TencentDB for CTSDB

Operation Guide

Product Documentation

Contents

Operation Guide
CAM
CAM Overview

Last updated：2025-04-30 16:33:26

Feature Introduction

Cloud Access Management (CAM) helps you securely and conveniently manage access to Tencent Cloud services and resources. With CAM, you can create sub-users, user groups, and roles, and control their access scope through policies. CAM supports SSO capabilities for users and roles, allowing you to set up interoperability between enterprise users and Tencent Cloud based on specific management scenes.
The Tencent Cloud root account you initially created has full access to all services and resources under the account. It is recommended to protect the credentials of the root account, use sub-users or roles for daily access, enable multi-factor authentication, and periodically rotate keys.

Overview

If you use multiple cloud platform services, such as Cloud Virtual Machine, Virtual Private Cloud and CloudDB, managed by different people but sharing your cloud account tokens, you might face the issues:
The risk of your key being compromised is high since multiple users are sharing it.
You cannot restrict access for other users, which may lead to misoperations and potential security risks.

Basic Concepts

Root Account

When you register for a Tencent Cloud accout, the generated account is the root account and has management permissions for all cloud resources under that root account. The root account is the fundamental entity for metering and billing Tencent Cloud's resource usage.

Sub-Account

A sub-account is created by a root account and fully belongs to the root account that creates it. It has a definite identity ID and credentials.

Identity Credential

It includes log-in credentials and access certificates. Log-in credentials refer to a user's log-in name and password. Access certificates refer to Cloud API keys (SecretId and SecretKey).

Resource

A resource is an object operated in cloud services, such as a TencentDB for CTSDB 3.0 instance.

Permissions and Policies

Permission: Refers to allowing or denying some users to perform specific operations and access certain resources under certain conditions.
Policy: Refers to the syntax specification that defines and describes one or more **permissions**. For a detailed description of the syntax, see Permissions and Policies.
Note:
By default, a root account has access permissions to all its resources, while a sub-account does not have access permissions to any resources under the root account. You need to create policies to allow sub-accounts to use the resources or permissions they require.
For detailed operations for the default permission policies and custom policies of CTSDB, see Permissions and Policies.
For detailed operations on authorizing permission policies to sub-accounts or cross-cloud accounts, see Authorizing Policies to Sub-accounts or Cross-Cloud Accounts.

Authorization Granularity

The authorization granularity of cloud products is divided into three levels according to the granularity: service level, operation level, and resource level.
Service level: This defines whether access permissions are authorized to the overall service. It can be divided into allowing full operation permissions for the service or denying all operation permissions for the service. Cloud products with service-level authorization granularity do not support authorizing specific APIs.
Operation level: This defines whether access permissions are authorized to specific APIs of the service. For example: Authorizing a certain account to perform read-only operations on the Cloud Database Service.
Resource level: This defines whether access permissions are authorized to a specific resource. This is the finest level of authorization granularity. For example: Authorizing a certain account to perform only read and write operations on a Cloud Database Service instance. Products that can support resource-level API authorization are identified as having resource-level authorization granularity.
Note:
For a detailed list of business APIs supported by CAM authorization in CTSDB 3.0, see Authorizable Resources and Operation APIs.

More Information

For more information about CAM, see Cloud Access Management in Product Documentation.

Permissions and Policies

Last updated：2025-04-30 16:33:26

CAM Policy Description

Basic Syntax

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

version: A required field in which currently only "2.0" is allowed.
statement: It describes the detailed information of one or more permissions. This element includes effect, action, resource, condition, and other related elements representing a single permission or a set of permissions. A policy should contain exactly one statement element.
effect: A required field that specifies whether the statement results in allow or explicit deny. The possible values are allow (grants permission) and deny (explicitly denies permission).
action: Required. It describes the allowed or denied actions. Actions can be APIs (described with the konisgraph: prefix) or feature sets (a specific group of APIs described with the permid prefix).
resource: A required field that specifies the authorized data. Resources are described using a six-segment format, with definitions varying by product.
condition: Required. It describes the constraints for policy enforcement. A condition consists of an operator, key, and value. Condition values can include time, IP address, and other parameters, depending on the service's supported conditions.

TencentDB for CTSDB 3.0 Action

In the operation **action** of CAM policy statements, you can specify any API operation from services that support CAM. For CTSDB, use APIs prefixed with `ctsdb:` , such as ctsdb:CreateCluster, ctsdb:CreateDatabase, ctsdb:DestroyCluster, ctsdb:DestroyDatabase. For a list of specific authorizable APIs, see Authorizable Resources and Operation APIs.

If you need to specify multiple operations in a single statement, separate them with commas, as shown below:

```
"action":["ctsdb:action1","ctsdb: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":["ctsdb:Describe*"]
```

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

```
"action": ["ctsdb:*"]
```

CTSDB 3.0 Resource

Each CAM policy statement applies to its resource. The general format of a resource path is as follows:

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

project_id: Not required. It is only for compatibility with early CAM logic format
service_type: The product abbreviation, such as CTSDB.
region: It indicates regional information, such as bj.
account: The root account information of the resource owner, such as uin/12xxx8.
resource: Specific resource details of each product, such as instance/instance_id or instance/*.
For example, you can specify it in the statement by using a specific instance (ctsdbi-8bfdai6s), as shown below:

```
"resource":[ "qcs::ctsdb:bj:uin/12xxx8:instance/ctsdbi-8bfdai6s"]
```

You can also use the * wildcard character to specify all instances belonging to a specific account, as shown below:

```
"resource":[ "qcs::ctsdb:bj:uin/12xxx8:instance/*"]
```

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

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

To specify multiple resources in one instruction, separate them with a comma. The following is an example of specifying two resources:

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

The following table describes the resources that can be used by CTSDB 3.0 and the corresponding resource description methods. Among them, words prefixed with $ are aliases, region refers to the region, and account refers to the account ID.

Resources	Resource Description Method in Authorization Policies
Instance	`qcs::ctsdb:$region:$account:instance/$instanceId`
VPC	`qcs::vpc:$region:$account:vpc/$vpcId`
Security Group	`qcs::cvm:$region:$account:sg/$sgId`

Default Permission Policy of CTSDB 3.0

CTSDB 3.0 supports the system permission policies in the following table. You can search for the default permission policy and its syntax for CTSDB 3.0 in the **Preset Policy** on the **Policies** page via the CAM Console.

