TencentDB for MySQL
Operation Guide
Product Documentation
Copyright Notice

©2013-2019 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
  Operation Overview
  Use Limits
Instance Lifecycle
  Maintaining Instance
    Setting Instance Maintenance Period
    Specifying Project for Instance
  Modifying Instance
    Upgrading Database Engine
    Upgrade from High-Availability Edition to Finance Edition
    Adjusting Database Instance Specification
Expanding Instance
  Read-Only Instance
  RO Group of Read-only Instance
Terminating Instance
Account Management
  Creating Account
  Resetting Password
  Modifying Account Permission
  Modifying Host
  Deleting Account
Database Management
  Logging in to phpMyAdmin
  Creating Database and Table
  Dropping Database/Table
Parameter Template Management
  Setting Instance Parameters
  Managing Parameter Template
Backup and Rollback
  Backup Mode
  Viewing Backup Capacity
  Restoring Database from Backup File
    Restoring Database from Physical Backup
    Restoring Database from Physical Backup File
  Database Rollback
Data Import and Export
  Batch Operating Instance
Data Import
Offline Migration of Data
Network and Security
Access Management
  Overview
  Authorization Policy Syntax
  Authorizable Resource Types
  Console Examples
TencentDB Security Group
Network Switch
Monitoring and Alarm
  Monitoring Feature
  Alarming Feature
Tag
  Overview
  Editing Tags
Operation Logs
During the use of TencentDB for MySQL, you may encounter problems related to instance access, instance maintenance, database and table creation as well as data backup and rollback. This document describes common operations in TencentDB for MySQL instances and relevant products.

**Instance**

A TencentDB for MySQL instance can contain multiple user-created databases and can be accessed using the same tools and applications as those for a standalone database instance. Below are common operations in TencentDB for MySQL instances, databases, and tables.

**Common operations**

- Accessing MySQL Instance
- Maintaining an instance
  - Setting Instance Maintenance Period
  - Specifying Project for Instance
- Modifying an instance
  - Upgrading Database Engine
  - Adjusting Database Instance Specification
- Scaling an instance
  - Read-Only Instance
  - RO Group of Read-only Instance
  - Disaster Recovery Instance
- Terminating Instance

**Database management**

- Creating a database and table
- Manipulating instances in batches
- Dropping a database and table
Parameter Template

A parameter template is used to manage how the parameters of a database engine are configured. A database parameter set is just like a container of engine configuration values which can be applied to one or more database instances. Below are common operations currently supported by a TencentDB instance parameter template.

Common operations

- Creating a Parameter Template
- Copying a Parameter Template
- Modifying a Parameter Template
- Importing Parameters

Data

Common data operations in TencentDB for MySQL are as follows:

Backup and rollback

- Restoring Database from Physical Backup
- Restoring Database from Physical Backup File
- Database Rollback

Data import and export

- Data Import
- Migrating data offline

Security Group

A TencentDB 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 databases.
Use Limits

Limits on Data Volume

Given the limited resources, TencentDB for MySQL imposes certain limits on data volume of all types of MySQL instances for the purpose of performance issue isolation. This document describes from a technical perspective what impact a single instance or table with a high data volume will have on MySQL:

**Instance with a high data volume:** the default storage engine for TencentDB is InnoDB. If the cache buffer can cache all data and index pages in the MySQL instance, the instance can support a large number of concurrent access requests. If the instance contains too much data, the cache and buffer will swap data in/out frequently; in this case, the performance bottleneck of MySQL will soon spread to IO, which will reduce the throughput. For example, a TencentDB instance designed to sustain up to 8,000 access requests per second can merely support 700 ones per second if the data volume is twice the size of the cache and buffer.

**Table with a high data volume:** if a table contains too much data, the cost for MySQL to manage table resources (data, indices, etc.) will change, which will affect the table processing efficiency. For example, if the size of a transaction table (InnoDB) exceeds 5 GB, the latency in update operations will soar, increasing the response time for transactions. In this case, the problem can only be solved through sharding and migration.

If the number of tables in a single instance exceeds 1 million, table backup, monitoring, and upgrade may fail, and database-level monitoring may be affected. Please control this value appropriately and make sure that it is below 1 million.

Limits on Number of Connections

The maximum number of connections to a MySQL instance is specified with the MySQL system variable `max_connections`. When the actual number exceeds `max_connections`, no more connections can be established.

The default number of connections to TencentDB can be viewed on the parameter settings page in the console, which can be adjusted if necessary. However, more connections mean that more system resources will be consumed; if the number of connections goes beyond what the actual system load capacity permits, the system service quality will be definitely undermined.

For more information on `max_connections`, please see MySQL's official documentation.
Limits on MySQL Client Version

It is recommended to use the MySQL client and library that come with CVM to connect to TencentDB instances.

Notes on slow queries

- For Linux CVM instances, you can use TencentDB's export tool to get slow query logs. For more information, please see Downloading Backup Files and Logs.
- For Windows CVM instances, slow query logs cannot be obtained directly at present. If you need them, please submit a ticket for assistance.

Notes on TencentDB binlog retention duration

TencentDB for MySQL binlogs can be retained for 7 (default value) to 732 days (customizable in automatic backup settings). The number of days set for log backup retention must be smaller than that for data backup retention.

If binlogs are retained for a prolonged period of time or increase too fast, more space will be needed for backup. If the space exceeds the free tier of backup capacity, fees will be incurred.

Notes on character set

Just as MySQL, the default character set in TencentDB is LATIN1 (ISO-8859-1).

Even though TencentDB supports changing the default character set, you are recommended to explicitly specify the table encoding format when creating it and specify the connection encoding during connection establishment. In this way, your application will be more portable.

For more information on the resources of MySQL character set, please see MySQL's official documentation.

The steps to change the TencentDB character set are as follows:

1. Run the following statements to change the default character set encoding for TencentDB instances:

   ```
   SET @@global.character_set_client = utf8;
   SET @@global.character_set_results = utf8;
   SET @@global.character_set_connection = utf8;
   SET @@global.character_set_server = utf8;
   ```

   After the statements are executed, `@@global.character_set_server` will be automatically synced to a local file for persistence in approximately 10 minutes, while the other 3 variables will not. The configured value will stay unchanged even after migration or restart.

2. Run the following statements to change the character set encoding for the current connection:

   ```
   SET @@session.character_set_client = utf8;
   SET @@session.character_set_results = utf8;
   SET @@session.character_set_connection = utf8;
   ```
3. For PHP programs, you can configure the character set encoding for the current connection by using the following function:

```php
bool mysqli::set_charset(string charset);
```

Or

```php
bool mysqli_set_charset(mysqli link, string charset);
```

4. For Java programs, you can configure the character set encoding for the current connection as shown below:

```java
jdbc:mysql://localhost:3306/dbname?useUnicode=true&characterEncoding=UTF-8
```

**Limits on operations**

1. Do not modify the information and permissions of the existing accounts for a MySQL instance; otherwise, some cluster services may become unavailable.
2. InnoDB is recommended for creating databases and tables, so that the instances can better support a large number of concurrent access requests.
3. Do not modify or terminate the master-slave relationship; otherwise, hot backup may fail.

**Limits on table name**

Please note that Chinese table names are not supported because they may result in failures of processes such as rollback and upgrade.

**Notes**

**Database account permission**

TencentDB for MySQL no longer provides the super user permission. To modify parameters that require this permission, you can use the parameter configuration feature in the console or submit a ticket for assistance.

**Network options**

You are recommended to use a VPC. In the VPC, you can freely define IP range segmentation, IP addresses, and routing policies. Compared with the classic network, VPC is more suitable for scenarios where custom network configurations are required. For the comparison of VPC and classic network, please see Managing Network.
Operation Scenarios

Maintenance time is a very important concept for TencentDB for MySQL. To ensure the stability of your TencentDB for MySQL instance, the backend system performs maintenance operations on the instance during the maintenance window from time to time. It is highly recommended that you set an acceptable maintenance time for your business instance, usually during off-peak hours, so as to minimize the potential impact on your business.

In addition, it is recommended that operations involving data migration be performed during the maintenance time too, such as instance specification adjustment, instance version upgrade, and instance kernel upgrade. Currently, the maintenance period concept is supported by master, read-only, and disaster recovery instances.

Take the database instance specification upgrade as an example. As this operation involves data migration, after the upgrade is completed, a momentary disconnection from the database may occur. When the upgrade is initiated, the switch time can be selected as during maintenance window, so that the instance specification switch will be enabled during the next maintenance window after the instance upgrade is completed. Please note that when you do so, the switch will not occur immediately after the database specification upgrade is completed; instead, the sync will continue till the instance goes into the next maintenance window when the switch will be performed. In this way, the overall time it takes to upgrade the instance may be extended.

- Before maintenance is carried out for TencentDB for MySQL, notifications will be sent to the contacts configured in your Tencent Cloud account through SMS and email.
- Instance switch is accompanied by a momentary disconnection from the database. Please make sure that your business has a reconnection mechanism.

Directions

Setting maintenance time
1. Log in to the TencentDB for MySQL Console. In the instance list, click the instance name or Manage in the "Operation" column to enter the instance details page.

2. Select Maintenance Info and click Modify.

   Maintenance Info Modify
   Maintenance Period: Mon. Tue. Wed. Thu. Fri. Sat. Sun
   Maintenance Time: 03:00-04:00

3. In the pop-up dialog box, select the Maintenance Period and Maintenance Time as needed and click OK.

   Modify maintenance period and time
   Maintenance Period: ✓ Mon ✓ Tue ✓ Wed ✓ Thu ✓ Fri ✓ Sat ✓ Sun
   Maintenance Time: Start Time: 03:00
   Duration: 1 hour

   OK Cancel

Immediate switch

If a task is configured to be switched during the maintenance window, but you need to switch it urgently under special circumstances, you can click Switch Now in the "Operation" column.

- Immediate switch is applicable to operations involving data migration such as instance specification adjustment, instance version upgrade, and instance kernel upgrade.
For version upgrade, if an instance is associated with multiple instances, the switch will be performed in the order from disaster recovery instance to read-only instance to master instance.
Specifying Project for Instance

Last updated: 2020-03-17 17:57:29

TencentDB for MySQL allows you to assign instances to different projects for easier management. To do so, log in to the TencentDB for MySQL Console, select the corresponding instance, and click **More > Assign to Project**.

- Read-only instances and disaster recovery instances are associated instances of the master instance and should be in the same project as the master instance.
- Assigning and moving database instances across projects 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 is **Default Project**.
- Assigned instances can be reassigned to other projects through the **Assign to Project** feature.
Modifying Instance
Upgrading Database Engine


Operation Scenario

This document describes how to upgrade the TencentDB for MySQL engine in the console. TencentDB for MySQL supports database engine upgrade:

- From MySQL 5.5 to MySQL 5.6
- From MySQL 5.6 to MySQL 5.7

Upgrade Rules

- Upgrading across major releases is not supported. For example, to upgrade a TencentDB for MySQL 5.5 instance to MySQL 5.7 or higher, you have to upgrade it to MySQL 5.6 first.
- The `create table ... as select ...` syntax is not supported.
- Master-slave sync in TencentDB for MySQL 5.6/5.7 is implemented based on GTID. Only InnoDB is supported by default.
- MyISAM tables will be converted to InnoDB tables during the process of upgrading from MySQL 5.5 to 5.6. **You are recommended to complete the conversion first before upgrading.**
- During upgrade, TencentDB for MySQL will clear the `slow_log` table. Please save the logs before upgrading if necessary.
- **If an instance to be upgraded is associated with other instances (e.g., master instance and read-only instances), these instances will be upgraded together to ensure data consistency.**
- TencentDB for MySQL upgrade involves data migration and generally takes a relatively long time. Please wait patiently. Your business will not be affected during the upgrade process and can be accessed normally.
- Instance switchover may be needed after an upgrade is completed (i.e., the MySQL instance may be disconnected for seconds). It is recommended that applications be configured with auto reconnection feature and that instance switchover be conducted during the instance maintenance period. For more information on maintenance period, see Setting Instance Maintenance Period.
- If the number of tables in a single instance exceeds one million, upgrade may fail, and database monitoring may be affected. Please control this value appropriately and make sure that it is below 1 million.
Directions

1. Log in to the TencentDB for MySQL Console.

2. Select the instance to be upgraded in the instance list and select More > Upgrade Version in the "Operation" column (MySQL 5.7 cannot be upgraded to a higher version).

3. In the pop-up window, select the database version to be upgraded to and click Upgrade. As database upgrading involves data migration, after the upgrade is completed, a very short disconnection from the MySQL database lasting for just seconds may occur. When the upgrade is initiated, the Switch Time can be selected as During maintenance window, so that the switch will be initiated within the next Maintenance Time after the instance upgrade is completed.

   If you do so, the switch will not occur immediately after the database specification upgrade is completed; instead, the sync will continue till the instance goes into the next maintenance period when the switch will be performed. In this way, the overall time it takes to upgrade the instance may be extended.
### Database Version Upgrade

Database version upgrade instructions:
- The master instance and the associated read-only and disaster recovery instance are upgraded to the target database version at the same time. The version can be upgraded via any associated instance.
- The upgrade process has no impact on existing business.
- There is a second-level interruption during the upgrade switch process. It is recommended to switch in maintenance time or off-peak period to reduce the impact on the service.

<table>
<thead>
<tr>
<th>Instance ID</th>
<th>Instance Name</th>
<th>Instance Type</th>
<th>Switch Time</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Read-only Instance</td>
<td>During maintenance window</td>
<td>MySQL5.7</td>
</tr>
</tbody>
</table>

**Switch Time**
- During maintenance window
- After upgrade completed
- Switch Time Description
  - Maintenance Time: 03:00-04:00 (Modify maintenance time on the instance details page)

**Version**
- MySQL5.5
- MySQL5.6 (Current Version)
- MySQL5.7

Upgrade related instances at the same time.  

<table>
<thead>
<tr>
<th>Instance ID/Name</th>
<th>Instance Type</th>
<th>Maintenance Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Master Instance</td>
<td>03:00-04:00</td>
</tr>
<tr>
<td></td>
<td>Read-only Instance</td>
<td>03:00-04:00</td>
</tr>
</tbody>
</table>

- I have read and agreed to Database Version Upgrade Rule

[Upgrade] [Cancel]
Upgrade from High-Availability Edition to Finance Edition

Operation Scenarios

This document describes how to upgrade an instance from the High-Availability Edition to the Finance Edition.

