

Replica Node  [Delete](#)

Time Consumed **3hr0.160min** If the instance has high load or a lot of data writes, adjustment time will be prolonged to ensure its stable operation.

Specify Switch Time

Set Switch Time  [📅](#) 15-minute deviation (Available switch time: 02-28 04:22:28 to 03-03 01:22:28)

If the switch failed, retry after 2 hours.

Configuration Fees **362775.21USD/hour** Original Price: 848222.00 USD/hour (Instance [Billing Details](#))



# Changing Instance Specification

Last updated : 2024-01-06 17:33:30

This document describes how to change instance specifications in the TDSQL console. You can expand the capacity of specified shards by changing their node specifications to improve the business processing performance.

## Note:

You can still use the old instance as usual during the adjustment.

The name, access IP, and access port of an instance will remain the same after the adjustment; however, the SQL passthrough ID (Setid) will change.

When the adjustment is completed, the database will be disconnected for several seconds. We recommend that you implement an automatic reconnection feature in your program.

During the adjustment, try avoiding operations such as modifying global parameters, instance name, or user password of the database.

## Directions

1. Log in to the [TDSQL console](#) and click the target instance ID in the instance list to enter the instance details page.
2. In **Configuration Info > Configuration** on the instance details page, you can see the specification configuration of each node of the instance. Click **Adjust Configurations**.

### Configuration Info

Database Version	MySQL 8.0.22
Configuration	8-core, 16 GB memory, 20 GB storage <a href="#">Adjust Configurations</a>
Backup and Log Space	16 GB (You'll get 100% of the instance capacity for free)
Used/Total	160MB / 20GB
Node Quantity	2
Creation Time	2022-08-05 16:57:21
SQL Engine Layer Version	"proxy-2.0.20-5.tl2_x86_64-R753D004" <a href="#">Shard Details</a>

3. On the **Shard Management** page, select a shard, click **Adjust Shard Configuration**, and select the target specification, disk capacity, and switch time.

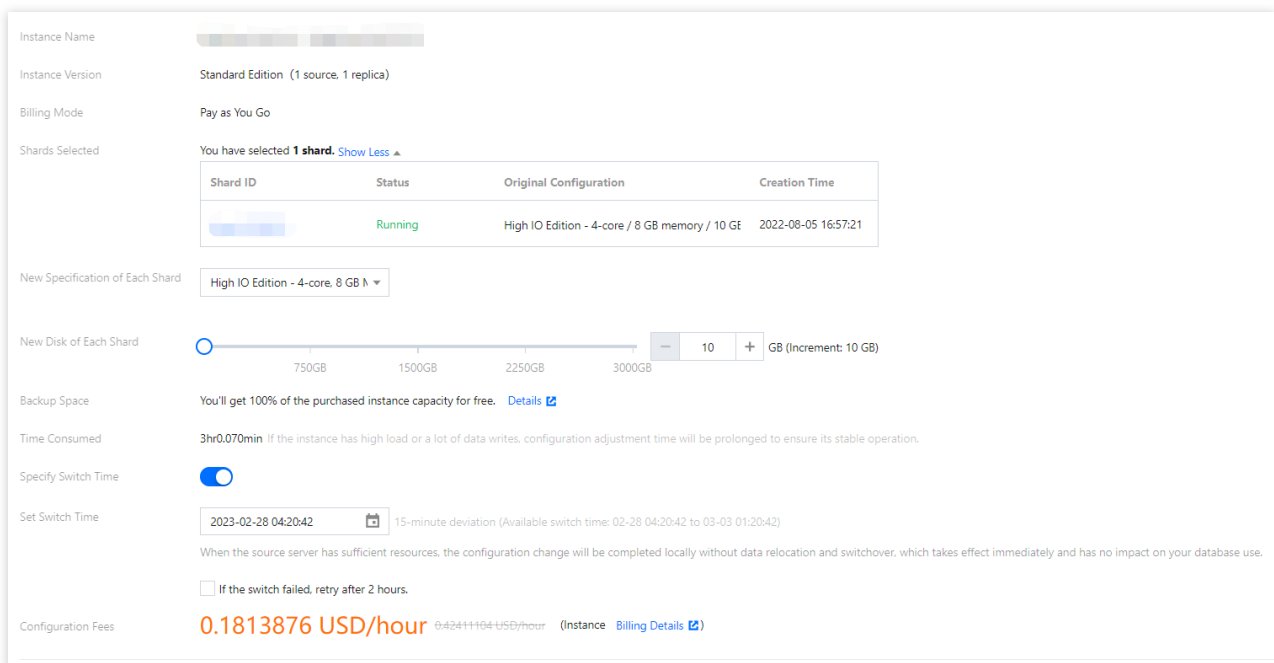
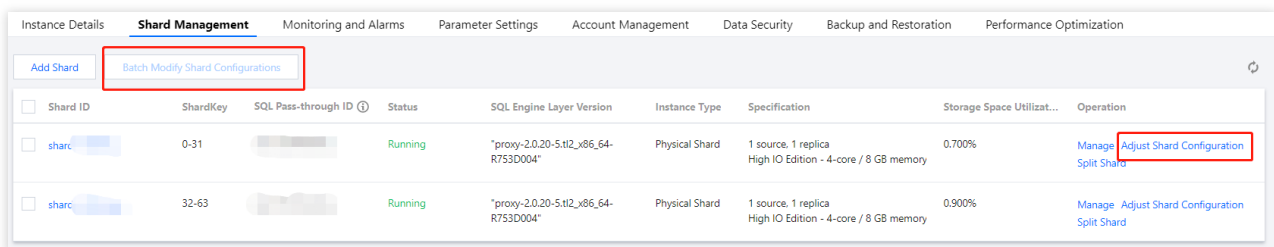
**Note:**

**Scheduled switch**

: You can choose to switch the database to its new configuration at a specified time, which is usually during off-peak hours and must be within 72 hours.

Generally, the switch time has a deviation of about 15 minutes, as there may be high amounts of write requests to large transactions, which will affect the data sync progress. In this case, the system will first guarantee sync between the new and old instances instead of performing the scheduled switch.

To ensure a successful switch, you can select the option for retry upon failure, and the system will try switching again two hours after a switch failure.



## Billing overview

If you upgrade a database instance, the price difference between original and upgraded specifications is deducted from your account. If the account balance is insufficient, you need to top it up.

**Upgrade fees = (price of target specification - price of original specification) \* remaining validity period**

# Restarting Instance

Last updated : 2024-01-06 17:33:30

This document describes how to restart an instance in the console.

## Overview

Instance restart is a common maintenance method for TDSQL for MySQL and is similar to restarting a local database.

## Notes

**Preparation for restart:** during the restart, the instance cannot provide services. Therefore, before the restart, please ensure that TDSQL for MySQL has stopped accepting business requests. During the restart, dirty pages will be generated if the business write volume is high. In this case, the restart may fail in order to shorten the business interruption.

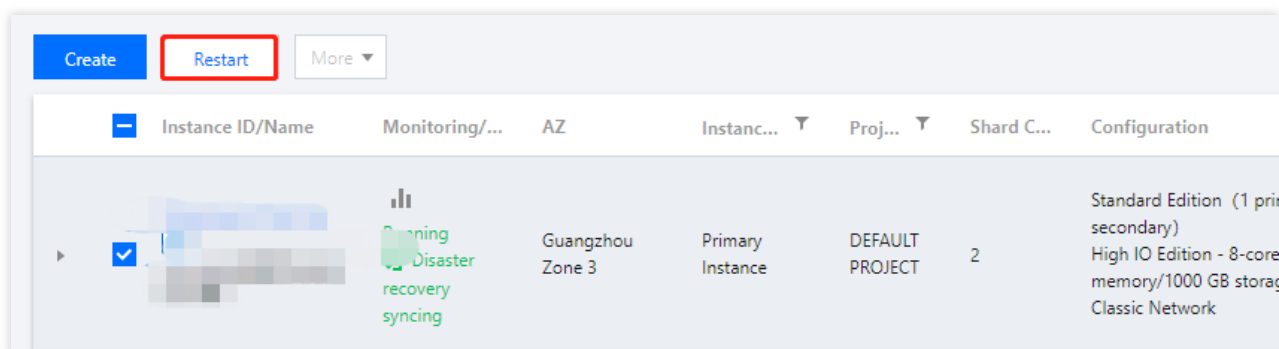
**Restart method:** you are recommended to restart an instance by following the steps provided by Tencent Cloud instead of running the restart command on the instance.

**Restart time:** generally, it takes only a few minutes to restart an instance.

**Physical instance features:** restarting an instance does not change its physical features or private IP.

## Directions

1. Log in to the [TDSQL for MySQL console](#), select one or more instances from the instance list, and click **Restart** at the top.



2. In the pop-up dialog box, check that all information is correct, and click **Confirm** to restart a single instance or multiple instances in batches.

# Disaster Recovery Read-Only Instance

Last updated : 2024-01-06 17:33:30

This document describes how to create and manage disaster recovery read-only instances in the console.

## Overview

TDSQL for MySQL provides cross-AZ/region disaster recovery read-only instances to enhance your capacity to deliver continuous services at low costs while improving data reliability for applications with greater service continuity, data reliability, and compliance requirements.

### Note:

Disaster recovery read-only instance costs the same as the source instance. For detailed pricing, see [Pricing](#).

## Use Cases

**Remote disaster recovery:** To ensure data security, you can use disaster recovery instances to back up your business and data in multiple regions. In the event that an instance becomes unavailable due to an AZ/region failure, you can quickly switch to a cross-AZ/region disaster recovery instance to minimize the impact on your business.

**Nearby access:** You can use an instance in a specific AZ as the source instance and those in other AZs/regions as read-only instances, which provides users with nearby access, remote read capabilities, and improved access speed.

**Multi-region deployment:** TDSQL for MySQL instance can be deployed across multiple regions. When an instance experiences network fluctuations or unavailability in an AZ/region, it can be switched to another AZ/region based on business needs.

## Features

Disaster recovery read-only instances provide separate database connection addresses for read-only access. They can be used for nearby access and data analysis at a lower cost of device redundancy.

A source instance can create one disaster recovery read-only instance that can be deployed in another region and AZ.

Disaster recovery read-only instances support high-availability (1-source-1-replica and 1-source-2-replica) architecture, which helps avoid single point of failure for databases.

If the source instance fails, the disaster recovery read-only instance can be activated in seconds to provide full read/write capability.

Data in a disaster recovery read-only instance is synced over a private network, which has lower latency and greater stability than a public network.

The traffic of data sync over the private network is currently free of charge during the promotion period. If fees will be charged for it, we will inform you in advance.

## Feature Limits

Disaster recovery read-only instance do not support parameter setting and account management features.

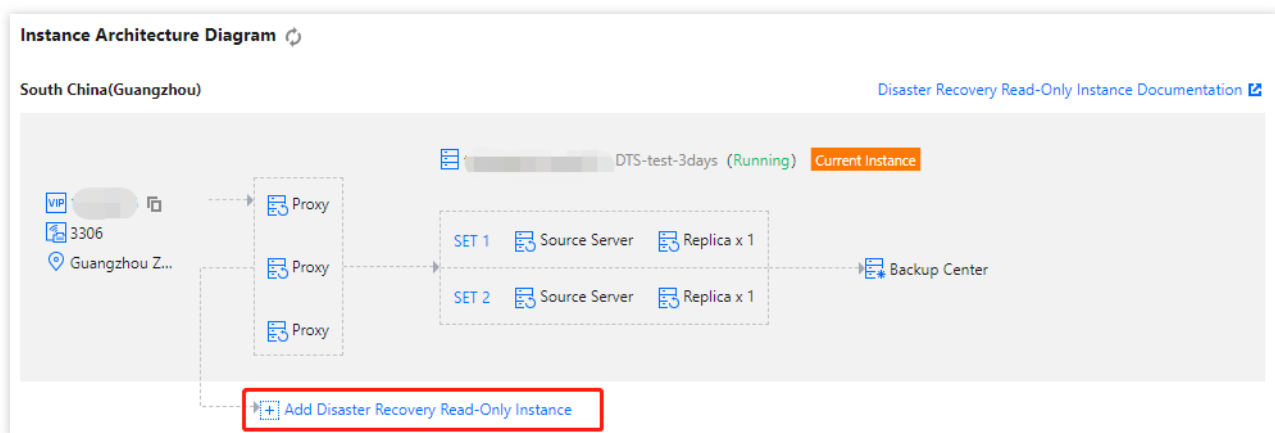
Database version of disaster recovery read-only instance is the same as that of the source instance by default.

Instance specification and disk size should be greater than or equal to that of the source instance.

## Directions

### Creating disaster recovery read-only instance

1. Log in to the [TDSQL for MySQL console](#) and click an instance ID in the instance list to enter the instance management page.
2. In instance architecture diagram on the instance details page, click **Add Disaster Recovery Read-Only Instance**, and enter instance purchase page.



3. On the purchase page, select the billing mode, region, and other basic information of the disaster recovery read-only instance, and click **Buy Now**.

#### Note:

The time required to complete the creation depends on the amount of data, and no operations can be performed on the source instance in the console during the creation. We recommend you do so at an appropriate time.

Only the entire instance data can be synced. Make sure that the disk space is sufficient.

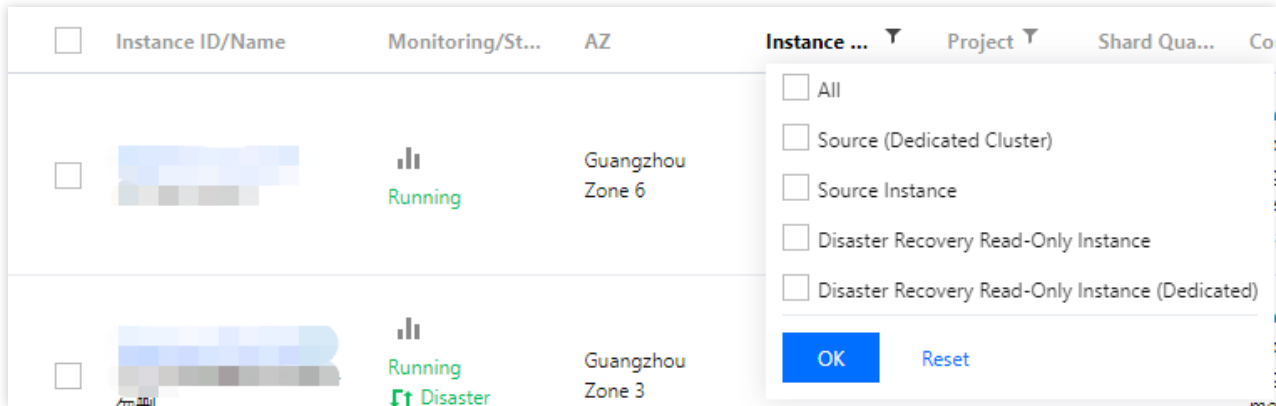
Make sure that the source instance is in the running status and no tasks are executing; otherwise, the sync task may fail.

4. Return to instance list after payment, initialize the instance, and you can proceed to the subsequent operations.

## Manage disaster recovery read-only instances

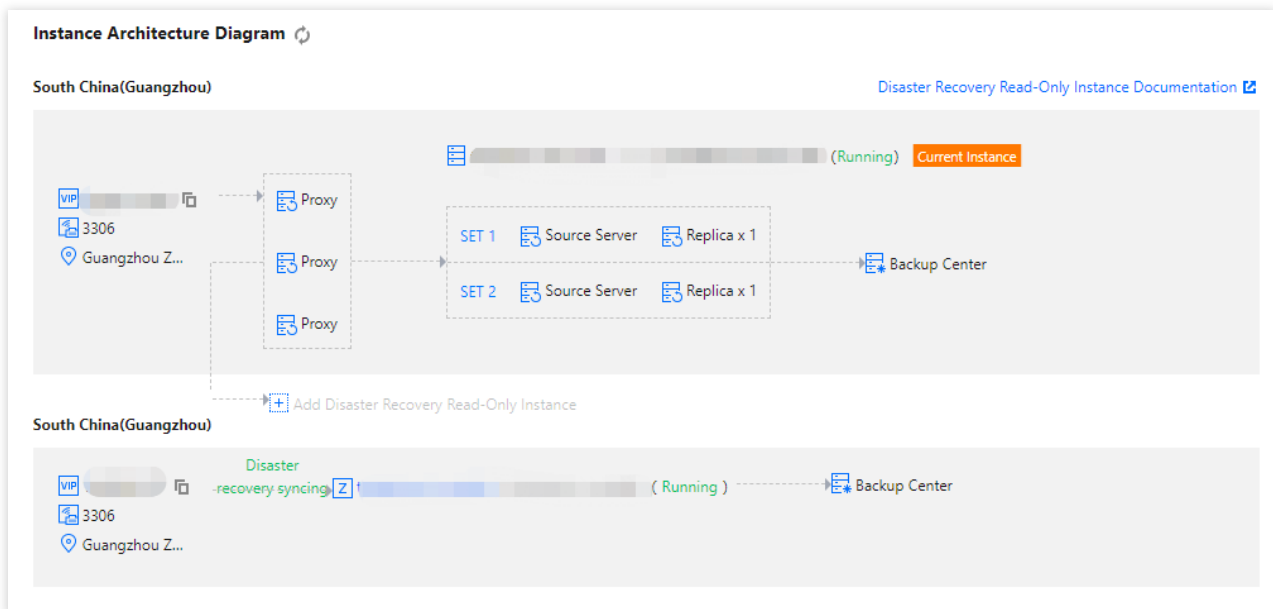
### View disaster recovery read-only instances

You can view disaster recovery read-only instances from the region where they reside, and filter them out in the instance list.



### View the relationship between the source instance and the disaster recovery read-only instance

In instance architecture diagram on the instance details page, you can view the relationship between the source instance and the disaster recovery read-only instance.



### Disaster recovery read-only instance feature

Disaster recovery read-only instance provides instance details, shard management, monitoring and alarms, parameter settings, data security, backup and restoration, and performance optimization features.

### Promoting disaster recovery read-only instance to source instance



You can promote a disaster recovery read-only instance to source instance in the console as needed.

1. Log in to the [TDSQL for MySQL console](#), select the target disaster recovery read-only instance in the instance list, and click the instance ID to enter the instance management page.
2. Click **Promote to Source Instance** in the top-right corner to promote the disaster recovery read-only instance to source instance. After the promotion, the sync link with the source instance will be disconnected, so that the promoted instance can get data write capability and full TDSQL for MySQL functionality.

**Note:**

The disconnected sync link cannot be reconnected. You must exercise caution with this operation.

# Changing Networks

Last updated : 2024-01-06 17:33:30

This document describes how to change the instance network type and modify the instance access address.

## Note:

Modifying the network configurations of an instance is highly risky. Do so only during off-peak hours. After modification, unless the original IP is assigned to another service or a custom IP repossession time is set, the original IP will remain valid for another 24 hours by default. We recommend you modify your business configuration accordingly as soon as possible.

## Modifying Private Network Address










You can modify the private network address of a TencentDB instance in VPC.

1. Log in to the [TDSQL for MySQL console](#) and click an instance ID in the instance list to enter the instance details page.
2. On the instance details page, click



next to **Private Network Address** to modify it. You can do so only when the current subnet has available IPs.

### Basic Info

Instance Name	
Instance ID	 
Running Status	Running
Instance Type	Primary Instance
Instance Version	Standard Edition (1 primary-1 secondary)
Region	South China (Guangzhou)
Private IP	  <a href="#">Security Group</a>
Private Port	3306  
Public IP	Enable
Network	 <a href="#">Change Subnet</a>
Project	DEFAULT PROJECT 

3. In the pop-up window, modify the private network address and click **OK**.

## Switching Between VPC Subnets

You can switch a TDSQL for MySQL instance's network between VPC subnets.

1. Log in to the [TDSQL for MySQL console](#) and click an instance ID in the instance list to enter the instance details page.
2. On the instance details page, click **Change Network** in the **Network** section.
3. In the pop-up window, select the subnet to switch to under the VPC, select **Auto-Assign IP** or **Specify IP**, set **Valid Hours of Old IP**, and click **OK**.

### Note:

The original IP address remains valid for another 24 hours by default after the network is changed. Change your business IP address accordingly within 24 hours.

You can also set **Valid Hours of Old IP** to 0–168 hours. If it is set to 0 hours, the IP is released immediately after the network is changed. This may affect your business.

As the product supports an intra-region active-active architecture, we recommend you choose a VPC subnet in the same region as your business server or the source node.

### Change Subnet

Changing subnet may cause the change of the instance IP. The original IP will become invalid after 24 hours. Modify the IP on the client in time.

Select a subnet

CID:   
253 subnet IPs in total, 242 subnet

To change the network, please go to the console to [Create VPC](#) or [Create Subnet](#)

In the current network environment, only devices in the VPC1 VPC can access this database instance.

It is recommended to select the same subnet as that of the business server or database instance primary node.

Auto-assign IP  
 Specify IP

## Switching Between VPCs

1. Log in to the [TDSQL for MySQL console](#) and click an instance ID in the instance list to enter the instance details page.
2. On the instance details page, click **Change Network** in the **Network** section.
3. In the pop-up window, select the VPC to switch to, select **Auto-Assign IP** or **Specify IP**, set **Valid Hours of Old IP**, and click **OK**.