Policy name	**Policy Permission Description**	**Policy Syntax Logic**

QcloudCTSDBFullAccess	Full read and write access permissions to CTSDB. The sub-account authorized with this permission has the same permission as the Tencent Cloud account, that is, the sub-account has all operation permissions of the console and API.	<pre>{
		"version": "2.0",
		"statement": [
		{
		"action": [
		"ctsdb:*"
		],
		"resource": "*",
		"effect": "allow"
		},
		{
		"action": [
		"monitor:DescribeBaseMetri
		"monitor:GetMonitorData"
		],
		"resource": "*",
		"effect": "allow"
		}
		]
		}</pre>

QcloudCTSDBReadOnlyAccess	Read-only permission: The sub-account authorized with this permission only has read-only permission for all resources of the Tencent Cloud account and does not have operation permissions of the console and API.	<pre>{
		"version": "2.0",
		"statement": [
		{
		"action": [
		"ctsdb:Describe*"
		],
		"resource": "*",
		"effect": "allow"
		},
		{
		"action": [
		"monitor:DescribeBaseMetri
		"monitor:GetMonitorData"
		],
		"resource": "*",
		"effect": "allow"
		}
		]
		}</pre>

Custom Permission Policies and Authorization

1. Custom permission policy supports rapidly creating through a policy generator, creating through tag authorization, creating by writing policy syntax, or creating based on product features or project permissions. For detailed operations, see Policy Guide. For a description of policy syntax, see CAM Policy Description.
2. When creating a user/user groups, there are no permissions by default. You can associate a policy for them to obtain corresponding operation permissions. For detailed operations, see Authorization Management.

Authorizing Policies for Sub-Accounts or Cross-Cloud Accounts

Last updated：2025-04-29 22:59:22

Sub-account permission segmentation between the Tencent Cloud accounts (root accounts) and sub-accounts, and authorizing different permissions to sub-accounts as needed, can avoid security risks resulting from the exposure of Tencent Cloud account keys.

Authorizing a Permission Policy for a Sub-Account

Background

Company A has enabled the TencentDB for CTSDB 3.0 service and needs its own team members to operate the cloud resources involved in the CTSDB 3.0 service. For security or trust considerations, Company A does not want to directly disclose the cloud account key to team members, but hopes to create corresponding sub-accounts for them. Sub-accounts can only operate cloud resources with root account authorization, and no need for independent metering and billing for sub-accounts. All expenses are accounted under the company's Tencent Cloud account, and sub-account operation permissions can be revoked or deleted at any time.

Directions

Step 1: Creating a Sub-Account User

You can create through the console or API interface.
Log in to Cloud Access Management (CAM) console of Tencent Cloud, and then enter the User List page to create. For detailed operation, see Creating Sub-Users.
Add sub-users and set permissions by accessing the key call AddUser interface. For details, see Adding Sub-Users.

Step 2 (Optional): Creating a Custom Permission Policy

1. Search for policy in the search box in the upper right corner on the Policies page in the CAM console. Preset policies are system default policies, and custom policies are defined by users based on business requirements. Search for policies based on actual conditions.

2. If the policy does not exist, you need to create custom policies. For specific operations, see Creating Custom Policies.

Step 3: Authorizing Permission Policies to Sub-Account Users

Find the permission policy to be associated in the Policies page of the CAM console, and associate it with the sub-account user. For detailed operations, see Authorization Management.
Find the sub-account user to be authorized in the User List page of the CAM console, and associate it with the policy. For detailed operations, see Authorization Management.

Step 4: Logging in to the Tencent Cloud Console via Sub-Accounts

Use a sub-account to log in to the Tencent Cloud console and access CTSDB 3.0. For detailed operations, see Logging in to the Console with the Sub-Account.
If you need to view and modify the user information of a sub-account, see Users Information.
If you want to revoke or delete sub-account operation permissions, see Deleting Sub-Users.

Authorizing a Permission Policy for a Cross-Cloud Account

Background

Company A has enabled the TencentDB for CTSDB 3.0 service and hopes that Company B can have partial business permissions for its CTSDB 3.0. For example, instance read and write permissions, database management, and more. Company B hopes to have a sub-account responsible for this part of the business. Company A can authorize Company B's sub-account to access the resources of CTSDB 3.0 through role access. For the specific concept and application scenarios of roles, see Role Overview.

Directions

Step 1: Company A Creating a Role for Company B

1. Log in to Tencent Cloud CAM console and enter the Role page.
2. Click **Create Role**, and in the **Select a role carrier** dialog box, select **Tencent Cloud account**.
3. On the configuration wizard page of **Create a Custom Role**, create a role.
a. On the **Enter role carrier information** page, select **Cloud account type** as **Another root account**, input the root account of Company B in **Account ID**, set other parameters according to the prompts, and click **Next**.
b. On the **Configure role policy** page, select the policies that need to be authorized for the role, and click **Next**.
c. In the **Role Name** input box on the **Review** page, set the role name, such as DevOpsRole. Review the selected policies, and click **Completed**.

Step 2: Company B Authorizing the Permission of Role Assumption to the Sub-Account

1. Log in to Tencent Cloud CAM console with the root account of Company B, and then enter the User List page to create a sub-account. For detailed operations, see Creating Sub-Users.
2. On the Policies page of the CAM console, click **Create a custom policy**.
3. In the dialog box of **Select a policy creation method**, select **Create according to the policy syntax**.
4. In the configuration wizard of **Create according to the policy syntax**, create a policy.

a. In the **Select a policy template** area, select **Blank Template** and click **Next**.

b. On the **Edit Policy** page, set the policy name in the **Policy Name** input box, such as sts:AssumeRole.

c. In **Policy Content**, assign permissions for the sub-account to assume roles according to the policy syntax and click **Completed**. The example is as follows:

```
{
 "version": "2.0",
 "statement": [
 {
     "effect": "allow",
     "action": ["name/sts:AssumeRole"],
     "resource": ["qcs::cam::uin/12345:RoleName/DevOpsRole"]
 }
 ]
}
```

5. Back to the **Policies** page, find the created custom policy, and click **Associate User/Group/Role** in **Operation** column.