- Only High-Availability Edition instances on MySQL 5.6 and 5.7 can be upgraded to the Finance Edition.
- The upgrade will not interrupt the instance service.

Directions

1. Log in to the TencentDB for MySQL Console. In the instance list, click an instance name or Manage in the "Operation" column to enter the details page.
2. In the "Configuration Info" section on the details page, click Upgrade to Finance Edition.

| Configuration Info |
|--------------------|-----------------|
| Architecture       | High-Availability Edition |
| Configuration      | 1 core 1000MB MEM, 25GE storage, Adjust Configurations |
| Version            | MySQL 5.5 Upgrade |
| Used/Total         | 18MB/25GB |
| Billing Mode       | Pay as you go |
| Creation Time      | 2020-01-02 15:09:11 |
| Expiration Time    | -- |
3. On the pop-up page, confirm that everything is correct and click **Upgrade**.

4. Confirm the price and return to the instance list where the instance status is "Changing configuration". After the status becomes "Running", the instance can be used normally in the console.
Adjusting Database Instance Specification

Last updated: 2020-03-17 17:58:05

Operation Scenario

TencentDB for MySQL supports quick adjustment of instance specification and allows flexible scaling operations. You can elastically adjust the specifications of MySQL instances according to your actual business conditions (at the initial stage, at the rapid development stage, during peak hours, or during off-peak hours), so as to better meet your needs such as full utilization of resources and real-time cost optimization.

Configuration Adjustment Rules

- You can adjust the configuration of a TencentDB for MySQL instance and its associated instances only when they are in normal status (running) and are not executing any tasks.
- You cannot cancel a configuration adjustment operation in progress.
- The name, access IP, and access port of an instance will remain the same after configuration adjustment.
- Data migration may be involved in configuration adjustment. During data migration, the TencentDB for MySQL instance can be accessed normally and the business will not be affected.
- Instance switchover may be needed after configuration adjustment is completed (i.e., the MySQL instance may be disconnected for seconds). It is recommended that applications be configured with auto reconnection feature and that instance switchover be conducted during the instance maintenance period. For more information, see Setting Instance Maintenance Period.
- During configuration adjustment, you should try to avoid such operations as modifying MySQL's global parameters and user password.

Directions

Adjusting the Instance Configuration in the Console

1. Log in to the TencentDB for MySQL Console.
2. Select the instance to be adjusted in the instance list and select More > Adjust Configuration in the "Action" column.
3. In the pop-up dialog box, select the desired configuration and click **Submit**.
   - Pay-as-you-go instance:
     - [Image]

**Adjusting the Instance Configuration through the API**

You can upgrade the instance configuration using the UpgradeDBInstance API. For more information, see [Upgrading a TencentDB Instance](#).

Degrading the instance configuration through API is unavailable for the time being. You can do so in the console if needed.
Operation Scenarios

TencentDB for MySQL now allows you to create one or more read-only instances, which are suitable for read/write separation and one-master-multiple-slave application scenarios and capable of greatly enhancing the read load capacity of your database.

Unified read/write separation addresses (i.e., read and write requests are separated automatically) are not supported currently. Read-only instances need to be accessed with separate IPs and ports.

Basic concepts

- **RO group**: it consists of one or more load balancing-enabled read-only instances. If there are multiple read-only instances in one RO group, read request volume can be evenly distributed among the instances. RO groups provide IPs and ports for access to databases.
- **Read-only instance**: a single-node (with no slave) instance that supports read requests. A read-only instance cannot exist independently; instead, it must be in an RO group.

Basic architecture

The MySQL master/slave binlog sync feature is adopted for read-only instances, which can sync the changes in the master instance (source database) to all read-only instances. Given the single-node architecture (without a slave) of read-only instances, repeated attempts to restore a failing read-only instance will be made. Therefore, you are recommended to choose an RO group over a read-only for...
higher availability.

Feature Limits

- Read-only instances can be purchased only for **high-IO GTID-enabled master instances on MySQL 5.6 or above with the InnoDB engine at a specification of 1 GB memory and 50 GB disk capacity or above**. If your master instance is below this specification, please upgrade it first.
- The minimum specification of a read-only instance is 1 GB memory and 50 GB disk capacity and must be at least 1.1 times the storage capacity used by the master instance.
- A master instance can create up to 5 read-only instances.
- Backup and rollback features are not supported.
- Data cannot be migrated to a read-only instance.
- Database creation and dropping are not supported and neither is phpMyAdmin (PMA).
- Operations including account creation, deletion, authorization and account name/password modification are not supported.

Notes
• There is no need to maintain account and database for read-only instances, which will be synced with those of the master instance.

• If the MySQL version is 5.6 but GTID is not enabled, you need to enable GTID in the console first before creating a read-only instance. The operation takes a long time, and the instance will be disconnected for several seconds. You are recommended to do so during off-hours and add a reconnection mechanism in the programs that access the database.

• Read-only instances only support the InnoDB engine.

• Data inconsistency between multiple read-only instances may occur due to the delays in data sync. You can check the sync between master instance and read-only instance in the console.

• The specification of a read-only instance can be different from that of the master instance, which makes it easier for you to upgrade the instance according to the load. You are recommended to keep the same specifications of read-only instances in the same RO group.

Directions

1. Log in to the TencentDB for MySQL Console.
2. In the instance list, select the instance for which to create a read-only instance and click Manage in the "Operation" column.
3. On the Instance Details tab, click Add Read-Only Instance in the instance architecture to enter the read-only instance management page.
4. On the Read-Only instance tab, click Create.
5. Select the desired read-only instance configuration on the purchase page. After confirming that everything is correct, click Buy Now.
TencentDB MySQL Read-only Instance

### Master Instance Info
- **Instance Name**: [Name]
- **Network**: High-Availability Edition
- **Architecture**: High-Availability Edition
- **Project**: [Project]
- **Availability Zone**: Shanghai Zone 4
- **Version**: MySQL 5.6
- **Instance ID**: [ID]
- **Region**: East China (Shanghai)
- **Instance specifications**: 4core8000MB MEM.500GB storage,

### Specify RO Group
- **Assigned by system**: Yes
- **Learn about RO Group**: [Link]
  
  System automatically assigns RO groups which are not enabled latency elimination. Please retain at least one instance.

### Region
- **Region**: East China (Shanghai)

### Version
- **Version**: MySQL 5.6

### Architecture
- **Architecture**: Single-node high IO edition
  
  Although the single-node architecture is cost-effective, there is a single point of failure for a single read-only instance. It is strongly recommended to purchase at least two read-only instances in the service RO group that requires availability.

### Availability Zone
- **Availability Zone**: Shanghai Zone 4

### Instance specifications
- **Instance specifications**: [Specifications]

### Fees
- **Configuration cost**: [Price]
  
  **Traffic Fee**: 0.00 USD

[Buy Now]
RO Group of Read-only Instance

Last updated: 2020-05-26 16:59:36

Operation Scenarios

TencentDB for MySQL allows you to create one or more read-only instances to form an RO group, which is suitable for read/write separation and one-master-multiple-slave application scenarios and capable of greatly enhancing the read load capacity of your database.

Prerequisites

- A master instance should be created before a read-only instance can be created. For more information, please see Purchase Guide.
- Before use, a TencentDB for MySQL instance needs to be initialized. For more information, please see Initializing TencentDB for MySQL Instance.

Directions

Creating RO group

1. Log in to the TencentDB for MySQL Console. In the instance list, click an instance name or Manage in the "Operation" column to enter the details page.
2. On the instance details page, click Add Read-only Instance in the Instance Architecture Diagram to enter the read-only instance management page.
3. On the read-only instance page, click Create to create a read-only instance.
4. Select the desired configuration of the instance on the purchase page. After confirming that everything is correct, click **Buy Now**.

If the "Specify RO Group" option is configured as **Create RO group**, the following basic information of the new RO group should be entered on the purchase page.

- **Group Name**: the RO group name doesn't have to be unique and can contain up to 60 letters, digits, \_\_ , \_ , and \_ .
- **Eliminate Instances with Out-of-limit Delay**: this option indicates whether to enable the removal policy. If a read-only instance is removed when its delay exceeds the threshold, it will become inactive, its weight will be set to 0 automatically, and warning notifications will be sent out (for more information on how to configure the RO instance elimination alarm and recipients, please see **Alarming Feature**). The instance will be put back into the RO group when its delay falls below the threshold. No matter whether this option is enabled, a read-only instance that is removed due to instance failure will rejoin the RO group when it is repaired.
- **Delay Threshold**: set a delay threshold for a read-only instance. When the threshold is exceeded, the instance will be removed from the RO group.
- **Min Retained Instances**: this is the minimum number of instances that have to be retained in the RO group. When there are fewer instances in the RO group, even if an instance exceeds the delay threshold, it will not be removed.

**Specify an RO group.**

<table>
<thead>
<tr>
<th>Specify RO Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically assigned by the system (not specified)</td>
<td>If multiple instances are purchased at a time, each instance will be distributed to an independent RO group, and their weights will be allocated by the system automatically by default.</td>
</tr>
<tr>
<td>Create an RO group</td>
<td>Create an RO group. If multiple instances are purchased at a time, all of them will be assigned to this new RO group, and their weights will be allocated by the system automatically by default.</td>
</tr>
<tr>
<td>Existing RO group</td>
<td>Specify an existing RO group. If multiple instances are purchased at a time, all of them will be assigned to this RO group. Their weights will be allocated as configured in the RO group. If automatic allocation by the system is set for the RO group, the instances will be added to the group automatically according to the purchased specifications. If custom allocation is set, their weight will be zero by default. <strong>As the same private ID is shared within an RO group, if a VPC is used, the</strong></td>
</tr>
</tbody>
</table>
same security group settings will be shared. If an RO group is specified, it is not possible to customize any security group when purchasing instances.

- Billing mode: read-only instances are pay-as-you-go.
- Select an instance specification and required disk capacity.
  - v. Return to the instance list. The status of the created instance is "Delivering". If the status changes to "Running", the read-only instance has been successfully created.

**Configuring RO group**

On the RO group configuration page, you can configure the basic information of the group such as name, removal policy, delay threshold, minimum number of retained instances, and read weight.

- Read-only instances in an RO group can use different specifications and their read traffic weights can be set.
- Read-only instances in the same RO group can have different expiration dates and billing methods.

1. On the instance list page, select the master instance for which to set an RO group and click **Manage** in the **Action** column.
2. On the RO group management tab on the **Read-only Instance** page, click **Configure** to enter the read-only instance RO group configuration page.
3. Configure the RO group options.

- **RO Group Name**: the group name doesn't have to be unique and can contain up to 60 letters, digits, -, _, and .

- **Eliminate Instances with Out-of-limit Delay**: this option indicates whether to enable the removal policy. If a read-only instance is removed when its delay exceeds the threshold, it will become inactive, its weight will be set to 0 automatically, and warning notifications will be sent out (for more information on how to configure the RO instance elimination alarm and recipients, please see Alarming Feature).

- **Delay Threshold**: set a delay threshold for a read-only instance. When the threshold is exceeded, the instance will be removed from the RO group.

- **Min Retained Instances**: this is the minimum number of instances that have to be retained in the RO group. When there are fewer instances in the RO group, even if an instance exceeds the delay threshold, it will not be removed.

- **Assign Read Weight**: the RO group supports two weight allocation methods: automatic allocation by the system and custom allocation. The weight value must be an integer between 0 and 100. Below is the list of read weights automatically set for High IO TencentDB for MySQL instances by the system:

<table>
<thead>
<tr>
<th>Instance Specification</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000 MB memory</td>
<td>1</td>
</tr>
<tr>
<td>2,000 MB memory</td>
<td>1</td>
</tr>
<tr>
<td>4,000 MB memory</td>
<td>2</td>
</tr>
<tr>
<td>8,000 MB memory</td>
<td>2</td>
</tr>
<tr>
<td>12,000 MB memory</td>
<td>4</td>
</tr>
<tr>
<td>16,000 MB memory</td>
<td>4</td>
</tr>
<tr>
<td>24,000 MB memory</td>
<td>8</td>
</tr>
<tr>
<td>32,000 MB memory</td>
<td>8</td>
</tr>
<tr>
<td>Memory Size</td>
<td>Weight</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------</td>
</tr>
<tr>
<td>48,000 MB memory</td>
<td>10</td>
</tr>
<tr>
<td>64,000 MB memory</td>
<td>12</td>
</tr>
<tr>
<td>96,000 MB memory</td>
<td>14</td>
</tr>
<tr>
<td>128,000 MB memory</td>
<td>16</td>
</tr>
<tr>
<td>244,000 MB memory</td>
<td>26</td>
</tr>
<tr>
<td>488,000 MB memory</td>
<td>50</td>
</tr>
</tbody>
</table>

- **Load Rebalancing:**
  
  If load rebalancing is disabled, modifying weight will take effect only for new loads but not affect the read-only instances accessed by existing persistent connections or cause short disconnection from the database.

  If load rebalancing is enabled, a short disconnection lasting for just seconds will occur to disconnect all connections from the database, and the loads of newly added connections will be balanced according to the set weights.

### Terminating and deleting RO group

- RO groups cannot be deleted manually.
- An RO group will be automatically deleted when the last read-only instance in it is terminated completely.
- Empty RO groups cannot be retained.
Terminating Instance


Operation Scenarios

Based on your business needs, you can return pay-as-you-go instances in the console in a self-service manner.

- After a pay-as-you-go instance is returned, it will be moved to the TencentDB recycle bin and retained there for 24 hours. During the retention period, the instance cannot be accessed but can be restored.

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

- After the instance is terminated, its data cannot be recovered, and its backup files will also be terminated, so the data cannot be restored in the cloud. Please store your backup files safely elsewhere in advance.
- When the instance is terminated, its IP resources will be released simultaneously. If the instance has read-only instances or disaster recovery instances:
  - Read-only instances will be terminated at the same time.
  - Disaster recovery instances will disconnect their sync connections and be promoted to master instances automatically.

Directions

1. Log in to the TencentDB for MySQL Console, select the target instance in the instance list, and select More > Terminate/Return or Terminate/Return & Refund in the "Operation" column.

2. In the pop-up dialog box, indicate your consent and click Terminate Now.
Terminate Instance

1 instance is selected to terminate, View Details

After completely terminating instance, data will not be retrieved, please back up the instance data in advance.

After the instance is completely terminated, the IP resources are reclaimed at the same time.