**Note:**

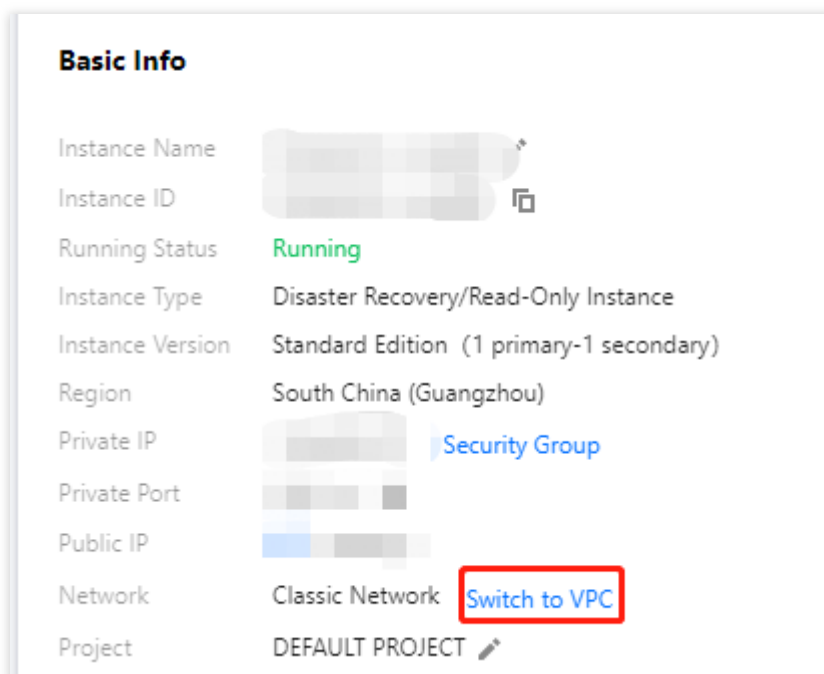
The original VIP address remains valid for another 24 hours by default after the network is changed. Change your business IP address accordingly within 24 hours.

You can also set **Valid Hours of Old IP** to 0–168 hours. If it is set to 0 hours, the IP is released immediately after the network is changed. This may affect your business.

As the product supports an intra-region active-active architecture, we recommend you choose a VPC subnet in the same region as your business server or the source node.

## Switching from Classic Network to VPC

1. Log in to the [TDSQL for MySQL console](#) and click an instance ID in the instance list to enter the instance details page.
2. On the instance details page, click **Switch to VPC** next to **Network**.



3. In the pop-up window, select a VPC, select **Auto-Assign IP** or **Specify IP**, and click **OK**.

**Note:**

The switch from classic network to VPC is irreversible.

After the switch, VPC access will take effect immediately. The original classic network access will be retained for 24 hours; therefore, other instances associated to the instance should be migrated to VPC within 24 hours so as to guarantee uninterrupted access.

As the product supports an intra-region active-active architecture, we recommend you choose a VPC subnet in the same region as your business server or the source node.

# Account Management

## Creating Account

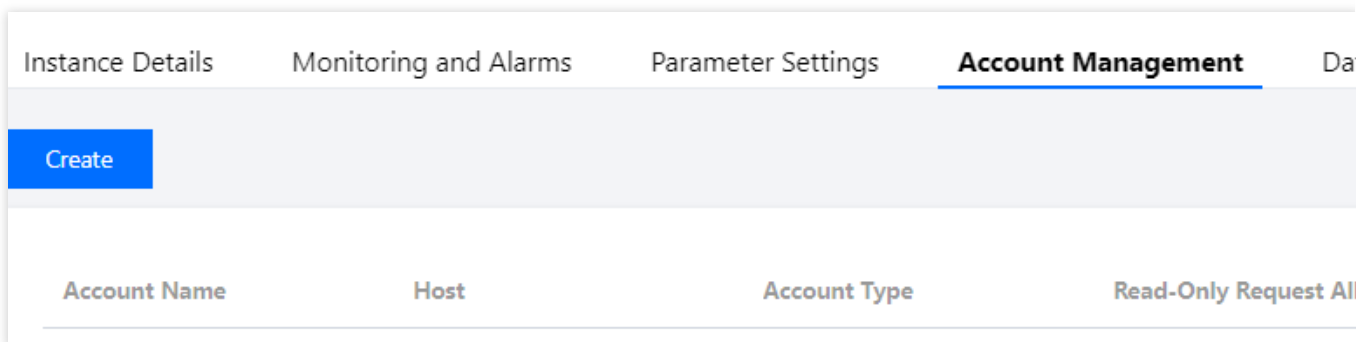
Last updated : 2024-01-06 17:33:30

### Overview

This document describes how to create a TencentDB for MySQL account in the console to manage and connect to the database instance.

### Directions

1. Log in to the [TDSQL console](#). In the instance list, click an instance ID or **Manage** in the **Operation** column to enter the instance management page.
2. On the instance management page, select **Account Management** and click **Create Account**.



3. In the pop-up dialog box, enter the account name, host, and password. After confirming that everything is correct, click **Next**.

Account ID: It must contain 1-32 letters, digits, or symbols, and start with a letter.

Host: It can be an IP and contain `%`.

Password: It must contain 8-32 lowercase letters, uppercase letters, digits, and symbols ( `()~!@#$%^&*~+=_ | { }` `[] : <> , . ? /` ), and cannot start with a slash (/).

Maximum connections: If left empty or `0` is passed in, the "max\_connections" parameter will take effect.

**Create**

Account Name \*

The account name contain 1-32 letters, digits, or symbols (\_), and must start with a letter.

Create as Read-Only Account

 Yes  No

If yes, you can set the parameters of the read-only account after clicking OK.

Host \*

It is in the format of an IP ending with %. You can also enter % or 127.0.0.1.

Set Password \*



The password must contain 8-32 characters in all of the following four types: lowercase letters, uppercase letters, digits, and symbols (()-!@#%&^\*+=\_[]:;<>.,?/). It cannot start with a slash (/).

Confirm Password \*



The password must contain 8-32 characters in all of the following four types: lowercase letters, uppercase letters, digits, and symbols (()-!@#%&^\*+=\_[]:;<>.,?/). It cannot start with a slash (/).

Maximum Connections

If left empty or `0` is passed in, the "max\_connections" parameter will take effect.

Remarks

Up to 256 characters for remarks

4. To create an RO account, you need to [configure read/write separation](#) for it. Confirm the information you enter, click **OK**.

-If **Source Server** is selected, read from the source server when the delay of replica server times out.

If **Report Errors** is selected, an error will be reported when all replica servers are delayed.

If **Read Only from Replica Server** is selected, ignore the replica delay and always read from replica server (generally used to fetch binlog for sync).

If your instance architecture is 1-source-1-replica, select **Read Only from Replica Server** carefully to prevent high-load tasks like large transactions from affecting backup tasks and replica server availability.



### Read-Only Account Settings

Account Name cycloneli

Host %

Read-Only Request Allocation Policy \*  Primary Server  Report Errors  
 Read Only from Replica Server

If "Primary Server" is selected, read from the primary server when the delay of replica server times out.

If "Report Errors" is selected, report errors for the replica delay.

If "Read Only from Replica Server" is selected, ignore the delay parameter and always read from replica server (generally used for fetch binlog for sync).

If your instance architecture is 1-source-1-replica, please select "Read Only from Replica Server" carefully to avoid the impact on the backup tasks and availability of the replica server by high-I/O tasks such as large transactions.

Specified Read-Only Replica Server \*



When the specified read-only replica server is enabled, the read-only requests will be automatically disconnected and will not be switched to another replica server if the source-replica delay exceeds the delay parameter.

When the specified read-only replica server is disabled, another available replica server will be automatically selected if the source replica delay exceeds the delay parameter.

Read-Only Replica Server Delay Parameter \*  sec

If the replica server delay exceeds this parameter value, the replica server is considered faulty. We recommend that you set this parameter to a value larger than 10.

OK

Cancel

5. In the **Modify Permissions** pop-up window, grant permissions as needed and click **Modify**. To discard the changes, click **Cancel Modification**.

Account name: cycloneli@%

**Modify the database permissions for one or more objects**

Global Privileges

▶ Object Level Privilege

- ALTER
- ALTER ROUTINE
- CREATE
- CREATE ROUTINE
- CREATE TEMPORARY TABLES
- CREATE VIEW
- DELETE
- DROP
- EVENT
- EXECUTE
- INDEX
- Select All

**Objects selected and permissions modified**

Global Privileges

Refresh Reset

Modify
Cancel Modification

## Related APIs

API Name	Description
<a href="#">CreateAccount</a>	Creates an account

# Modifying Account Permissions

Last updated : 2024-01-06 17:33:30

## Overview

You can grant global/object-level privileges for TDSQL for MySQL accounts in the console.

## Directions

1. Log in to the [TDSQL console](#). In the instance list, click an instance ID or **Manage** in the **Operation** column to enter the instance management page.
2. On the instance management page, select the **Account Management** tab, find the account for which to modify the permission, and click **Modify Permissions**.

Account Name	Host	Account Type	Read-Only Request Alloca...	Creation Time	Update Time
cycloneli	%	General Account	None	2022-12-19 16:40:14	2022-12-19 16:4

3. In the pop-up dialog box, select or deselect permissions and click **OK** to complete the modification.

Global Privileges: Grant permissions to all databases in the instance.

Object-Level Privileges: Grant permissions to certain databases in the instance.

Account name: cycloneli@%

**Modify the database permissions for one or more objects**

**Objects selected and permissions modified**

Global Privileges

Object Level Privilege

- ALTER
- ALTER ROUTINE
- CREATE
- CREATE ROUTINE
- CREATE TEMPORARY TABLES
- CREATE VIEW
- DELETE
- DROP
- EVENT
- EXECUTE
- INDEX
- Select All

Global Privileges

↔

Refresh Reset

Modify
Cancel Modification

## Related APIs

API Name	Description
<a href="#">DescribeAccountPrivileges</a>	Queries account permission
<a href="#">GrantAccountPrivileges</a>	Sets account permission

# Cloning Account

Last updated : 2024-01-06 17:33:30

## Overview

You can clone a database account in the TDSQL for MySQL console, and retain its original account password to provide different permissions.

## Directions

1. Log in to the [TDSQL console](#). In the instance list, click an instance ID or **Manage** in the **Operation** column to enter the instance management page.
2. On the database management page, select the **Account Management** tab, find the account for which to reset the password, and click **Clone Account**.

Account Name	Host	Account Type	Read-Only Request Alloca...	Creation Time	Update Time
cycloneli	%	General Account	None	2022-12-19 16:40:14	2022-12-19 16:4

3. In the pop-up window, enter the source server IP, account name, and password (the name and password can be the same as that of the original account), then click **Confirm and Go Next**.

## Clone Account >

Account Name \*

The account name contain 1-32 letters, digits, or symbols (\_-), and must start with a letter.

Clone Original Account Password

Create as Read-Only Account  Yes  No

If yes, you can set the parameters of the read-only account after clicking OK.

Host \*

It is in the format of an IP ending with %. You can also enter % or 127.0.0.1.

Set Password \*

The password must contain 8-32 characters in all of the following four types: lowercase letters, uppercase letters, digits, and symbols (0~!@#\$%^&\*~+=\_[]:;<>.,?/). It cannot start with a slash (/).

Confirm Password \*

The password must contain 8-32 characters in all of the following four types: lowercase letters, uppercase letters, digits, and symbols (0~!@#\$%^&\*~+=\_[]:;<>.,?/). It cannot start with a slash (/).

Maximum Connections

If left empty or `0` is passed in, the "max\_connections" parameter will take effect.

Remarks

Up to 256 characters for remarks

4. Return to the account management page to view the cloned account.

## Related APIs

API Name	Description
<a href="#">CloneAccount</a>	Clones an account

# Configuring Read/Write Separation

Last updated : 2024-01-06 17:33:30

## Read/Write Separation Based on Read-only Account

1. Log in to the [TDSQL for MySQL Console](#). In the instance list, click an instance ID or **Manage** in the "Operation" column to enter the instance management page.
2. Select the **Manage Account** tab and click **Create**.
3. In the pop-up dialog box, set the account information, set **Create as read-only account** to **Yes**, and click **Confirm and Go Next**.
4. In the pop-up dialog box, you can set **Read-Only Request Allocation Policy** to define the read policy when a secondary server failure (or long delay) occurs and configure the "Read-Only Secondary Server Delay Parameter", and then click **OK**.

Select **Primary Server** to read from the primary server when the delay of secondary server exceeds the limit.

Select **Report Errors** to report an error when the delay of secondary server exceeds the limit.

Select **Read Only from Secondary Server** to ignore the delay parameter and always read from the secondary server (this is generally used to pull binlogs for sync).

Set the **Read-Only Secondary Server Delay Parameter** to define the data sync delay threshold, which is used together with **Primary Server** and **Report Errors** under the **Read-Only Request Allocation Policy**.



### Read-only Account Settings ✕

Account Name test

Master Server %

Read-only Request Allocation Policy \*  Master Server  Report Errors  
 Read Only from Slave Server

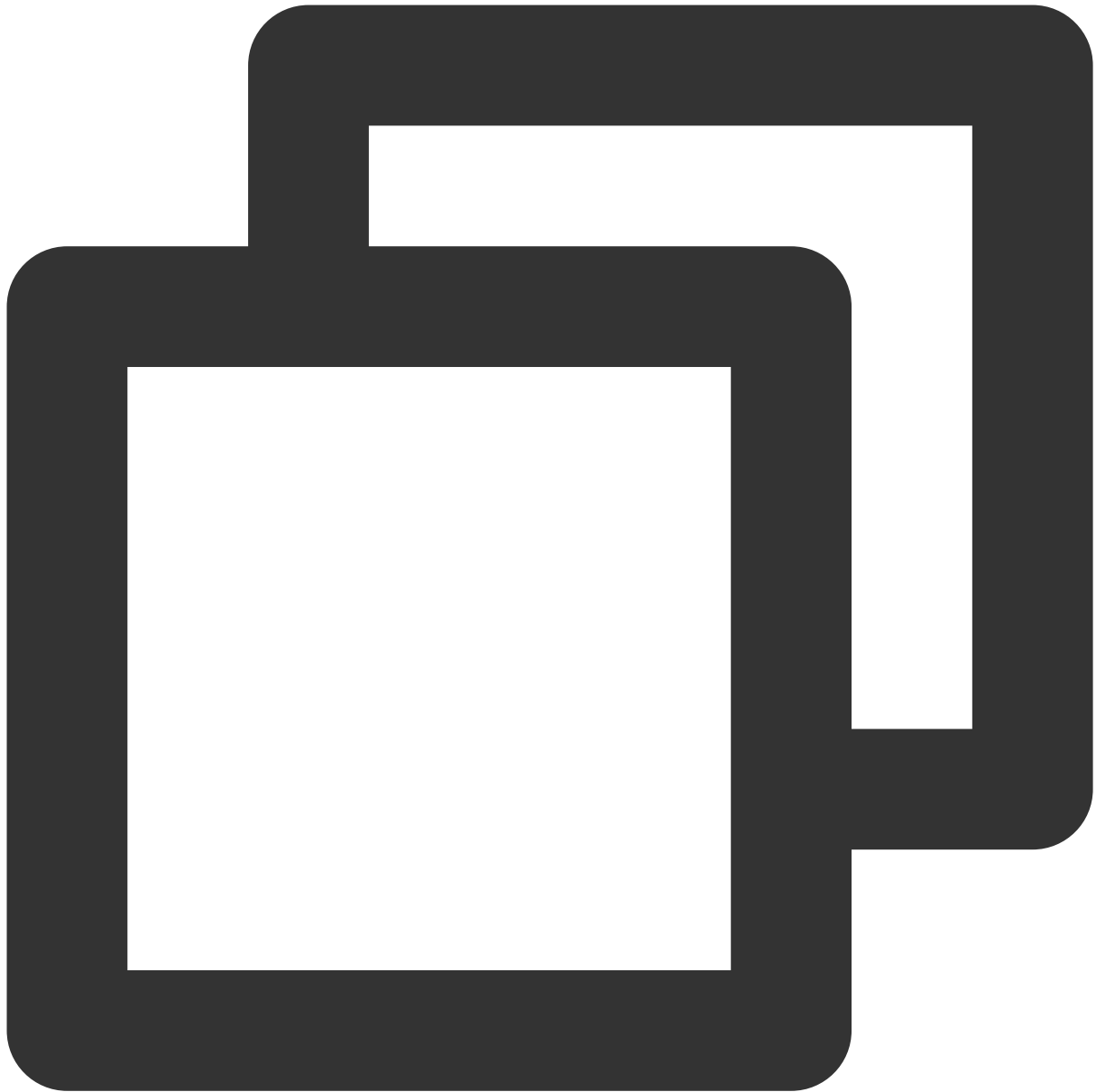
If "Master Server" is selected, read from the master server when the delay of slave server times out.  
If "Report Errors" is selected, report errors for the slave delay.  
If "Read Only from Slave Server" is selected, ignore delay parameter and always read from slave server (generally used to fetch binlog for sync).

Read-only slave server delay parameter \*  sec

If the slave server delay exceeds this parameter value, the slave server is considered faulty. It is recommended to set this parameter to a value larger than 10.

## Read/Write Separation Based on Comment

Add the `/*slave*/` field before each SQL statement to be "read" by the secondary server, and add the `-c` parameter after "mysql" to parse the comment, such as `mysql -c -e "/*slave*/sql"`, to automatically assign "read" requests to the secondary server. Below are examples:



```
//Read from the primary server//  
select * from emp order by sal, deptno desc ;  
//Read from the secondary server//  
/*slave*/ select * from emp order by sal, deptno desc ;
```

**Note:**

This feature only supports read from the secondary server (SELECT) rather than other operations. Non-SELECT statements will fail.

The `-c` parameter needs to be added after `mysql` to parse the comment.

`/*slave*/` must be in lowercase, and no spaces are needed before and after the statement.

If the MAR (strong sync) mechanism is affected by a secondary server exception, read from the secondary server will be automatically switched to read from the primary server.

# Resetting Account Password

Last updated : 2024-01-06 17:33:30

## Overview

If you forgot your database account password or need to modify it while using TDSQL for MySQL, you can reset it in the console.

### Note:

We recommended that you regularly reset the password at least once every three months for the sake of data security.

## Directions

1. Log in to the [TDSQL console](#). In the instance list, click an instance ID or **Manage** in the **Operation** column to enter the instance management page.
2. On the instance management page, select **Account Management** tab, find the account for which to reset the password, and select **More > Reset Password**.

Account Name	Host	Account Type	Read-Only Request Alloca...	Creation Time	Update Time
cycloneli	%	General Account	None	2022-12-19 16:40:14	2022-12-19 16:4

3. In the pop-up window, enter the **New Password** and **Confirm Password** and click **OK**.

### Note:

To avoid the risks caused by creating, modifying, and deleting account information, we recommend that you configure [access management](#), and reset the password with caution.

### Reset Password ✕

**!** To avoid your business risks caused by creating, modifying, or deleting account info, it is recommended to carefully control the function menu permissions (API keyword: \*Account\*) when you configure access management.

Instance Name

Account Name

Host

Set Password \*

The password must contain 8-32 characters in all of the following four types: lowercase letters, uppercase letters, digits, and symbols (~!@#\$%^&\*+ =\_[]: <>.,?/). It cannot start with a slash (/).

Confirm Password \*

The password must contain 8-32 characters in all of the following four types: lowercase letters, uppercase letters, digits, and symbols (~!@#\$%^&\*+ =\_[]: <>.,?/). It cannot start with a slash (/).

## Related APIs

API Name	Description
<a href="#">ResetAccountPassword</a>	Resets account password

# Deleting Account

Last updated : 2024-01-06 17:33:30

## Overview

This document describes how to delete a TDSQL for MySQL account in the console.

### Note:

A database account cannot be recovered once deleted. Ensure that the account is no longer in use and proceed with caution.

## Directions

1. Log in to the [TDSQL console](#). In the instance list, click an instance ID or **Manage** in the **Operation** column to enter the instance management page.
2. On the instance management page, select **Account Management** tab, find the account for which to reset the password, and select **More > Delete Account**.

Account Name	Host	Account Type	Read-Only Request Alloca...	Creation Time	Update Time
cycloneli	%	General Account	None	2022-12-19 16:40:14	2022-12-19 16:4

3. In the pop-up dialog box, confirm that everything is correct and click **OK**.

## Related APIs

API Name	Description
<a href="#">DeleteAccount</a>	Deletes an account

# Security Management Access Management Overview

Last updated : 2024-01-06 17:33:30

If you use multiple Tencent Cloud services such as TencentDB, CVM, and VPC that are managed by different users sharing your Tencent Cloud account key, you may face the following problems:

Your password is shared by multiple users, leading to high risk of compromise.

You cannot limit the access permission of other users, which is easy to pose a security risk due to faulty operations.

This is exactly why CAM has been developed.

For a detailed description of CAM, see [CAM Overview](#).

After connecting to CAM, you can allow different users to manage different services through sub-accounts so as to avoid the above problems. By default, a sub-account doesn't have permission to use a TencentDB instance or related resources. Therefore, you need to create a policy to grant the required permission to the sub-account.

A policy is a syntax rule used to define and describe one or more permissions. It can authorize or deny the use of the designated resources by a user or user group. For more information on CAM policy, see [Policy Syntax](#). For more information on how to use a CAM policy, see [Policy](#).

If you do not need to manage the access permission to TencentDB resources for sub-accounts, you can skip this chapter. This will not affect your understanding and usage of other parts in the documentation.

## Getting Started

A CAM policy must authorize or deny the use of one or more TencentDB operations. At the same time, it must specify the resources that can be used for the operations (which can be all resources or partial resources for certain operations). A policy can also include the conditions set for the manipulated resources.

### Note:

You are recommended to manage TencentDB resources and authorize TencentDB operations through CAM policies.

Although the experience stays the same for existing users who are granted permission by project, it is not recommended to continue managing resources and authorizing operations in a project-based manner.