Associate the custom policy with the sub-account of Company B and click **OK**.

Step 3: Company B Using the Sub-Account to Access Cloud Resources Through the Role

1. Log in to the console with the sub-account of Company B. In the profile photo pull-down menu in the console, select **Switch role**.

2. On the **Switch Role** page, enter the root account of Company B and role name. Click **Switch Role** to switch to the role identity of Company A.

More References

If you need to modify a role, see Modifying Roles.

If you need to delete a role, see Deleting Roles.

For more information on using CAM, see User Guide.

Authorizable Resources and Operation APIs

Last updated：2025-04-29 22:25:02

Basic Information

The authorization granularity of cloud products in CAM can be divided into three levels according to the granularity: service level, operation level, and resource level.
Service level: This defines whether access permissions are authorized to the overall service. It can be divided into allowing full operation permissions for the service or denying all operation permissions for the service. Cloud products with service-level authorization granularity do not support authorizing specific APIs.
Operation level: This defines whether access permissions are authorized to specific APIs of the service. For example: Authorizing a certain account to perform read-only operations on the Cloud Virtual Machine (CVM) service .
Resource level: This defines whether access permissions are authorized to a specific resource. This is the finest level of authorization granularity. For example: Authorizing a certain account to perform only read and write operations on a CVM instance. Products that can support resource-level API authorization are identified as having resource-level authorization granularity.
The API authorization granularity of the TencentDB for CTSDB 3.0 is divided into two levels: resource level and operation level.
Resource-level API: This type of API supports authorization for a specific resource.
Operation-level API: This type of API does not support authorization for a specific resource. If the policy syntax specifies a specific resource during authorization, CAM will judge that this API is not in the authorization scope, that is, it is judged as lacking permission.

Write Operations

API Name	API Description	Authorization Granularity	Six-Segment Resource Style
CreateCluster	Creating an instance	Operation level	*
DestroyCluster	Deleting an instance	Resource level	qcs::ctsdb:${region}:uin/${uin}:instance
CreateDatabase	Creating a database	Resource level	qcs::ctsdb:${region}:uin/${uin}:instance
DestroyDatabase	Deleting a	Resource level	qcs::ctsdb:${region}:uin/${uin}:instance

	database		
ModifyAccountPassword	Modifying the account password	Resource level	qcs::ctsdb:${region}:uin/${uin}:instance
ModifyCluster	Modifying the instance information	Resource level	qcs::ctsdb:${region}:uin/${uin}:instance
ModifyClusterHorizontalDowngrade	Scaling in an instance horizontally	Resource level	qcs::ctsdb:${region}:uin/${uin}:instance
ModifyClusterHorizontalUpgrade	Scaling out an instance horizontally	Resource level	qcs::ctsdb:${region}:uin/${uin}:instance
ModifyClusteVerticalDowngrade	Vertically downgrading an instance	Resource level	qcs::ctsdb:${region}:uin/${uin}:instance
ModifyClusterVerticalUpgrade	Vertically upgrading an instance	Resource level	qcs::ctsdb:${region}:uin/${uin}:instance
ModifyDatabase	Changing database configuration	Resource level	qcs::ctsdb:${region}:uin/${uin}:instance
ModifyClusterSecurity	Modifying an instance security group	Resource level	qcs::ctsdb:${region}:uin/${uin}:instance

Read Operations

API Name	API Description	Authorization Granularity	Six-Segment Resource Style
DescribeAccounts	Viewing the account list	Resource level	qcs::ctsdb:${region}:uin/${uin}:instance/$instanceId
DescribeDatabases	Querying a database	Resource level	qcs::ctsdb:${region}:uin/${uin}:instance/$instanceId

	instance		

Managing an Instance
Creating an Instance

Last updated：2025-04-30 16:33:26

Overview

Configure a cluster of instances of TencentDB for CTSDB 3.0 for official use.

Region

Currently, creating instances is supported in **Guangzhou, Beijing, and Shanghai**, and the subsequent regions are under planning and preparation.

Prerequisites

A Tencent Cloud account has been registered, and real-name verification has been completed, and the application for the beta test of the TencentDB for CTSDB 3.0 has been approved.
To register a Tencent Cloud account: click Sign up for a Tencent Cloud account.
To complete the identity verification: click here to complete Identity Verification.
Specifications that planned database instances need to meet.
For Virtual Private Cloud (VPC) and security group for which database instances have been planned, see Virtual Private Cloud and Security Group.

Directions

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the console page, select **Version 3.0**.
3. Click **Create an Instance** to enter the purchase page of **Time Series Database CTSDB Version 3.0**.
4. See the following table to configure the following parameters and purchase an instance.

Classification	Interface Parameter	Parameter Description	Configuration Description

Basic Configuration	**Billing Mode**	Only supports **Monthly Subscription.**	-
	Region	The region to which the instance belongs	Select the region already supported by the product.
	Availability Zone	The availability zone which the instance belongs to.	Fixed as **Multi-AZ**.
	Network	Select the specific Virtual Private Cloud and its subnet. The Cloud Virtual Machine (CVM) is used to connect to the private network address automatically assigned to the TencentDB. This connection method uses the private high-speed network and has low delay. The CVM and database should be in the same account and the same VPC (ensure the same region). A VPC has a region attribute (such as Guangzhou), while a subnet has an availability zone attribute (such as Guangzhou Zone 1). A VPC can be divided into one or more subnets. Subnets in the same VPC can interconnect with one another by default, while subnets in different VPCs (regardless of whether they are in the same region) are isolated by default.	Select the configured VPC and subnet from the dropdown list. If the existing network does not meet the requirements, click **Create VPC** or **Create Subnet** to create the required network environment.
Instance configuration	**Instance Type**	Only **Dedicated** instance supports monthly subscription billing.	-
	Node Specification for Time Series	Select the CPU and memory specifications of the time series compute node.	Select the required compute specification from the dropdown list. According to the required storage space size and timeline, select appropriate resources. For details, see Instance Specifications.

