TencentDB for TcaplusDB

Operation Guide

Contact Us

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

Contents

Operation Guide
Managing Cluster and Table Group
Changing cluster connection password

Last updated: 2024-10-15 17:18:11

Overview

This document describes how to change a cluster's connection password in the TcaplusDB Console and update the expiration time of the old password.

Prerequisites

You have created a cluster and a table group. For more information, please see Creating Cluster and Creating Table Group.

Directions

Changing connection password

1. Go to the Cluster List page, at the connection password of the cluster, click **Change Password**, in the pop-up dialog box, enter the old password, new password, and confirm the new password, then click **Confirm**.

> **Note**
> For delayed modification, choose **Update Password** and select the expiration time of the old password.

Search for the required CAM policy as needed, and click to complete policy association.

2. Once the request is successfully submitted, the expiration time of the old password will be displayed on the cluster details page, before which the old password will remain valid and you cannot submit another request to update the password.

Updating old password expiration time

> **Note**
> Before the old password expires, you can update its expiration time to shorten or extend the period before replacing it.

1. Go to the Cluster List page, at the connection password of the cluster, click **Change Password**, in the pop-up dialog box, change the expiration time, then click **Confirm**.
- **Old Password**: old password that will expire, i.e., the old password you entered when you changed the connection password.
- **New Password**: new password that has not taken effect yet, i.e., the new password you entered when you changed the connection password.
- **Delayed Modification**: choose **Update Old Password Expiration Time**.
- **Old Password Expiration Time**: select a new expiration time for the old password.
2. Return to the cluster details page and you will see that the expiration time of the old password has been updated.

> **Note**
> After the expiration time, the old password will expire, and you can submit a new request to update the password.

Modifying cluster name

Last updated: 2024-10-15 17:18:33

Overview

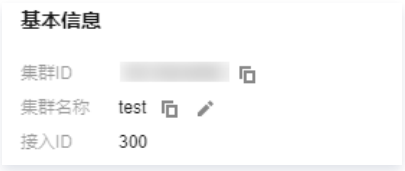
This document describes how to rename a cluster in the TcaplusDB Console.

Prerequisites

You have created a cluster and a table group. For more information, please see Creating Cluster and Creating Table Group.

Directions

1. Enter the Cluster List page, click a cluster ID to enter the cluster details page.
2. Click the modify button next to the Cluster Name to rename the cluster. The new cluster name must be unique under the account.



3. In the pop-up Modify Cluster Name dialog box, enter a new cluster name and click **Confirm**.

Modifying table group name

Last updated：2024-10-15 17:18:56

Overview

This document describes how to rename a table group in the TcaplusDB Console.

Prerequisites

You have created a cluster and a table group. For more information, please see Creating Cluster and Creating Table Group.

Directions

1. Enter the Table Group List, select **Operate** column's **More** > **Modify**.
2. In the pop-up dialog, modify the table group name, click **Modify Table Group**. Please ensure it does not duplicate the name of another table group in the same cluster.

Backing up Cluster and Table Group

Last updated: 2024-10-15 17:19:14

This article introduces how to back up clusters and table groups through the TcaplusDB console.

Prerequisites

Clusters and table groups have been created respectively. For more information, please see:

- Create a Cluster
- Creating Table Group

Backup settings

Cluster

There are two types of clusters: exclusive resource clusters and non-exclusive resource clusters. They differ in the backup retention time settings. See below for details.

Exclusive Resource Cluster

In exclusive resource clusters, you can modify the data retention time and database transaction log retention time (defaults to 7 days if not modified). Ensure that the data backup retention time N days >= database transaction log backup retention time M days. Expired backups will be automatically deleted.

Non-Exclusive Resource Cluster

In non-exclusive resource clusters, the database transaction log retention time is fixed at 7 days and cannot be modified. Expired backups will be automatically deleted.
You can modify the data retention time N days (default is 7 days if not modified): If N <= 7 days, you can rollback to any point in time within N days; If N > 7 days, you can rollback to any point in time within the first 7 days, and after 7 days, only to the automatic backup (cold backup) points. Expired backups will be automatically deleted.

Cluster Settings Method

1. Go to Cluster List page, click **Operations** column **Backup Settings**.
2. In the pop-up Backup Settings dialog box, after modifying the backup retention time, click **Confirm**.

Table group

The retention time for the table group database streaming logs is fixed at 7 days and cannot be modified. After expiration, backups will be automatically deleted.
The data retention time can be modified to N days (if not modified, it will default to 7 days): When N <= 7 days, data can be rolled back to any point within N days; When N > 7 days, data can be rolled back to any point within the first 7 days, and only to the automatic backup (cold backup) point after 7 days. After expiration, backups will be automatically deleted.

Table Group Settings Method

1. Enter the Cluster List page, select the cluster to be operated on, then select the target table group, and in the target table group**Actions** column, choose **More** > **Backup Settings**.
2. In the pop-up Backup Settings dialog box, after modifying the backup retention time, click **Confirm**.

Priority of Backup Policy Effectiveness

The hierarchical relationship between cluster, table group, and table is Cluster → Table Group → Table. The priority of backup policy effectiveness in case of conflicts is: Table > Table Group > Cluster. For detailed effective strategies in case of backup policy conflicts, refer to the table below, where "✓" indicates the backup strategy has been configured for that level, and "-" indicates it has not.

Cluster Policy	Table Group Policy	Table Policy	Effective Policy
✓	-	-	Cluster Policy

–	✓	–	Table Group Policy
–	–	✓	Table Policy
✓	✓	–	Table Group Policy
✓	–	✓	Table Policy
✓	✓	✓	Table Policy

For example, if a cluster policy is set and there are three table groups (1, 2, 3) in the cluster, only table group 1 has a retention period set. Therefore, table group 1 will follow its own policy, while table groups 2 and 3 will inherit the cluster policy as they do not have individual policies set.
Similarly, a table will only follow a specific table policy if it is set; otherwise, it will inherit the policy from the cluster.

Automatic Backup

TcaplusDB automatically backs up the cluster and table groups from 02:00 to 06:00 every day.

Backup History

Go to the Table List page, click the table ID to enter the table backup page, and you can view the backup history in the **Data Backup List**.
Among them,

- There is only one way to back up clusters/table groups: automatic backup.
- The number of stored files indicates the number of files into which the data backup is divided.
- File size indicates the size of the backup file.
- Backup time indicates the time when the backup task was started.
- File expiration time indicates the time until which the backup file will be retained. The system will automatically delete the file after this time.
- Backup status shows the result of the backup task (success/failure).

Terminating Clusters

Last updated: 2024-10-15 17:19:50

Overview

This document describes how to terminate a cluster in the TcaplusDB Console.

Prerequisites

- The cluster has been created. Please see Creating a Cluster.
- There are no table groups and tables in the cluster.

Directions

> **Note**
> A cluster cannot be recovered once terminated, so please do so with caution.