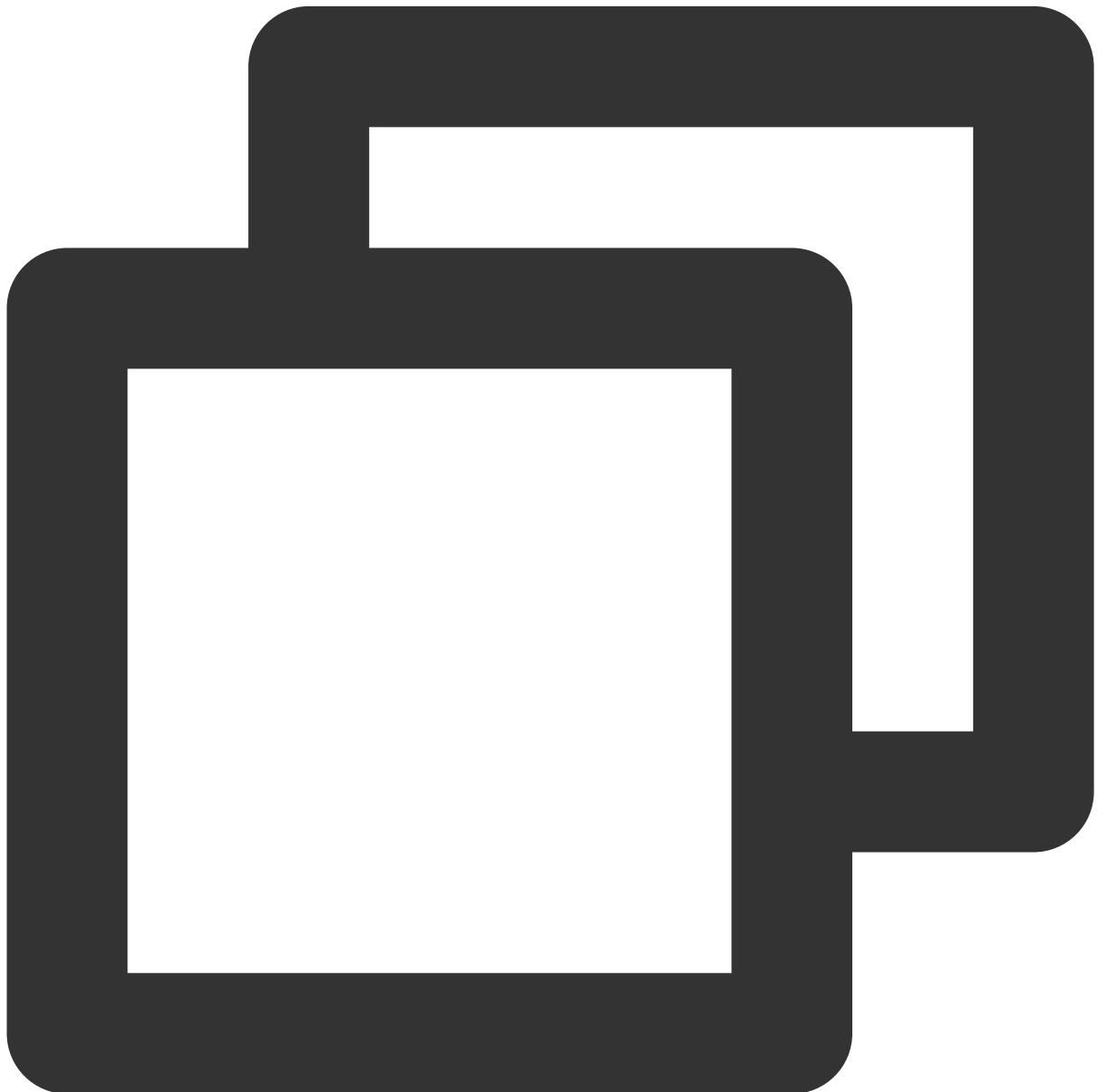
Effectiveness conditions cannot be set for TencentDB for the time being.

# Policy Structure

Last updated : 2024-01-06 17:33:30

## Policy Syntax

CAM policy configuration example:



```
{
```



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

**version** is required. Currently, only "2.0" is allowed. (This value actually represents the version of TencentCloud APIs acceptable to CAM.)

**statement** describes the details of one or more permissions. This element contains a permission or permission set of other elements such as effect, action, resource, and condition. One policy has only one statement.

**action** describes the allowed or denied action. An action entered here is a string prefixed with "dcdb:" and suffixed with an [TDSQL API](#). This element is required.

**resource** describes the details of authorization. A resource is described in a six-piece format. Detailed resource definitions vary by product. For more information on how to specify a resource, see the documentation for the product whose resources you are writing a statement for. This element is required.

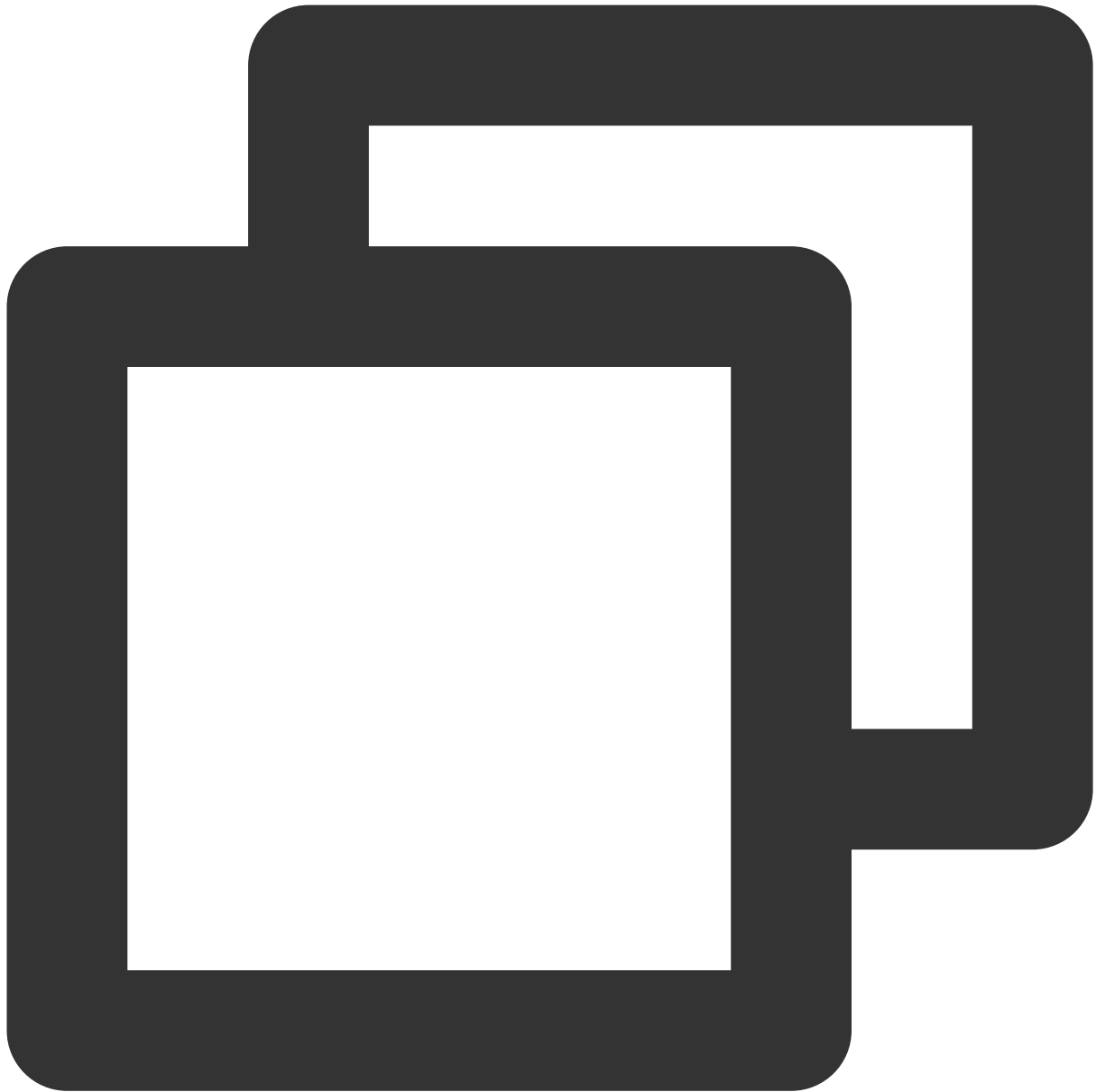
**condition** describes the condition for the policy to take effect. A condition consists of operator, action key, and action value. A condition value may contain information such as time and IP address. Some services allow you to specify additional values in a condition. This element is optional.

**effect** describes whether the result produced by the statement is "allowed" (allow) or "denied" (deny). This element is required.

## Actions in TencentDB

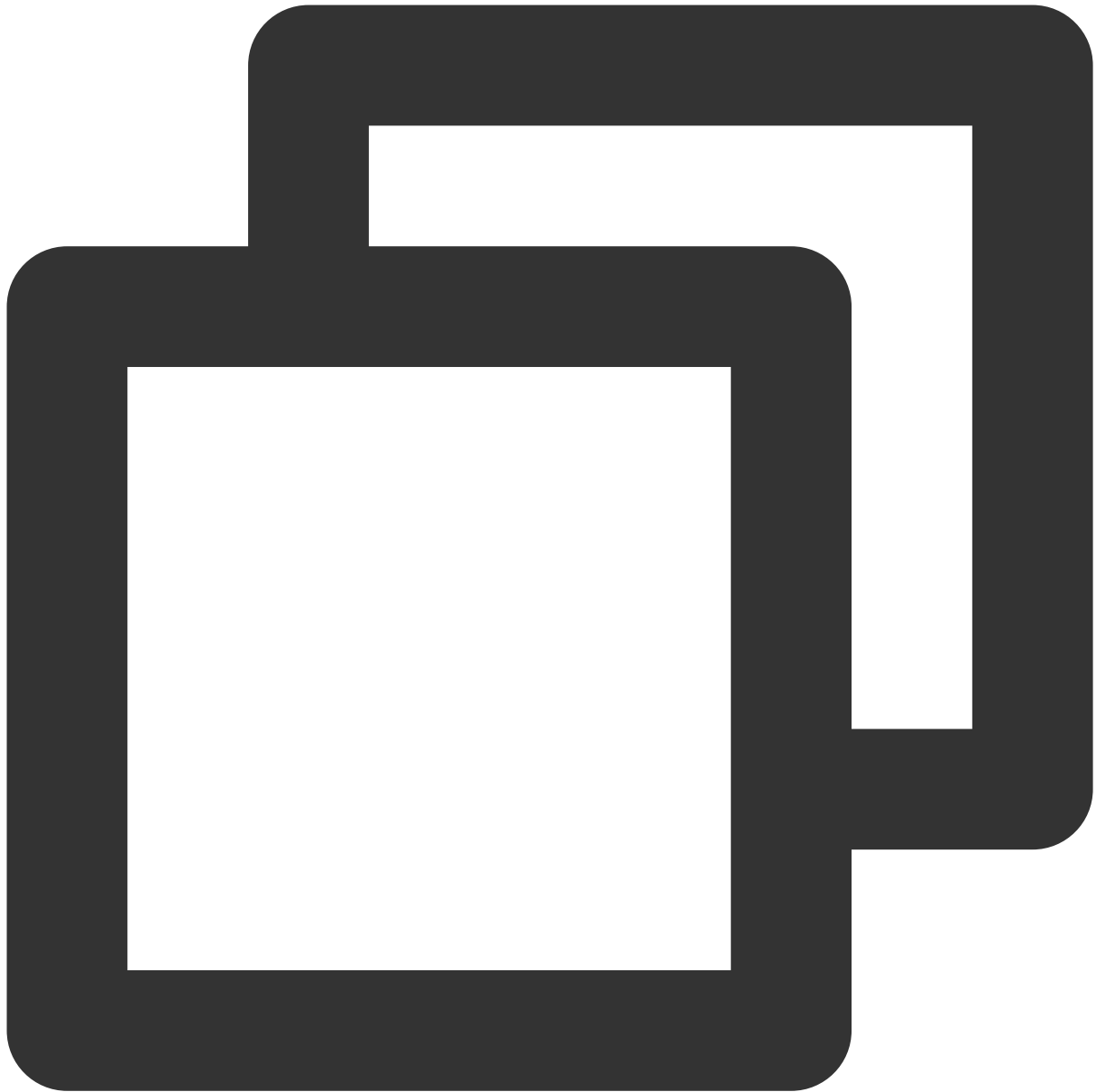
In a TencentDB policy statement, you can specify any API action from any service that supports TencentDB. APIs prefixed with "dcdb:" should be used for TencentDB, such as dcdb:CreateDBInstance (creating an instance - monthly subscription) or dcdb:CloseDBExtranetAccess (disabling public network access).

To specify multiple actions in a single statement, separate them with commas, as shown below:



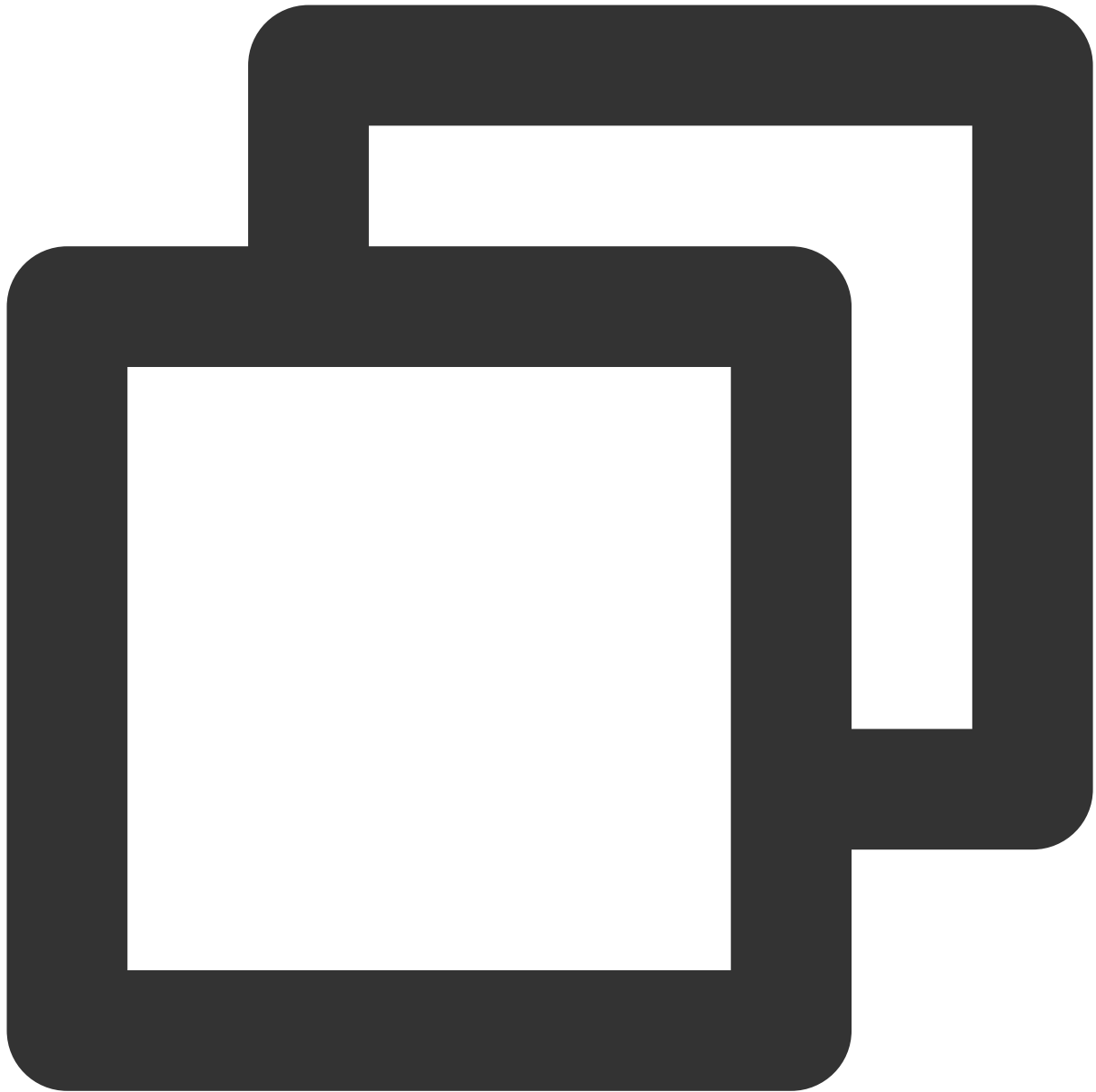
```
"action": ["dcdb:action1", "dcdb:action2"]
```

1. You can also specify multiple actions using a wildcard. For example, you can specify all actions whose names begin with "Describe", as shown below:



```
"action": ["dcdb:Describe*"]
```

2. If you want to specify all operations in TencentDB, use a wildcard as shown below:

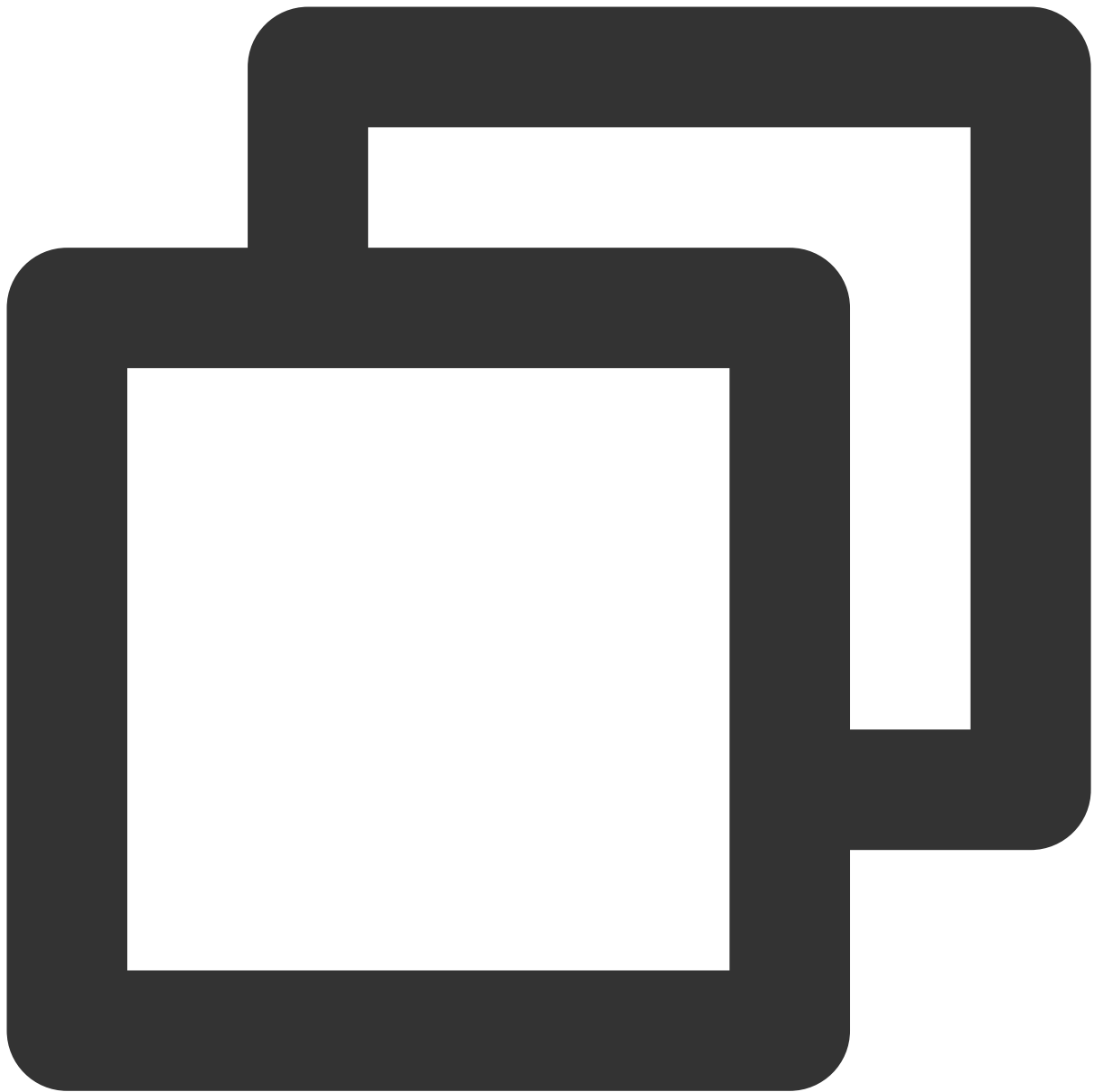


```
"action": ["dcdb:*"]
```

## TencentDB Resources

Each CAM policy statement has its own resources.

Resources are generally in the following format:



```
qcs:project_id:service_type:region:account:resource
```

**project\_id** describes the project information, which is only used to enable compatibility with legacy CAM logic and can be left empty.