	Time Series Node Quantity	Configure the number of compute nodes.	Value range: 3-32.
	Data Node Specification	The data node specification is fixed as 15-core 60 GB.	-
	Number of Data Nodes	Configure the number of data nodes.	Valid values: 9, 18, 27, 36, 45, and 54.
	Number of Data Replicas		
	Storage Capacity	Automatically calculate the data storage disk capacity according to the number of selected nodes.	The storage capacity of a single data node is 3,000 GB.
	Specification Preview	Preview the configured time series node specifications and data node specifications.	-
Other	**Tag**	Set a tag to an instance. You can manage instances by tag.	Select the configured tag from the dropdown list. If the existing tag is not suitable, click Add to select the tag key and tag value.
	Security Group	Set security group rules for an instance to control inbound traffic to the database.	You can select existing security groups in the **Select Existing Security Groups** drop-down list, or click **Customize Security Groups** to set new security group inbound rules. For specific operations, see Security Group.
	Instance Name	Set the instance name.	**Name after creation**: The instance name will be consistent with the instance ID by default. After the instance is created, you can modify it as needed. **Name Immediately**: Enter the instance name in the following input box. Name requirements: 1 to 60 characters, which can contain Chinese characters, uppercase and lowercase letters, digits, "-", "_", and ".".

Password	Set the instance access password.	Password complexity requirements: 8 to 64 characters, including at least three of the following character types: uppercase and lowercase letters, digits, and characters (such as ~!@#$%^&*_-+=|(){}[]:;<>,.?/).
Re-Enter password	Re-enter the password to ensure its accuracy.	-
Auto-Renewal	Whether to enable automatic renewal. Once enabled, the fee will be automatically deducted from your Tencent Cloud account when the monthly subscription instance is about to expire.	After purchase, you can also manually enable automatic renewal depending on the actual business situation. For specific operations, see Enabling Automatic Renewal.
Terms of Service	Describe the service contents, service fees, usage rules, intellectual property rights and other relevant terms of the CloudDB.	Check **I have read and agree to Cloud database service terms**.
Duration	In the monthly subscription mode, you need to select the purchase duration of instances.	Select the instance purchase duration by full month or full year from the dropdown list. The maximum purchase duration is **5** years.
Quantity	Select the number of purchased instances.	Currently, an account can only purchase one instance.

5. Confirm the configuration fees. Click **Purchase Now** to automatically return to the instance list page. The current instance **Status** is **Creating**, and wait for the instance status to be updated to **Running** to use the instance.

Viewing an Instance

Last updated：2025-04-30 16:33:26

Overview

After purchasing the TencentDB for CTSDB 3.0, you can intuitively and quickly view the details of instances on the console, including their running status, resource usage, and network status, and efficiently perform operation and maintenance management on the instance.

Prerequisites

Creating an Instance has been finished.
The instance is not terminated.

Viewing the Instance List

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the console page, select **Version 3.0**.
3. In the Instance List, search for the instance you want to view. The meaning of each parameter is shown in the following table.

Parameter Name	Parameter Description
ID/Name	Instance ID and name. System will randomly allocate an ID number for each instance. Hover over the instance name and click to re-edit the instance name.
Status	Current running status of the instance.
Region	The region to which the instance belongs.
Network	VPC name of the instance.
Configuration	Instance type, specification configuration information of computing nodes and data nodes Instance type: Only **dedicated** is supported.

	Time sequence node: 2 cores 8 GB / 3 nodes, corresponding to the CPU cores, memory specifications / quantity of computing nodes. Data node; 15 cores 60 GB/9 nodes, corresponding to the CPU cores, memory specifications/node quantity of data nodes; 719.87 MB/13500 GB, corresponding to the used disk capacity/total disk capacity.
Billing mode	Billing mode: Currently only supports **Monthly Subscription** in prepaid mode. Expiration time: the expiration time of instance use.
Creation time	The time point for a successful instance creation.
Tag	Tags of the instance, making it easy to manage instance resources by tags.
Operation	Click on **Manage** to enter the **Instance Details** page. Click **More** > **Return and Refund** to return instance resources. For detailed operations, please refer to Returning Instances. Click **More** > **Edit Tag**, you can set the **Tag Key** and **Tag Value** in the **Edit Tag** window. For specific operations, see Editing Tag.

Viewing Instance Details

Click on **Instance ID** in the instance list, or click on **Manage** in the **Operation** column to enter the **Instance Details** page.

Page Area	Parameter Name	Parameter Description
Basic information	**Instance ID**	The system randomly allocates an ID number to the instance. Click to directly copy the instance ID.
	Instance Name	The name configured for the instance when it was created. If it is not configured, it will be left empty. Click to rename the instance.
	Region	The region to which the instance belongs
	Zone	The default settings are **Multi-AZ** deployment, with data replicas automatically distributed across multiple availability zones, providing higher availability and disaster recovery capabilities.

	Status	The instance is in the running status. If it is **Running**, it means that the instance currently has no tasks running.
	Tag	Tag keys of instances.
Compute	**Time Series Node Specification**	Instance configuration's compute specifications: 2 cores 8 GB / 3 nodes, indicating the number of CPU cores and memory specifications / quantity of billing resources. click **Adjust** to readjust the specification. For details, see Modification of Specifications.
	Billing Mode	Billing mode of computing resources.
Storage	**Data Node**	Instance configuration's data node specifications. click **Adjust** to readjust the specification. For details, see Modification of Specifications.
	Instance storage capacity	Used disk capacity and total disk capacity.
	Billing Mode	Billing mode of storage resource.
	Data Replica	Quantities of storage data replicas.
	Consistency	Requirements for data consistency. **Strong consistency** refers to reading the latest data.
	Storage Type	Currently, only **SSD Local disk** storage is supported.
Network information	**VPC**	VPC Information.
	Time Series Node Private Network Address	Time Series Node Connection Address.
	Analysis Node Private Network Address	deprecated, ignore it.
Configuration information	**Creation time**	Instance creation time.
	Expiration Date	Expiration time of annual and monthly subscription billing.

Modification of Specifications

Last updated：2025-04-29 22:26:23

Overview

In daily operation and maintenance, when the configuration of your purchased instances does not meet (is higher or lower than) the current business needs, you can quickly adjust the specifications of your TencentDB for CTSDB 3.0 instance according to the actual situation of your business (such as business initial period, rapid business development period, business peak period, business trough period), to better achieve full use of resources and real-time optimization of costs.