If the instance has associated read-only or disaster recovery instances:

- Read-only instances will be terminated at the same time.
- The DR instance will stop the sync connection and automatically promote to master instance.

Refund after the instance is completely terminated:

- The amount refunded without any reason will be refunded to the original payment account in 5 days.
- The normal self-refund amount will be returned to your Tencent Cloud account by the proportion of the cash and voucher amount paid for the purchase.
- For orders from promotional reward channel, the refund will be charged 25% of their actual cash payment amount. These types of orders do not support self-service refunds, please submit a ticket to request a refund.

I have read and agreed to Termination Rules

Terminate Now  Cancel
Operation Scenario

Besides the default root account created by the system, you can create other business accounts in the TencentDB for MySQL Console based on your actual business needs.

Directions

1. Log in to the TencentDB for MySQL Console.
2. In the instance list, select the instance for which to create an account and click the instance name or Manage in the Operation column to enter the instance management page.
3. Select Database Management > Account Management and click Create Account.
4. In the pop-up dialog box, enter the account name, server, password, and confirm password and click OK.
   - The database account name can contain 1-16 letters, digits, and underscores (_) and must begin with a letter and end with a letter or digit.
   - The server address authorized to the database account can be an IP and contain "%". Multiple servers should be separated by ",", ",", ",", "|", line breaks, or spaces.
   - The password must contain 8-64 characters in at least two of the following character types: letters, digits, and special characters (\_\+-\&=!@#$%^*()\_\+-\&=!@#$%^*()).
5. After successful creation, the database account can be managed in the database account list of the current instance.

Related APIs

<table>
<thead>
<tr>
<th>API Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateAccounts</td>
<td>Creates a TencentDB account</td>
</tr>
</tbody>
</table>
Reseting Password

Last updated: 2020-05-15 16:37:20

Operation Scenarios

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

- For TencentDB for MySQL, the password resetting function has been connected to CAM; therefore, you are recommended to exercise tighter control over the permission to the password resetting API or sensitive resources of TencentDB for MySQL instances by granting such permission only to appropriate personnel.
- For data security, you are recommended to regularly reset the password at least once every three months.

Directions

1. Log in to the TencentDB for MySQL Console. In the instance list, click an instance name or Manage in the "Operation" column to enter the instance management page.
2. Select Database Management > Manage Account, find the account for which to reset the password, and select More > Reset Password.
3. In the pop-up dialog box, enter and confirm the new password and then click OK.

The database password should contain 8–64 characters in at least two of the following character types: letters, digits, and special symbols (_+-=&=!@#$%^*()).
### Related APIs

<table>
<thead>
<tr>
<th>API Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ModifyAccountPassword</td>
<td>Modifies the password of TencentDB account</td>
</tr>
</tbody>
</table>
Modifying Account Permission

Last updated: 2020-03-17 17:59:06

Operation Scenario

You can manage the permission of existing database accounts in the TencentDB for MySQL Console. Specifically, you can grant database accounts global or object-level permission and cancel such permission.

Directions

1. Log in to the TencentDB for MySQL Console.
2. In the instance list, select the instance for which to modify the permission and click the instance name or Manage in the Operation column to enter the instance management page.
3. Select Database Management > Account Management, find the account for which to modify the permission, and click More > Modify Permissions.
4. In the pop-up dialog box, select or deselect the permission and click OK to complete the modification.
   - Global permission: Grants full permission to all databases in the instance.
- **Object-level permission**: Grants permission to certain databases in the instance.

### Set Permissions

You've selected 1 account. View Details

<table>
<thead>
<tr>
<th>Global Privileges</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Object Level Privilege</td>
<td>DROP, INSERT, SELECT, TRIGGER, CREATE TEMPORARY TABLES, CREATE VIEW, DELETE, CREATE EVENT, REFERENCES, CREATE VIEW, UPDATE, CREATE EVENT, EXECUTE, LOCK TABLES, ALTER, EXECUTE, LOCK TABLES, ALTER ROUTINE, CREATE, INDEX, PROCESS</td>
</tr>
<tr>
<td>All</td>
<td></td>
</tr>
</tbody>
</table>

### Related APIs

<table>
<thead>
<tr>
<th>API Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ModifyAccountPrivileges</td>
<td>Modifies the permission of a TencentDB instance account</td>
</tr>
</tbody>
</table>
Modifying Host
Last updated : 2020-03-17 17:59:20

Operation Scenario

By modifying the host address authorized by the database account in the TencentDB for MySQL Console, you can control client access to the database so as to improve access security.

Directions

1. Log in to the TencentDB for MySQL Console.
2. In the instance list, select the instance to be modified and click the instance name or Manage in the Operation column to enter the instance management page.
3. Select Database Management > Account Management, find the account for which to modify the host, and select More > Modify Host.

4. In the pop-up dialog box for modifying host, enter the new host address and click OK.

The host address may come in the format of IP address. To allow all clients to access the database using the database account, enter %.
Modify Host

Instance: key/al_cdb238150
Name:
Account Name: mysql.sys
Server: localhost
New Host: 
Enter the host.

IP format, supporting %

OK  Cancel
Deleting Account

Operation Scenario

To disable a created database account, you can delete it in the TencentDB for MySQL Console.

In order to avoid accidental deletion from interrupting normal use by your business, you need to make sure that the database account to be deleted is no longer used by any applications.

Directions

1. Log in to the TencentDB for MySQL Console.
2. In the instance list, select the instance for which to delete an account and click the instance name or Manage in the Operation column to enter the instance management page.
3. Select Database Management > Account Management, find the account to be deleted, and select More > Delete Account.
4. In the pop-up dialog box, click **OK** to delete the account.

![Delete Account Dialog](image)

**Related APIs**

<table>
<thead>
<tr>
<th>API Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeleteAccounts</td>
<td>Deletes a TencentDB account</td>
</tr>
</tbody>
</table>
Database Management
Logging in to phpMyAdmin

Operation Scenarios

This document describes how to enter the phpMyAdmin (PMA) Console through the TencentDB for MySQL Console.

Directions

1. Log in to the TencentDB for MySQL Console, select a running instance in the instance list, and click Login in the "Operation" column.

![Instance List](image)

2. On the login page of the Data Management Console (DMC), enter "root" for the account and the password configured for the root account during initialization, and then click Login.

If you forgot the password, please reset it as instructed in Resetting Password.
3. On the data management page, you can view the instance status and basic information and create tables. Click **Go to PMA** to access the database.

4. Connect to the MySQL database through phpMyAdmin where you can view the modes and objects of the MySQL database and perform operations such as creating tables and inserting and querying data.
Creating Database and Table

Last updated: 2020-06-15 13:02:51

This document describes how to create databases and tables in TencentDB for MySQL instances.

Concepts

- **Instance**: a standalone database environment running in Tencent Cloud, which can include multiple databases created by users and can be accessed using the same tools and applications as those for a standalone database instance.
- **Database**: a warehouse that organizes, stores, and manages data based on its structure.

Creating Database

1. Log in to the phpMyAdmin Console, click **New** or **Databases** to enter the database creation page.

2. Enter the database name, select the collation (utf8_general_ci by default), and click **Create**.

   - **Database name**: a database name contains 1-64 characters, and must be unique in the instance.
   - **Collation**: click next to "Create database" to be redirected to MySQL official documentation for details.
3. Select the desired database and click **Operations** on the navigation bar at the top to enter the database operation page, where you can **Create table**, **Remove database**, or perform other
operations. You can also move, rename, or copy the database after creation.

Creating Table

1. Log in to the phpMyAdmin Console. Select the database where you want to create a table, click **New** or enter the table name and select the number of columns in the **Create table** bar, and then click **Go**.

   Table name: a table name contains 1-64 characters, and must be unique in the database.
2. On the table creation page, if you need to add columns, you can enter the number of columns to be added in the **Add** box and then click **Go**. You can enter the column information in **Structure** and partition information in **PARTITION definition** (see [MySQL partitioning chapter](#)). After entering all the information, click **Save** to create the table.

You can click ![next to the fields for more information.](image)
Via the GUI of the phpMyAdmin Console

Dropping a Database

1. Log in to the phpMyAdmin Console, click the name of database to be managed to enter the database management page, and click **Operation**.

2. You can perform various operations on databases on this page, such as **creating a table** and **dropping a database**. To drop a database, click **Drop Database (DROP)**.

Dropping a Table

Select the database for which to drop a table. You can perform various operations on tables on this page, such as **viewing**, **structuring**, **searching**, and **dropping**. Click **Drop**.
Via SQL Commands in the phpMyAdmin Console

Dropping a Database

1. Log in to the phpMyAdmin Console. To drop a database with an SQL command, click `SQL`.

2. Run the following command to drop a database.

   drop database <database name>;

Dropping a Table
1. To drop a table with an SQL command, click **SQL**.

![phpMyAdmin interface](image.png)

2. Run the following command to drop a table.

   ```sql
   drop table <table name>;
   ```
You can view and modify certain parameters in the TencentDB for MySQL Console or through API and query parameter modification logs in the console.

Modifying Parameter Value

- If the modified parameter requires instance restart for it to take effect, the system will ask you whether to restart. You are recommended to do so during off-peak hours and ensure that your application has a reconnection mechanism.

- Before the parameter modification is submitted, you can click next to the parameter or Cancel on the modification page to cancel the modification.

Modifying parameters in batches

1. Log in to the TencentDB for MySQL Console. In the instance list, click an instance name or Manage in the "Operation" column to enter the instance management page.

2. Select Database Management > Parameter Settings and click Batch modify parameters.

3. In the "Current Value" column, select the parameters to be modified. After confirming that everything is correct, click Confirm Modification.
4. In the pop-up dialog box, indicate your consent and click OK.

Modifying a single parameter
1. Log in to the TencentDB for MySQL Console. In the instance list, click an instance name or Manage in the "Operation" column to enter the instance management page.
2. Select Database Management > Parameter Settings, select the row of the target parameter, and click the pencil icon in the "Current Value" column to modify the parameter value.

3. Enter the target parameter value as prompted in the "Acceptable Values" column and click the checkmark to save the change. You can click the cross icon to cancel the operation.
4. In the pop-up dialog box, click **OK**.

**Importing from parameter template**

1. Log in to the TencentDB for MySQL Console. In the instance list, click an instance name or **Manage** in the "Operation" column to enter the instance management page.
2. Select **Database Management > Parameter Settings** and click **Import from Templates**.

3. In the pop-up dialog box, select the parameter template and click **Import and Overwrite Original Parameters**.

**Importing parameters**

1. Log in to the TencentDB for MySQL Console. In the instance list, click an instance name or **Manage** in the "Operation" column to enter the instance management page.
2. Select **Database Management > Parameter Settings** and click **Import Parameters**.

3. In the pop-up dialog box, select the file for upload, and click **Import and Overwrite Original Parameters**.
Viewing Parameter Modification Record

1. Log in to the TencentDB for MySQL Console. In the instance list, click an instance name or Manage in the "Operation" column to enter the instance management page.

2. Select Database Management > Parameter Settings and click Recent modifications.

3. On the record of recent modifications page, you can view the recent parameter modification records.
Managing Parameter Template

You can use a parameter template to manage how the parameters of a database engine are configured. A database parameter set is just like a container of engine configuration values which can be applied to one or more database instances.

The parameter template has the following features. You can log in to the TencentDB for MySQL Console and select Parameter Templates on the left sidebar to view and modify parameters:

- Specify the default parameter template.
- Create templates by modifying the default parameters to generate optimized custom parameter schemes.
- Generate templates by importing parameters from MySQL configuration file `my.conf`.
- Save parameter settings as templates.
- Import parameters from templates when setting parameters for one or multiple instances.

All database instances that have applied a parameter template will not get all parameter updates of the template. If you want to apply new parameters to a batch of database instances, you can apply them by importing a template during batch parameter settings.

Creating a Parameter Template

To use your own database parameter template, simply create a new one, modify the required parameters, and apply it to your database.

1. Log in to the TencentDB for MySQL Console.
2. Select Parameter Template on the left sidebar.

3. Click Create Template and configure the following parameters in the pop-up dialog box:
   - Template Name: enter a unique template name.
- **Database Version**: select the required database version.
- **Template Description**: enter a brief description of the parameter template.

![Create Parameter Template](image)

4. After confirming that everything is correct, click **Create and Set Parameters**.
5. After the creation is completed, you can modify, import, and export parameters on the template details page.

### Applying a Parameter Template to a Database

1. Select **Instance List** on the left sidebar and click an instance name to enter the management page.
2. Select **Manage Database > Parameter Settings > Import from Template**.
3. In the pop-up dialog box, select a parameter template and click **Import and Overwrite Original Parameters**.

### Copying a Parameter Template

If you have already created a database parameter template and want to include most of its custom parameters and values in the new template, simply copy the parameter template.

**Method 1. Copy an existing parameter template**

1. Select **Parameter Templates** on the left sidebar and click **View Details** in the "Operation" column of the template to be copied.
2. On the details page, click **Save as Template** at the top.
3. Configure the following parameters in the pop-up dialog box:
   - **Template Name**: enter a unique template name.
   - **Template Description**: enter a brief description of the parameter template.
4. After confirming that everything is correct, click **Save**.

**Method 2. Copy a parameter template using the instance parameter setting feature**

1. Select **Instance List** on the left sidebar and click an instance name to enter the management page.
2. Select **Manage Database > Parameter Settings > Save as Template**.
3. Configure the following parameters in the pop-up dialog box:
   - **Template Name**: enter a unique template name.
   - **Template Description**: enter a brief description of the parameter template.
4. After confirming that everything is correct, click **Create and Save**.

**Deleting a Parameter Template**

If a parameter template is created redundantly or no longer needed, it can be easily deleted.

1. Select **Parameter Template** on the left sidebar.
2. In the parameter template list, select the template to be deleted and click **Delete** in the "Operation" column.
3. Click **OK** in the pop-up dialog box.

**Modifying a Parameter**

After purchasing a TencentDB for MySQL instance, you can use its default parameter values, adjust such values based on your business needs, or modify the parameter configuration of its parameter template which then can be applied to other instances in the same business scenario.

**Method 1. Modify parameter values by using the parameter configuration feature**

1. Select **Instance List** on the left sidebar and click an instance name to enter the management page.
2. Click **Parameter Settings** on the **Manage Database** tab.
3. On the parameter configuration page, click **Batch Modify Parameters** to modify parameters in batches. Then, click **Confirm Modifications**.
   - Or, on the parameter configuration page, click the **Edit** icon next to the **Current Value** of a parameter to modify the specific parameter. Then, click the **Save** icon next to the value.