**service\_type** describes the product abbreviation such as DCDB.

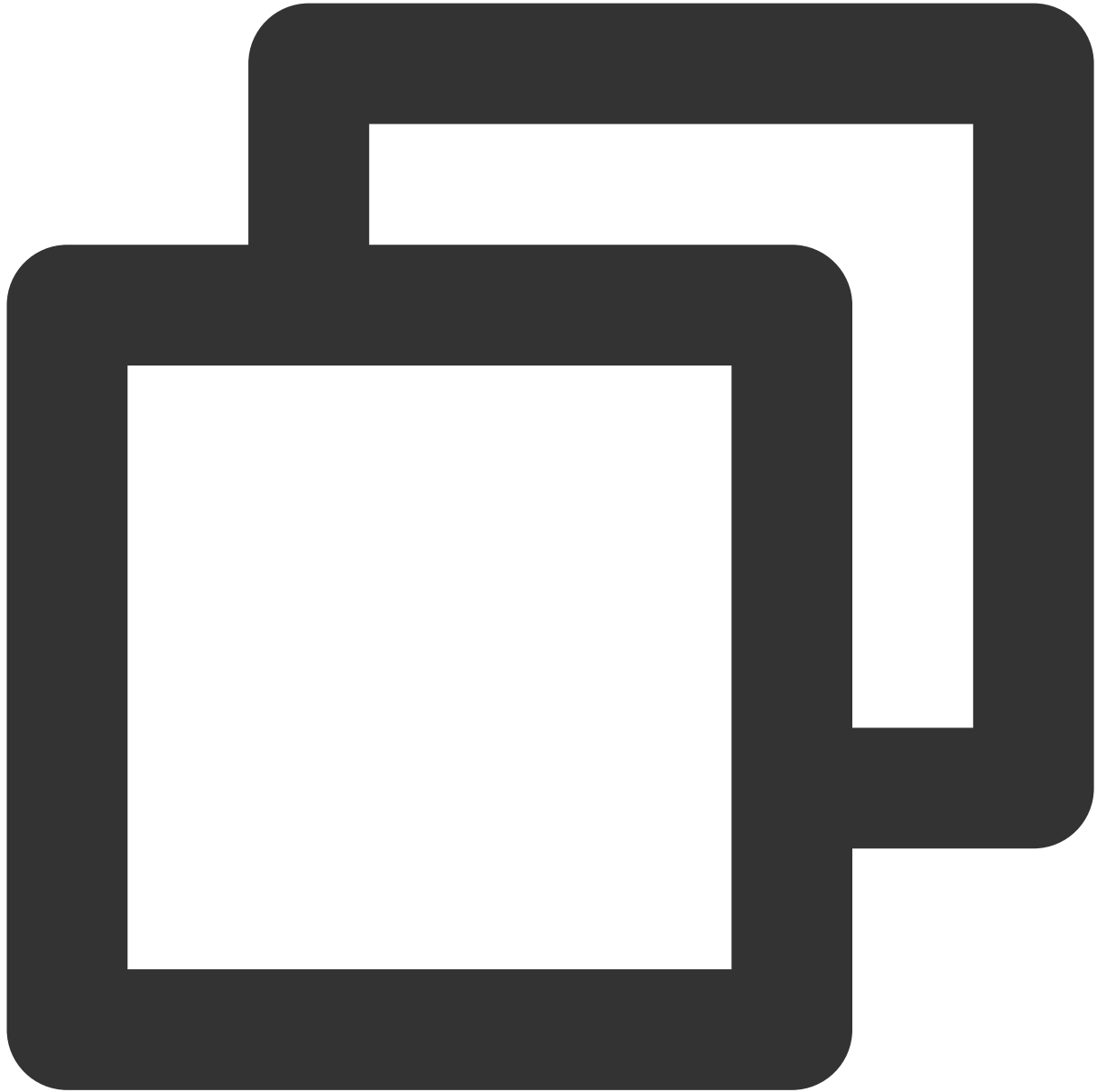
**region** describes the region information, such as ap-guangzhou. For more information, see [Regions](#).

**account** is the root account of the resource owner, such as "uin/65xxx763".

**resource** describes detailed resource information of each product, such as instance/instance\_id1 or instance/\*.

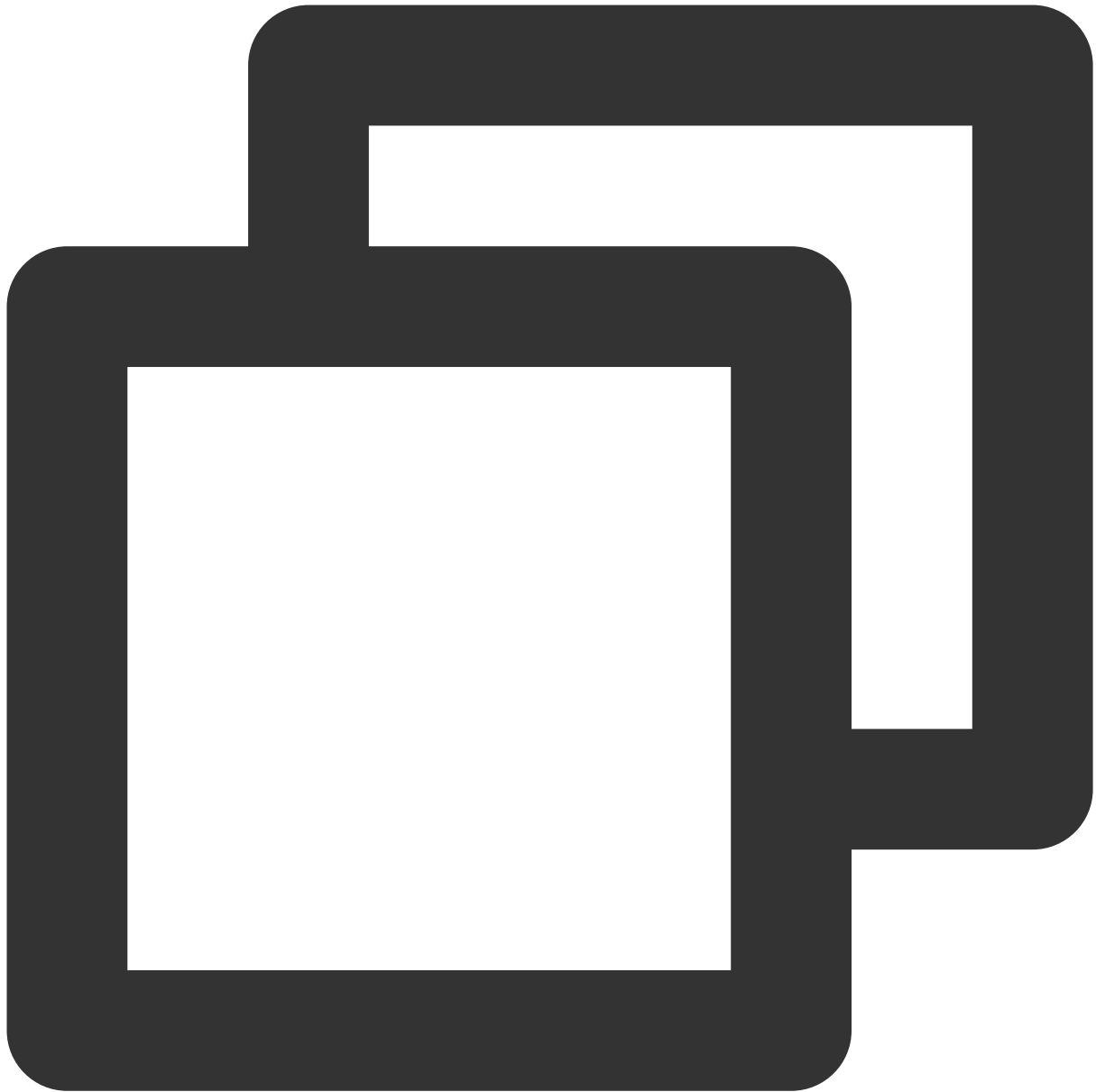
For example:

You can specify a resource for a specific instance (dcdb-k05xdcta) in a statement as shown below:



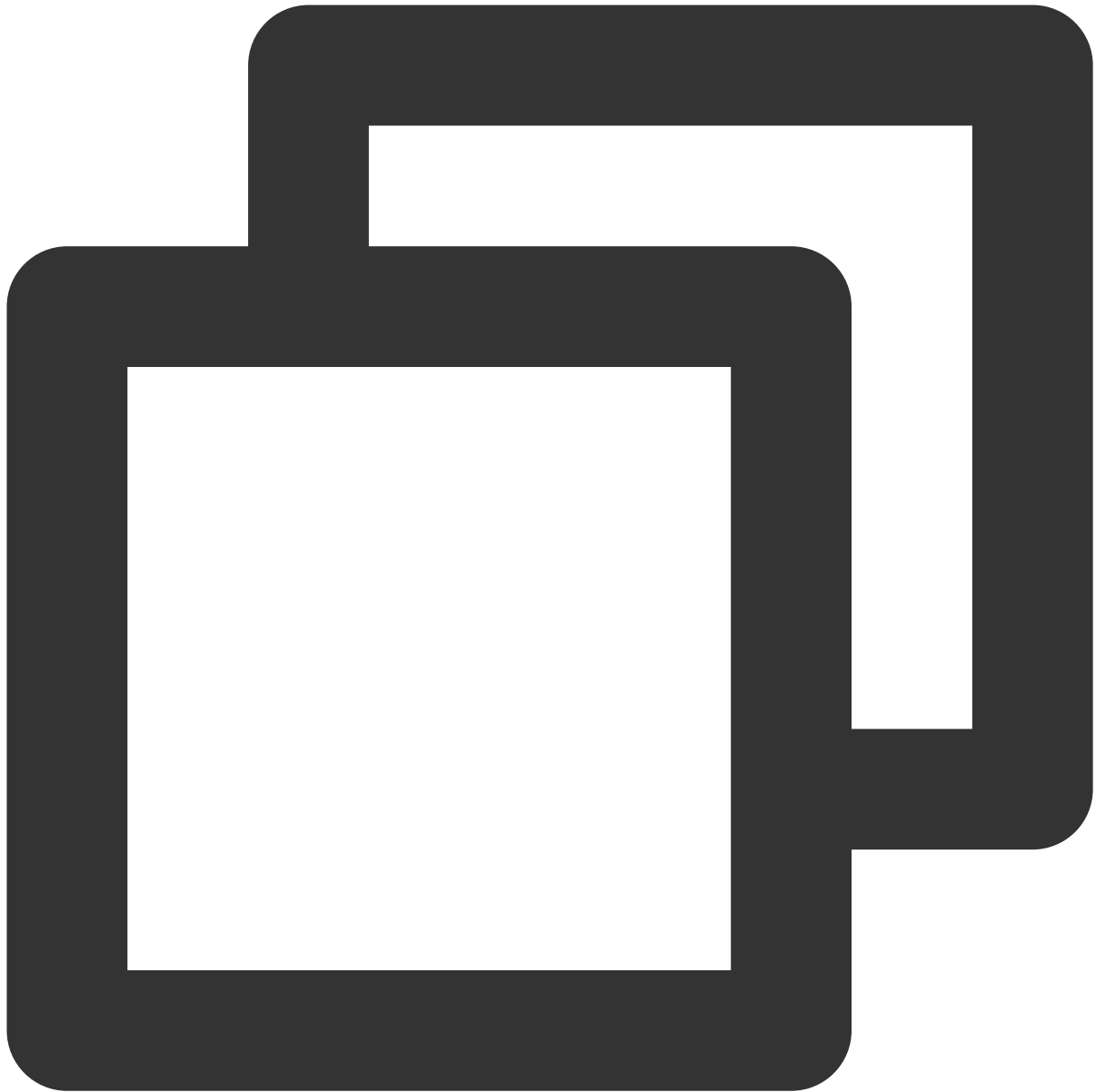
```
"resource": [ "qcs::dcdb:ap-guangzhou:uin/65xxx763:instance/dcdb-k05xdcta" ]
```

1. You can also use the wildcard "\*" to specify it for all instances that belong to a specific account as shown below:



```
"resource": [ "qcs::dcdb:ap-guangzhou:uin/65xxx763:instance/*" ]
```

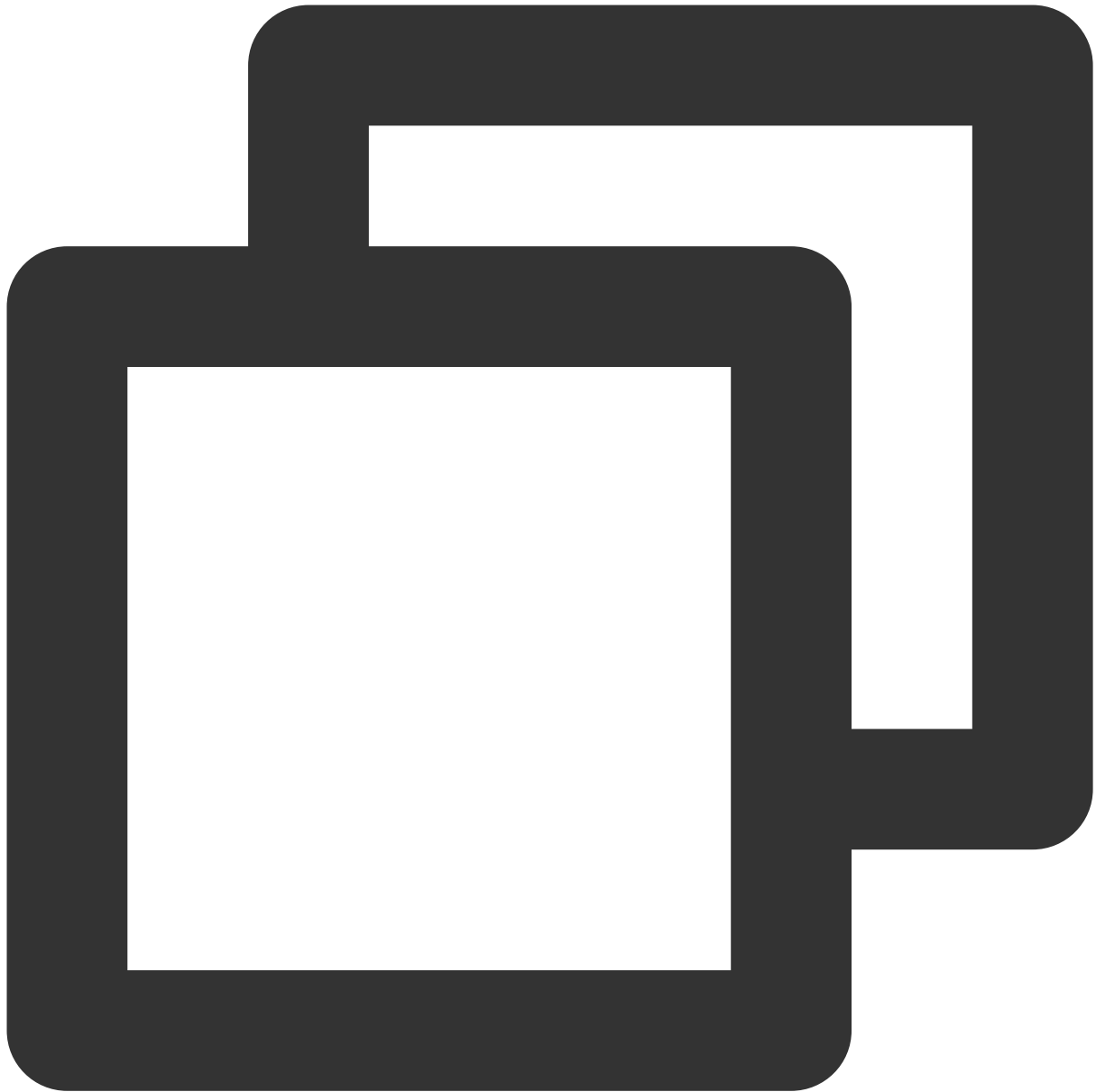
2. If you want to specify all resources or a specific API action does not support resource-level permission control, you can use the wildcard "\*" in the "resource" element as shown below:



```
"resource": ["*"]
```

3. To specify multiple resources in a single command, separate them with commas. Below is an example where two resources are specified:





```
"resource": ["resource1", "resource2"]
```

The table below describes the resources that can be used by TencentDB and the corresponding resource description methods.

In the table, words prefixed with \$ are placeholders.

"region" is region.

"account" is account ID.

Resource	Resource Description Method in Authorization Policy

---

Instance	``qcs::dcdb:\$region:\$account:instance/\$instanceId``
----------	--

# Resource-level Permissions Supported

Last updated : 2024-01-06 17:33:30

Resource-level permission can be used to specify which resources a user can manipulate. TencentDB supports certain resource-level permission. This means that for some TencentDB operations, you can control the time when a user is allowed to perform operations (based on mandatory conditions) or to use specified resources. The following table describes the types of resources that can be authorized in TencentDB.

Types of resources that can be authorized in CAM:

Resource Type	Resource Description Method in Authorization Policy
TencentDB instance-related <code>qcs::dcdb:\$region:\$account:instance/*</code> <code>qcs::dcdb:\$region:\$account:instance/\$instanceId</code>	

The table below lists the TencentDB API operations which currently support resource-level permission control as well as the resources and condition keys supported by each operation. When specifying a resource path, you can use the "\*" wildcard in the path.

Any TencentDB API operation not listed here does not support resource-level permission. If a TencentDB API operation does not support resource-level permission, you can still authorize a user to perform this operation, but you must specify \* for the resource element of the policy statement.

## The following operations support resource-level permission control

Operation Name	API Name	Effective in Console After Configuration
Recovering a dedicated instance	ActiveDedicatedDBInstance	Yes
Binding security groups	AssociateSecurityGroups	Yes
Checking IP status	CheckIpStatus	Yes
Cloning an account	CloneAccount	Yes
Disabling public network access for an instance	CloseDBExtranetAccess	Yes

Copying account permission	CopyAccountPrivileges	Yes
Creating an account	CreateAccount	Yes
Creating an instance	CreateDCDBInstance	Yes
Deleting an account	DeleteAccount	Yes
Querying account permission	DescribeAccountPrivileges	Yes
Querying the account list	DescribeAccounts	Yes
Querying audit logs	DescribeAuditLogs	Yes
Querying audit rule details	DescribeAuditRuleDetail	Yes
Querying the audit rule list	DescribeAuditRules	Yes
Querying audit policies	DescribeAuditStrategies	Yes
Querying the price for batch instance renewal	DescribeBatchDCDBRenewalPrice	Yes
Querying instance objects	DescribeDatabaseObjects	Yes
Querying instance database names	DescribeDatabases	Yes
Querying column information of an instance table	DescribeDatabaseTable	Yes
Getting the log list	DescribeDBLogFiles	Yes
Querying monitoring information	DescribeDBMetrics	Yes
Viewing database parameters	DescribeDBParameters	Yes
Querying security group information of an instance	DescribeDBSecurityGroups	Yes
Getting slow log recording details	DescribeDBSlowLogAnalysis	Yes
Getting the slow log list	DescribeDBSlowLogs	Yes
Querying instance sync mode	DescribeDBSyncMode	Yes
Getting instance details	DescribeDCDBInstanceDetail	Yes
Viewing the instance list	DescribeDCDBInstances	Yes
Querying price	DescribeDCDBPrice	Yes

Querying the renewal price of an instance	DescribeDCDBRenewalPrice	Yes
Querying purchasable AZs	DescribeDCDBSaleInfo	Yes
Querying instance shards	DescribeDCDBShards	Yes
Querying the upgrade price of an instance	DescribeDCDBUpgradePrice	Yes
Querying dedicated cluster specification	DescribeFenceShardSpec	Yes
Querying flow status	DescribeFlow	Yes
Querying the latest DBA check result	DescribeLatestCloudDBAReport	Yes
Viewing backup log settings	DescribeLogFileRetentionPeriod	Yes
Querying order information	DescribeOrders	Yes
Querying projects	DescribeProjects	Yes
Querying security group information of a project	DescribeProjectSecurityGroups	Yes
Querying instance specification	DescribeShardSpec	Yes
Getting SQL logs	DescribeSqlLogs	Yes
Unbinding security groups from Tencent Cloud resources in batches	DisassociateSecurityGroups	Yes
Setting account permission	GrantAccountPrivileges	Yes
Initializing instances	InitDCDBInstances	Yes
Isolating a dedicated instance	IsolateDedicatedDBInstance	Yes
Modifying database account remarks	ModifyAccountDescription	Yes
Setting auto-renewal in batches	ModifyAutoRenewFlag	Yes
Renaming an instance	ModifyDBInstanceName	Yes
Modifying security groups bound to a TencentDB instance	ModifyDBInstanceSecurityGroups	Yes
Modifying instance project	ModifyDBInstancesProject	Yes
Modifying database parameters	ModifyDBParameters	Yes

Modifying instance sync mode	ModifyDBSyncMode	Yes
Modifying instance network	ModifyInstanceNetwork	Yes
Modifying instance VIP	ModifyInstanceVip	Yes
Modifying backup log settings	ModifyLogFileRetentionPeriod	Yes
Enabling public network access	OpenDBExtranetAccess	Yes
Renewing an instance	RenewDCDBInstance	Yes
Resetting account password	ResetAccountPassword	Yes
Enabling smart DBA	StartSmartDBA	Yes
Scaling an instance	UpgradeDCDBInstance	Yes
Upgrading a dedicated instance	UpgradeDedicatedDCDBInstance	Yes

# Console Examples

Last updated : 2024-01-06 17:33:30

## Sample CAM Policies for TencentDB

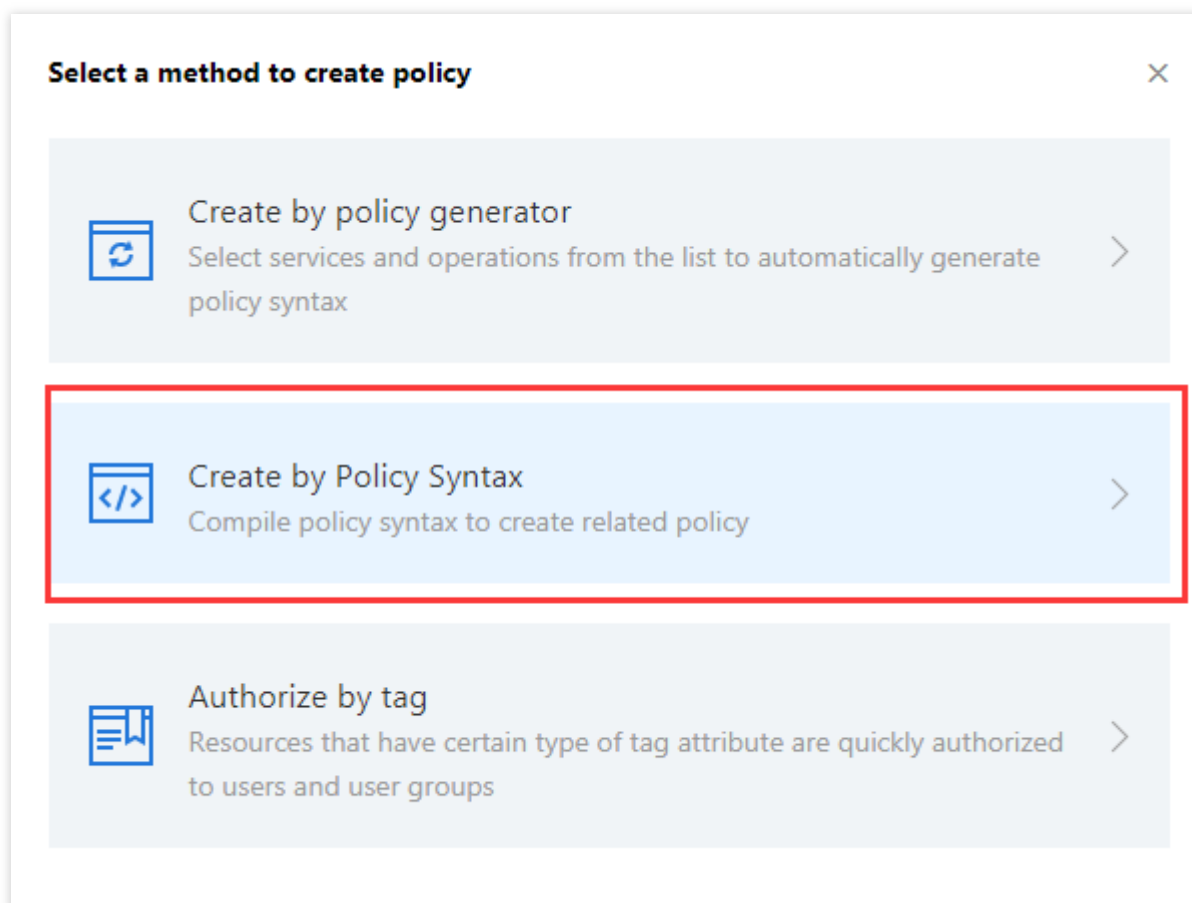
You can grant a user the permission to view and use specific resources in the TencentDB console by using a CAM policy. The sample below shows how to allow a user to use certain policies in the console.