1. Go to the Cluster List page, and in the **Operations** column of the desired cluster, click **Terminate**.

2. In the pop-up dialog, click **Confirm** to terminate the cluster. If the target cluster contains table groups, it cannot be terminated.

Terminating Table Group

Last updated: 2024-10-15 17:20:19

Overview

This document describes how to terminate a table group in the TcaplusDB Console.

Prerequisites

- To create a cluster and a table group, please refer to Creating Cluster and Creating Table Group.
- Make sure there are no tables in the table group. Please refer to Dropping Table.

Directions

1. Go to the Table Group List and in the **Operations** column of the desired table group, select **More** > **Terminate**.

2. In the pop-up dialog, click **Confirm** to terminate the table group. If the target table group contains any tables in a normal state or in the recycle bin, the table group cannot be terminated.

Managing Table
Viewing Table Information

Last updated: 2024-10-15 17:21:02

Overview

This document describes how to view table information in the TcaplusDB console.

Prerequisites

A table has been created, please see Create Table.

Directions

1. Go to the Table List page to view the information of the created tables, including Table ID, Table Status, Table Name, Cluster Name (ID), Table Group (ID), etc.
2. Click the table ID to enter the table management page and view table details.

- The **Table Details** page provides basic information about the table, network information, and reserved configuration information. Click the modify button next to "Remarks" to edit the remarks.
- The **Table Configuration** page provides the table field Definition information, Create Global Index.
- The **Table Monitoring** page offers Table Monitoring information. You can select monitoring data of different periods, granularities, and perform data comparisons across different time cycles.
- The **Table Rollback** page provides the Table Rollback feature.
- The **Table Buffer Writing** page allows you to enable or disable the table buffer writing state.

Modifying Table

Last updated：2024-10-15 17:21:26

Overview

This document describes how to modify a table in the TcaplusDB console. If you want to modify the structure definition of a table, you can do so by modifying the table under the condition that the new definition meets the TcaplusDB table modification rules.

Prerequisites

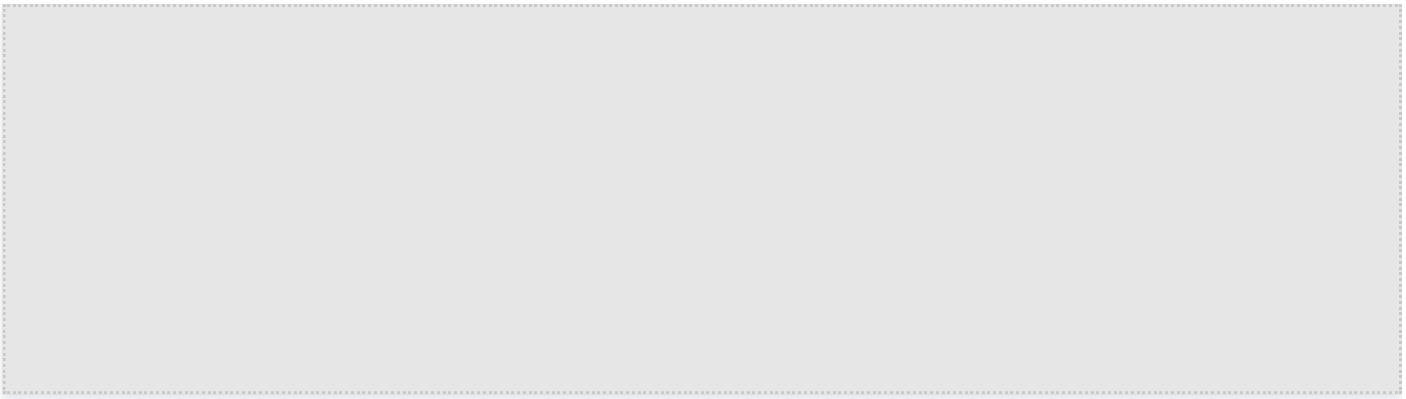
A table has been created, please see Create Table.

Directions

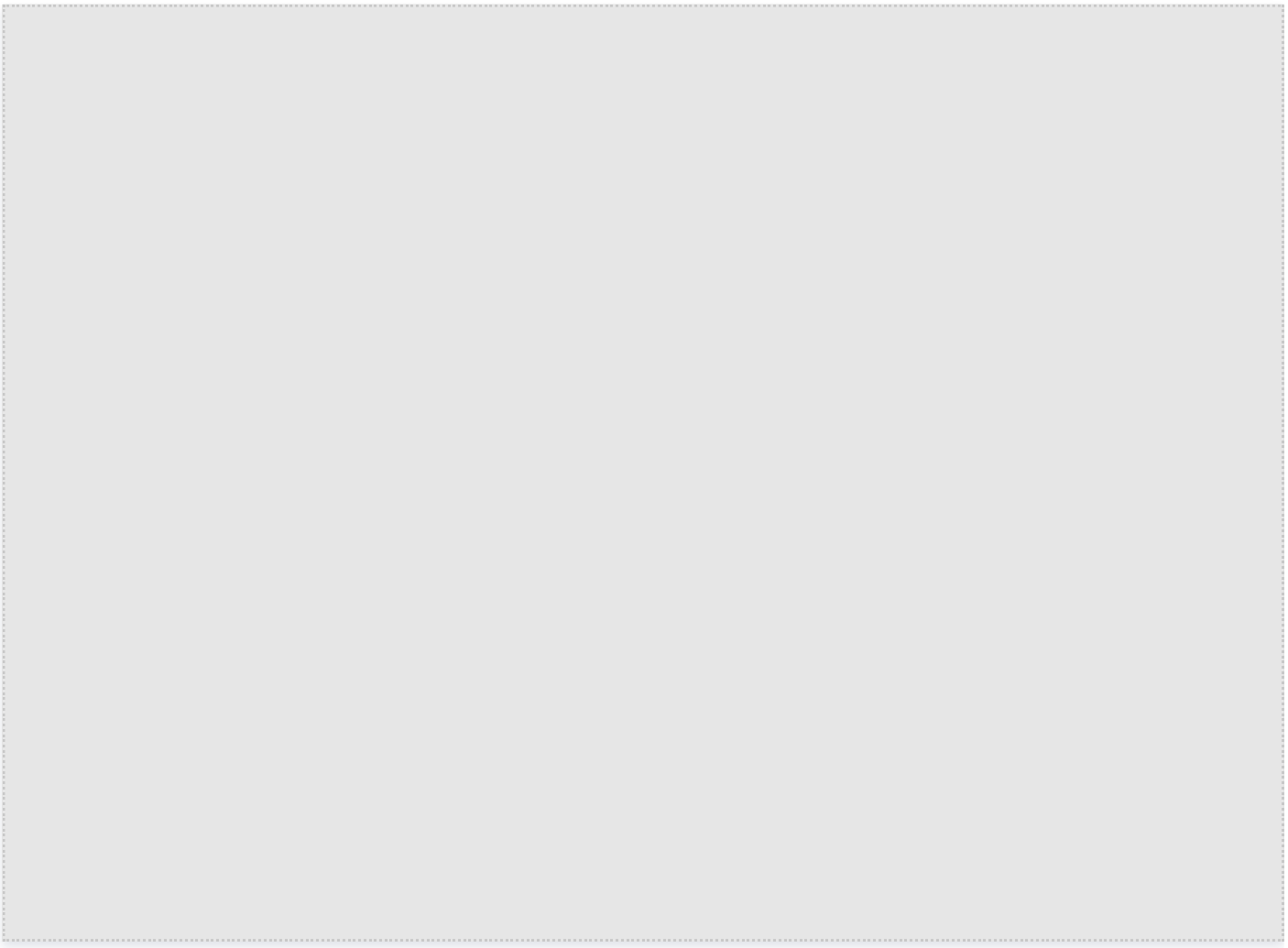
1. On the Table List page, select the desired table. In the **Operations** column, choose **More** > **Modify**, or select multiple tables and click **Batch Modify** at the top.
2. In the pop-up modification dialog box, upload or select a new table Definition file and click **Compare Differences**.