**Method 2. Modify parameter values in a new or existing parameter template**
1. Select **Parameter Template** on the left sidebar.
2. In the parameter template list, select the template to be modified and click **View Details** in the "Operation" column.
3. On the details page, click **Batch Modify Parameters** to modify parameters in batches. Then, click **Confirm Modifications**.
   Or, on the details page, click the **Edit** icon next to the **current parameter value** of a parameter to modify the specific parameter. Then, click the **Save** icon next to the value.

### Importing Parameters

You can use or modify the default parameter values provided by a TencentDB for MySQL instance or import existing parameter configuration in your business system. Please note that parameters not in the parameter setting list or parameter template list won't be imported.

#### Method 1. Import parameters by using a parameter template

1. Select **Parameter Template** on the left sidebar.
2. In the parameter template list, select the template to be modified and click **View Details** in the "Operation" column.
3. Click **Import Parameters** on the details page.
4. Click **Select File** in the pop-up dialog box.
5. When selecting the local parameter configuration file, please note that the file format should be the same as that used by the MySQL database server. You can also use the file template of the exported parameters; otherwise, the system will prompt for importing failure.
6. Click **Import and Overwrite Original Parameters**.

#### Method 2. Import parameters by using the instance parameter setting feature

1. Select **Instance List** on the left sidebar and click an instance name to enter the management page.
2. Click **Parameter Settings** on the **Manage Database** tab.
3. Click **Import Parameters** on the parameter configuration page.
4. Click **Select File** in the pop-up dialog box.
5. When selecting the local parameter configuration file, please note that the file format should be the same as that used by the MySQL database server. You can also use the file template of the exported parameters; otherwise, the system will prompt for importing failure.
6. Click **Import and Overwrite Original Parameters**.
Backup and Rollback

Backup Mode

Last updated: 2020-04-29 17:22:53

Backup Overview

**Backup modes**

TencentDB for MySQL High-Availability Edition supports **auto backup** and **manual backup** of databases.

**Backup types**

TencentDB for MySQL High-Availability Edition supports two backup types:

- **Physical backup**, which is a full copy of physical data (supported for both auto backup and manual backup).
- **Logical backup**, which backs up SQL statements (only supported for manual backup).

- To restore a database from a physical backup, you need to use xbstream to decompress the package first. For more information, please see [Restoring Database from Physical Backup](#).
- If the number of tables in a single instance exceeds one million, backup may fail, and database monitoring may be affected. Please control the number of tables in one single instance appropriately and make sure that it is below one million.
- As the data of tables created by the MEMORY storage engine is stored in the memory, physical backups cannot be created for such tables. To avoid data loss, it is recommended to replace them with InnoDB tables.

<table>
<thead>
<tr>
<th>Physical Backup Advantages</th>
<th>Logical Backup Disadvantages</th>
</tr>
</thead>
</table>

© 2013-2019 Tencent Cloud. All rights reserved.
## Physical Backup Advantages

- High backup speed.
- Streaming backup and compression are supported.
- High success rate.
- Simple and efficient restoration.
- Faster backup-based coupling operations such as adding real-only and disaster recovery instances.
- 1/8 of average time needed for creating a logical backup.
- 10 times faster than logical backups during import.

## Logical Backup Disadvantages

- Long time needed to restore as it takes time to run SQL and build indexes.
- Low backup speed, especially when there are massive amounts of data.
- Possible increase in master-slave delay due to the pressure on instances during backup.
- Possible loss of precision information of floating points.
- Potential backup failures due to wrong views and other problems.
- Slower backup-based coupling operations such as adding read-only and disaster recovery instances.

### Backup objects

#### Data Backup

MySQL v5.5, 5.6, and 5.7 (High-Availability Edition):
- Auto backup supports full physical backup.
- Manual backup supports full physical backup, full logical backup, and single-database/table logical backup.
- Both auto backup and manual backup can be compressed and downloaded.
- Auto backups cannot be manually deleted, but their retention periods can be set.
- Manual backups can be manually deleted in the console and will be retained until they are deleted.

#### Log Backup

MySQL v5.5, 5.6, and 5.7 (High-Availability Edition):
- Log files occupy the instance’s backup capacity.
- Log files can be downloaded but cannot be compressed.
- Retention periods can be set for log files.

### Notes

- Starting from February 26, 2019, the auto backup feature of TencentDB for MySQL will only support physical backup (default type) and no longer provide logical backup. Existing automatic logical backups will be switched to physical backups automatically.

  This will not affect your business access, but may have impact on your auto backup habit. If you need logical backups, you can use the manual backup method in the TencentDB for MySQL Console or call the relevant API to generate logical backups.

- Both logical and physical backup files will be compressed, so some files may be unusable after being downloaded. In that case, you can use the table backup feature in manual logical backup. For more information, please see manual backup.
• Instance backup files occupy backup capacity. Please develop a backup schedule and plan the backup capacity appropriately to avoid potential extra fees in the future.
• It is recommended to back up your database during off-hours.
• To avoid situations where the required backup files are deleted after the retention period lapses, please download them to the local file system in a timely manner.
• DDL operations are prohibited during the backup process so as to avoid backup failure due to table locking.
• Backup capacity in excess of the free tier will incur fees. For more information, please see Backup Capacity Billing Description.

Backing up MySQL Data Automatically

1. Log in to the TencentDB for MySQL Console, click an instance name on the instance list page to enter the management page, and select **Backup and Restore > Auto Backup Settings**.

![Auto Backup Settings](image)

2. Select backup parameters in the pop-up window as detailed below and click **OK**:

   The **rollback feature** relies on the backup cycle and retention days of backup files. Reducing the frequency of auto backup and retention period will affect the rollback feature for instance data. Please configure backup appropriately based on your actual needs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup cycle</td>
<td>To ensure data security, please back up your data at least twice a week. The default value is Monday to Sunday.</td>
</tr>
</tbody>
</table>
| Backup time     | ◦ The default backup initiation time is automatically assigned by the system.  
                  ◦ You can select a custom time range (preferably during off-peak hours). This is just the start time of the backup process and does not indicate the end time.  
                  For example, if the time range is 02:00-06:00, the system will initiate a backup at a point in time during 02:00-06:00, which depends on the backend backup policy and backup system conditions. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data backup retention period</td>
<td>Data backup files can be retained for 7 (default value) to 732 days.</td>
</tr>
<tr>
<td>Log backup retention period</td>
<td>Log backup files can be retained for 7 (default value) to 732 days.</td>
</tr>
<tr>
<td></td>
<td>The number of days set for log backup retention must be smaller than that for data backup retention.</td>
</tr>
</tbody>
</table>

**Backup Settings**

Auto backup now uses a fast physical backup with high success rate and no longer supports logical backup.

If you want to export a logical backup, you can use the manual backup function that supports the logical backup by table.

**Data Backup Configuration**

- **Backup Period**: Mon, Tue, Wed, Thu, Fri, Sat, Sun
- **Backup Time**: Default Time, Custom
- **Data Backup Retention Time**: 7 days

It ranges from 7 to 732 days. The backup set is automatically deleted upon expiration.

**Log Backup Configuration**

- **Log Backup Retention Time**: 7 days

It ranges from 7 to 732 days, and must be less than or equal to the data backup days. The backup set is automatically deleted upon expiration.

**Backup Notes**

1. Prolonging the retention days of data backup and log backup may incur charges for additional backup space.
2. Shortening the retention days of log backup may affect the data rollback period of the instance.

**Back up MySQL Data Manually**

The manual backup feature allows you to initiate a backup task manually.
Manual backup supports full physical backup, full logical backup, and single-database/table logical backup.
You can delete manual backups in the backup list to release backup capacity.
When the instance is performing daily auto backup, you cannot initiate a manual backup task.

1. On the instance list page, click an instance name to enter the management page, and select **Backup and Restore > Manual Backup**.
2. Select backup modes and objects in the pop-up window and click **OK**.

For single-database/table logical backup, select the database or table to be backed up in **Select database & table** in the left column and add the selected item to the right column. If you don't have a database, please create a database/table first.
Backup Settings

Logical backup specifies the table mode to back up only the data structure and data content. Currently, views, stored procedures, user-defined functions, triggers and other contents are not supported.

Select backup mode
- Logical cold backup
- Physical cold backup

Select an object
- Whole instance
- Specify Table

Select Table

Selected (0 databases) tables

Loading completed. 1 database is found.

Select the database name, support query.

OK  Cancel
Operation Scenarios

The backup capacity occupied by TencentDB for MySQL instance backup files is allocated by region. It is equivalent to the total storage capacity used by all MySQL database backups in a region, including automatic data backups, manual data backups, and log backups. Increasing the backup retention time or manual backup frequency will use more database backup storage capacity.

This document describes how to view the MySQL instance backup capacity and free tier in the console.

Directions

1. Log in to the TencentDB for MySQL Console and select **Database Backup** on the left sidebar.

2. Select a region at the top to view its backup overview and list.
Overview Page

The overview page is divided into three sections: total backups, backup trend, and backup statistics.

- **Total backups**: This section displays the size and quantity of all, data, and log backups as well as the free tier and paid capacity.
  
  - Green: The total backup capacity used does not exceed the free tier.
  - Orange: The total backup capacity used has exceeded the free tier and incurred fees.

- **Backup trend**: This section displays the trends of each backup count.
- **Backup statistics**: This section displays the names/IDs of instances in the current region as well as the size and quantity of all, data, log, automatic, and manual backups.

Click an instance name/ID to enter the instance details page; the backup capacity can be sorted by backup size; you can search for a backup by instance name/ID in the search box in the top-right corner.

Backup list

The backup list can be divided into data backups and log backups. You can click an instance name/ID in the list to enter the instance details page. The backup list supports filtering by time period and fuzzy search by instance name/ID.
Data backup list

- Filtering by information field is supported:
  - Type: All, logical cold backup, physical cold backup.
  - Backup mode: All, automatic, manual.
  - Backup method: Currently, only full backup is supported.
- Backups can be sorted by backup time, task start time, task end time, and backup size.
- Click Details in the "Operation" column to enter the instance backup and restoration page, where you can click Download to download backups. Only manual backups can be deleted.

Log backup list

- Log backups are calculated based on the end time of logs.
- Backups can be sorted by log data start time and end time.
- Click Details in the "Operation" column to enter the instance backup and restoration page, where you can click Download to download logs.
Restoring Database from Backup File

Restoring Database from Physical Backup

Operation Scenarios

To save storage capacity, both physical and logical backups in TencentDB for MySQL will be compressed and packaged. Specifically, a backup file is compressed with qpress first and then packed with xbstream offered by Percona.

The open-source software tool Percona XtraBackup can be used to back up and restore databases. This document describes how to use XtraBackup to restore a physical backup file of a TencentDB for MySQL instance to a CVM-based self-created database.

- XtraBackup only supports Linux but not Windows.
- For more information on how to restore data on Windows, please see Offline Migration of Data.

Prerequisites

- Download and install XtraBackup.
  XtraBackup can be downloaded at Percona's official website. Please select Percona XtraBackup 2.4.6 or higher. For more information on how to install the tool, please see Percona XtraBackup 2.4.
- Supported instance versions: TencentDB for MySQL 5.5, 5.6, and 5.7 high-availability edition and finance edition.
- Instances with data encryption enabled cannot be restored from a physical backup.

Directions

Step 1. Download the backup file

You can download data backups and log backups of TencentDB for MySQL instances in the console.

Each IP can have up to 10 download links by default, with a download speed limit of 20–30 Mbps each.
1. Log in to the TencentDB for MySQL Console. In the instance list, click an instance name or Manage in the "Operation" column to enter the instance management page.

2. On the instance management page, click Backup and Restore > Data Backup List, select the backup to download, and then click Download in the "Operation" column.

3. You are recommended to copy the download address in the pop-up dialog box, log in to a (Linux) CVM instance in the same VPC as the TencentDB instance, and run the `wget` command for download over the private network at a higher speed.

- You can also select Download to download it directly, which takes more time though.
- `wget` command format: `wget -c 'backup file download address' -O custom filename.xb`

Below is a sample:

```bash
```

**Step 2. Unpack the backup file**

1. Run the xbstream command to unpack the backup file to the target directory.

   ```bash
   xbstream -x -C /data < ~/test.xb
   ```

- `/data` is used as an example in this document. You can replace it with a real path according to the actual situation.
- Replace `~/test.xb` with your backup file.
The unpacking result is as shown below:

![Unpacking result]

**Step 3. Decompress the backup file**

1. Download qpress by running the following command.

   ```bash
   wget http://www.quicklz.com/qpress-11-linux-x64.tar
   ```

   If an error is displayed for the `wget` download operation, you can go to QuickLZ's official website to download the qpress locally, and then upload it to the Linux CVM instance. For more information, please see [Uploading Files to Linux CVM with SCP](#).

2. Extract the qpress binary files by running the following command.

   ```bash
   tar -xf qpress-11-linux-x64.tar -C /usr/local/bin
   source /etc/profile
   ```

3. Then, decompress all `.qp` files in the target directory by running the following command:

   ```bash
   xtrabackup --decompress --target-dir=/data
   ```

   - `/data` is the target directory where the backup file was previously stored. You can replace it with a real path according to the actual situation.
   - The `--remove-original` option is supported only in Percona Xtrabackup 2.4.6 and higher.
   - `xtrabackup` won't delete the original files during decompression by default. If you want to delete them upon the completion of decompression, add the `--remove-original` parameter to the above command.
Step 4. Prepare the backup file

After a backup file is decompressed, perform the "apply log" operation by running the following command.

```
xtrabackup --prepare --target-dir=/data
```

If the execution result contains the following output, it means that the preparation succeeded.

```
InnoDB: Starting shutdown...
InnoDB: Shutdown completed; log sequence number 922620089
```

Step 5. Modify the configuration file

1. Run the following command to open the `backup-my.cnf` file.

   ```
   vi /data/backup-my.cnf
   ```

   The target directory `/data` is used as an example in this document. You can replace it with a real path according to the actual situation.

2. Given the existing version issues, the following parameters need to be commented in the extracted file `backup-my.cnf`.