Prerequisites

The instance is currently **Running** normally.

Modification of Compute Specifications

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the right page, select **Version 3.0**.
3. In the Instance List, find the instance you need to view.
4. In the Instance List, click the instance ID or click **Manage** in its **Operation** column to access the **Instance Details** page.
5. On the **Instance Details** page, in the **Compute** section, click **Adjust** next to **Time Series Node Specification**. In the **Time Series Node Adjustment** pop-up, reselect the CPU cores and memory specifications of the compute nodes required for the business in the drop-down list of **Time Series Node Specification**; in the drop-down list of **Time Series Node Count**, reselect the quantity of compute nodes required for the business.

6. In the **Adjust the preview**, compare the current specifications with the new specifications, confirm the specification change, and click **OK**.

Modification of Storage Specification

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the right page, select **Version 3.0**.

3. In the Instance List, find the instance you need to view.
4. Click on **Instance ID** in the instance list, or click on **Manage** in the **Operation** column to enter the **Instance Details** page.
5. On the **Instance Details** page, in the **Storage** section, click **Adjust** next to **Data Node**. In the **Adjust storage node** pop-up, reselect the CPU cores and memory specifications of the data nodes required for the business in the drop-down list of **Data Node Specification**; in the drop-down list of **Number of data nodes**, reselect the quantity of data nodes required for the business.

6. In the **Adjust the preview**, compare the current specifications with the new specifications, confirm the specification change, and click **OK**.

Returning Instances

Last updated：2025-04-29 22:27:40

Overview

When the purchased monthly subscription exclusive instance is no longer needed, you can initiate a self-return operation on the console page. The billing system will settle the fees and return the refund amount to the account.

Return Operation

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the right page, select **Version 3.0**.
3. In the Instance List, find the instance to be returned and select **More** > **Return and Refund** in its operation column.

4. In the **Return and Refund** window, confirm the information of the instance to be returned, check **I have agreed to the Termination Rules**, and click **View refund information**.

5. On the following unsubscribe information page, confirm the **Refund List** information, check the refund amount, and click **Confirm Refund**.

6. In the **Please confirm your refund method and amount** window, confirm the information, and click **Confirm Refund**.
7. Wait for the task execution to complete. On the **Transaction succeeded** page, you can perform the following operations.
Click **View My Orders** to jump to the **Order Management** page of **Billing Center**, where you can view the progress of the refund order.
Click **Go to Console** to jump to the CTSDB Instance List page. The status of the instance has been changed to **Pending termination**, which means that the return process has been completed and instance in this status will no longer incur any fees.

Recovering Instances to Be Terminated

1. Log in to the CTSDB Console using a Tencent Cloud account.

2. At the top of the right page, select **Version 3.0**.
3. In the Instance List, find the instance to be recovered and select **More** > **Start** in its operation column.

4. In the **Renew the selected instances** window, confirm the recovery of instance information, select **Renewal Period**, confirm **Fees**, and click **OK**.

5. On the **Please confirm the following product information** page, confirm the renewal information and order amount, and click **Submit Order** in the lower right corner to complete the fee payment and recover the instance.

Editing Tags

Last updated：2025-04-29 22:28:53

TencentDB for CTSDB 3.0 supports editing instance tags in the console, which makes it easy for you to manage instances by tags.

Background

Tags consist of tag keys and tag values, and they can be used to mark CTSDB 3.0 instances. If there are various cloud resources in your Tencent Cloud account, with multiple associations among different resource types, and the number of cloud resources increasing day by day, the management difficulty will also change accordingly. You can use tags to group and classify resources with the same or related functions. When it comes to daily operation and maintenance or problem location, you can quickly retrieve resources based on tags, perform batch operations, and achieve efficient operation and maintenance.

Billing Instructions

Tag management is one of the free services provided by the cloud platform for your cloud platform account at no additional charge. You can directly access the Control Console to use the product.

Usage Instructions

One tag consists of one tag key and one tag value (tagKey:tagValue).
A maximum of 50 tags can be bound to one instance.
The same tag key on one instance can only correspond to one tag value.

Prerequisites

An instance is created.

Directions

1. Log in to the CTSDB Console using a Tencent Cloud account.

2. At the top of the right page, select **Version 3.0**.
3. In the instance list, find the instance for which you want to edit the tag.
4. Select any of the following methods to enter the **Edit Tag** page.
In the **Operation** column of the target instance, select **More** > **Edit Tag**.
Click the target instance ID, and click

on the right side of the **Tag** in the **Basic Information** area of the **Instance Details** page.
5. In the **Edit Tag** window, reselect the appropriate tag key in the **Tag Key** drop-down list and select the corresponding tag value in the **Tag Value** input box. Click **Add** to add multiple tags.

6. (Optional) If the existing tag does not meet your business requirements, execute the following operations:
6.1 In the upper right corner of the current page, click **manage tags**.
6.2 On the **Tag List** page, click **Create Tag**.
6.3 On the **Create Tag** page, carefully understand the note information for setting tags.
6.4 In the **Tag Key** input box, set a new tag value, and in the **Tag Value** input box, enter the corresponding tag value.
The requirements for setting the label key are as follows:
- Character length should be between [1, 63].
- English letters and digits can be entered.
- Special symbols can be entered: plus sign "+", equal sign "=", underline "_", dash "-", English dot ".", English colon ":", slash "/", at"@", English brackets "()", and square brackets "[]".
6.5 Click **OK** to complete the creation.
6.6 Then return to the **Edit Tag** page of the CTSDB instance, click **reload** in the drop-down list of **Tag Key**, and you can select the newly created tag key and then select the corresponding tag value.
7. Click **OK** to complete the settings.

More References

For more information on tag management, see Tag Management.

Automatic Backup

Last updated：2025-04-29 22:31:32

To prevent data loss due to system failures and other factors, TencentDB for CTSDB 3.0 supports data automatic backup.

Backup Policies

CTSDB 3.0 currently only supports system default automatic backup policies and does not support custom backup policies.

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the right page, select **Version 3.0**.
3. Find the target instance in the instance list.
4. In the row of the target instance, click the instance ID or click **Manage** in the **Operation** column to access the **Instance Details** page.
5. On the **Backup List** tab, click **Automatic Backup Settings** on upper-right corner.
6. In the **Automatic Backup Settings** small window, you can refer to the system default backup policies, as shown below.