> **Note**
> - The primary key field cannot be deleted.
> - The name and type of the primary key field cannot be modified.
> - You cannot add new primary key fields.
> - A general field marked as required cannot be deleted.
> - The name and type of fields with the same identifier cannot be modified.
> - A new general field should be named according to the naming convention.

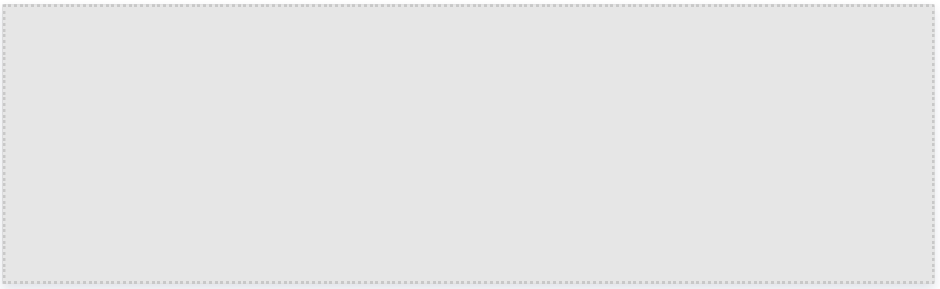
3. In the popup dialog, you can view the comparison results. If the new table Definition does not meet the TcaplusDB table modification rules, a prompt will appear here.



4. Click on the **Preview** of the comparison preview column to view the comparison between the new and old table structures.



5. After confirming there are no errors, click **OK** to submit the table modification request. A success message will be returned upon successful modification.



After modification, the new table structure can be viewed on the table configuration page.

Deleting a Table

Last updated: 2024-10-15 17:21:49

Overview

This document describes how to delete a table in the TcaplusDB console.

> **Note**
> If you delete a table, all of its data will be completely cleared and cannot be recovered.

Tables with the status RUNNING can be deleted. After deletion, the table will be moved to the Recycle Bin, and the data in the table will still exist.

Prerequisites

A table has been created, please see Create Table.

Directions

1. On the Table List page, select the desired table, in the **Operation** column, select **More** > **Delete**, or select multiple tables and click the **Batch Operation** > **Delete Table** at the top.
2. In the pop-up delete dialog box, click **OK**, and the table will be moved to the Recycle Bin.
3. In the left navigation bar, select **Recycle Bin**. In the Recycle Bin, you can perform a **Delete** operation to permanently remove the table from the system or a **Recover** operation to restore the table to the RUNNING state.

Clearing a Table

Last updated: 2024-10-15 17:22:11

Overview

This document describes how to clear table data in the TcaplusDB console.

> **Note**
> If you clear a table, all of its data will be completely cleared and cannot be recovered.

Prerequisites

A table has been created, please see Create Table.

Directions

1. On the Table List page, either locate the desired table and select **Operations** > **More** > **Cleanup**, or select multiple tables and choose **Batch Operations** > **Table Cleanup** at the top.
2. In the pop-up cleanup dialog, click **Confirm**.

3. After the cleanup is successful, a task link for this operation will be returned. Click the task ID in the result remarks column to view task details.

Expanding Table

Last updated：2024-10-15 17:30:41

Overview

This document describes how to modify the table quota in the TcaplusDB Console.

Prerequisites

A table has been created, please see Create Table.

Directions

1. On the Table List page, select the desired table, click **Operation** column **Scale-out**, or select multiple tables, then choose **Batch Operation** > **Batch Expansion** at the top.
2. In the popup dialog, confirm the target parameters for expansion, including capacity, reserved read, and reserved write, and click **OK**.

> **Note**
> Table expansion is to modify the table quota. After the modification, the backend will automatically reserve enough resources for the table and expand it automatically when the traffic of access to the table increases.

Backing up Table

Last updated: 2024-10-15 17:31:04

Overview

This document describes how to back up a table in the TcaplusDB Console.

Prerequisites

A table has been created, please see Create Table.

Directions

Backup settings

TcaplusDB table's database streaming logs have a fixed retention period of 7 days and cannot be modified. After expiration, the backup will be automatically deleted.
TcaplusDB allows users to set the data retention period to N days: If N <= 7 days, data can be rolled back to any point within N days; if N > 7 days, data can be rolled back to any point within the first 7 days, and thereafter only to the time of automatic backups (cold backups). After expiration, the backup will be automatically deleted.

Configuration Method

1. Go to the Table List page, click on the table ID to enter the table backup page, and click on **Backup Settings** in the upper left corner.
2. In the pop-up Backup Settings dialog box, after modifying the backup retention time, click **Confirm**.

Priority of Backup Policy Effectiveness

The hierarchical relationship among the cluster, table group, and table is: Cluster → Table Group → Table. When there is a conflict in backup policies, the priority of effectiveness is: Table > Table Group > Cluster. For details on the effective policy in case of conflict, see the table below, where "✓" means the backup policy is configured at that level, and "–" means it is not.

Cluster Policy	Table Group Policy	Table Policy	Effective Policy
✓	–	–	Cluster Policy
–	✓	–	Table Group Policy
–	–	✓	Table Policy
✓	✓	–	Table Group Policy
✓	–	✓	Table Policy
✓	✓	✓	Table Policy

For example, if a cluster policy is set and there are three table groups (1, 2, 3) under this cluster, only Table Group 1 has a set retention period. Therefore, Table Group 1 will follow its own policy, while Table Group 2 and Table Group 3, without specific policies, will inherit the cluster policy.
Similarly, a table will only follow a specific table policy if it is set; otherwise, it will inherit the policy from the cluster.

Automatic Backup

TcaplusDB automatically backs up tables daily from 02:00 to 06:00.

Manual Backups

If users need to back up tables manually, they can do so in the console.
Method 1:
1. Go to the Table List page, select multiple tables, and choose **Batch Operation** > **Backup Table** at the top.
2. In the pop-up Backup dialog box, after entering the remarks information, click **Confirm**.

Method 2:
Go to the Table List page, click the table ID to enter the table backup page, and click **Manual Backup** in the upper left corner to back up this table.