### Step 6. Modify file attributes

Modify file attributes and check whether files are owned by a TencentDB for MySQL user.

```bash
chown -R mysql:mysql /data
```

```
34884
-rw-r----- 1 mysql mysql 424 11月 9 18:15 backup-my.cnf
-rw-r----- 1 mysql mysql 12582912 11月 9 18:12 ibdata1
-rw-r----- 1 mysql mysql 12582912 11月 9 16:30 ibtmp1
-rw-r----- 1 mysql mysql 10485760 11月 9 16:30 undo001
drwxr-x--- 2 mysql mysql 4096 11月 9 16:30 mysql
drwxr-x--- 2 mysql mysql 4096 11月 9 16:30 test
drwxr-x--- 2 mysql mysql 4096 11月 9 16:30 performance_schema
drwxr-x--- 2 mysql mysql 4096 11月 9 16:30 sbtest
```
Step 7. Start the mysqld process and log in for verification

1. Start the mysqld process.

```
mysqld_safe --defaults-file=/data/backup-my.cnf --user=mysql --datadir=/data &
```

2. Log in to the MySQL client for verification.

```
mysql -uroot
```

```
Welcome to the MySQL monitor. Commands end with ; or \
Your MySQL connection id is 2
Server version: 5.6.23 Source distribution

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
mysql> show databases;

+------------------+
| Database          |
+------------------+
| information_schema|
| test             |
+------------------+

2 rows in set (0.00 sec)

mysql>
```

Backup FAQs

See Common Issues and Failure Reasons.
Restoring Database from Physical Backup File

Last updated: 2020-06-03 14:06:29

Operation Scenarios

To save storage capacity, physical and logical backups in TencentDB for MySQL will be compressed with qpress and then packed with xbstream offered by Percona.

The open-source Percona XtraBackup can be used to back up and restore databases. This document describes how to use XtraBackup to restore a logical backup file of TencentDB for MySQL instance to a self-built database on CVM.

- XtraBackup only supports Linux but not Windows.
- For more information on how to restore data on Windows, please see Database Rollback, Data Migration with Command Line Tool, and Migrating Data Through DTS.

Prerequisites

- Download and install XtraBackup.
  XtraBackup can be downloaded at Percona's official website. Please select Percona XtraBackup 2.4.6 or higher. For more information on installation, please see Percona XtraBackup 2.4.
- Supported instance version: TencentDB for MySQL 5.5, 5.6, and 5.7 High-Availability Edition and Finance Edition.

Directions

Step 1. Download the backup file

1. Log in to the TencentDB for MySQL Console. In the instance list, click an instance name or Manage in the "Operation" column to enter the instance management page.
2. On the instance management page, click Backup and Restore > Data Backup List, select the backup file to download, and then click Download in the "Operation" column.
3. We recommend that you copy the download address in the pop-up dialog box, log in to a (Linux) CVM instance in the same VPC as the TencentDB instance, and run the `wget` command to download over the private network for higher speed.
You can also click **Download** to download it directly, which may take longer.
- **wget** command format: wget -c 'backup file download address' -O custom filename.xb

Example:

```
wget -c 'https://mysql-database-backup-bj-118.cos.ap-beijing.myqcloud.com/12427%2Fmysql%2F42d-11ea-b887-6eb82b%2Fdata%2FAutomatic-delete%2F2019-11-28%2FAutomatic%2Fxtrabackup%2Fbk_204_10385%2Fcdcb-1pe7bexs_backup_20191128044644.xb?sign=q-sign-algorithm%3Dsha1%26q-ak%3D1%26q-sign-time%3D1574269%3B1575417469%26q-key-time%3D1575374269%3B1517469%26q-header-list%3D%26q-url-param-list%3D%26q-signature%3D%26q-filename%3D%2141731_backup_20191128044644.xb%22&response-content-disposition=attachment%3Bfilename%3D%2141731_backup_20191128044644.xb%22&response-content-type=application%2Foctet-stream' -O test0.xb
```

### Step 2. Unpack the backup file

Unpack the backup file with xbstream.

```
xbstream -x < test0.xb
```

Replace `test0.xb` with your backup file.

The unpacking result is as shown below:

![Unpacking result](image)

### Step 3. Decompress the backup file

1. Download qpress by running the following command:

```
wget http://www.quicklz.com/qpress-11-linux-x64.tar
```
If an error is displayed during the `wget` download, you can go to QuickLZ’s official website to download qpress locally and upload it to the Linux CVM instance. For more information, please see Upload Files via SCP.

2. Extract the qpress binary files by running the following command:

```
tar -xf qpress-11-linux-x64.tar -C /usr/local/bin
source /etc/profile
```

3. Decompress the backup file with qpress.

```
qpress -d cdb-jp0zua5k_backup_20191202182218.sql.qp
```

Find the backup file with .sql.qp extension by decompression time and replace `cdb-jp0zua5k_backup_20191202182218` with its filename.

The decompressing result is as shown below:

![Decompressing result]

Step 4. Import the backup file into the target database

Import the .sql file into the target database by running the following command:

```
mysql -uroot -P3306 -h127.0.0.1 -p < cdb-jp0zua5k_backup_20191202182218.sql
```

- This document takes importing into a local MySQL instance with port 3306 as an example. You can replace it as needed.
• Replace `cdb-jp0zua5k_backup_20191202182218.sql` with the `.sql` file extracted by qpress.
Database Rollback

Last updated: 2020-04-21 10:18:47

Operation Scenarios

TencentDB will not alter any of your data. Data corrupted due to personal reasons can be recovered through rollback in a self-service manner. A rollback feature is provided to roll back databases or tables in Tencent Cloud based on data backup and log backup (binlog), and real-time data rollback is supported.

By re-constructing periodical images and real-time transactions, the TencentDB rollback tool can roll back a database or table to the specified point in time where the time slices of all data are guaranteed to be identical. A new database or table will be generated in the original instance by the rollback operation, and during the process, the original database or table can be accessed normally. Upon the completion of rollback, you can see both the new and original databases/tables.

Notes

- The rollback feature is subject to the backup cycle and retention days set for automatic backup. It enables data rollback based on data backup + log backup (binlog) according to the configured retention days and backup cycle. For the backup cycle settings, please see Backing up MySQL Data Automatically. To ensure MySQL data security, set the automatic backup cycle to at least twice a week.
  - For example, if you set the backup cycle to every Monday and Thursday and the backup retention days to 7 days, then you can roll back to any day within the retention period.
  - For example, if you set the backup cycle to every Sunday and the backup retention days to 10 days, then you can roll back to any day within the retention period.

Directions

1. Log in to the TencentDB for MySQL Console.
2. Choose one or more instances to be rolled back from the instance list and select More > Rollback.

- If rollback is to be performed on only one instance, you can also go to the instance management page and click Rollback in the top-right corner.
- Up to 5 rollback tasks can be initiated at a time under the same APPID.
3. Select the table to be rolled back and click **Next step: set the rollback time and database table name**.

- Only tables whose name contains digits, letters, underscores, or their combinations can be rolled back, while those whose name contains special characters are not supported.
- In the rollback mode with a specified table, a maximum of 500 databases or tables in the same instance can be rolled back at a time.
- If the table to be rolled back has been dropped, you need to log in to the TencentDB instance and create a table first before performing rollback in the console.
- If the cold backup before rollback does not contain the table, rollback will fail.
- If the rollback involves composite operations on other database tables during the trace of binlogs, the SQL statement may fail.
- If the rollback involves foreign keys and other constraints of the table during the trace of binlogs, the SQL statements may fail.
4. Set the post-rollback table name and rollback time and click **Rollback**.

- Each instance can be set with only one rollback time.
- If you choose to set a batch rollback time, all tables will be rolled back at the specified time.
- If you choose to set a single-table rollback time, tables will be rolled back at their respective rollback time.
- The table name after rollback can contain up to 64-bit letters, digits, decimal points (.), dashes (-), underscores (_), and $.
5. After submission, go to **Operation Log > Rollback Log** where you can view the rollback progress. Click **View Details** to view the rollback log in real time.

6. Upon the completion of rollback, select **Manage Database > Database List** and you can see the new table after rollback in the original instance.
Data Import and Export
Batch Operating Instance

Operation Scenarios

TencentDB for MySQL supports importing SQL files via the console, allowing you to execute SQL statements in the selected database. You can also use this feature to create databases/tables and change table structures to initialize or modify the instance.


Directions

1. Log in to the TencentDB for MySQL Console. In the instance list, click an instance name or Manage in the "Operation" column to enter the instance management page.
2. Select Database Management > Database List and click Data Importing.
3. On the pop-up page, click Add File to import the file. After the upload is completed, click Next.

- To avoid database unavailability caused by corruption of system tables, do not import data from system tables such as the mysql.user table.
- Only incremental import is supported. If there is obsolete data in the database, clear the data before the importing operation.
- A single file does not exceed 2 GB. The file name only allows letters, numbers, and underlines.
- Uploaded files are valid for 14 days and will be automatically deleted after expiration.
4. On the database selection page, select the target database and click **Next**.

5. On the confirmation page, after confirming that the imported data is correct, enter the account and password and click **Import**.

- The import cannot be rolled back. Please confirm the import information.
- If you forgot the password, please reset it as instructed in **Resetting Password**.
The import cannot be rolled back. Please confirm the import information.

**Import File**

<table>
<thead>
<tr>
<th>File Name</th>
<th>Time</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>demo.sql</td>
<td>2020/04/26 11:44:59</td>
<td>21 Byte</td>
</tr>
</tbody>
</table>

**Target Database**

<table>
<thead>
<tr>
<th>Database Name</th>
<th>Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lab1-CD001</td>
</tr>
</tbody>
</table>

**Database account**

- Output the database account with operation permissions

**Database password**

- Please enter the password
The data migration feature of DTS can be used to import data to TencentDB for MySQL. For more information, see Data Migration.
Offline Migration of Data

Last updated: 2020-05-21 09:49:45

Data Migration Through Console

There are two modes for migrating data through the console: physical backup and logical backup. For more information, please see:

- Restoring Database from Physical Backup
- Restoring Database from Logical Backup

Data Migration with Command Line Tool

1. Generate the SQL file to be imported with the MySQL command line tool "mysqldump" in the following way:

   - The data files exported using mysqldump must be compatible with the SQL specification of your purchased TencentDB for MySQL version. You can log in to the database and get the MySQL version information by running the `SELECT version();` command. The name of the generated SQL file can contain letters, digits, and underscores but not "test".
   - Make sure that the same source and target database versions, source and target database character sets, and mysqldump tool versions are used. You can specify the character set using the parameter `--default-character-set`.

   ```shell
   shell > mysqldump [options] db_name [tbl_name ...] > bak_pathname
   ```

   Here, `options` is the export option, `db_name` is the database name, `tbl_name` is the table name, and `bak_pathname` is the export path.

   For more information on how to export data with mysqldump, please see MySQL's official documentation.

2. Import data to the target database with the MySQL command line tool as follows:

   ```shell
   shell > mysql -h hostname -P port -u username -p < bak_pathname
   ```

   Here, `hostname` is the target server for data restoration, `port` is the port of target server, `username` is the username of the database on the target server, and `bak_pathname` is the full path to the backup file.
Migrating data (Windows)

1. Use the Windows version of mysqldump to generate the SQL file to be imported. For more information, please see the description in Data Migration with Command Line Tool.

2. Enter the command prompt and import the data into the target database with the MySQL command line tool.

```bash
$ mysql -h <hostname> -u <username> -p <target> <source> <target>
Enter password: ************
```

3. Log in to the target MySQL database, run the `show databases;` command, and you can see that the backup database has been imported into the target database.

```
mysql> show databases;
+--------------------+
| Database            |
+--------------------+
| information_schema  |
| la                 |
| lalalalalaa        |
| mysql              |
| performance_schema |
| sakila             |
| test               |
| world              |
+--------------------+
10 rows in set (0.01 sec)
```

Migrating data (Linux)

This document uses a Linux CVM instance as an example. For more information on how to access a database from a CVM instance, please see Accessing MySQL Database.

1. Log in to the CVM instance and generate the SQL file to be imported with the MySQL command line tool "mysqldump". Take the `db_blog` database in TencentDB as an example:
2. Use the MySQL command line tool to restore the data to the target database.

3. Log in to the target MySQL database, run the `show databases;` command, and you can see that the backup database has been imported into the target database.

---

**Issues with Character Set of Imported Data Files**

1. If no character set is specified during data file import into TencentDB, the one set by the database will be used.

2. Otherwise, the specified character set will be used.

3. If the specified character set is different from that of TencentDB, garbled text will be displayed.

For more information, please see the character set description in [Use Limits](#).
Network and Security
Access Management
Overview

If you use multiple Tencent Cloud services such as TencentDB, CVM, and VPC which are managed by
different users who share your Tencent Cloud account key, the following problems may exist:

- 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 privileges. 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.

- 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 in TencentDB for the time being.
<table>
<thead>
<tr>
<th>Task</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about the basic policy structure</td>
<td>Policy Syntax</td>
</tr>
<tr>
<td>Define operations in a policy</td>
<td>TencentDB Operations</td>
</tr>
<tr>
<td>Defines resources in a policy</td>
<td>TencentDB Resource Path</td>
</tr>
<tr>
<td>Resource-level permission supported by TencentDB</td>
<td>Resource-level Permission Supported by TencentDB</td>
</tr>
<tr>
<td>Console sample</td>
<td>Console Sample</td>
</tr>
</tbody>
</table>
Authorization Policy Syntax

Last updated: 2020-04-01 16:46:07

Policy Syntax

CAM policy:

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

- **version** is required. Currently, only "2.0" is allowed.
- **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.
  - **effect** describes whether the result produced by the statement is "allowed" (allow) or "denied" (deny). This element is required.
  - **action** describes the allowed or denied action (operation). An operation can be an API (prefixed with "cdb:"). This element is required.
  - **resource** describes the details of authorization. A resource is described in a six-segment format. Detailed resource definitions vary by product. 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 required.

TencentDB Operations

In a TencentDB policy statement, you can specify any API action from any service that supports TencentDB. APIs prefixed with "cdb:" should be used for TencentDB, such as cdb:CreateDBInstance or cdb:CreateAccounts.

To specify multiple operations in a single statement, separate them with commas, as shown below:
"action":["cdb:action1","cdb:action2"]

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

"action":["cdb:Describe*"]

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

"action":["cdb:*"]

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 COS.
- **region** describes the region information, such as ap-guangzhou.
- **account** is the root account of the resource owner, such as uin/653339763.
- **resource** describes detailed resource information of each product, such as instanceId/instance_id1 or instanceId/*.