7. Click **OK** to close the small window.

Viewing the Backup List

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the right page, select **Version 3.0**.
3. Find the target instance in the instance list.
4. In the row of the target instance, click the instance ID or click **Manage** in the **Operation** column to access the **Instance Details** page.
5. On the **Backup List** tab, select the backup time area of the backup file in the time box on upper-left corner.
6. You can access all the backup information for this time period, as shown below.

System Monitoring
Monitoring Overview

Last updated：2025-04-30 16:33:26

TencentDB for CTSDB 3.0 supports real-time monitoring of monitoring metric data of instance resources via Tencent Cloud Observability Platform (TCOP). TCOP presents monitoring data statistics in various ways such as visual charts, tables, and large screens, and supports setting alarm rules. It also helps the user learn about anomalies of database services immediately via message push, and adjust database performance promptly, ensuring stable business operations.

Monitoring Granularity

CTSDB 3.0 supports viewing monitoring data in the last 30 days. For different time spans, the time granularity of monitoring data collection varies, and the retention duration of monitoring data also varies. For specific information, see the table below.

<table>
<tr><th>Time Span</th><th>Time Granularity</th><th>Monitoring Data Retention Period</th></tr>
<tr><td>5 minutes</td><td>1 minute</td><td rowspan="9">1 minute: 15 days.
5 minutes, 1 hour: 31 days.</td></tr>
<tr><td>30 minutes</td><td rowspan="2">1 minute and 5 minutes</td></tr>
<tr><td>1 hour</td></tr>
<tr><td>3 hours</td><td rowspan="5">1 minute, 5 minutes, and 1 hour</td></tr>
<tr><td>12 hours</td></tr>
<tr><td>2 days</td></tr>
<tr><td>7 days</td></tr>
<tr><td>30 days</td></tr>
</table>

Monitoring Operations

Operation Scenario	Operation Description	Operation Guide

Viewing monitoring metrics	Check monitoring views of each performance metric	Monitoring Metrics
Configuring Alarm	Configure alarm thresholds for each performance metric	Alarm Configuration
Creating a dashboard	The Dashboard will automatically show monitoring data in well-presented charts on the monitoring dashboard, making the monitoring data more intuitive.	Creating a Dashboard

Monitoring Metrics
Exclusive Monitoring Metrics

Last updated：2025-04-29 22:35:26

The exclusive instance of TencentDB for CTSDB 3.0 performs monitoring and statistics across four dimensions: instances, compute nodes, data nodes, and databases, including more than 40 indicator items such as requests, latency, and resource utilization, providing completely transparent monitoring services.

Instance Monitoring

Instance monitoring refers to the monitoring and analysis of requests, response time, and resource consumption of the entire database instance. For specific metrics, see the table below.

Monitoring Grouping	Monitoring Indicator	Metric Meaning	Unit
Request monitoring	**Average Read Latency**	The average latency of read request command executions.	ms
	Average Write Latency	The average latency of write request command executions.	ms
	Total Requests	The number of all requests command executions per second.	Count/s
	Total Request Failure Rate	The percentage of all failed requests to the total requests. Failed execution includes requests that are rejected by the database and timeout requests.	%
	Total Request Rejection Rate	The percentage of requests rejected by the database to the total requests.	%
	Read Requests	The number of read request command executions per second.	Count/s
	Read Request Failure Rate	The percentage of failed read request command executions to the read requests. Failed executions include requests that	%

		are rejected by the database and timeout requests.	
	Read Request Rejection Rate	The percentage of read request commands rejected by the database to the read requests.	%
	Write Points	The number of data points written into the instance.	Count/s
	Write Requests	The number of write request command executions per second.	Count/s
	Write Request Failure Rate	The percentage of failed write request command executions.	%
	Write Request Rejection Rate	The percentage of write request commands rejected by the database.	%
Resource monitoring	**Series Count**	The number of time sequences stored in the database.	Count
	Storage Utilization Of Object	Describes the percentage of storage usage and purchase specs.	%
	Storage Used	Describes the actual usage of data storage.	GBytes
	Average CPU Utilization of Compute Node	The compute node CPU utilization, taking the average of all nodes.	%
	Max CPU Utilization of Compute Node	The compute node CPU utilization, taking the maximum value of all nodes.	%
	Average Memory Utilization of Compute Node	The compute node memory utilization, taking the average of all nodes.	%
	Max Memory Utilization of Compute Node	The compute node memory utilization, taking the maximum value of all nodes.	%
	Average CPU Utilization of Data	The data node CPU utilization, taking the average of all nodes.	%

	Node		
	Max CPU Utilization of Data Node	The data node CPU utilization, taking the maximum value of all nodes.	%
	Average Memory Utilization of Data Node	The data node memory utilization, taking the average of all nodes.	%
	Max Memory Utilization of Data Node	The data node memory utilization, taking the maximum value of all nodes.	%
	Inbound Traffic	The volume of data received by the database instance per second.	Bytes
	Outbound Traffic	The volume of data sent by the database instance per second.	Bytes
	Series Utilization	The ratio of the actual number of timelines used in the database to the total timeline capacity.	%

Compute Node Monitoring

Compute node monitoring refers to the monitoring and statistics of CPU and memory resource consumption of compute nodes in a database cluster. For specific metrics, see the table below.