Backup History

Go to the Table List page, click the table ID to enter the table backup page, and you can view the backup history in the **Data Backup List**.
Among them,

- There are two types of backups: Automatic Backup/Manual Backup.
- The number of stored files indicates the number of files into which the data backup is divided.
- File size indicates the size of the backup file.
- Backup time indicates the time when the backup task was started.
- File expiration time indicates the time until which the backup file will be retained. The system will automatically delete the file after this time.
- Backup status shows the result of the backup task (success/failure).
- Operation: Only manual backup files can be deleted.

Rolling back Table

Last updated: 2024-10-15 17:31:26

Overview

This document describes how to roll back specified records in the TcaplusDB Console.

Prerequisites

A table has been created, please see Create Table.

Directions

1. Enter the Table List page, select the required table, and in the **Actions** column select **More** > **Rollback**.
2. In the pop-up dialog box, upload a .txt file containing the field values of the target record.
   The file format is as follows:
   For instance, if the user's table definition is as follows, the primary keys are openid, tconndid, timekey.

```
syntax = "proto2";
package myTcaplusTable;
import "tcaplusservice.optionv1.proto";
message tb_online {
 option(tcaplusservice.tcaplus_primary_key) = "openid,tconndid,timekey";
 required int32 openid = 1; //QQ Uin
 required int32 tconndid = 2;
 required string timekey = 3;
 required string gamesvrid = 4;
 optional int32 logintime = 5 [default = 1];
 repeated int64 lockid = 6 [packed = true];
 optional pay_info pay = 7;
 message pay_info {
     optional uint64 total_money = 1;
     optional uint64 pay_times = 2;
 }
}
```

   If you need to roll back the record with key openid=100, tconndid=1, timekey='123456', you need to prepare a file containing the keys as follows, with the first line being the primary key field names separated by spaces, and from the second line onwards, the primary key values to be rolled back:

```
openid tconndid timekey
100 1 123456
```

3. After key.txt has been uploaded, select the rollback time and click [Submit] to proceed.

Create Global Index

Last updated：2024-10-15 17:31:48

Overview

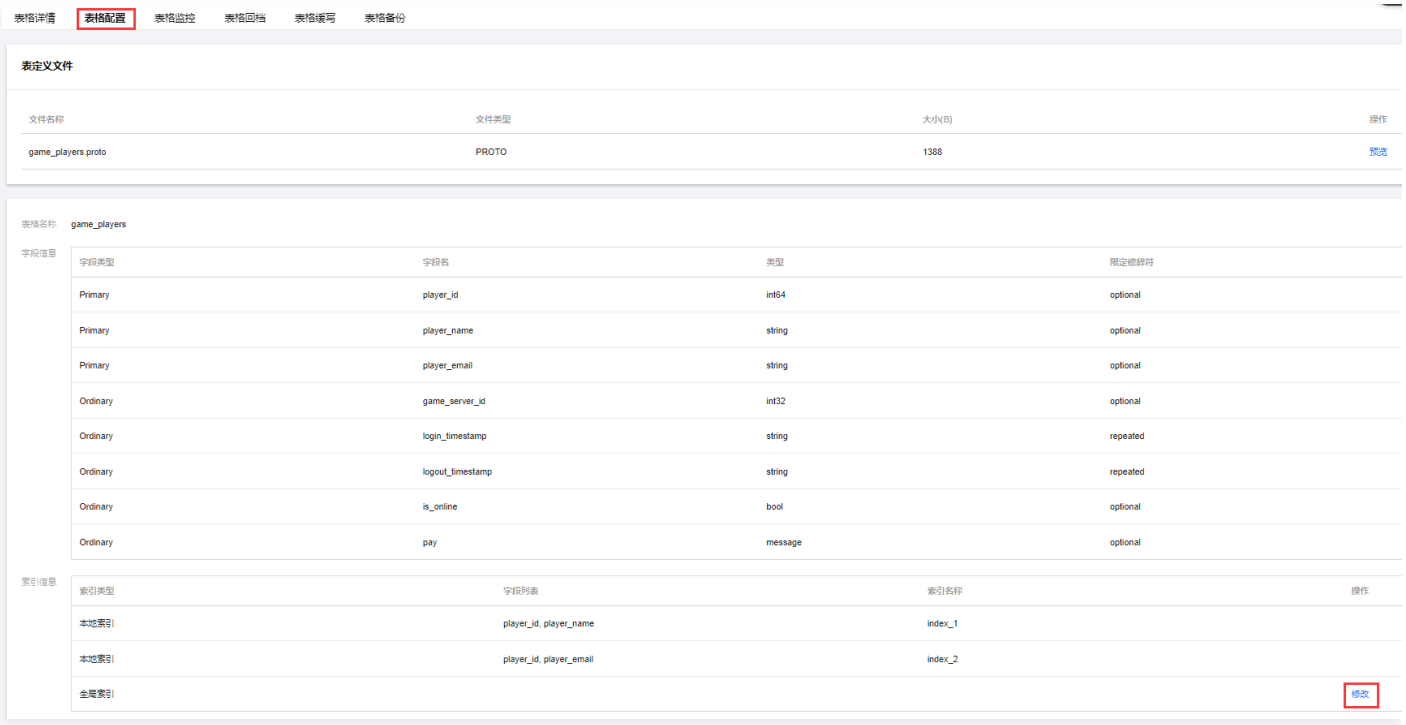
This article provides instructions on how to create a global index through the TcaplusDB console.

Prerequisites

A table has been created, please see Create Table.

Directions

1. Enter the Table List page, click the Table ID to enter the table management page.
2. Select the **Table Configuration** page, and in the Index Information section below the global index, click **Modification**.



3. Select and configure the corresponding global index fields, then click **Save**.

Monitoring and Alarms
Table Monitoring

Last updated: 2024-10-15 17:32:23

To facilitate users in viewing and understanding the operation information of TcaplusDB, TcaplusDB provides a variety of performance monitoring items. TcaplusDB supports table monitoring and offers an independent monitoring view for each table. Users can log in to the TcaplusDB Console, click the Table ID to enter the table management page and view the monitoring view on the **Table Monitoring** page.

Note
- You can also get instance monitoring metrics by calling the Cloud Database TcaplusDB Monitoring Data Interface in Cloud Monitor.
- Currently, you can view the monitoring data of TcaplusDB for the last 60 days.