For example, you can specify a resource for a specific instance (cdb-k05xdcta) in a statement as shown below:

```
"resource":[ "qcs::cdb:ap-guangzhou:uin/653339763:instanceId/cdb-k05xdcta"]
```

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

```
"resource":[ "qcs::cdb:ap-guangzhou:uin/653339763:instanceId/**"]
```

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

```
"resource":[ "*"]
```
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, where words prefixed with $ are placeholders, `project` refers to a project ID, `region` refers to a region, and `account` refers to an account ID.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Resource Description Method in Authorization Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>VPC</td>
<td>qcs::vpc:$region:$account:vpc/$vpcId</td>
</tr>
<tr>
<td>Security group</td>
<td>qcs::cvm:$region:$account:sg/$sgId</td>
</tr>
</tbody>
</table>
Authorizable Resource Types

Last updated: 2020-04-01 16:46:08

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

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Resource Description Method in Authorization Policy</th>
</tr>
</thead>
</table>
| TencentDB instance-related  | qcs::cdb:$region:$account:instanceId/*  
                             | qcs::cdb:$region:$account:instanceId/$instanceId                   |

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.

**List of APIs supporting authorization at resource level**

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Resource Path</th>
</tr>
</thead>
</table>
| AddTimeWindow         | qcs::cdb:$region:$account:instanceId/*  
                             | qcs::cdb:$region:$account:instanceId/$instanceId |
| AssociateSecurityGroups | qcs::cdb:$region:$account:instanceId/*  
                             | qcs::cdb:$region:$account:instanceId/$instanceId |
| CloseWanService       | qcs::cdb:$region:$account:instanceId/*  
                             | qcs::cdb:$region:$account:instanceId/$instanceId |
| CreateAccounts        | qcs::cdb:$region:$account:instanceId/*  
                             | qcs::cdb:$region:$account:instanceId/$instanceId |
| CreateBackup          | qcs::cdb:$region:$account:instanceId/*  
                             | qcs::cdb:$region:$account:instanceId/$instanceId |
| CreateDBImportJob     | qcs::cdb:$region:$account:instanceId/*  
                             | qcs::cdb:$region:$account:instanceId/$instanceId |
| DeleteAccounts        | qcs::cdb:$region:$account:instanceId/*  
                             | qcs::cdb:$region:$account:instanceId/$instanceId |
| DeleteBackup          | qcs::cdb:$region:$account:instanceId/*  
                             | qcs::cdb:$region:$account:instanceId/$instanceId |

Last updated: 2020-04-01 16:46:08
<table>
<thead>
<tr>
<th>API Operation</th>
<th>Resource Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeleteTimeWindow</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeAccountPrivileges</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeAccounts</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeBackupConfig</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeBackupDatabases</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeBackupDownloadDbTableCode</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeBackups</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeBackupTables</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeBinlogs</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeDatabases</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeDBImportRecords</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeDBInstanceCharset</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeDBInstanceConfig</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeDBInstanceGTID</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeDBInstanceRebootTime</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeDBSwitchRecords</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>API Operation</td>
<td>Resource Path</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DescribeDBSecurityGroups</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeInstanceParamRecords</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeInstanceParams</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeRoGroups</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeRollbackRangeTime</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeSlowLogs</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeSupportedPrivileges</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeTables</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeTimeWindow</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeDatabasesForInstances</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeMonitorData</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DescribeTableColumns</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DropDatabaseTables</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>InitDBInstances</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>IsolateDBInstance</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>ModifyAccountDescription</td>
<td>qcs::cdb:$region:$account:instanceId/*&lt;br&gt;qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>API Operation</td>
<td>Resource Path</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>ModifyAccountPassword</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>ModifyAccountPrivileges</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>ModifyAutoRenewFlag</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>ModifyBackupConfig</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>ModifyBackupInfo</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>ModifyDBInstanceName</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>ModifyDBInstanceProject</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>ModifyDBInstanceSecurityGroups</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>ModifyDBInstanceVipVport</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>ModifyInstanceParam</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>ModifyDBInstanceModes</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>ModifyTimeWindow</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>ModifyProtectMode</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>OfflineDBInstances</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>OpenDBInstanceGTID</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>OpenWanService</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>API Operation</td>
<td>Resource Path</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>ReleaseIsolatedDBInstances</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>RestartDBInstances</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>StartBatchRollback</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>SubmitBatchOperation</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>SwitchDrInstanceToMaster</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>SwitchForUpgrade</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>DisassociateSecurityGroups</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>UpgradeDBInstance</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
<tr>
<td>UpgradeDBInstanceEngineVersion</td>
<td>qcs::cdb:$region:$account:instanceId/*</td>
</tr>
<tr>
<td></td>
<td>qcs::cdb:$region:$account:instanceId/$instanceId</td>
</tr>
</tbody>
</table>

**List of APIs not supporting authorization at resource level**

For a TencentDB API operation that does not support authorization at the resource level, you can still authorize a user to perform it, but you must specify the resource element in the policy statement as the resource element in the policy statement.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>API Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateDBInstanceHour</td>
<td>Creates a pay-as-you-go TencentDB instance</td>
</tr>
<tr>
<td>CreateParamTemplate</td>
<td>Creates a parameter template</td>
</tr>
<tr>
<td>DeleteParamTemplate</td>
<td>Deletes a monitoring template item</td>
</tr>
<tr>
<td>DescribeProjectSecurityGroups</td>
<td>Queries security group information of a project</td>
</tr>
<tr>
<td>DescribeDefaultParams</td>
<td>Queries the list of default configurable parameters</td>
</tr>
<tr>
<td>DescribeParamTemplateInfo</td>
<td>Queries the parameter template details</td>
</tr>
<tr>
<td>DescribeParamTemplates</td>
<td>Queries the list of parameter templates</td>
</tr>
<tr>
<td>API Operation</td>
<td>API Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>DescribeAsyncRequestInfo</td>
<td>Queries the execution result of an async task</td>
</tr>
<tr>
<td>DescribeTasks</td>
<td>Queries the list of tasks for a TencentDB instance</td>
</tr>
<tr>
<td>DescribeUploadedFiles</td>
<td>Queries the list of imported SQL files</td>
</tr>
<tr>
<td>ModifyParamTemplate</td>
<td>Modifies a parameter template</td>
</tr>
<tr>
<td>RenewDBInstance</td>
<td>Renews a TencentDB instance</td>
</tr>
<tr>
<td>StopDBImportJob</td>
<td>Stops a data import task</td>
</tr>
</tbody>
</table>
Operation Scenarios

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.

Directions

Full read/write permission policy for TencentDB

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

Enter the policy management page. Click Service Type and select TencentDB for MySQL in the dropdown list. Then, you can see this policy in the results.

The policy syntax is as follows:

```json
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "cdb:*"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```
"action": [
  "vpc:*"
],
"resource": "+",
"effect": "allow"
},
{
"action": [
  "cvm:*"
],
"resource": "qcs::cvm::sg/*",
"effect": "allow"
},
{
"action": [
  "cos:*"
],
"resource": "+",
"effect": "allow"
},
{
"effect": "allow",
"action": ["monitor:*"],
"resource": "+"]

The above policy achieves its goal by allowing the user to separately authorize the use of TencentDB, VPC, security group, COS, KMS, and all resources available in the monitor with the CAM policy.

**Read-only permission policy for TencentDB**

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

You are recommended to configure the read-only policy for TencentDB.
You can enter the policy management page. Click Service Type and select TencentDB for MySQL in the drop-down list. Then, you can see this policy in the results.

The policy syntax is as follows:

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

**Read-only permission policy for TencentDB-related resources**

To grant a user permission to view TencentDB instances and related resources (VPC, security group, COS, and monitor) but create, delete, or modify them, implement the policy named QcloudCDBReadOnlyAccess for the user.

You can enter the policy management page. Click Service Type and select TencentDB for MySQL in the drop-down list. Then, you can see this policy in the results.

The policy syntax is as follows:

```json
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "cdb:Describe*"
            ],
            "resource": "*",
            "effect": "allow"
        },
        {
            "action": [
                "vpc:Describe*",
                "vpc:Inquiry*",
                "vpc:Get*"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```
The above policy achieves its goal by allowing the user to separately authorize the use of the following operations with the CAM policy.

- All operations in TencentDB that begin with "Describe".
- All operations in VPC that begin with "Describe", "Inquiry", or "Get".
- All operations in security groups that begin with "DescribeSecurityGroup".
- All operations in COS that begin with "List", "Get", and "Head" as well as the "OptionsObject" operation.
- All operations in the monitor.

**Policy for granting a user permission to use APIs not at the resource level**

To grant a user permission to use only APIs not at the resource level, implement the policy named QcloudCDBProjectToUser for the user.

Enter the policy management page. Click **Service Type** and select TencentDB for MySQL in the dropdown list. Then, you can see this policy in the results.

The policy syntax is as follows:

```json
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "cdb:BalanceRoGroupLoad",
            ],
            "resource": "*",
            "effect": "allow"
        },
        {
            "action": [
                "cos:List",
                "cos:Get",
                "cos:Head",
                "cos:OptionsObject"
            ],
            "resource": "*",
            "effect": "allow"
        },
        {
            "effect": "allow",
            "action": "monitor:*",
            "resource": "*"
        }
    ]
}
```
Policy for granting a user permission to manipulate a 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 "cdb-xxx" in Guangzhou.

```json
{
  "version": "2.0",
  "statement": [
    {
      "action": "cdb:*",
      "resource": "qcs::cdb:ap-guangzhou::instanceId/cdb-xxx",
      "effect": "allow"
    }
  ]
}
```
Policy for granting a user permissions to manipulate TencentDB instances in batches

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

```
{
    "version": "2.0",
    "statement": [
        {
            "action": "cdb:*",
            "resource": ["qcs::cdb:ap-guangzhou::instanceId/cdb-xxx", "qcs::cdb:ap-guangzhou::instanceId/cdb-yyy", "qcs::cdb:ap-beijing::instanceId/cdb-zzz"],
            "effect": "allow"
        }
    ]
}
```

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

To grant a user the permission to manipulate databases 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": "cdb:*",
            "resource": "qcs::cdb:ap-guangzhou::*",
            "effect": "allow"
        }
    ]
}
```

Custom policy

If preset policies cannot meet your requirements, you can create custom policies as shown below. If permission is granted by resource, for a TencentDB API operation that does not support authorization at the resource level, you can still authorize a user to perform it, but you must specify * as the resource element in the policy statement.
The syntax of a custom policy is as follows:

```json
{
    "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".
TencentDB Security Group

Last updated: 2020-05-26 17:29:20

Operation Scenarios

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 with the same network security isolation demands in one region can be put into the same security group, which is a logical group. TencentDB and CVM share the security group list and are matched with each other within the security group based on rules.

- TencentDB for MySQL security group currently only supports network access control for VPC and public networks but not the classic network.
- Security groups that currently support public network access are available only in the Guangzhou, Shanghai, Hong Kong (China), Beijing, Chengdu, Chongqing, Seoul, and Tokyo regions.
- As no outbound traffic is generated for TencentDB instances, outbound rules do not take effect for TencentDB.
- TencentDB for MySQL security groups support master instances, read-only instances, and disaster recovery instances.
- Security group is not supported for the TencentDB for MySQL Basic Edition.

Security Group Configuration for TencentDB

Step 1. Create a security group

1. Log in to the CVM Console.
2. Select Security Group on the left sidebar, select a region, and click Create.
3. In the pop-up dialog box, configure the following items and click OK.
   - Template: select an appropriate template based on the service to be deployed on the TencentDB instance in the security group, which simplifies the security group rule configuration, as shown below:

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open all ports</td>
<td>All ports are opened to the public and private networks. This may present security issues.</td>
<td>-</td>
</tr>
</tbody>
</table>
Open ports 22, 80, 443, and 3389 and the ICMP protocol are opened to the internet. All ports are opened to the private network. This template does not take effect for TencentDB.

<table>
<thead>
<tr>
<th>Port Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open 22, 80, 443, and 3389 and the ICMP protocol. All ports are opened to the private network.</td>
<td></td>
</tr>
</tbody>
</table>

- **Custom**
  - You can create a security group and then add custom rules. For detailed directions, please see "Step 2. Add a security group rule" below.

- **Name**: custom name of the security group.
- **Project**: the default project is selected by default. You can also select another one for easier management.
- **Remarks**: a short description of the security group for easier management.

### Step 2. Add a security group rule

1. On the Security Group page, click **Modify Rule** in the "Operation" column on the row of the security group for which to configure a rule.
2. On the security group rule page, click **Inbound Rules > Add Rule**.
3. In the pop-up dialog box, set the rule.
   - **Type**: "Custom" is selected by default. You can also choose another system rule template.
     - MySQL(3306) is recommended.
   - **Source**: traffic source (inbound rule) or destination (outbound rule). You need to specify one of the following options:

<table>
<thead>
<tr>
<th>Source/Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 address or IPv4 address range</td>
<td>In CIDR format (such as 203.0.113.0, 203.0.113.0/24, or 0.0.0.0/0, where 0.0.0.0/0 indicates all IPv4 addresses).</td>
</tr>
<tr>
<td>IPv6 address or IPv6 address range</td>
<td>In CIDR format (such as FF05::B5, FF05:B5::/60, ::/0, or 0::0/0, where ::/0 or 0::0/0 indicate all IPv6 addresses).</td>
</tr>
</tbody>
</table>
| ID of referenced security group. You can reference the ID of: | - Current security group: CVM instance associated with the current security group.  
- Another security group: ID of another security group in the same region under the same project. |
| Reference IP address object or IP address group object in a parameter template. | - |

- **Protocol port**: enter the protocol type and port range or reference an IP address object or IP address group object in a parameter template.
To connect to TencentDB for MySQL, port 3306 must be opened.

- Policy: "Allow" is selected by default.
  - Allow: traffic to this port is allowed.
  - Reject: data packets will be discarded without any response.
- Remarks: a short description of the rule for easier management.

4. Click Complete to finish adding the inbound rule.

Use cases

Scenario: you have created a TencentDB for MySQL instance and want to access it from a CVM instance.
Solution: when adding security group rules, select MySQL(3306) in Type to open port 3306. You can also allow all IPs or specified IPs (IP ranges) based on your actual needs so as to configure IP sources that can access TencentDB for MySQL through CVM.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Source</th>
<th>Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>MySQL(3306)</td>
<td>All IP: 0.0.0.0/0 Specified IP: enter the specified IPs or IP ranges</td>
<td>TCP: 3306</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Step 3. Configure a security group

A security group is an instance-level firewall provided by Tencent Cloud for controlling inbound traffic of TencentDB. You can associate a security group with an instance when purchasing it or later in the console.