Monitoring Metrics	Metric Meaning	Unit
CPU Utilization of Compute Node	The CPU utilization of compute nodes.	%
Memory Utilization of Compute Node	The memory utilization of compute nodes.	%
Inbound Traffic of Compute Node	The volume of data received by the compute node per minute.	Bytes
Outbound Traffic of Compute Node	The volume of data sent by the compute node per minute.	Bytes
Write Points of Compute Node	The number of data points written into the compute node.	Count/s

Average Read Latency of Compute Node	The average latency of read request executions of compute nodes.	ms
Average Write Latency of Compute Node	The average latency of write request executions of compute nodes.	ms
Read Requests of Compute Node	The number of read request command executions per second on the compute node.	Count/s
Read Request Failure Rate of Compute Node	The percentage of read request execution failures of compute nodes to the write requests, including execution failures such as those rejected by the database and timeout requests.	%
Read Request Rejection Rate of Compute Node	The percentage of read request commands of compute nodes rejected by the database to the write requests.	%
Total Requests of Compute Node	The number of all request command executions per second on the compute node.	Count/s
Total Request Failure Rate of Compute Node	The percentage of all request execution failures of compute nodes to all requests, including execution failures such as those rejected by the database and timeout requests.	%
Total Request Rejection Rate of Compute Node	The percentage of all request commands of compute nodes rejected by the database to the total requests.	%
Write Requests of Compute Node	The number of write request command executions per second on the compute node.	Count/s
Write Request Failure Rate of Compute Node	The percentage of write request execution failures of compute nodes to the read requests, including execution failures such as those rejected by the database and timeout requests.	%
Write Request Rejection Rate of Compute Node	The percentage of write request commands of compute nodes rejected by the database to the read requests.	%

Data Node

Monitoring Metrics	Metric Meaning	Unit
CPU Utilization of Data Node	The CPU utilization of data nodes.	%
Memory Utilization of Data Node	The memory utilization of data nodes.	%

Database Monitoring

Database monitoring refers to the statistics of database task execution and disk usage.

Monitoring Metrics	Metric Meaning	Unit
Count Of CQ Jobs	Describes the total number of CQ tasks.	Count
Success Rate Of CQ Jobs	Describes the percentage of CQ tasks that are successfully executed on time.	%
Storage Used Of Single Database	Describes the percentage of disk occupancy of a single database.	GBytes

Viewing Monitoring Metrics

Last updated：2025-04-30 16:33:26

Overview

TencentDB for CTSDB 3.0 supports viewing trend graphs of monitoring metrics at any time, helping you quickly analyze the operation and performance of CTSDB to adjust and optimize CTSDB in a timely manner and predict risks in advance.

Usage Instructions

The monitoring data is kept for 30 days, and you cannot view the monitoring information before 30 days.
After receiving the alarm message reported by Tencent Cloud, you need to troubleshoot anomalies according to the alarm message.

Viewing Monitoring Metrics

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the right page, select **Version 3.0**.
3. In the Instance List, find the instance you need to view.
4. Click the target instance ID, or click **Manage** in the **Operation** column to enter the **Instance Details** page.
5. Select the **Instance Monitoring** tab, click

 in the time box, and select the period for which you want to get the monitoring view.
6. In the **Time granularity** drop-down list, configure the time interval on the monitoring view timeline.
7. In the **Disable** drop-down list, select the time for automatic data update. Options available are 30s, 5min, 30min, and 1h.

8. View the monitoring view of changes in each monitoring metric of the instance, node, and database during this period.
In each monitoring view, hover the mouse over the view to see the metric data at any time point. Below the view, you can directly see the maximum, minimum, and average values of the metric.
In each monitoring view area, click

to configure the alarm. For specific operations, see Alarm Configuration.
In each monitoring view area, click

to view the monitoring view of the metric in full screen.
In each monitoring view area, click

and select **Export data** to export the monitoring data in a table format for local viewing. Select **Import image** to export the monitoring view as an image for local viewing.

Instance Monitoring

Compute Node Monitoring

Database Monitoring

Data Node Monitoring

Configuring Alarm

Last updated：2025-04-29 22:33:22

Overview

This is to prevent the system from being affected when some monitoring metrics reach a certain value. You can set alarm rules for these monitoring metrics to enable the alarm system to automatically check the monitoring data and send an alarm notification to the administrator when the monitoring data meets the conditions. This helps you understand business exceptions the first time and resolve them quickly.

Background

Tencent Cloud Observability Platform (TCOP) is a real-time monitoring and alarm service for cloud product resources. TencentDB for CTSDB 3.0 provides alarms for monitoring metrics through TCOP. The alarm monitors some specific metrics within a certain period and sends alarm notifications by various methods (such as WeChat and SMS) every several time periods based on the given threshold. For more information, see Tencent Cloud Observability Platform(TCOP).

Billing Instructions

TCOP allows you to configure alarm policies to monitor key metrics of instances, which can be used for free. Currently, only **SMS and phone alarms** are charged. For details,see Billing Overview of TCOP.

Prerequisites

Enable the TCOP service.
The CTSDB instance status is **Running**.
Information about alarm notification objects has been collected, including emails, SMS, and phone calls.

Directions

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the right page, select **Version 3.0**.

3. In the Instance List, find the instance you need to view.
4. Click the target instance ID, or click **Manage** in the **Operation** column to enter the **Instance Details** page.
5. Select the **Instance Monitoring** tab. In the upper right corner of each monitoring view, click

to enter the **Create Alarm Policy** page.
6. On the **Create Alarm Policy** page, see the following table to configure the alarm policy. For the basic concept of alarm policy, see Creating Alarm Policy.

Parameter Name	Parameter Interpretation
Policy Name	Customize the name of an alarm policy for easy identification.
Remarks	Briefly describe the alarm policies for easy identification.
Monitoring Type	Select **Cloud Product Monitoring**.
Policy type	The policy types that can be set are as follows: **Cloud database/CTSDB/InfuxDB/Instance** **Cloud database/CTSDB/InfuxDB/compute node** **Cloud database/CTSDB/InfuxDB/Database**
Tag	Specify a tag for the alarm policy.
Alarm Object	Select **Instance ID**: The alarm policy is bound to the specified database instance. Select **Instance Group**: The alarm policy is bound to the specified database instance group. For instructions on creating an instance group, see Instance Group. Select **All Objects**: The alarm policy is bound to all instances for which the current account has permissions. Select **Tag**: The alarm policy is bound to all instances related to the current tag key and tag value.
Trigger Condition	**Select Template**: Select a template file from the drop-down list. Alarms will be reported according to the preset trigger conditions of the template file. For specific configuration, see Configuring Trigger Condition Templates. **Configure manually**: Configure the threshold conditions for triggering an alarm for each metric in the **Metric Alarm** area below. The threshold type in the **Metric Alarm** area can be static or dynamic. **Static**: A constant threshold is manually set, and an alarm is sent when the trigger conditions are met. **Dynamic**: Abnormalities are determined based on the threshold boundaries calculated by machine learning algorithms.