Table Monitoring Metrics

Tencent Cloud Monitor provides the following monitoring metrics for TcaplusDB tables:

Metric Name (Chinese)	Metric Name (English)	Meaning of Metric	Metric Unit
Average error rate	Average Error Rate	Average percentage of table operation errors	%
General error rate	General Error Rate	Percentage of general table operation errors	%
Actual read capacity units	Actual Read Capacity Units	Number of actual read capacity units of table	Count/s
Average read latency	Average Read Latency	Average latency in data read	us
System error rate	System Error Rate	Percentage of system errors	%
Storage capacity	Storage Capacity	Storage capacity used by table	KBytes
Average write latency	Average Write Latency	Average latency in data write	us
Actual write capacity units	Actual Write Capacity Units	Number of actual write capacity units of table	Count/s

Configuring Alarm

Last updated: 2024-10-15 17:32:44

Overview

You can create alarm policies to trigger alarms and send relevant messages when the status of cloud products changes. The created alarms determine whether to trigger notifications based on the monitoring metrics compared to the given threshold at intervals.
When the status change triggers an alarm, you can take appropriate preventive or remedial measures in time. Therefore, properly creating alarm policies can help you enhance the robustness and reliability of manufacturing process control systems. For more information on alarms, see TCOP's alarm configurations.
To send an alarm for a specific status of a product, you need to create an alarm policy at first. An alarm policy is composed of three compulsory components, that is, the name, type and alarm triggering conditions. Each alarm policy is a set of alarm triggering conditions with the logical relationship "or", that is, as long as one of the conditions is met, an alarm will be triggered. The alarm will be sent to all users associated with the alarm policy. Upon receiving the alarm, the user can view the alarm and take appropriate actions in time.

> **Note**
> Make sure that you have set the default alarm recipient; otherwise, the default alarm policy of TencentDB won't be able to send notifications.

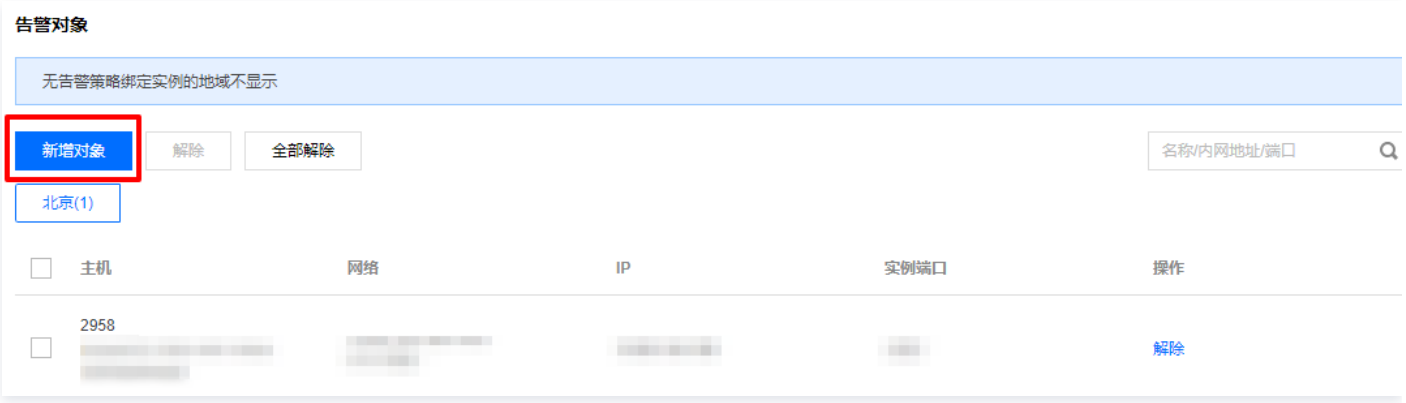
Directions

Creating Alarm Policy

1. log in to the TCOP Console, and select **alarm configurations** > **alarm policies** from the left navigation.
2. In the alarm policy list, click **Create**.
3. Set the policy name, policy type, target product, alarm object, and trigger condition.
   - Policy Type: select CDB | TDSQL.
   - Alarm Object: select all objects or specified tables. The object to be associated with can be found by selecting the region where the object is located or searching for the ID of the object.
   - Trigger Condition: an alarm trigger is a semantic condition consisting of metric, comparison relationship, threshold, statistical period, and duration.
   - Supported alarm channels include SMS, email, and WeChat notifications.
4. After confirming everything is correct, click **Complete**.

Associated Object

After the alarm policy is created, you can associate 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. In the alarm policy management page, click **Add Object**.



3. Select the cloud products to associate, click **Apply** to link the alarm objects.

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. In the alarm policy management page, in the **Alarm Recipients** column, click **Edit**.
3. Select the user group to be notified, set the relevant information, and click **Save** to complete the alarm recipient settings.

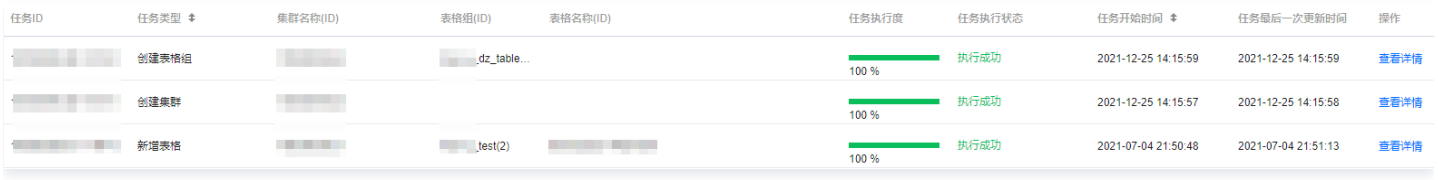
Task List

Last updated：2024-10-15 17:33:15

This document describes how to view a TcaplusDB task.

Viewing the task list

Most of the operations in TcaplusDB involve creating tasks. Enter the Task Management page to view the information of each task.



任务ID	任务类型	集群名称(ID)	表格组(ID)	表格名称(ID)	任务执行度	任务执行状态	任务开始时间	任务最后一次更新时间	操作
[redacted]	创建表格组	[redacted]	[redacted]dz_table...		100 %	执行成功	2021-12-25 14:15:59	2021-12-25 14:15:59	查看详情
[redacted]	创建集群	[redacted]			100 %	执行成功	2021-12-25 14:15:57	2021-12-25 14:15:58	查看详情
[redacted]	新增表格	[redacted]	[redacted]test(2)	[redacted]	100 %	执行成功	2021-07-04 21:50:48	2021-07-04 21:51:13	查看详情

View Task Details

In the task list, click **Operation** column and then **View Details** to see the detailed task information. The details include task ID, task type, cluster name (ID), table group (ID), table name (ID), task content, start time, last update time, execution progress, and result prompt.

CAM
CAM Overview

Last updated: 2024-10-15 17:33:48

Known issues

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

- The risk of your key being compromised is high since multiple users are sharing it.
- The access permission of other users is not under control. They can introduce security risks caused by misoperations.

Solution

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 the TcaplusDB service or resources. Therefore, you need to create a policy to grant the required permission to the sub-account.

CAM (Cloud Access Management, CAM) can help you securely and conveniently manage access to Tencent Cloud services and resources. You can use CAM to create sub-users, user groups, and roles, and control their access scope via policies. CAM supports SSO capabilities for users and roles. You can set up interoperability between enterprise users and Tencent Cloud according to specific management scenarios. Your initially created Tencent Cloud root account has full access to all Tencent Cloud services and resources within the account. It is recommended to safeguard the credentials of the root account, use sub-users or roles for daily access, and enable multi-factor authentication and scheduled key rotation.