Currently, security groups can be configured only for TencentDB for MySQL instances in VPC.

1. Log in to the TencentDB for MySQL Console.
2. In the instance list, select the instance for which to configure a security group and click Manage in the "Operation" column to enter the instance management page.
4. In the pop-up dialog box, select the security group to be bound and click OK.

Security Group Rule Import

1. On the Security Group page, click the ID/name of the target security group.
2. On the inbound rules or outbound rules tab, click Import Rule.
3. In the pop-up dialog box, select an edited inbound/outbound rule template file and click Start Import.
If there are existing rules in the security group, export them before importing new rules. Existing rules are overwritten after importing.

Security Group Clone

1. On the Security Group page, select a security group and click **More > Clone** in the "Operation" column.
2. In the pop-up dialog box, select the target region and target project and click **OK**. If the new security group needs to be associated with a CVM instance, do so by managing the CVM instances in the security group.

Security Group Deletion

1. On the security group page, select the security group to be deleted and click **More > Delete** in the "Operation" column.
2. Click **OK** in the pop-up dialog box. If the current security group is associated with a CVM instance, it must be disassociated before it can be deleted.
Network Switch

Last updated: 2020-05-26 16:53:53

Operation Scenarios

Tencent Cloud supports **classic network and VPC**, which are capable of offering a diversity of smooth services. On this basis, we provide more flexible services as shown below to help you manage network connectivity with ease.

- **Network switch**
  - Switch from classic network to VPC: a single TencentDB instance can be switched from classic network to VPC.
  - Switch from VPC A to VPC B: a single TencentDB instance can be switched from VPC A to VPC B.

- **Custom IP**

Notes

- Switching the network may cause the change of instance's private IP. The original IP will become invalid after 24 hours by default. Please modify the instance IP on the client promptly. If the repossession time for the old IP address is set to 0 hours, the old IP address will be reposessed immediately after the network switch.
- You can only select VPC and subnet in the region and AZ of the instance.
- The switch from classic network to VPC is irreversible. After the switch to a VPC, the TencentDB instance cannot communicate with Tencent Cloud services in another VPC or classic network.
- Instances where the data replication mode is strong sync replication do not support the above-mentioned switches.

Directions

1. Log in to the TencentDB for MySQL Console. In the instance list, click the instance name or **Manage** in the "Operation" column to enter the instance details page.
2. According to the type of network switch, click **Switch to VPC** or **Change Network** after "Network" in the basic instance information section.
3. In the pop-up dialog box, select a VPC and corresponding subnet and click **OK**.

- If there is no IP address specified, one will be automatically assigned by the system.
You are recommended to select the VPC where the CVM instance resides; otherwise, the CVM instance will not be able to access TencentDB for MySQL over the private network, unless a peering connection or a CCN instance is created between the two VPCs.

- **Switch from classic network to VPC**
- **Switch from VPC A to VPC B**

4. Return to the instance details page where you can view the network of the instance.
Monitoring and Alarm

Monitoring Feature

Last updated: 2020-06-09 11:19:14

To make it easier for you to view and stay up to date with how instances work, TencentDB for MySQL provides a wide variety of performance monitoring metrics and convenient monitoring features (custom view, time comparison, merged monitoring metrics, etc). You can log in to the TencentDB for MySQL Console and view them in Instance Monitoring on the instance management page.

- You can also view instance monitoring metrics by calling the GetMonitorData API in Cloud Monitor.
- If the number of tables in a single instance exceeds one million, database monitoring may be affected. Please control this value appropriately and make sure that it is below one million.

Types of Instances for Monitoring

TencentDB for MySQL master, read-only, and disaster recovery instances can be monitored, and each instance is provided with a separate monitoring view for easy query.

Types of Monitoring

Four types of monitoring are available for TencentDB for MySQL: resource monitoring, engine monitoring (general), engine monitoring (extended), and deployment monitoring. You can view the metrics of different monitoring types to gain a quick and accurate understanding of how instances perform and operate.

- **Resource monitoring** provides monitoring data of CPU, memory, disk, and network.

- **Engine monitoring (general)** provides monitoring data of the number of connections, locks, hotspot tables, and slow queries, helping you troubleshoot issues and optimize the performance.

- **Engine monitoring (extended)** provides a wider variety of engine-related monitoring metrics so as to assist you in identifying existing or potential database problems as much as possible.
• **Deployment monitoring** provides monitoring metrics with regard to master-slave delay. It divides into master and slave:

  • Master deployment monitoring: when the monitored instance is a master instance which is not a slave of any instance, replicating relevant monitoring data from the master won’t work, and the IO and SQL threads are disabled. Replicating relevant monitoring data can work and the IO and SQL threads can be enabled only when the monitored instance is a disaster recovery or a read-only instance.

  • Slave deployment monitoring: the master instance and disaster recovery instance in High-Availability Edition come in a master/slave architecture by default. As a result, replicating relevant monitoring data from the slave can work only when the monitored instance is a master or disaster recovery instance. Such data can be used to reflect the delay distance and time between the master or disaster recovery instance and its hidden slave nodes. You are recommended to keep an eye out for the relevant monitoring data of the slave. If the master or disaster recovery instance fails, its monitored hidden slave nodes can be promoted into the master instance quickly.

Monitoring Granularity

TencentDB for MySQL has adopted an adaptive policy for monitoring granularity since August 11, 2018, which means that you cannot select a monitoring granularity as desired for the time being. The adaptive policy is as follows:
<table>
<thead>
<tr>
<th>Time Span</th>
<th>Monitoring Granularity</th>
<th>Adaptation Description</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0h, 4h]</td>
<td>5 seconds</td>
<td>The time span is below 4 hours, and the monitoring granularity is 5 seconds</td>
<td>1 day</td>
</tr>
<tr>
<td>(4h, 2d]</td>
<td>1 minute</td>
<td>The time span is above 4 hours but below 2 days, and the monitoring granularity is 1 minute</td>
<td>15 days</td>
</tr>
<tr>
<td>(2d, 10d]</td>
<td>5 minutes</td>
<td>The time span is above 2 days but below 10 days, and the monitoring granularity is 5 minutes</td>
<td>31 days</td>
</tr>
<tr>
<td>(10d, 30d]</td>
<td>1 hour</td>
<td>The time span is above 10 days but below 30 days, and the monitoring granularity is 1 hour</td>
<td>62 days</td>
</tr>
</tbody>
</table>

Currently, you can view monitoring data of TencentDB for MySQL in the last 30 days.

**Monitoring Metrics**

Cloud Monitor provides the following monitoring metrics for TencentDB for MySQL instances in the instance dimension:

For more information on how to use TencentDB monitoring metrics, please see the [GetMonitorData API](#) in Cloud Monitor.

<table>
<thead>
<tr>
<th>Metric Name</th>
<th>Metric</th>
<th>Unit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations/sec</td>
<td>qps</td>
<td>Operations/second</td>
<td>Number of SQL statements executed by the database per second (including insert, select, update, delete, and replace). QPS mainly represents the actual processing capability of the TencentDB instance</td>
</tr>
<tr>
<td>Metric Name</td>
<td>Metric</td>
<td>Unit</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Slow Queries</td>
<td>slow_queries</td>
<td>-</td>
<td>Number of queries that take more than \textit{long_query_time} second(s) to be executed</td>
</tr>
<tr>
<td>Full Table Scans</td>
<td>select_scan</td>
<td>Scans/second</td>
<td>Number of full-table scans executed per second</td>
</tr>
<tr>
<td>Queries</td>
<td>select_count</td>
<td>Queries/second</td>
<td>Number of queries executed per second</td>
</tr>
<tr>
<td>Updates</td>
<td>com_update</td>
<td>Updates/second</td>
<td>Number of updates executed per second</td>
</tr>
<tr>
<td>Deletions</td>
<td>com_delete</td>
<td>Deletions/second</td>
<td>Number of deletions executed per second</td>
</tr>
<tr>
<td>Insertions</td>
<td>com_insert</td>
<td>Insertions/second</td>
<td>Number of insertions executed per second</td>
</tr>
<tr>
<td>Overwrites</td>
<td>com_replace</td>
<td>Overwrites/second</td>
<td>Number of overwrites executed per second</td>
</tr>
<tr>
<td>Total Requests</td>
<td>queries</td>
<td>Requests/second</td>
<td>All executed SQL statements such as set and show.</td>
</tr>
<tr>
<td>Opened Connections</td>
<td>threads_connected</td>
<td>-</td>
<td>Number of currently open connections</td>
</tr>
<tr>
<td>Connection Utilization</td>
<td>connection_use_rate</td>
<td>%</td>
<td>Number of open connections/maximum connections</td>
</tr>
<tr>
<td>Query Utilization</td>
<td>query_rate</td>
<td>%</td>
<td>Actual QPS/recommended QPS</td>
</tr>
<tr>
<td>Used Space Disk</td>
<td>real_capacity</td>
<td>MB</td>
<td>This includes only MySQL's data directories but not logs such as binlog, relaylog, undolog, errorlog, and slowlog</td>
</tr>
</tbody>
</table>