### Note:

As TDSQL for MySQL was formerly known as DCDB, its API keyword in CAM is `dcd` .

### Syntax for creating custom policy

1. Enter the [Policy Syntax](#) configuration page and click **Create Custom Policy**.
2. Click **Create by Policy Syntax** in the pop-up window.



3. Select **Blank Template** and click **Next**.

1 Select policy template >
 2 Edit Policy

Template Type:

All Templates ▼

Search policy name

Q

### Select template type

All Templates (282 items in total)

<div style="border: 2px solid red; padding: 5px; margin-bottom: 10px;"> <input checked="" type="radio"/> Blank Template <span style="border: 1px solid #ccc; padding: 2px 5px;">Custom</span> </div> <div style="margin-bottom: 10px;"> <input type="radio"/> QCloudResourceFullAccess <span style="border: 1px solid #ccc; padding: 2px 5px;">System</span>                      This policy allows you to manage all cloud assets in your account.                 </div> <div style="margin-bottom: 10px;"> <input type="radio"/> QcloudNARMSReadOnlyAccess <span style="border: 1px solid #ccc; padding: 2px 5px;">System</span>                      QcloudNARMSReadOnlyAccess                 </div> <div style="margin-bottom: 10px;"> <input type="radio"/> QcloudAccessForBAASRole <span style="border: 1px solid #ccc; padding: 2px 5px;">System</span>                      QcloudAccessForBAASRole                 </div> <div style="margin-bottom: 10px;"> <input type="radio"/> QcloudAccessForCDNRole <span style="border: 1px solid #ccc; padding: 2px 5px;">System</span>                      CDN permissions (including but not limited to): CLS (add/delete/modify/query CLS logsets/log topics, and search...                 </div> <div style="margin-bottom: 10px;"> <input type="radio"/> QcloudAccessForCloudAuditCARole <span style="border: 1px solid #ccc; padding: 2px 5px;">System</span> </div>	<div style="margin-bottom: 10px;"> <input type="radio"/> AdministratorAccess <span style="border: 1px solid #ccc; padding: 2px 5px;">System</span>                      This policy allows you to manage users and their permissions, financial                 </div> <div style="margin-bottom: 10px;"> <input type="radio"/> QCloudFinanceFullAccess                      This policy allows you to manage your account, such as payment and                 </div> <div style="margin-bottom: 10px;"> <input type="radio"/> QcloudAccessForAegisRole                      Aegis\' access to cloud resource                 </div> <div style="margin-bottom: 10px;"> <input type="radio"/> QcloudAccessForBKRole <span style="border: 1px solid #ccc; padding: 2px 5px;">System</span>                      BlueKing\'s access to cloud resource                 </div> <div style="margin-bottom: 10px;"> <input type="radio"/> QcloudAccessForCFSRole                      CFS permissions(including but not limited to): data key, encrypt/decrypt data                 </div> <div style="margin-bottom: 10px;"> <input type="radio"/> QcloudAccessForCloudStu                 </div>
--	---

Next

4. Enter the corresponding policy syntax.



✓ Select policy template > ✓ Edit Policy

---

Policy Name \*

Notes

### Edit Policy Content

```
1 {  
2   "version": "2.0",  
3   "statement": []  
4 }
```

[Policy Syntax Description](#) [Support service list](#)

## Associating sub-account/collaborator and verifying

After the policy is created, associate it with a user/group. After the association is completed, use another browser (or server) to verify whether the sub-account/collaborator can work normally. If the policy syntax is written correctly, you can observe the following:

You have normal access to the intended target products and resources and can use all the expected features.

You will be prompted that "You do not have permission to perform this operation" when accessing other unauthorized products or resources.

**Note:**

To avoid mutual impact of multiple policies, we recommend you associate only one policy with a sub-account at a time.

The change to account access permission will take effect within 1 minute.

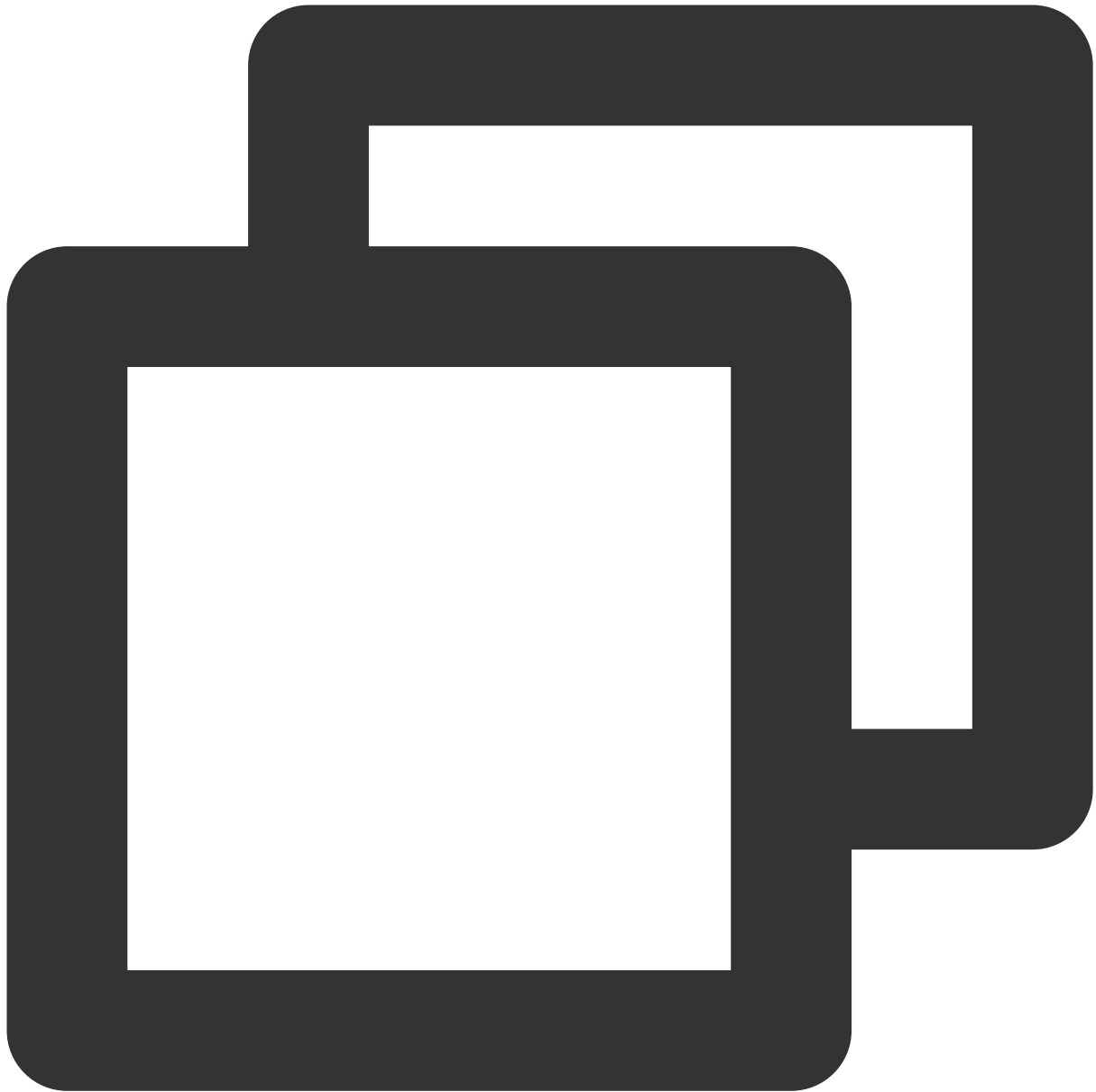
## Appendix. Commonly Used Policy Syntax

### Policy for authorizing the use of all features in all TencentDB instances

To grant a user permission to create and manage TencentDB instances, implement the policy named

`QcloudDCDBFullAccess` for the user.

The policy syntax is as follows:



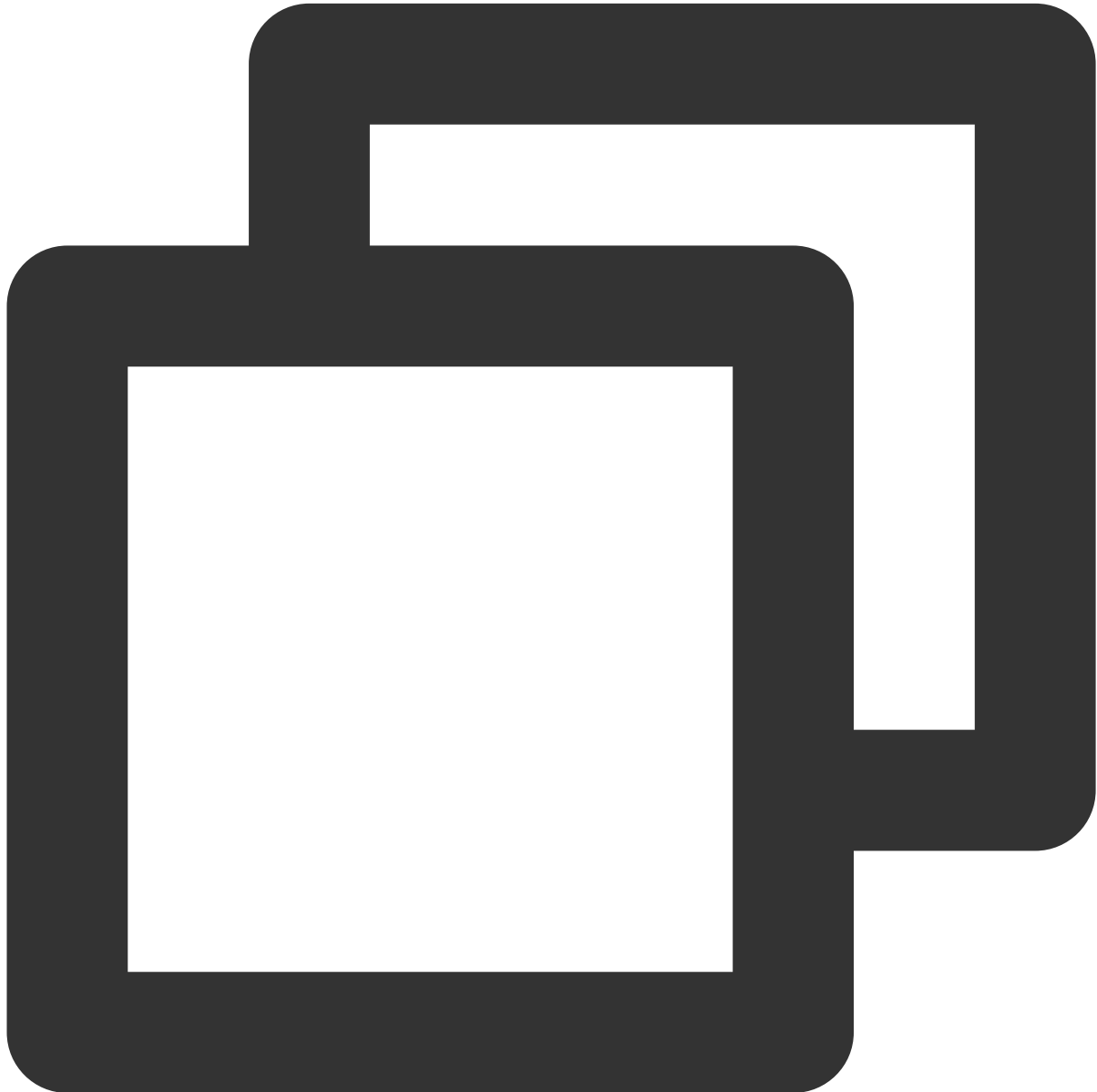
```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "dcdb:*"
      ],
      "resource": "*",
      "effect": "allow"
    }
  ]
}
```

```
}
```

## Policy for authorizing the query of all TencentDB instances

To grant a user permission to view TencentDB instances but not create, delete, or modify them, implement the policy named `QcloudDCDBInnerReadOnlyAccess` for the user.

The policy syntax is as follows:



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

```

```
{
  "action": [
    "dcdb:Describe*"
  ],
  "resource": "*",
  "effect": "allow"
}
```

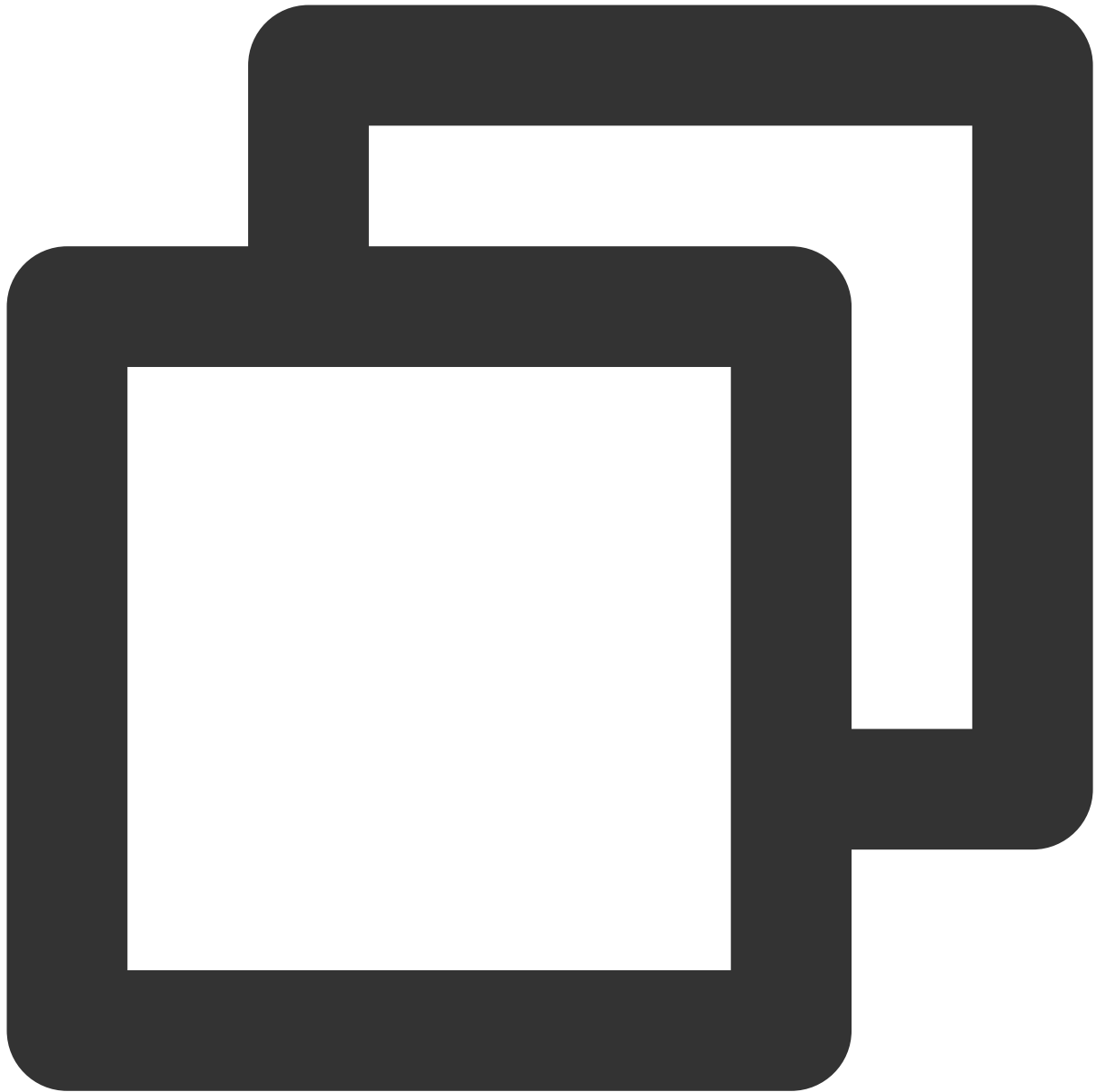
The above policy achieves its goal by allowing the user to separately authorize the use of all operations beginning with "Describe" in TencentDB with the CAM policy.

**Note:**

As not all functional APIs are covered currently, you may see that a small number of operations are not included in CAM, which is normal.

**Policy for granting user permission to manipulate TencentDB instances in one specific region**

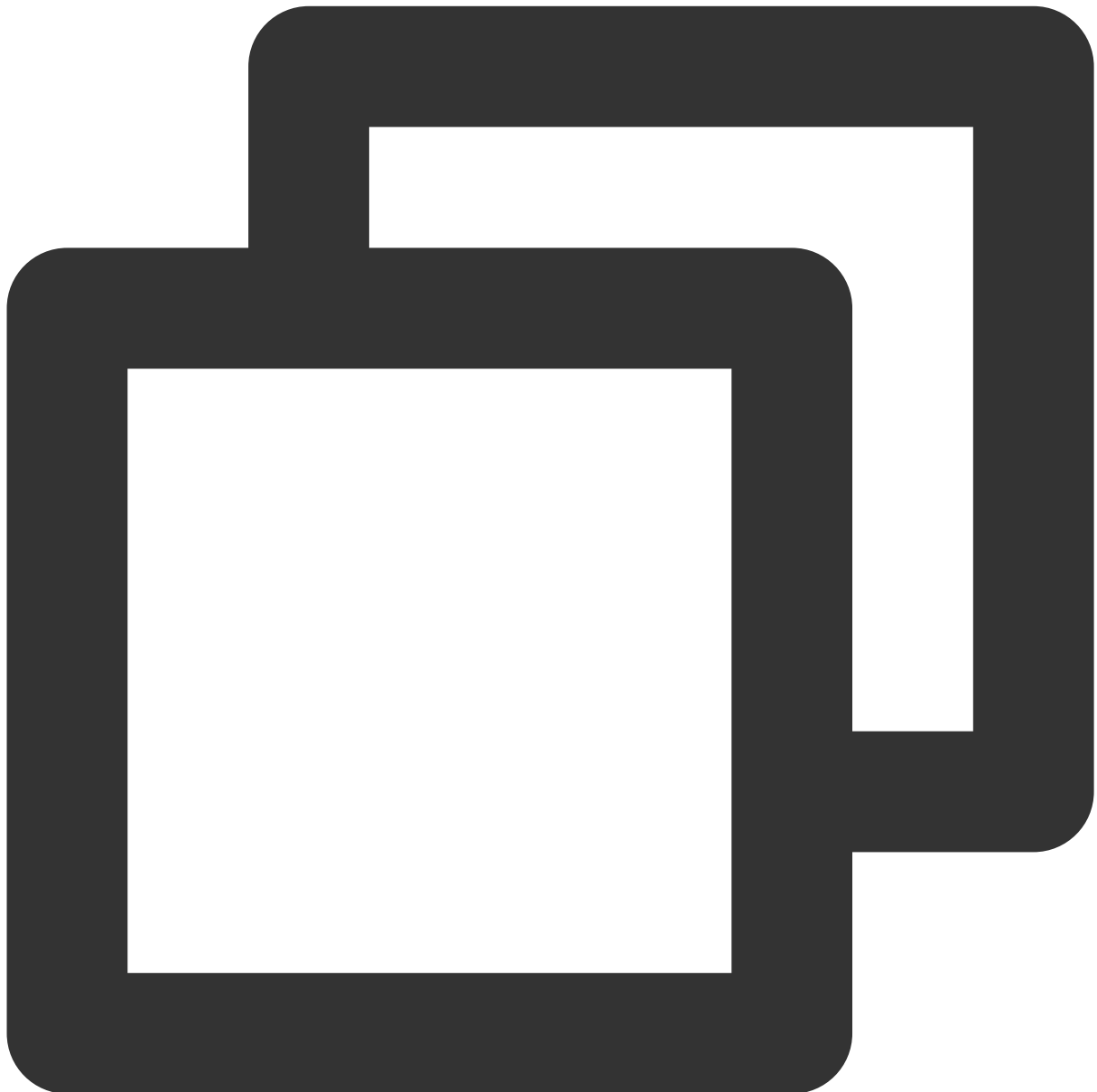
To grant a user the permission to manipulate TencentDB instances in a specific region, associate the following policy with the user. For example, the policy below allows the user to manipulate the TencentDB instances in Guangzhou.