When using CAM, you can associate a policy with a user or user group to allow or deny them to use specified resources to complete specified tasks. For more basic information about CAM policies, please see Policy Syntax.

If you do not need to manage CAM for TcaplusDB resources of sub-accounts, you can skip this chapter. Skipping these sections will not affect your understanding and use of the other parts of the document.

Quick Start

A CAM policy must either allow or deny one or more TcaplusDB operations. You must also specify which resources can be used for the operations (it can be all resources or part of the resources for some operations), and the policy can include conditions where the resources can be used.

Some TencentCloud API operations for TcaplsuDB do not support resource-level permissions, which means that you cannot specify resources when using those API operations but must specify all resources.

Task	Link
Basic Policy Structure	Policy syntax
Defining Operations in the Policy	TcaplusDB Operations
Defining Resources in A Policy	TcaplusDB Resource Path
Resource-level Permissions supported by TcaplusDB	Resource-level Permissions supported by TcaplusDB
Console Example	Console Example

Authorized Resource Types

Last updated: 2024-10-15 17:34:09

Introduction to Resource-level Permissions

Resource-level permissions specify which resources users can operate on. TcaplusDB partially supports resource-level permissions, allowing users to perform operations on specific resources or have access to specific resources.
Types of resources that can be authorized by TcaplusDB in CAM are as follows:

Resource type	Resource Description Method in Authorization Policies
Cluster	`qcs::tcaplusdb:$region:$account:cluster/$clusterId`
Table Group	`qcs::tcaplusdb:$region:$account:tablegroup/$clusterId/$tablegroupId`
Table	`qcs::tcaplusdb:$region:$account:table/$tableId`

TcaplusDB Cluster-related, TcaplusDB Table Group-related and TcaplusDB Table-related respectively introduce the currently supported TcaplusDB API operations with resource-level permissions, as well as the supported resources and conditional keys for each operation. When setting resource paths, you need to replace `$region`, `$account`, and other variable parameters with your actual parameter information. You can also use the * wildcard in the path. For related operation examples, see Console Example.

> **Note**
> For TcaplusDB API operations that do not support resource-level permissions, you can still grant users permission to use these operations, but the resource element in the policy statement must be specified as *.

List of APIs not supporting resource-level permissions

API Operations	API Overview
CreateBackup	Creating backup
CompareIdlFiles	Upload and verify the table modification file
VerifyIdlFiles	Upload and verify the table creation file
DescribeUinInWhitelist	Querying whether the current user is in the allowlist
DescribeRegions	Querying region list.
DeleteIdlFiles	Deleting IDL description file
DescribeIdlFileInfos	Querying table description file details
DescribeTasks	Queries the list of tasks

List of APIs supporting resource-level permissions

TcaplusDB Cluster-related

API Operations	Resource path
CreateCluster	`qcs::tcaplusdb:$region:$account:cluster/*` `qcs::tcaplusdb:$region:$account:cluster/$clusterId`
ModifyClusterName	`qcs::tcaplusdb:$region:$account:cluster/*` `qcs::tcaplusdb:$region:$account:cluster/$clusterId`
DeleteCluster	`qcs::tcaplusdb:$region:$account:cluster/*` `qcs::tcaplusdb:$region:$account:cluster/$clusterId`

DescribeClusters	qcs::tcaplusdb:$region:$account:cluster/* qcs::tcaplusdb:$region:$account:cluster/$clusterId
ModifyClusterPassword	qcs::tcaplusdb:$region:$account:cluster/* qcs::tcaplusdb:$region:$account:cluster/$clusterId

TcaplusDB Table Group-related

API Operations	Resource path
CreateTableGroup	qcs::tcaplusdb:$region:$account:tablegroup/* qcs::tcaplusdb:$region:$account:tablegroup/$clusterId/$tablegroupId
DeleteTableGroup	qcs::tcaplusdb:$region:$account:tablegroup/* qcs::tcaplusdb:$region:$account:tablegroup/$clusterId/$tablegroupId
DescribeTableGroups	qcs::tcaplusdb:$region:$account:tablegroup/* qcs::tcaplusdb:$region:$account:tablegroup/$clusterId/$tablegroupId
ModifyTableGroupName	qcs::tcaplusdb:$region:$account:tablegroup/* qcs::tcaplusdb:$region:$account:tablegroup/$clusterId/$tablegroupId

TcaplusDB Table-related

API Operations	Resource path
CreateTables	qcs::tcaplusdb:$region:$account:table/* qcs::tcaplusdb:$region:$account:table/$tableId
ClearTables	qcs::tcaplusdb:$region:$account:table/* qcs::tcaplusdb:$region:$account:table/$tableId
DeleteTables	qcs::tcaplusdb:$region:$account:table/* qcs::tcaplusdb:$region:$account:table/$tableId
DescribeTables	qcs::tcaplusdb:$region:$account:table/* qcs::tcaplusdb:$region:$account:table/$tableId
DescribeTablesInRecycle	qcs::tcaplusdb:$region:$account:table/* qcs::tcaplusdb:$region:$account:table/$tableId
ModifyTableMemos	qcs::tcaplusdb:$region:$account:table/* qcs::tcaplusdb:$region:$account:table/$tableId
ModifyTableQuotas	qcs::tcaplusdb:$region:$account:table/* qcs::tcaplusdb:$region:$account:table/$tableId
ModifyTables	qcs::tcaplusdb:$region:$account:table/* qcs::tcaplusdb:$region:$account:table/$tableId
RecoverRecycleTables	qcs::tcaplusdb:$region:$account:table/* qcs::tcaplusdb:$region:$account:table/$tableId
RollbackTables	qcs::tcaplusdb:$region:$account:table/* qcs::tcaplusdb:$region:$account:table/$tableId

Authorization Policy Syntax

Last updated: 2024-10-15 17:34:31

Policy Syntax

CAM policy:

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

- **version**: Required. Currently, only the value "2.0" is allowed.
- **statement** : Used to describe the detailed information of one or more permissions. This element includes the permissions or permission sets of multiple other elements such as effect, action, resource, condition, etc. A policy has one and only one statement element.
- **effect**: Required. It describes the outcome of a declaration, which can be an "allow" or an "explicit deny". There are two situations: Allow (permit) and deny (explicitly deny).
- **action** : It is required, used to describe the operations that are allowed or denied. Operations can be APIs or feature sets (a specific set of APIs described with a permid prefix).
- **resource**: it is required, which describes the detailed data authorized. A resource is described in a six-segment format, and the detailed resource definition varies by product.
- **Effective conditions condition**: Required, describing the constraints for when the policy takes effect. Conditions include the operator, the operation key, and the operation value. TcaplusDB currently does not support special conditions, so this item does not need to be configured.