©2013-2019 Tencent Cloud. All rights reserved.
<table>
<thead>
<tr>
<th>Metric Name</th>
<th>Metric</th>
<th>Unit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Occupied Disk Space</td>
<td>capacity</td>
<td>MB</td>
<td>This includes MySQL's data directories and logs such as binlog, relaylog, undolog, errorlog, and slowlog</td>
</tr>
<tr>
<td>Sent Data Volume</td>
<td>bytes_sent</td>
<td>MB/s</td>
<td>Number of bytes sent per second</td>
</tr>
<tr>
<td>Received Data Volume</td>
<td>bytes_received</td>
<td>MB/s</td>
<td>Number of bytes received per second</td>
</tr>
<tr>
<td>Disk Utilization</td>
<td>volume_rate</td>
<td>%</td>
<td>Used disk space/purchased instance space</td>
</tr>
<tr>
<td>Query Cache Hit Rate</td>
<td>qcache_hit_rate</td>
<td>%</td>
<td>Query cache hit rate</td>
</tr>
<tr>
<td>Query Cache Utilization</td>
<td>qcache_use_rate</td>
<td>%</td>
<td>Query cache utilization</td>
</tr>
<tr>
<td>Table Locks Awaited</td>
<td>table_locks_waited</td>
<td>Locks/second</td>
<td>Number of table locks due to the failure to obtain tables immediately</td>
</tr>
<tr>
<td>Temp Tables</td>
<td>created_tmp_tables</td>
<td>Tables/second</td>
<td>Number of temp tables created per second.</td>
</tr>
<tr>
<td>InnoDB Cache Hit Rate</td>
<td>innodb_cache_hit_rate</td>
<td>%</td>
<td>InnoDB cache hit rate</td>
</tr>
<tr>
<td>InnoDB Cache Utilization</td>
<td>innodb_cache_use_rate</td>
<td>%</td>
<td>cache utilization</td>
</tr>
<tr>
<td>InnoDB Disk Reads</td>
<td>innodb_os_file_reads</td>
<td>Reads/second</td>
<td>Number of reads to disk files by the InnoDB engine per second</td>
</tr>
<tr>
<td>InnoDB Disk Writes</td>
<td>innodb_os_file_writes</td>
<td>Writes/second</td>
<td>Number of writes to disk files by the InnoDB engine per second</td>
</tr>
<tr>
<td>Metric Name</td>
<td>Metric</td>
<td>Unit</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InnoDB fsync Count</td>
<td>innodb_os_fsyncs</td>
<td>Calls/second</td>
<td>Number of calls of the fsync function by the InnoDB engine per second</td>
</tr>
<tr>
<td>InnoDB Opened Tables</td>
<td>innodb_num_open_files</td>
<td>-</td>
<td>Number of tables currently opened by the InnoDB engine</td>
</tr>
<tr>
<td>MyISAM Cache Hit Rate</td>
<td>key_cache_hit_rate</td>
<td>%</td>
<td>MyISAM engine cache hit rate</td>
</tr>
<tr>
<td>MyISAM Cache Utilization</td>
<td>key_cache_use_rate</td>
<td>%</td>
<td>MyISAM engine cache utilization</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>cpu_use_rate</td>
<td>%</td>
<td>Overuse of idle resources is permitted. The CPU utilization may exceed 100%</td>
</tr>
<tr>
<td>MEM Utilization</td>
<td>memory use rate</td>
<td>%</td>
<td>Overuse of idle resources is permitted. The memory utilization may exceed 100%</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>memory use</td>
<td>MB</td>
<td>Overuse of idle resources is permitted. The actual memory usage may exceed the purchased specification</td>
</tr>
<tr>
<td>Temp Files</td>
<td>created_tmp_files</td>
<td>Files/second</td>
<td>Number of temp files created per second</td>
</tr>
<tr>
<td>Opened Tables</td>
<td>opened_tables</td>
<td>-</td>
<td>Number of opened tables</td>
</tr>
<tr>
<td>Submissions</td>
<td>com_commit</td>
<td>Commits/second</td>
<td>Number of submissions per second</td>
</tr>
<tr>
<td>Rollbacks</td>
<td>com_rollback</td>
<td>Rollback/second</td>
<td>Number of rollbacks per second</td>
</tr>
<tr>
<td>Metric Name</td>
<td>Metric</td>
<td>Unit</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Created Threads</td>
<td>threads_created</td>
<td>-</td>
<td>Number of threads created to process connections</td>
</tr>
<tr>
<td>Running Threads</td>
<td>threads_running</td>
<td>-</td>
<td>Number of active (non-idle) threads</td>
</tr>
<tr>
<td>Max Connections</td>
<td>max_connections</td>
<td>-</td>
<td>Maximum number of connections</td>
</tr>
<tr>
<td>Temp Disk Tables</td>
<td>created_tmp_disk_tables</td>
<td>Tables/second</td>
<td>Number of temp disk tables created per second</td>
</tr>
<tr>
<td>Requests of Reading Next Row</td>
<td>handler_read_rnd_next</td>
<td>Requests/second</td>
<td>Number of requests to read the next row per second</td>
</tr>
<tr>
<td>Internal Rollbacks</td>
<td>handler_rollback</td>
<td>Rollbacks/second</td>
<td>Number of transaction rollbacks per second</td>
</tr>
<tr>
<td>Internal Submissions</td>
<td>handler_commit</td>
<td>Commits/second</td>
<td>Number of transaction commits per second</td>
</tr>
<tr>
<td>InnoDB Empty Pages</td>
<td>innodb_buffer_pool_pages_free</td>
<td>-</td>
<td>Number of empty memory pages in the InnoDB engine</td>
</tr>
<tr>
<td>Total InnoDB Pages</td>
<td>innodb_buffer_pool_pages_total</td>
<td>-</td>
<td>Total number of memory pages occupied by the InnoDB engine</td>
</tr>
<tr>
<td>InnoDB Logical Reads</td>
<td>innodb_buffer_pool_read_requests</td>
<td>Reads/second</td>
<td>Number for logical read requests completed by the InnoDB engine per second</td>
</tr>
<tr>
<td>InnoDB Physical Reads</td>
<td>innodb_buffer_pool_reads</td>
<td>Reads/second</td>
<td>Number for physical read requests completed by the InnoDB engine per second</td>
</tr>
<tr>
<td>Metric Name</td>
<td>Metric</td>
<td>Unit</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InnoDB Reads</td>
<td>innodb_data_read</td>
<td>Bytes/s</td>
<td>Number of bytes read by the InnoDB engine per second</td>
</tr>
<tr>
<td>Total InnoDB Reads</td>
<td>innodb_data_reads</td>
<td>Reads/second</td>
<td>Number of data reads completed by the InnoDB engine per second</td>
</tr>
<tr>
<td>Total InnoDB Writes</td>
<td>innodb_data_writes</td>
<td>Writes/second</td>
<td>Number of data writes completed by the InnoDB engine per second</td>
</tr>
<tr>
<td>InnoDB Writes</td>
<td>innodb_data_written</td>
<td>Bytes/s</td>
<td>Number of bytes written by the InnoDB engine per second</td>
</tr>
<tr>
<td>InnoDB Rows Deleted</td>
<td>innodb_rows_deleted</td>
<td>Rows/second</td>
<td>Number of rows deleted in the InnoDB engine per second</td>
</tr>
<tr>
<td>InnoDB Rows Inserted</td>
<td>innodb_rows_inserted</td>
<td>Rows/second</td>
<td>Number of rows inserted in the InnoDB engine per second</td>
</tr>
<tr>
<td>InnoDB Rows Updated</td>
<td>innodb_rows_updated</td>
<td>Rows/second</td>
<td>Number of rows updated by the InnoDB engine per second</td>
</tr>
<tr>
<td>InnoDB Rows Read</td>
<td>innodb_rows_read</td>
<td>Rows/second</td>
<td>Number of rows read by the InnoDB engine per second</td>
</tr>
<tr>
<td>Average Lock Time of</td>
<td>innodb_row_lock_time_avg</td>
<td>Milliseconds</td>
<td>Average time of row lock in the InnoDB engine</td>
</tr>
<tr>
<td>InnoDB's Acquiring Rows</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InnoDB Row Lock Waits</td>
<td>innodb_row_lock_waits</td>
<td>Locks/second</td>
<td>Number of row locks waited by the InnoDB engine per second</td>
</tr>
<tr>
<td>Metric Name</td>
<td>Metric</td>
<td>Unit</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unused Blocks in Key Cache</td>
<td>key_blocks_unused</td>
<td>-</td>
<td>Number of unused blocks in the key cache in the MyISAM engine</td>
</tr>
<tr>
<td>Used Blocks in Key Cache</td>
<td>key_blocks_used</td>
<td>-</td>
<td>Number of used blocks in the key cache in the MyISAM engine</td>
</tr>
<tr>
<td>Data Blocks Read by Key Cache</td>
<td>key_read_requests</td>
<td>Reads/second</td>
<td>Number of block reads from the key cache by the MyISAM engine per second</td>
</tr>
<tr>
<td>Data Blocks Read by Disks</td>
<td>key_read</td>
<td>Reads/second</td>
<td>Number of block reads from the disk by the MyISAM engine per second</td>
</tr>
<tr>
<td>Data Blocks Written into Key Cache</td>
<td>key_write_requests</td>
<td>Writes/second</td>
<td>Number of block writes to the key cache by the MyISAM engine per second</td>
</tr>
<tr>
<td>Data Blocks Written into Disks</td>
<td>key_write_requests</td>
<td>Writes/second</td>
<td>Number of block writes to the disk by the MyISAM engine per second</td>
</tr>
<tr>
<td>Master-Slave Delay Distance</td>
<td>master_slave_sync_distance</td>
<td>MB</td>
<td>Master-slave binlog delay</td>
</tr>
<tr>
<td>Master-Slave Delay Time</td>
<td>seconds_behind_master</td>
<td>Seconds</td>
<td>Master-slave delay time</td>
</tr>
<tr>
<td>IO Thread Status</td>
<td>slave_io_running</td>
<td>Status value (0: yes, 1: no, 2: connecting)</td>
<td>IO thread status</td>
</tr>
<tr>
<td>SQL Thread Status</td>
<td>slave_sql_running</td>
<td>Status value (0: yes, 1: no)</td>
<td>SQL thread status</td>
</tr>
</tbody>
</table>
Alarming Feature

Last updated : 2020-04-29 17:22:54

Operation Scenarios

You can create an alarm to warn you of the status change of a cloud product and send related messages. The created alarm determines whether an alarm-related notification needs to be triggered according to the comparison results between a monitoring metric and a specific threshold at every interval. You can take appropriate precautionary or remedial measures in a timely manner when the alarm is triggered. Therefore, properly created alarms can help you improve the robustness and reliability of your applications. For more information on alarms, please see Alarm Configuration in Cloud Monitor.

If you want to send an alarm message for a specific status of a product, you need to create an alarm policy first, which is composed of three mandatory components: name, type, and alarm trigger condition. Each alarm policy is a set of alarm trigger conditions in the logical OR relationship, i.e., as long as one of the trigger conditions is satisfied, the alarm will be triggered. The alarm notification will be sent to all users associated with the alarm policy. They can take appropriate actions after receiving the notification.

Directions

Creating alarm policy

1. Log in to the Cloud Monitor Console and select Alarm Configuration > Alarm Policy on the left sidebar.
2. In the alarm policy list, click Create.
3. Set the policy name, policy type, target product, alarm object, and trigger condition.
   - Policy type: it divides into master monitoring and slave monitoring, which are applicable to different types of instances.
     - Deploy monitoring on the master: when the monitored instance is a master instance which is not a slave of any instance, replicating relevant monitoring data from the master won't work, and the IO and SQL threads are disabled. Replicating relevant monitoring data can work and the IO and SQL threads can be enabled only when the monitored instance is a disaster recovery or a read-only instance.
Deploy monitoring on the slave: the master instance and disaster recovery instance in high-availability edition come in a master/slave architecture by default. As a result, replicating relevant monitoring data from the slave can work only when the monitored instance is a master or disaster recovery instance. Such data can be used to reflect the delay distance and time between the master or disaster recovery instance and its hidden slave nodes. You are recommended to keep an eye out for the relevant monitoring data of the slave. If the master or disaster recovery instance fails, its monitored hidden slave nodes can be promoted into the master instance quickly.

- Trigger condition: it is a semantic condition composed of metric, comparison, threshold, statistical period, and duration. For example, if the metric is disk utilization, the comparison is >, the threshold is 80%, the statistical period is 5 minutes, and the duration is two statistical periods, then the data on disk utilization of a database will be collected once every five minutes, and an alarm will be triggered if the disk utilization exceeds 80% for two consecutive times.
- The object instance to be associated with can be found by selecting the region where the object is located or searching for the instance ID of the object.

4. After confirming that everything is correct, click **Complete**.

**Associating objects**

After the alarm policy is created, you can associate some alarm objects with it. When an alarm object satisfies an alarm trigger condition, an alarm notification will be sent.

1. In the alarm policy list, click the name of an alarm policy to enter the alarm policy management page.
2. Click **Add Object** on the alarm policy management page.
3. Select a desired Tencent Cloud product and click **Apply** to associate it with the alarm policy.
Setting alarm recipient

Alarm recipients are those who will receive alarm messages.

1. In the alarm policy list, click the name of an alarm policy.
2. On the alarm policy management page, select Alarm Recipient and click Edit.
3. Select the user group to be notified, set relevant options, and click Save.
Tag Overview

Overview

A tag is a key-value pair provided by Tencent Cloud to identify a resource in the cloud. For more information, see Tag Overview.
You can manage TencentDB for MySQL resources in a categorized manner by using tags in various dimensions such as business, purpose, and person-in-charge, making it easier to find the right resources. Tags have no semantic meaning for Tencent Cloud and are parsed and matches strictly based on strings. During the course of use, you only need to pay attention to applicable use limits. Below is a specific use case to show how a tag is used.

Case Background

A company owns 10 TencentDB for MySQL instances in Tencent Cloud. Distributed in three departments (ecommerce, gaming, and entertainment), these instances are used to serve internal business lines such as marketing, game A, game B, and post-production. The OPS owners of the three departments are John, Jane, and Harry, respectively.

Setting a Tag

To facilitate management, the company categorizes its TencentDB for MySQL resources with tags and defines the following tag key-value pairs.

<table>
<thead>
<tr>
<th>Tag Key</th>
<th>Tag Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Ecommerce, gaming, and entertainment</td>
</tr>
<tr>
<td>Business</td>
<td>Marketing, game A, game B, and post-production</td>
</tr>
<tr>
<td>OPS owner</td>
<td>John, Jane, and Harry</td>
</tr>
</tbody>
</table>

These tag keys/values are bound to TencentDB for MySQL instances in the following way:

<table>
<thead>
<tr>
<th>instance-id</th>
<th>Department</th>
<th>Business</th>
<th>OPS Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdb-abcdef1</td>
<td>Ecommerce</td>
<td>Marketing</td>
<td>Harry</td>
</tr>
<tr>
<td>cdb-abcdef2</td>
<td>Ecommerce</td>
<td>Marketing</td>
<td>Harry</td>
</tr>
<tr>
<td>cdb-abcdef3</td>
<td>Gaming</td>
<td>Game A</td>
<td>John</td>
</tr>
</tbody>
</table>
### Using a Tag

For more information on how to create and delete a tag, see [Getting Started with Tags](#).

For more information on how to edit a tag in TencentDB for MySQL, see [Editing a Tag](#).

<table>
<thead>
<tr>
<th>instance-id</th>
<th>Department</th>
<th>Business</th>
<th>OPS Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdb-abcdef3</td>
<td>Gaming</td>
<td>Game B</td>
<td>John</td>
</tr>
<tr>
<td>cdb-abcdef4</td>
<td>Gaming</td>
<td>Game B</td>
<td>Game B</td>
</tr>
<tr>
<td>cdb-abcdef5</td>
<td>Gaming</td>
<td>Game B</td>
<td>Game B</td>
</tr>
<tr>
<td>cdb-abcdef6</td>
<td>Gaming</td>
<td>Game B</td>
<td>Jane</td>
</tr>
<tr>
<td>cdb-abcdef7</td>
<td>Gaming</td>
<td>Game B</td>
<td>Jane</td>
</tr>
<tr>
<td>cdb-abcdef8</td>
<td>Entertainment</td>
<td>Post-production</td>
<td>Harry</td>
</tr>
<tr>
<td>cdb-abcdef9</td>
<td>Entertainment</td>
<td>Post-production</td>
<td>Harry</td>
</tr>
<tr>
<td>cdb-abcdef10</td>
<td>Entertainment</td>
<td>Post-production</td>
<td>Harry</td>
</tr>
</tbody>
</table>
You can edit resource tags by the following steps.

### Editing the tag of a single instance

1. Log in to the TencentDB for MySQL Console and select **Instance List** on the left sidebar.
2. Select **More > Edit Tag** in the "Operation" column of the instance whose tag you want to edit.
3. In the pop-up dialog box, add, modify, or delete a tag, and click **OK**.

### Editing the tags of multiple instances

1. Select the instances whose tags you want to edit from the instance list, and click **More > Edit Tag** at the top of the list.
2. In the pop-up dialog box, add, modify, or delete tags, and click **OK**.
Operation Logs

Last updated: 2020-03-18 10:49:41

Operation Scenarios

An 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 administrator (DBA) analyzes slow query statements and finds out the reasons why slow queries occur is known as "slow query analysis".

TencentDB for MySQL High-Availability Edition and Single-Node High-IO Edition instances provide an operation log management feature to help you quickly locate faults and issues. You can view the slow log details, error log details, rollback logs of an instance and download slow logs on the operation logs page in the console.

You can also view and download database logs on the command line interface (CLI) or through TencentDB APIs. For more information, please see Querying Backup Logs and Querying Binary Logs.

Notes on Slow Queries in MySQL

- **long_query_time**: slow query threshold parameter down to the microsecond level. The default value is 10s. When an SQL statement takes more time to execute, it will be recorded in a slow log.
  - When the `long_query_time` parameter is adjusted, existing slow logs will not be affected. For example, if the slow log threshold parameter is 10s, slow logs will be reported for exceeding queries; after this value is modified to 1s, the previously reported logs will still be displayed.
- **log_queries_not_using_indexes**: whether to log unindexed queries. Default value: OFF.

Directions

1. Log in to the TencentDB for MySQL Console.

2. In the instance list, click an instance name or Manage in the "Operation" column to enter the instance management page.

3. Go to the Operation Logs page, on which you can view the slow log details, error log details, and rollback logs of the instance and download slow logs.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slow log details</td>
<td>Records SQL statements that took more than 10s to execute in the database in the past month</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Slow log download</td>
<td>Provides the ability to download slow logs</td>
</tr>
<tr>
<td>Error log details</td>
<td>Records logs of database execution errors</td>
</tr>
<tr>
<td>Rollback logs</td>
<td>Records the status and progress of rollback tasks</td>
</tr>
</tbody>
</table>

4. On the **Slow Log Download** page, you can click **Download** in the "Operation" column to download slow logs.

5. In the pop-up dialog box, you can click **Local Download** to download directly. You can also choose to copy the download address, log in to a Linux CVM instance in the same VPC as the TencentDB instance, and use the `wget` command for download.

   - `wget` command format: `wget -c 'log file download address' -O custom filename.log`
   - Below is an example:

     ```
     ```

   - Logs with a size of 0 KB cannot be downloaded.