```
{
  "version": "2.0",
  "statement": [
    {
      "action": "dcd:*",
      "resource": "qcs::dcd:ap-guangzhou::*",
      "effect": "allow"
    }
  ]
}
```

## Policy for granting user permission to manipulate TencentDB instances in multiple specific regions

To grant a user the permission to manipulate TencentDB instances in a specific region, associate the following policy with the user. For example, the policy below allows the user to manipulate the TencentDB instances in Guangzhou and Chengdu.

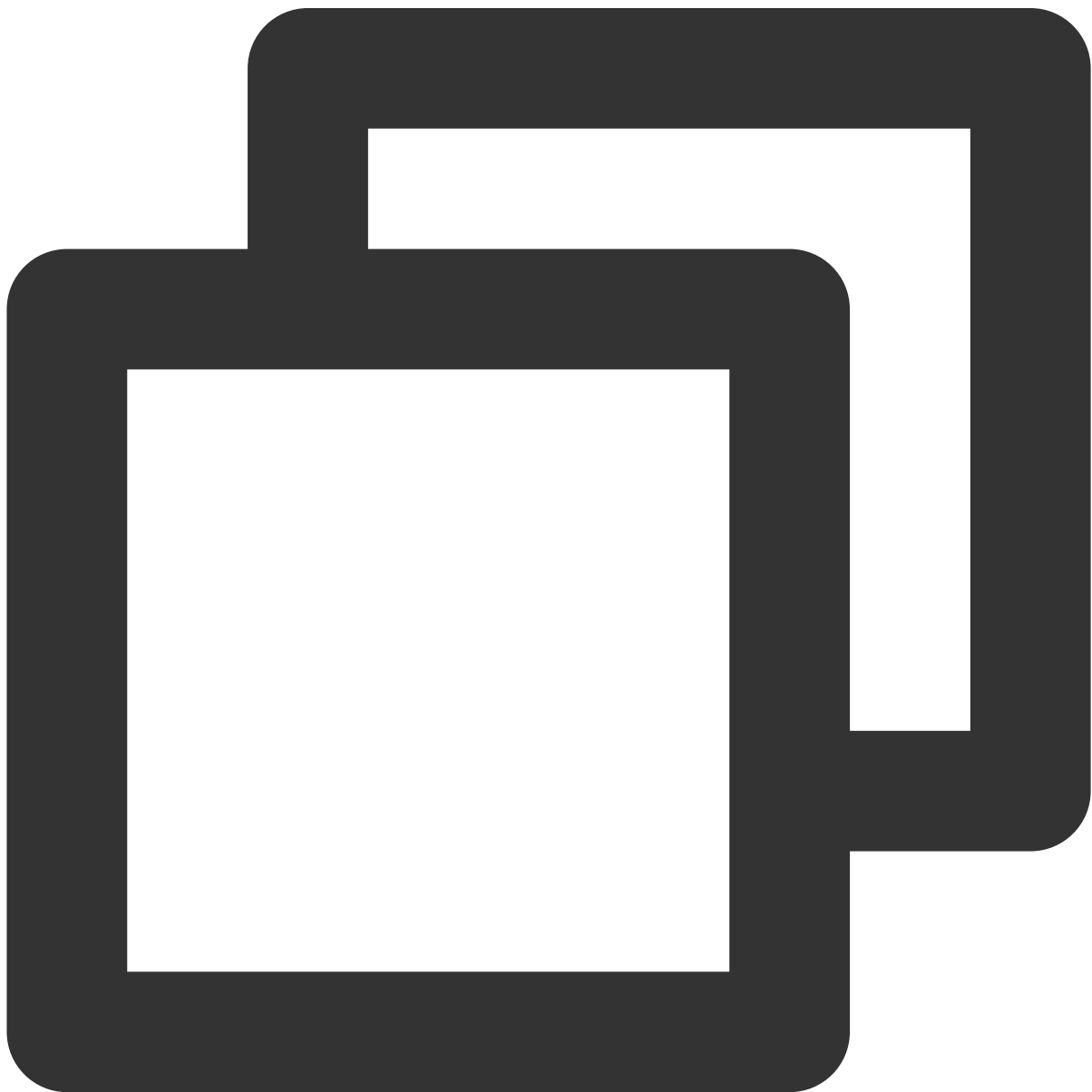


```
{  
  "version": "2.0",  
  "statement": [  
    {
```

```
    "action": "dcdb:*",
    "resource": "qcs::dcdb:ap-guangzhou::*", "qcs::dcdb:ap-chengdu::*",
    "effect": "allow"
  }
]
```

### Policy for granting user permission to manipulate one specific TencentDB instance

To grant a user the permission to manipulate a specific database, associate the following policy with the user. For example, the policy below allows the user to manipulate the TencentDB instance "dcdb-xxx" in Guangzhou.

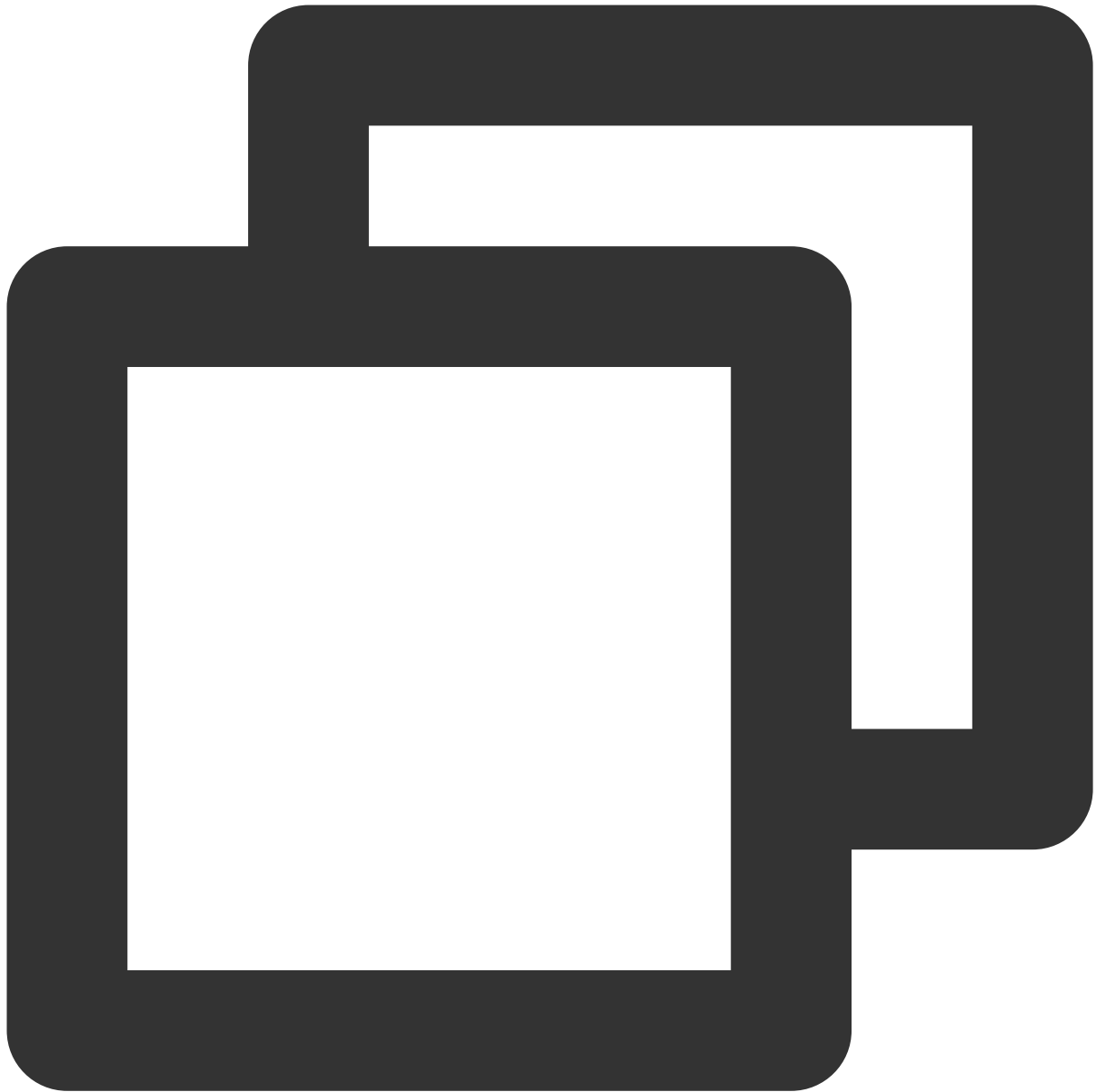




```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "dcdb:*"
      ],
      "resource": "qcs::dcdb:ap-guangzhou::instance/dcdb-xxx",
      "effect": "allow"
    }
  ]
}
```

### Policy for granting user permission to manipulate multiple TencentDB instances

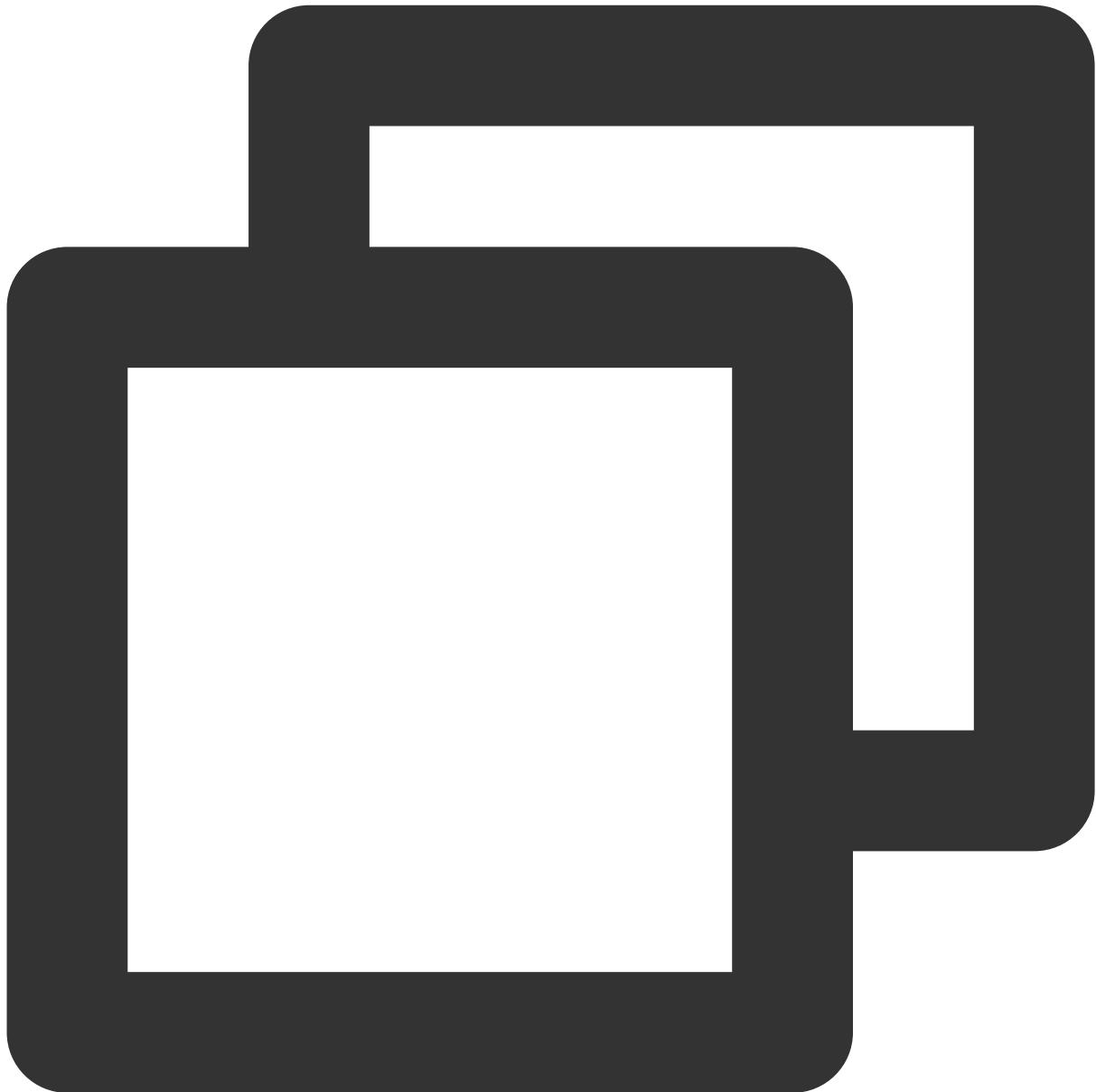
To grant a user the permission to manipulate TencentDB instances in batches, associate the following policy with the user. For example, the policy below allows the user to manipulate the TencentDB instances "dcdb-xxx" and "dcdb-yyy" in Guangzhou and "dcdb-zzz" in Beijing.



```
{
  "version": "2.0",
  "statement": [
    {
      "action": "dcdb:*",
      "resource": ["qcs::dcdb:ap-guangzhou::instance/dcdb-xxx", "qcs::dcdb:ap"],
      "effect": "allow"
    }
  ]
}
```

## Policy for granting user different permissions to manipulate multiple TencentDB instances

To grant a user the permission to manipulate TencentDB instances in batches, associate the following policy with the user. For example, the policy below allows the user to manipulate the TencentDB instances "dcdb-xxx" and "dcdb-yyy" in Guangzhou and "dcdb-zzz" in Beijing.

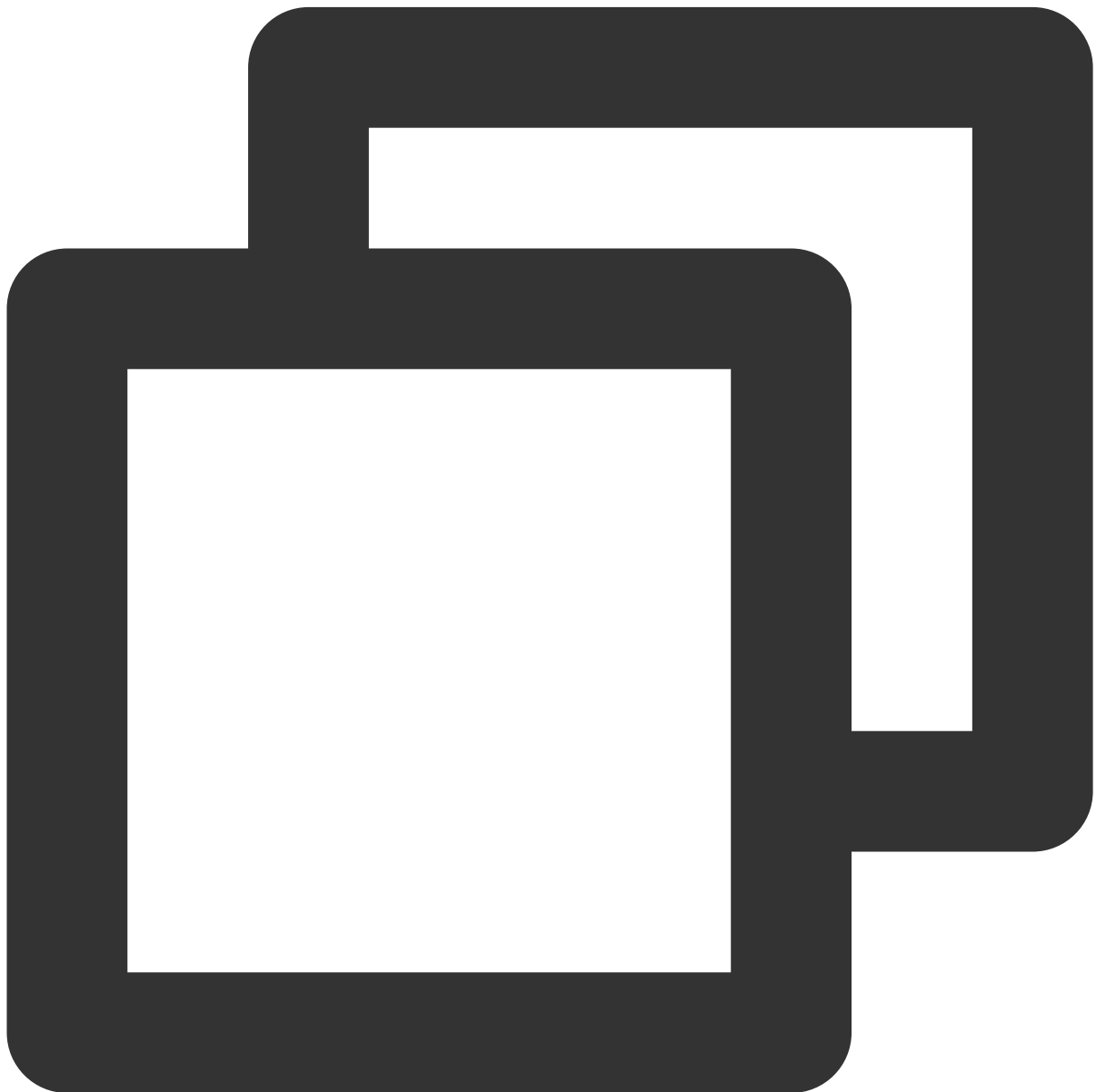


```
{
  "version": "2.0",
  "statement": [
    {
      "action": "dcdb:Describe*", "dcdb:Create*",
```

```
    "resource": ["qcs::dcdm:ap-guangzhou::instance/dcdm-xxx", "qcs::dcdm:ap-guangzhou::instance/dcdm-xxx"],  
    "effect": "allow"  
  }  
]  
}
```

## Denying user permission to create TencentDB accounts

To deny a user permission to create TencentDB accounts, configure `"effect": "deny"`.

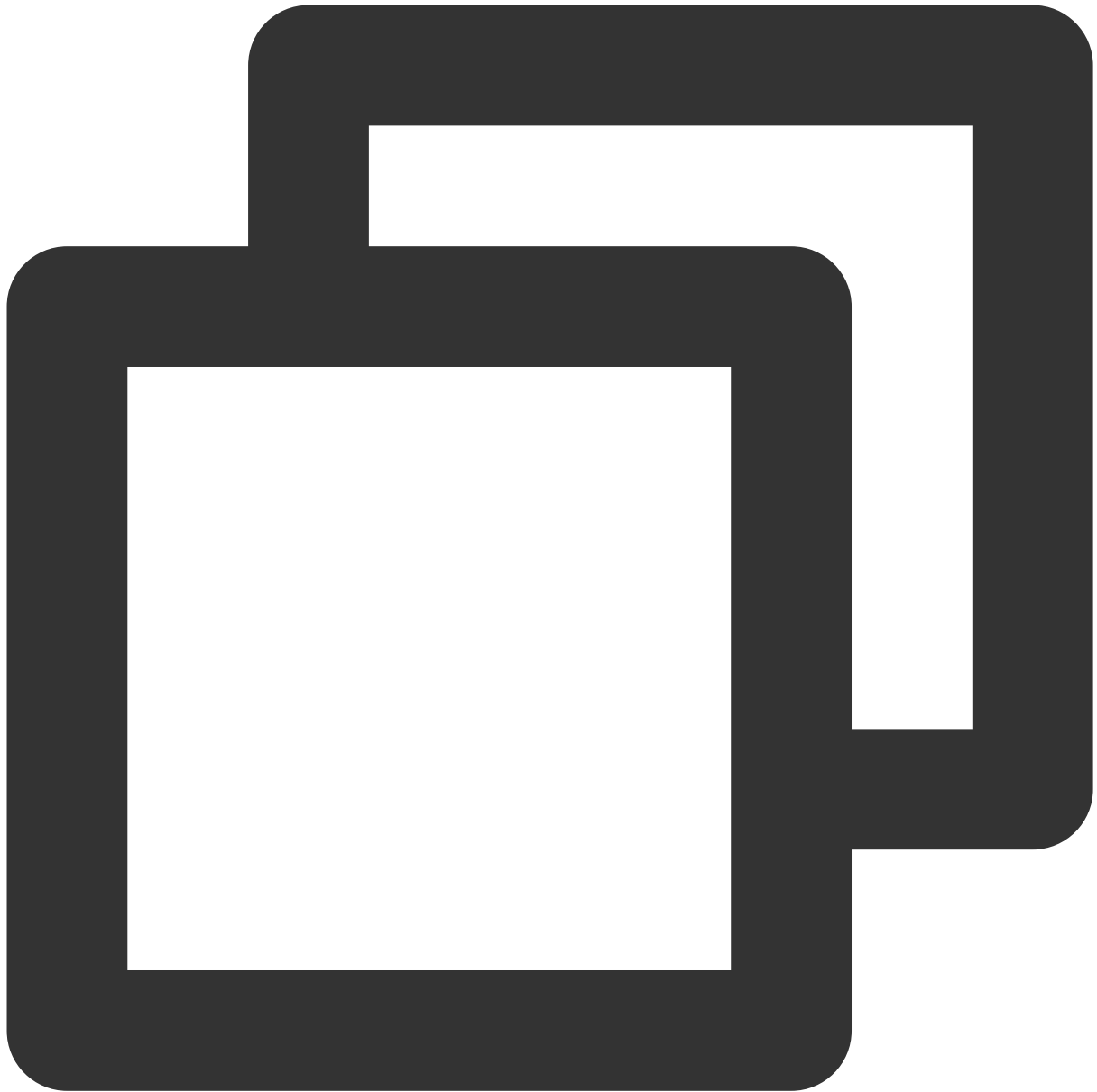


```
{
```

```
"version": "2.0",
"statement": [
  {
    "action": "dcdb:CreateAccount",
    "resource": "*",
    "effect": "deny"
  }
]
```

## Other custom policies

If preset policies cannot meet your requirements, you can create custom policies as shown below:



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