TcaplusDB Operations

In CAM Policy Statements, you can specify any API action from any CAM-supported service. For TcaplusDB, use API actions prefixed with name/tcaplusdb:, such as name/tcaplusdb:DescribeClusters or name/tcaplusdb:DeleteCluster.
To specify multiple actions in a single statement, separate them with commas, as shown below:

```
"action":["name/tcaplusdb:action1","name/tcaplusdb:action2"]
```

You can also use wildcard characters to specify multiple actions. For example, you can specify all actions whose names begin with the word " Describe " as follows:

```
"action":["name/tcaplusdb:Describe*"]
```

To specify all operations in TcaplusDB, use the * wildcard character, as follows:

```
"action":["name/tcaplusdb:*"]
```

TcaplusDB Resource Path

Each TcaplusDB policy statement has its own resources.
Resource paths are generally in the following format:

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

project_id: Describes project information, only for compatibility with early CAM logic, no need to fill in.
service_type: Product abbreviation tcaplusdb.
region: Regional information, such as ap-shanghai. If specifying a particular resource, there is no need to fill in the region.
account: Main account information of the resource owner, such as uin/164xxx472.
resource: Specific resource details for each product, such as clusters being cluster/19168929215 or cluster/*; clusters, table groups, and tables cannot perform cascading authentication. If access control for all tables or table groups under a certain cluster is needed, not only does the cluster require access control, but table groups or tables also need to be individually authenticated. The table below describes the resources that TcaplusDB can use and their corresponding resource description methods.

Resources	Resource Description Method in Authorization Policies
Cluster	qcs::tcaplusdb:$region:$account:cluster/$clusterId
Table group	qcs::tcaplusdb:$region:$account:tablegroup/$clusterId/$tablegroupId
Table	qcs::tcaplusdb:$region:$account:table/$tableId

For example, you can specify a resource for a specific cluster (cluster ID: 19168929215) in a statement as shown below:

```
"resource":[ "qcs::tcaplusdb:ap-shanghai:uin/164xxx472:cluster/19168929215"]
```

You can also use the * wildcard character to specify all clusters in the Shanghai region belonging to a specific account, as follows:

```
"resource":[ "qcs::tcaplusdb:ap-shanghai:uin/164xxx472:cluster/*"]
```

If you want to specify all resources, or if a particular API action does not support resource-level permissions, use the * wildcard character in the Resource element, as follows:

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

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

```
"resource":
["qcs::tcaplusdb::uin/164xxx472:cluster/19168929215","qcs::tcaplusdb::uin/164xxx472:cluster/21168929215"]
```

Console Example

Last updated: 2024-10-15 17:34:51

Overview

You can grant a user the permission to view and use specific resources in the TcaplusDB Console by using a CAM policy. This document describes how to grant the permission to view and use specified resources, thereby showing you how to use certain policies in the console.

Directions

Full access policy in TcaplusDB

If you want users to have permissions to create and manage TcaplusDB instances, you can use the policy named QcloudTcaplusDBFullAccess for them.
This policy grants users permission to operate all resources in TcaplusDB. The specific steps are as follows:
Refer to Authorization Management to grant the preset policy QcloudTcaplusDBFullAccess to the user.

Read-only policy in TcaplusDB

If you want users to have query permissions for TcaplusDB instances but no permissions to create, delete, or modify, you can use the policy named QcloudTcaplusDBReadOnlyAccess for them.
This policy grants users permission to perform all operations in TcaplusDB that start with the words "Describe" and "Inquiry." The specific steps are as follows:
Refer to Authorization Management to grant the preset policy TcaplusDB to the user.

Policy for granting user permission to manipulate a specific cluster

To grant a user the permission to manipulate a specific TcaplusDB cluster, you can associate the following policy with the user. The steps are as follows:

1. Create a custom policy as instructed in Policy.
   This example policy allows users to perform all operations on the TcaplusDB cluster with the ID 19168929215. The policy content can be set by referring to the following policy syntax:

```
{
 "version": "2.0",
 "statement": [
     {
         "action": "tcaplusdb:*",
         "resource": "qcs::tcaplusdb:ap-shanghai:uin/1231xxx166:cluster/19168929215",
         "effect": "allow"
     }
 ]
}
```

2. Locate the created policy and click [Bind User/Group] in the "Operation" column.
3. In the pop-up "Bind User/User Group" window, select the users/groups you need to authorize, and click [OK].

Policy for granting user permission to manipulate all TcaplusDB resources

To grant a user the permission to manipulate all TcaplusDB resources, associate the following policy with the user. The steps are as follows:

1. Create a custom policy as instructed in Policy.
   This example policy grants users permission to operate all resources in TcaplusDB. The policy content can be set by referring to the following policy syntax:

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

```
    {
        "action": "tcaplusdb:*",
        "resource": "qcs::tcaplusdb:::*",
        "effect": "allow"
    }
 ]
}
```

2. Locate the created policy and click [Bind User/Group] in the "Operation" column.
3. In the pop-up "Bind User/User Group" window, select the users/groups you need to authorize, and click [OK].

Policy for denying user all permissions of certain TcaplusDB tables

To deny a user the permission to manipulate certain TcaplusDB tables, associate the following policy with the user. The steps are as follows:

1. Based on creating a custom Definition policy, create a custom Definition policy.
   This example policy prohibits users from having operational permissions on the tables (IDs are tcaplus-c8d1caa4 and tcaplus-d8d1cbb4). Policy content can be set according to the following policy syntax:

```
{
 "version": "2.0",
 "statement": [
    {
        "action": "tcaplusdb:*",
        "resource": [
                    "qcs::tcaplusdb::uin/16xxx472:table/tcaplus-c8d1caa4",
                    "qcs::tcaplusdb::uin/16xxx472:table/tcaplus-d8d1cbb4",
                    ],
        "effect": "deny"
    }
 ]
}
```

2. Locate the created policy and click [Bind User/Group] in the "Operation" column.
3. In the pop-up "Bind User/User Group" window, select the users/groups you need to authorize, and click [OK].

Custom Policies

If you feel the preset policies do not meet your requirements, you can achieve your goal by creating a custom Definition policy.
For specific operation steps, please refer to creating a custom Definition policy.
For more TcaplusDB-related policy syntax, please refer to Authorization Policy Syntax.

Tag
Tag Overview

Last updated: 2024-10-15 17:35:24

Introduction

Tag is a label provided by Tencent Cloud for identifying cloud resources, consisting of a key-value pair (Key-Value). For more details, please see Tag Overview.
You can use Tags to categorize and manage TcaplusDB resources according to different dimensions (e.g., business, purpose, person in charge, etc.). Tags allow for the convenient filtering and selection of corresponding resources. Tencent Cloud does not assign any semantic meaning to the key-value pairs of Tags; they are strictly parsed and matched as strings. Just pay attention to the corresponding Usage Restrictions during use.
Below, we introduce the use of Tags with a specific case.

Case Background

A company has three TcaplusDB clusters on Tencent Cloud, belonging to three different game businesses. The operations managers for the three game businesses are Zhang San, Li Si, and Wang Wu, respectively.

Setting Tags

For easy management, the company uses Tags to categorize and manage corresponding TcaplusDB resources, defining the following Tag keys/values.

Tag key	Tag value
Business	Game1, Game2, Game3
OPS Owner	Tom, Jane, and Harry

These Tag keys/values are bound to TcaplusDB, and the relationship between resources and Tag keys/values is shown in the table below:

Resource ID	Business	OPS Owner
tcaplus-abcdef1	Game1	Wang Wu
tcaplus-abcdef2	Game2	Li Si
tcaplus-abcdef3	Game3	Zhang San

Using Tags

- For methods of creating and deleting Tags, please refer to Managing Tags.
- For methods of editing TcaplusDB Tags, please refer to Editing Tags.

Editing Tags

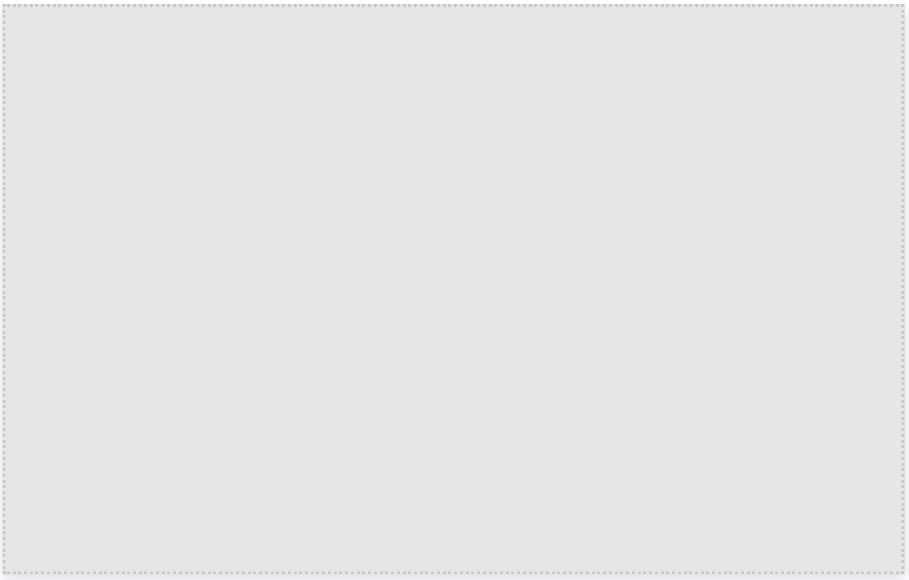
Last updated: 2024-10-15 17:35:46

This document describes different tag editing methods.

Editing Cluster Tag

1. Log in to TcaplusDB Console, and select **Cluster List** page from the left navigation panel.
2. In the Cluster List, within the **Action** row of the cluster needing Tag editing, click **Edit Tag**.

3. In the pop-up dialog, you can add, modify, or delete Tags. After confirming the accuracy, click **OK**.



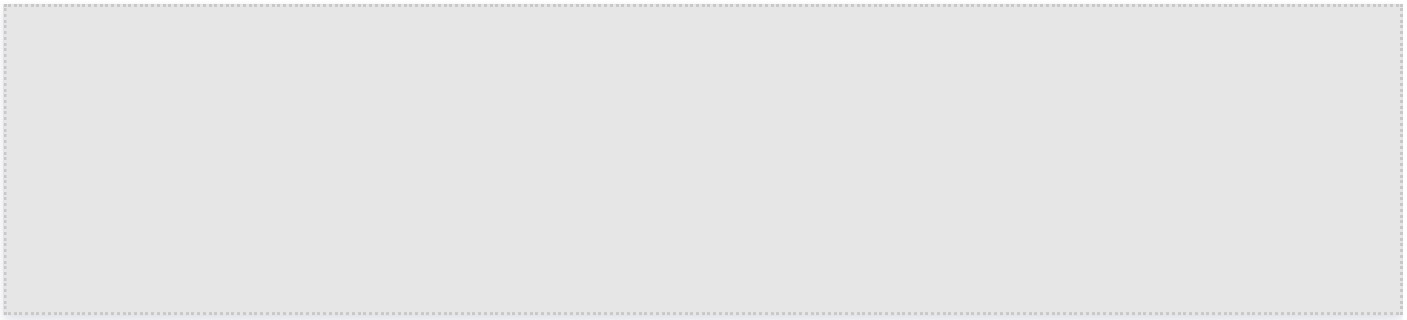
Editing Table Group Tag

1. Log in to TcaplusDB Console, and select **Cluster List** page from the left navigation panel.
2. In the table group list on the right, within the **Action** column of the table group needing Tag editing, select **More** > **Edit Tag**.

3. In the pop-up dialog, you can add, modify, or delete Tags. After confirming the accuracy, click **OK**.

Editing Tag of One Table

1. Log in to TcaplusDB Console, and select **Table List** page from the left navigation panel.
2. In the Table List, within the **Action** column of the table needing Tag editing, select **More** > **Edit Tag**.

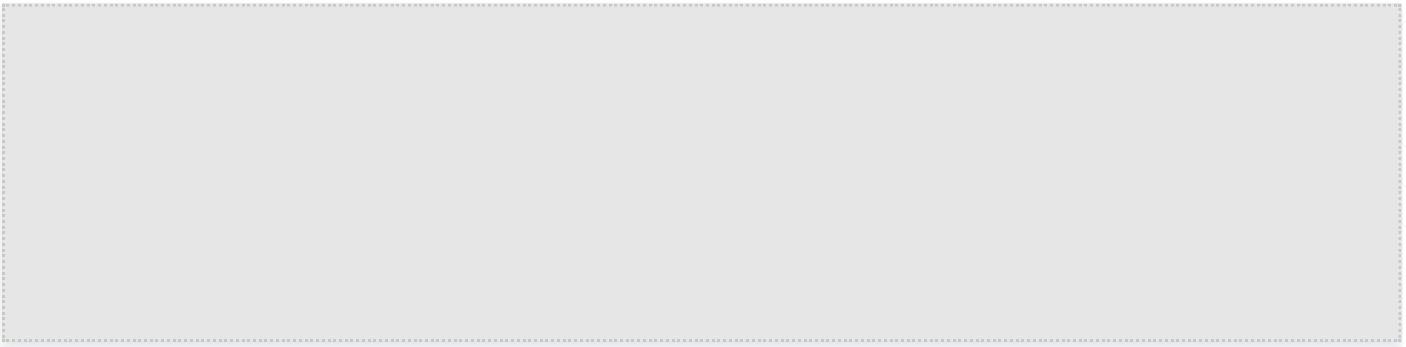


3. In the pop-up dialog, you can add, modify, or delete Tags. After confirming the accuracy, click **OK**.

Editing Tag of Multiple Tables

1. Log in to TcaplusDB Console, and select **Table List** page from the left navigation panel.
2. In the Table List, check the table(s) needing Tag editing, and at the top, select **Batch Operation** > **Set Tag**.

> **Note:**
> The selected tables must be in the same cluster.



3. In the pop-up dialog, you can add, modify, or delete Tags. After confirming the accuracy, click **OK**.