```
}
```

Replace "Action" with the operation to be allowed or denied.

Replace "Resource" with the resources that you want to authorize the user to manipulate.

Replace "Effect" with "Allow" or "Deny".

# CAM-enabled Operations

Last updated : 2024-01-06 17:33:30

## The following operations support resource-level permission control

Operation Name	API Name	Effective in Console After Configuration
Recovering a dedicated instance	ActiveDedicatedDBInstance	Yes
Binding security groups	AssociateSecurityGroups	Yes
Checking IP status	CheckIpStatus	Yes
Cloning an account	CloneAccount	Yes
Disabling public network access for an instance	CloseDBExtranetAccess	Yes
Copying account permission	CopyAccountPrivileges	Yes
Creating an account	CreateAccount	Yes
Creating an instance	CreateDCDBInstance	Yes
Deleting an account	DeleteAccount	Yes
Querying account permission	DescribeAccountPrivileges	Yes
Querying the account list	DescribeAccounts	Yes
Querying audit logs	DescribeAuditLogs	Yes
Querying audit rule details	DescribeAuditRuleDetail	Yes
Querying the audit rule list	DescribeAuditRules	Yes
Querying audit policies	DescribeAuditStrategies	Yes
Querying the price for batch instance renewal	DescribeBatchDCDBRenewalPrice	Yes
Querying instance objects	DescribeDatabaseObjects	Yes
Querying instance database names	DescribeDatabases	Yes
Querying column information of an instance table	DescribeDatabaseTable	Yes



Getting the log list	DescribeDBLogFiles	Yes
Querying monitoring information	DescribeDBMetrics	Yes
Viewing database parameters	DescribeDBParameters	Yes
Querying security group information of an instance	DescribeDBSecurityGroups	Yes
Getting slow log recording details	DescribeDBSlowLogAnalysis	Yes
Getting the slow log list	DescribeDBSlowLogs	Yes
Querying instance sync mode	DescribeDBSyncMode	Yes
Getting instance details	DescribeDCDBInstanceDetail	Yes
Viewing the instance list	DescribeDCDBInstances	Yes
Querying price	DescribeDCDBPrice	Yes
Querying the renewal price of an instance	DescribeDCDBRenewalPrice	Yes
Querying purchasable AZs	DescribeDCDBSaleInfo	Yes
Querying instance shards	DescribeDCDBShards	Yes
Querying the upgrade price of an instance	DescribeDCDBUpgradePrice	Yes
Querying dedicated cluster specification	DescribeFenceShardSpec	Yes
Querying flow status	DescribeFlow	Yes
Querying the latest DBA check result	DescribeLatestCloudDBAReport	Yes
Viewing backup log settings	DescribeLogFileRetentionPeriod	Yes
Querying order information	DescribeOrders	Yes
Querying projects	DescribeProjects	Yes
Querying security group information of a project	DescribeProjectSecurityGroups	Yes
Querying instance specification	DescribeShardSpec	Yes
Getting SQL logs	DescribeSqlLogs	Yes
Unbinding security groups from Tencent	DisassociateSecurityGroups	Yes

Cloud resources in batches		
Setting account permission	GrantAccountPrivileges	Yes
Initializing instances	InitDCDBInstances	Yes
Isolating a dedicated instance	IsolateDedicatedDBInstance	Yes
Modifying database account remarks	ModifyAccountDescription	Yes
Setting auto-renewal in batches	ModifyAutoRenewFlag	Yes
Renaming an instance	ModifyDBInstanceName	Yes
Modifying security groups bound to a TencentDB instance	ModifyDBInstanceSecurityGroups	Yes
Modifying instance project	ModifyDBInstancesProject	Yes
Modifying database parameters	ModifyDBParameters	Yes
Modifying instance sync mode	ModifyDBSyncMode	Yes
Modifying instance network	ModifyInstanceNetwork	Yes
Modifying instance VIP	ModifyInstanceVip	Yes
Modifying backup log settings	ModifyLogFileRetentionPeriod	Yes
Enabling public network access	OpenDBExtranetAccess	Yes
Renewing an instance	RenewDCDBInstance	Yes
Resetting account password	ResetAccountPassword	Yes
Enabling smart DBA	StartSmartDBA	Yes
Scaling an instance	UpgradeDCDBInstance	Yes
Upgrading a dedicated instance	UpgradeDedicatedDCDBInstance	Yes

# Security Group Configuration

Last updated : 2024-01-06 17:33:30

A security group is a stateful virtual firewall capable of filtering. As an important means for network security isolation provided by Tencent Cloud, it can be used to set network access controls for one or more TencentDB instances. Instances in VPC with the same network security isolation demands in one region can be put into the same security group, which is a logical group (not supported for instances in the classic network currently). TencentDB and CVM share the security group list and are matched with each other within the security group based on rules. Rules not supported by TencentDB will not take effect.

## Note:

TencentDB security groups provide network access control for VPCs, and support public network access for the instances with public network access enabled in Guangzhou, Chengdu, Shanghai, Beijing, and Nanjing regions.

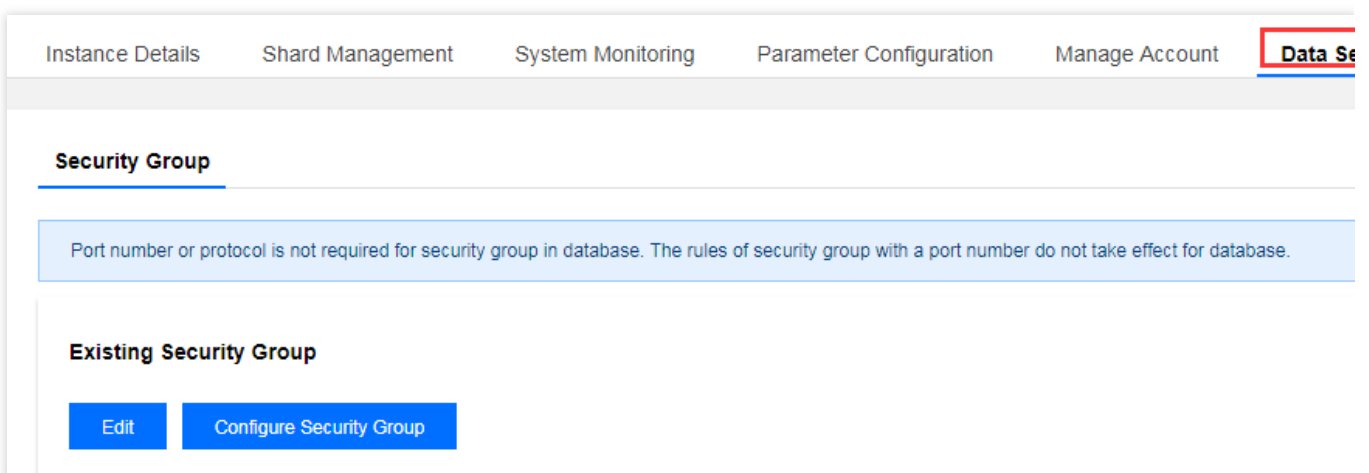
## TencentDB Security Group Management

Log in to the [TDSQL for MySQL console](#), click an instance ID in the instance list to enter the management page, and select **Data Security** > **Security Group** to manage security groups.

## Note:

TencentDB shares the security group rules of CVM. You can match or adjust the rule priority as needed on the TencentDB security group management page.

You cannot create or delete security group rules on the TencentDB security group management page. For details, see [Viewing a Security Group](#).



## Security Group Policy

Security group policies are divided into "allowing" and "rejecting" traffic. You can configure security group rules to allow or reject inbound traffic of instances deployed in VPC.

## Default Policy of a TencentDB Security Group

Currently, if you select VPC as the network type when purchasing a TencentDB instance, there is no need to associate a security group. In this case, the default policy is to "open all IPs and ports to internet".

## Security Group Templates

You can create a security group from scratch or from a template, and control the inbound and outbound packets of CVMs by configuring rules for the security group.

## Security Group Rules

Security group rules are used to control the inbound and outbound traffic of instances associated with the security group (filtered based on the rules from top to bottom). By default, a new security group rejects all traffic (All Drop). You can modify security group rules at any time, and the new rules take effect immediately.

Each security group rule contains the following items:

**Protocol and port:** As TencentDB only provides access over fixed ports, security group rules configured with other ports won't take effect for TencentDB. For example, if the TencentDB instance uses port 3306 for access, you can configure `TCP:3306` or `ALL` in the security group rule.

**Authorization type:** Access based on address ranges (CIDR/IP).

**Source (inbound rules) or target (outbound rules):** Choose one of the following options:

Specify a single IP in CIDR notation.

Specify a single IP in CIDR notation.

**Policy:** Allow or reject the access request.

## Security Group Priority

You can set security group priority in the TencentDB console, and the smaller the number, the higher the priority. If an instance is associated with multiple security groups, the priority is used to evaluate the security rules for the instance.

In addition, if the last policy in multiple security groups associated with an instance is **ALL Traffic Denied**, then the last policy **ALL Traffic Denied** of all security groups except the one with the lowest priority will not take effect.

## Security Group Restrictions

Security groups are applicable to TencentDB instances in [VPC](#).

The security group policy is only valid for the private IP. Enable the database public network access with CVM to ensure the best security for the business.

Each user can set up to 50 security groups under the same project in the same region.

A maximum of 100 inbound or outbound rules can be configured for a security group. As TencentDB doesn't have any active outbound traffic, outbound rules don't apply to it.

A TencentDB instance can be associated with multiple security groups, and a security group can be associated with multiple TencentDB instances. No limit is imposed on the number.

### Note:

We do not recommend associating too many instances with a security group, although no limit is imposed on the number of instances.

Feature	Quantity
Security group	50/region
Access policy	100 (inbound/outbound)
Number of security groups associated with an instance	No limit
Number of instances associated with a security group	No limit

## Creating/Managing/Deleting Security Group Rules

To create, manage, and delete security group rules, you can go to the [Security Group] page (<https://console.intl.cloud.tencent.com/cvm/securitygroup>). For details, see [Viewing a Security Group](#).

# Transparent Data Encryption (TDE)

Last updated : 2024-01-06 17:33:30

## Overview

TDSQL for MySQL comes with the transparent data encryption (TDE) feature. Transparent encryption means that the data encryption and decryption are transparent to users. TDE supports real-time I/O encryption and decryption of data files. It encrypts data before it is written to disk, and decrypts data when it is read into memory from disk, which meets the compliance requirements of static data encryption.

This document describes how to enable data encryption and encrypt/decrypt data in the console.

## Prerequisites

The TDE feature is currently supported only for Percona 5.7 in Hong Kong (China) and MySQL 8.0.24.

### Note:

To use the TDE feature, [submit a ticket](#) for application.

[KMS](#) must be activated in advance or as prompted when TDE is enabled.

KMS key permissions must be granted in advance or as prompted when TDE is enabled.

## Notes

After KMS is activated, KMS fees may be incurred as detailed in [Purchase Method](#).

TDE cannot be disabled once enabled.

If disaster recovery read-only instances are created, TDE cannot be enabled.

After TDE is enabled, disaster recovery read-only instances cannot be created.

After TDE is enabled, the database instances cannot be restored from a backup file. We recommend you restore them as instructed in [Rolling Back Database](#).

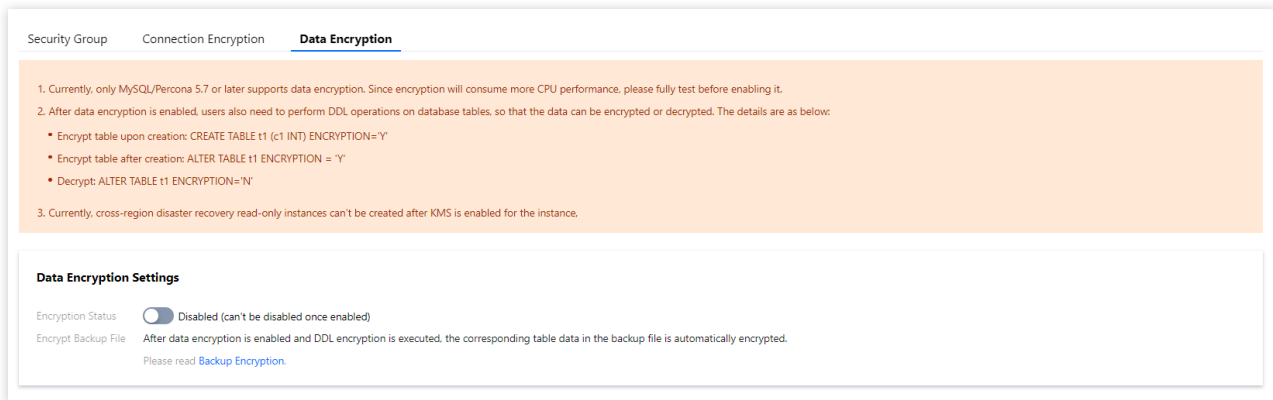
TDE enhances the security of static data while compromising the read-write performance of encrypted databases.

Therefore, use it based on your actual needs.

After TDE is enabled, more CPU resources will be consumed, and about 5% of the performance will be compromised.

## Directions

1. Log in to the [TDSQL for MySQL console](#) and click an instance ID or **Manage** in the **Operation** column to enter the instance management page.
2. On the instance management page, select **Data Security** > **Data Encryption** and toggle on **Encryption Status**.



3. In the pop-up dialog box, activate KMS, grant the KMS key permissions, select a key, and click **OK**.

## Settings

### Notes

1. The data encryption feature may incur the Key Management Service (KMS) service fee. For details, see [KMS Purchase Guide](#)
2. After the feature is enabled, DDL operation is required to encrypt or decrypt the tablespace data.
3. If you want to disable this feature, you need to decrypt all the tablespaces, and submit a ticket after disabling the KMS service.
4. You can't create disaster recovery read-only instance for the instance after data encryption is enabled.

KMS Service Disabled [Enable KMS](#) 

KMS Key Authorization Authorized

Select Key  Use auto-generated key

I have read and agreed to the supplementary statement about data encryption in [TencentDB Service Level Agreement](#)

I have read and agreed to [Disclaimer of Tencent Cloud for Information Security During Data Encryption](#)

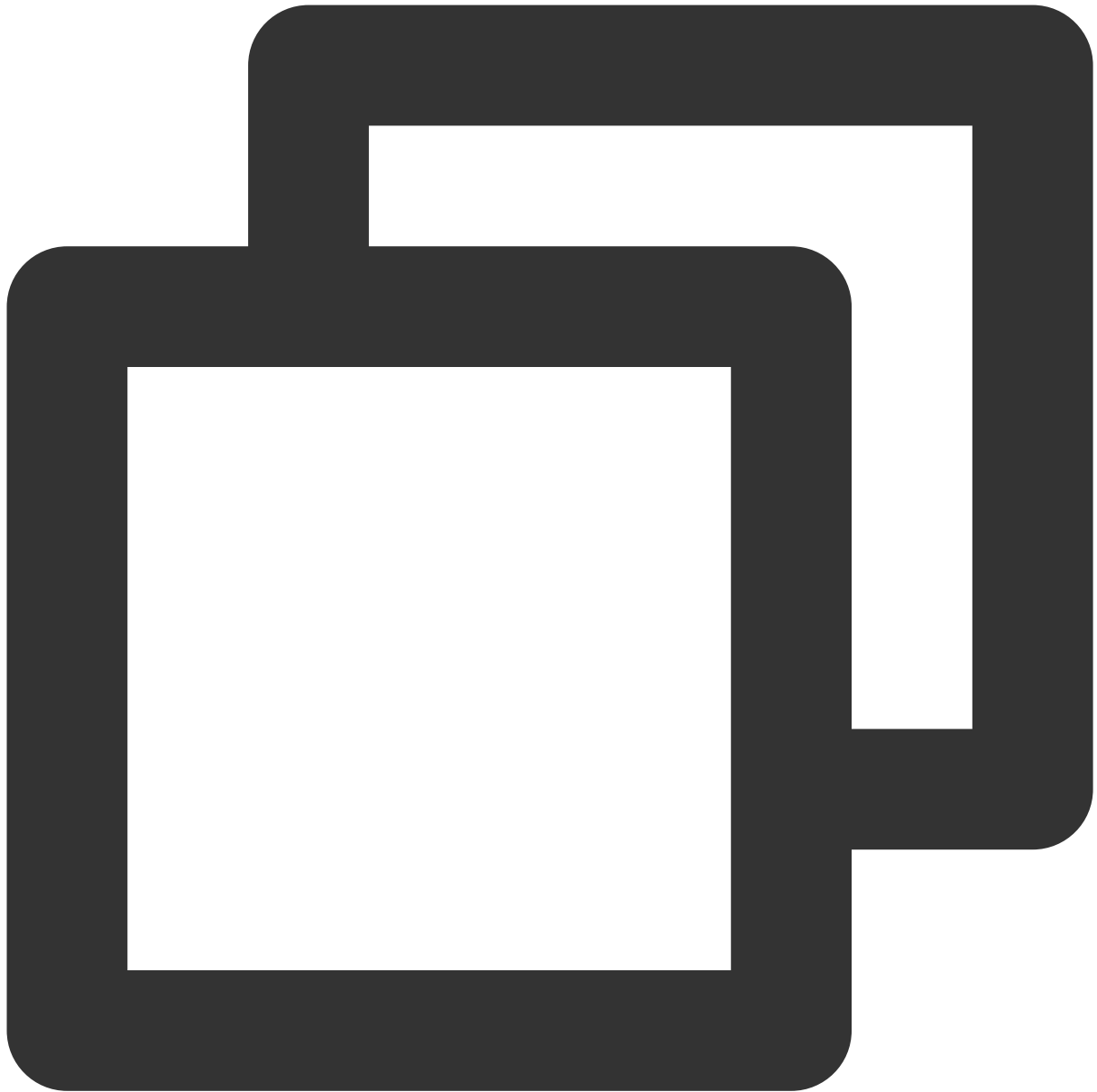
OK

Cancel

4. After data encryption is enabled, you must perform DDL operations on database tables to encrypt or decrypt data as instructed below:

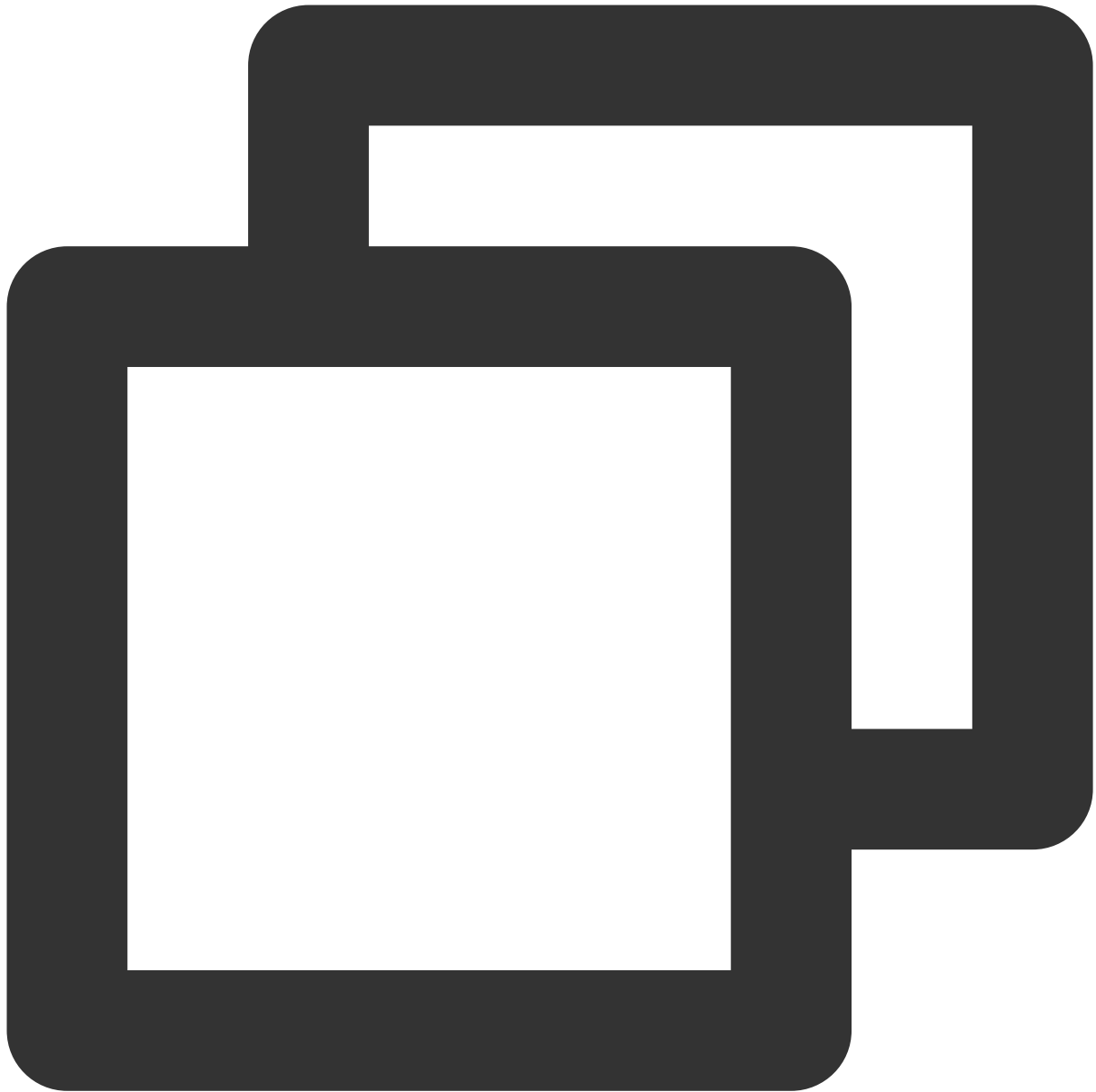
Encrypt a new table:





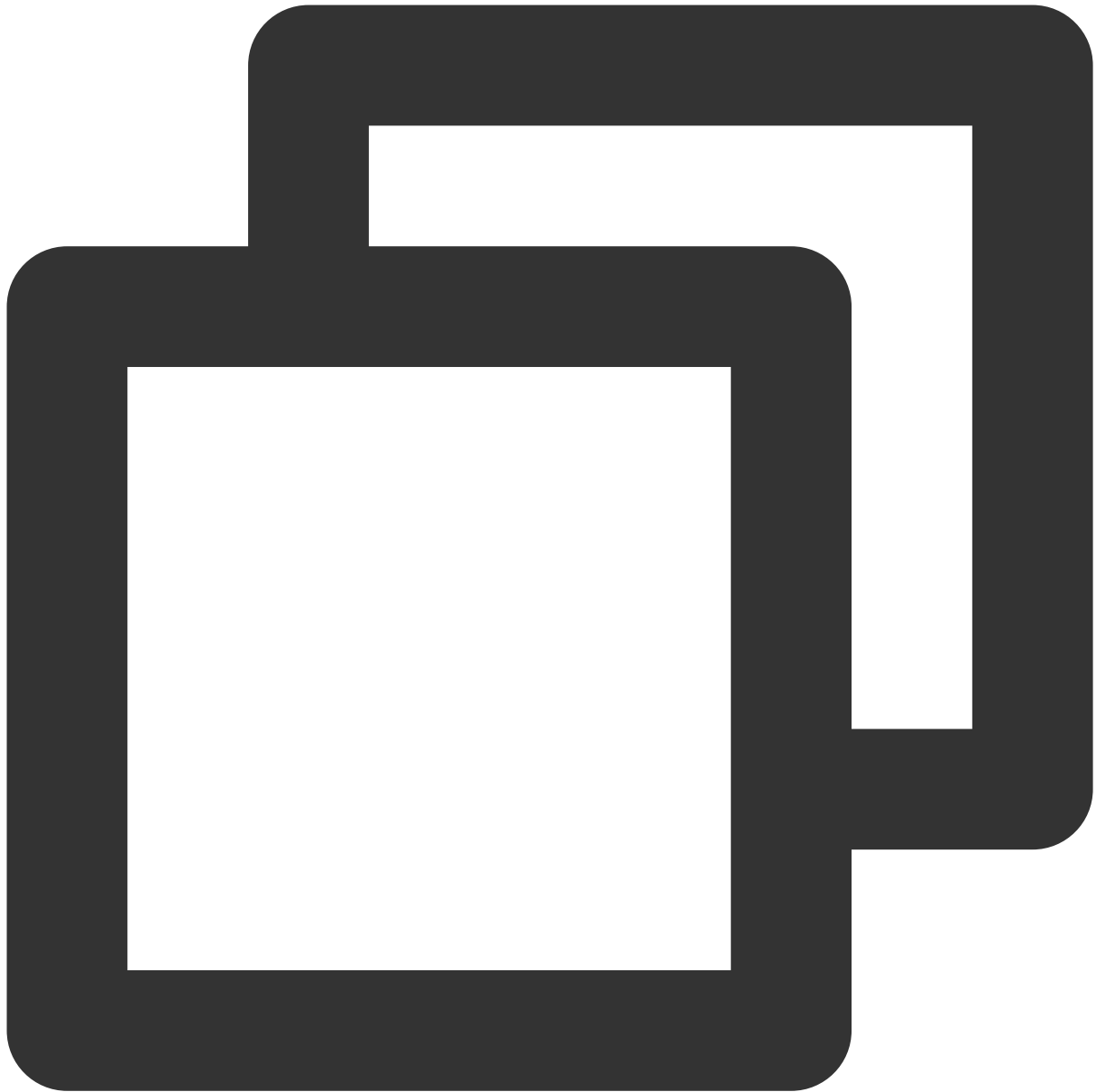
```
CREATE TABLE t1 (c1 INT) ENCRYPTION='Y'
```

Encrypt an existing table:



```
ALTER TABLE t1 ENCRYPTION='Y'
```

Decrypt a table:



```
ALTER TABLE t1 ENCRYPTION='N'
```

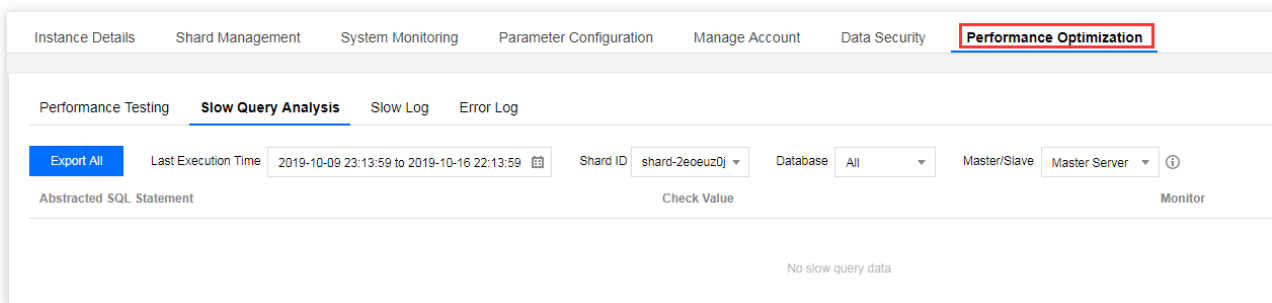
# Slow Query Analysis

Last updated : 2024-01-06 17:33:30

## Feature Description

A SQL statement query that takes more time than the specified value is referred to as a "slow query", and the corresponding statement is called a "slow query statement". The process where a database admin (DBA) analyzes slow query statements and finds out the reasons why slow queries occur is known as "slow query analysis".

Log in to the [TDSQL for MySQL console](#), click an instance ID in the instance list to enter the management page, and select the **Performance Optimization > Slow Query Analysis** tab to perform slow query analysis.



### Note:

Click



in the top-right corner to customize displayed fields.

Currently, slow query analysis can only be performed and viewed in each shard separately.

To download slow logs, you need to copy the download address, [log in to a \(Linux\) CVM instance in the same VPC as the database instance](#), and run the `wget` command for download over the private network.

## Main Parameters

### Main default settings

Slow query feature: Enabled by default.

Slow query threshold (`long_query_time`): One second by default, that is, only query statements executed for more than one second will be logged.

Analyzed data output delay: 1–5 minutes.

Logging duration: 30 days, depending on the backup and log settings.

## Analysis list fields

**Checksum** (`checksum`): A sequence of digits used to identify a slow query statement (64-bit by default).

**Abstracted SQL Statement** (`fingerprint`): A slow query statement with user data hidden.

**Database**: The database in which the slow query statement was executed.

**Account**: The account under which a slow query statement occurs.

**Last Execution Time** (`last_seen`): The time when the slow query statement was last executed within the specified time range.

**First Execution Time** (`first_seen`): The time when the slow query statement was first executed within the specified time range.

**Total** (`ts_cnt`): The number of executions of the slow query statement within the specified time range.

**Execution Proportion (%)**: The ratio of total executions of the slow query statement to the total executions of all slow query statements within the specified time range.

**Total Time** (`query_time_sum`): The total time consumed by the slow query statement within the specified time range.

**Total Time (%)**: The ratio in percentage of the total time consumed by the slow query statement to the total time consumed by all slow query statements within the specified time range.

**Average Time** (`query_time_avg`): The average time is calculated by dividing the total time consumed by the slow query statement by the total number of executions of the slow query statement.

**Min Time** (`query_time_min`): The minimum among all execution time of the slow query statement.

**Max Time** (`query_time_max`): The maximum among all execution time of the slow query statement.

**Total Lock Time** (`lock_time_sum`): The total lock time of the slow query statement.

**Total Lock Time Ratio**: The ratio in percentage of the total lock time of the slow query statement to the total lock time of all slow query statements.

**Average Lock Time** (`lock_time_avg`): The average time calculated by dividing the total lock time of the slow query statement by the total number of locks of the slow query statement.

**Min Lock Time** (`lock_time_min`): The minimum among all lock time of the slow query statement.

**Max Lock Time** (`lock_time_max`): The maximum among all lock time of the slow query statement.

**Sent Rows** (`Rows_sent_sum`): The total number of data rows sent by the slow query statement.

**Scanned Rows** (`Rows_examined_sum`): The total number of data rows scanned by the slow query statement.

**Host Address** (`Host`): The host from which this slow query comes.

**Monitoring**: Click to view the analysis details of the SQL statement.

**SQL Example**: Typical example of SQL statement.

# Backup and Rollback

## Backup Mode

Last updated : 2024-01-06 17:33:30

TDSQL for MySQL supports full backup and incremental backup.

## Backup Type

### Full backup

You can set the backup retention period for full backups, which is set to seven days by default.

### Incremental backup

Incremental backup is implemented based on binlogs, which are generated in real time. The binlogs occupy some disk space and are periodically uploaded to the TencentDB backup system.

## Custom Backup Time

1. Log in to the [TDSQL for MySQL console](#) and click an instance ID or **Manage** in the **Operation** column to enter the instance management page.
2. Click **Backup and Restoration** in the instance management page.
2. On the **Backup and Restoration > Backup and Log Settings** page, you can set the storage period and backup execution time.

Storage Time: Data and log backups can be retained for 1 to 365 days. Default value: 7 days.

Backup Execution Time: It can be set to any time period in hours.

### Note:

Log backup is enabled by default and cannot be disabled. Logs include error logs, slow logs, and transaction logs (binlogs).

<a href="#">← Instance Details</a>			<a href="#">Shard Management</a>	<a href="#">Monitoring and Alarms</a>	<a href="#">Parameter Settings</a>	<a href="#">Account Management</a>	<a href="#">Data Se</a>
<a href="#">Cold Backup List</a>	<a href="#">Rollback Instance</a>	<a href="#">Binlog List</a>	<b><u>Backup and Log Settings</u></b>				
Item	Storage Time		Backup Execution Time				
Backup and Log Storage Days	365 days		00:00~23:59				

# Downloading Backup File

Last updated : 2024-01-06 17:33:30

## Overview

You can download the cold backup data and binlogs in the TDSQL for MySQL console.

## Directions

1. Log in to the [TDSQL for MySQL console](#) and click an instance ID or **Manage** in the **Operation** column to enter the instance management page.
2. Select **Backup and Restoration > Cold Backup List** or **Binlog List**
3. Select the target shard ID and time. Then, click **Download** in the **Operation** column.
4. In the pop-up dialog box, click **Get Download Address** to get the download address in a VPC.
5. Log in to CVM (Linux system) under the VPC where the database resides as instructed in [Customizing Linux CVM Configurations](#) and run the `wget` command to download the file.

### Note:

Download from Public Network: Enable this option in **Download Settings** on the **Database Backup** page. Then, you can directly copy the download link to a browser for download.


Download from Private Network: Access the instance in the VPC and use the `wget` command for download: `wget -O <custom name.log> '<file download address>'` .

The address is valid for 15 minutes. Refresh the page to get a new one after expiration.



## Download

### Notes

1. To ensure data security, **Each address is valid for 15 minutes**. Upon expiration, click "Get Download Address" to get a new one.
2. Download over public network: Enable it on "Database Backup" > "Download Settings", and copy the address to the browser for download.
3. Download over private network: Run the `wget` command (format: `wget -O <custom filename.log> <download address>`) for download in a VPC.
4. View and download [Help Documentation](#) 

Get Download Address

Close

# Backup Encryption

Last updated : 2024-01-06 17:33:30

## Feature Overview

TDSQL for MySQL offers the transparent data encryption (TDE) feature that makes data encryption and decryption transparent to users. TDE supports data file encryption and decryption in real time. It allows data files to be encrypted before being written to disk and decrypted when read into memory from disk, meeting the static data encryption compliance requirements.

TDE is only supported for Percona 5.7 in Hong Kong region, but it will be available to more kernel versions in the future. You can access **Data Security > Data Encryption** on the instance management page in the [TDSQL console](#). After data encryption is enabled, the database instances can't be restored from a backup file. It is recommended to restore them as instructed in [Rolling Back Database](#).

### Note:

To use the data encryption feature, [submit a ticket](#) to apply for it.

## Notes

Currently, you can't create disaster recovery read-only instances for the instance with KMS enabled. For more information about KMS, see [Getting Started with KMS](#).

TDE can't be disabled once enabled.

TDE enhances the security of static data while compromising the read-write performance of encrypted databases.

Therefore, use it based on your actual needs.

After TDE is enabled, more CPU resources will be consumed, and about 5% of the performance will be compromised.

# Rolling Back Database

Last updated : 2024-01-06 17:33:30

## Rollback Description

TDSQL for MySQL can roll back data to any time point in the last 30 days based on the retention of backups and logs. With the database rollback feature, system loss can be minimized.

The rollback feature of TDSQL for MySQL doesn't affect a production instance and can directly roll back data to a new pay-as-you-go instance created by Tencent Cloud. This new rollback instance is a standard one, and you can configure it based on your needs.

## Limits

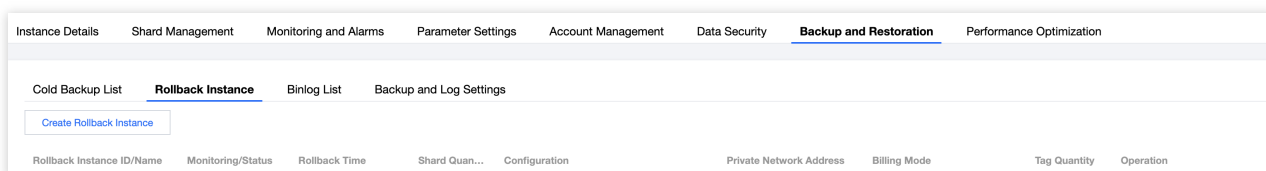
During the rollback and creation of a temp instance, some management features of the production instance in Tencent Cloud console will be unavailable, and these features will become available after the operation is completed.

The binlogs may be forcibly sharded during the rollback operation, and files smaller than 100 MB in size will be backed up separately.

The newly purchased instance after rollback will have the parameter information of the production instance in Tencent Cloud console (such as account, and database parameters, etc.). Therefore, you must pay attention to account management.

## Instance Rollback


1. Log in to [TDSQL for MySQL Console](#), click the instance ID, and enter the instance management page.
2. On the instance management page, select the **Backup and Restoration** > **Rollback Instance** tab and click **Create Rollback Instance**.



3. In the pop-up window, set the rollback time and click **OK**.

### Rollback Settings ✕

Create a pay-as-you-go instance (the rollback instance) based on the data of the selected instance (the data source instance) backed up at the specified point in time

Set Rollback Time \*  

1. The rollback time must be within the backup retention period (2022-05-19 16:09:21 - 2022-05-26 14:44:29).
2. The pay-as-you-go instance will be created based on backup data without affecting the data source instance.

4. On the instance purchase page, adjust configuration based on your needs, click **Buy Now**, and wait for instance rollback to be completed.

5. After the rollback is completed, you can view the generated rollback instance on the **Backup and Restoration > Rollback Instance** page or in the instance list.

# Data Migration

Last updated : 2024-01-06 17:33:30

You can migrate data to TDSQL for MySQL through [DTS](#) as instructed in [Migration from MySQL to TDSQL for MySQL](#).

# Database Audit

## Enabling Database Audit

Last updated : 2024-01-06 17:33:30

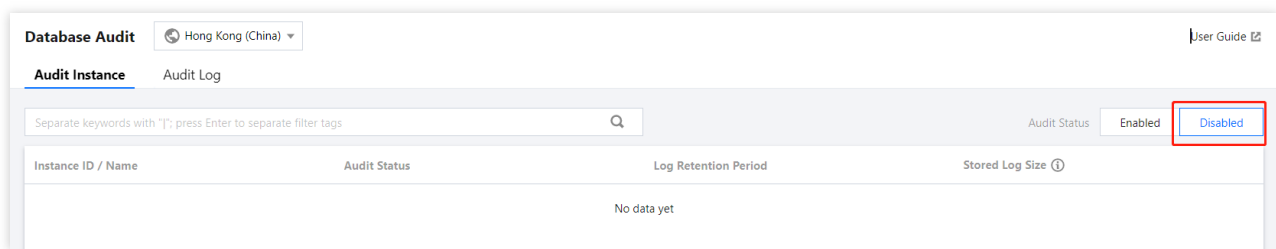
TDSQL for MySQL has database audit capability, which can record accesses to databases and executions of SQL statements to help you manage risks and improve the database security.

### Note:

The database audit feature is currently in the beta testing. To use this feature, [submit a ticket](#).

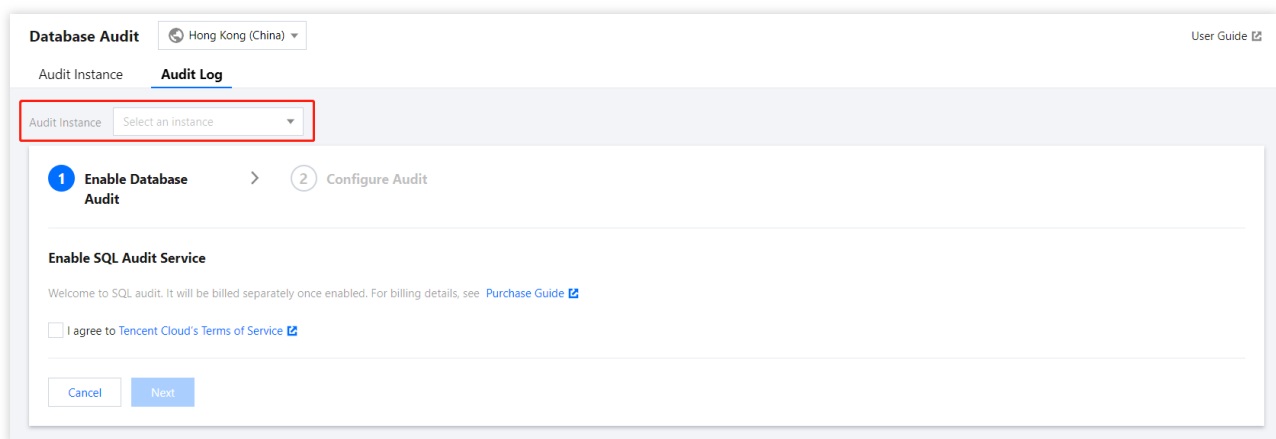
## Enabling SQL Audit

1. Log in to the [TDSQL 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 audit-disabled instances.



### Note:

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



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 **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 Logs](#)

# Viewing Audit Logs

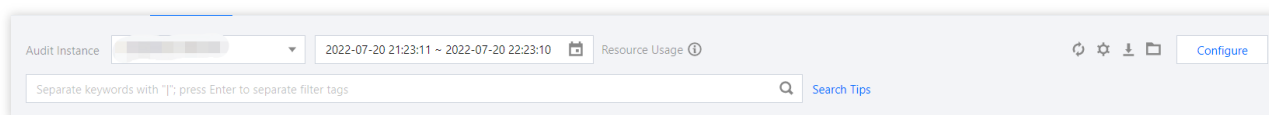
Last updated : 2024-01-06 17:33:30

## Viewing Logs

1, Log in to [TDSQL for MySQL Console](#), select **Database Audit** on the left sidebar, select a region at the top, and click the **Audit Log** tab.

2. In the audit instance section on the **Audit Log** tab, select a database instance with audit enabled to view its SQL audit logs. Or, on the **Audit Instance** tab, click an instance ID to enter the **Audit Log** tab and view audit logs.

### Tool list



Click the time box and select a time period to view the audit results in the selected time period.

#### Note:

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

You can search by key tag to view audit results. Common key tags include SQL command, client IP, database name, database account, execution time, affected rows, and returned rows.

When entering multiple key tags in the text box for search, you can separate them by pressing **Enter**.

You can filter IP addresses by using the wildcard ". For example, if you enter "client IP: 10.0.0.0", IP addresses that start with "10.0.0.0" will be searched.

### 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.

## SQL Audit Fields

You can click the following icon on the **Audit Log** tab of the TDSQL for MySQL console to obtain and view the complete SQL audit log.



Audit Instance [redacted] 2022-07-20 21:23:11 ~ 2022-07-20 22:23:10 Resource Usage [info]

Separate keywords with "|"; press Enter to separate filter tags [search icon] Search Tips

Time ↕	Client IP	Database Name	User Account	SQL Details	Returned Rows	Affecte... ↕	Executi... ↕
No data yet							

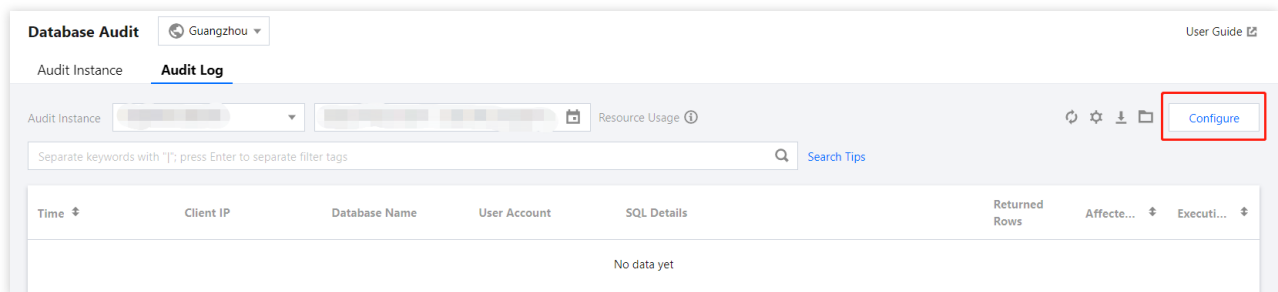
# Modifying Log Retention Period

Last updated : 2024-01-06 17:33:30

This document describes how to modify the log retention period after the database audit service is activated.

## Directions

1. Log in to [TDSQL for MySQL Console](#), select **Database Audit** on the left sidebar, select a region at the top, and click the **Audit Log** tab.
2. In the top-right corner of the **Audit Log** tab, click **Configure**.



3. In the pop-up window, modify the log retention period and click **Submit**.