	For more information, see Create Alarm Policy.
Alarm Notification	You can select a preset or user-customized notification template. Each alarm policy can be bound to at most three notification templates. See Notification Template for details.

7. Confirm that the configuration is correct and click **Complete**. For more information about alarms, see Alarm Overview.

Database Management

Last updated：2025-04-29 22:38:54

Overview

Database management is a crucial part of database management. A database refers to a DATABASE, which includes operations such as database creation, deletion, and modification. TencentDB for CTSDB 3.0 supports visualization management of databases in the console. You can perform intuitive and efficient database management through buttons and menu items on the interface.

Creating a Database

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the right page, select **Version 3.0**.
3. Find the target instance in the instance list.
4. In the row of the target instance, click the instance ID or click **Manage** in the **Operation** column to access the **Instance Details** page.
5. Select the **Database Management** tab and click **Create database**.
6. In the **Create database** window, see the following table to configure database parameters.

Interface Parameter	Parameter Description	Configuration Method
Database name	Edit the database name.	Enter 1 to 32 characters. Start with a letter or digit. It can include uppercase and lowercase letters, digits, "-", "_", and ".".
Data Expiration Deletion Time	Identifies whether the database has the TTL feature enabled. Configures the data expiration deletion time. Data will be automatically deleted upon reaching the set expiration time.	**Enable**: Configure the expiration deletion time in the input box below. Unit: days. **Disable**: Disable the automatic deletion upon expiration feature.
Remarks	Describes the information of the newly created database.	Enter remarks in the input box.

7. Click **OK**. You can find the newly created database in the database list.

Modify a Database

1. On the **Database Management** page in the console, you can view all databases in this instance.
2. In the database list, find the database that needs to be modified.

3. Click **Modify** in the **Operation** column.
4. In the **Modify database** window, modify the **Data Expiration Deletion Time** as needed.

5. Click **OK** to complete the modification.

Deleting a Database

1. On the **Database Management** page in the console, you can view all databases in this instance.
2. In the database list, find the database that needs to be deleted.
3. Click **Delete** in the **Operation** column.
4. In the **Delete Database** window, confirm the name of the database to be deleted.

Note:

Data cannot be recovered after the database is terminated. Back up your data in advance.

5. Click **Confirm Deletion** to complete the operation.

Account Management
Multi-Account Management

Last updated：2025-04-30 16:31:26

TencentDB for CTSDB 3.0 supports a multi-account authorization mechanism. By creating multiple user accounts, database administrators can customize permissions for each user to ensure they can only access authorized data scopes. This subdivision of permissions not only prevents excessive concentration of permissions but also reduces potential data security risks.

Creating Accounts

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the right page, select **Version 3.0**.
3. Find the target instance in the instance list.
4. In the row of the target instance, click the instance ID or click **Manage** in the **Operation** column to access the **Instance Details** page.
5. Select the **Account Management** tab and click **Create an account** in the upper left corner.
6. In the **Create Account** window, enter the account name as required in the input box of **Account Name**, enter the password corresponding to the account according to the password complexity requirements in the input box of **Password**, and enter the password again in the input box of **Re-enter the Password**.
7. Click **Confirm**. In the account list, you can see the created accounts.

Authorizing Created Accounts

1. In the account list on the **Account Management** tab, find the account name to be authorized.
2. In the **Operation** column of the account to be authorized, click **Modify Permissions**.
3. In the **Edit Permissions** window, on the left side of the **Permissions** setting area, select the **Database Name** that needs to be authorized, and in the right area, set **Read-Only** or **Read-Write** permissions for the database name.
4. Click **Confirm** to complete the configuration.

Resetting Passwords

Last updated：2025-04-29 22:41:19

Overview

If you forget your password or need to update your old password regularly, you can reset your password directly in the console.

Prerequisites

Creating an Instance has been finished.
The instance status is **Running**.

Resetting the Password

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the right page, select **Version 3.0**.
3. Find the target instance in the instance list.
4. In the row of the target instance, click the instance ID or click **Manage** in the **Operation** column to access the **Instance Details** page.
5. Select the **Account Management** tab, find the account for which to reset the password in the account list, and click **Reset Password** in its **Operation** column.

Note:
The default account is the administrator account, and its name is named after the instance ID.
6. In the **Reset Password** window, enter a new password in the input box behind **Password** and re-enter the new password in the input box behind **Re-enter the Password** to confirm.
Password complexity requirements: 8 to 64 characters, which should include at least three of the following types: uppercase and lowercase letters, digits, and characters of ~!@#$%^&*_-+=|(){}[]:;<>,.?/
7. Click **OK** to complete the reset.

Managing a Security Group

Last updated：2025-05-19 15:45:41

Background

Security group is a stateful virtual firewall with filtering feature, which is used to set the network access control of single or multiple CloudDB. It is an important means of network security isolation provided by the cloud platform. The security group is a logical grouping, allowing you to add CloudDB instances from the same region with similar network security isolation requirements to the same security group. The CloudDB shares the security group list with the CVM and others. The security groups are matched based on rules. See Detailed Description of Security Groups for specific rules and restrictions.

Directions

Step 1: Creating Security Groups

Note:

The CloudDB security group currently only supports network control of Virtual Private Cloud (VPC) private network access and does not support network control of basic networks for the time being.

1. Log in to the VPC Console.
2. Select the **Security Group** page in the left sidebar, select the region at the top of the right page and click **Create**.
3. In the pop-up window, complete the following configurations. Confirm and click **OK**.

Template: Select **Custom**， After the security group is successfully created, add the security group rules as needed.
Name: Customize the security group name.
Project: By default, select default project, but it can be designated as other projects for easier management.
Remark: It is customized and briefly describes the security group for easier management.
Advanced configuration: Add a tag to the security group.
4. If **Template** is **Custom**, click **Add rules now** in the **Note** dialog box and perform the following steps.

Step 2: Set the security group inbound rules

Note：

The CloudDB does not actively generate outbound traffic. Therefore, configuring outbound rules has no actual impact on them.

When using Tencent Cloud CVM to connect to TencentDB for CTSDB 3.0, you need to configure **outbound rules** in the Tencent CVM security group and add the IP address and port of CTSDB 3.0 to the outbound rules. Configure

inbound rules in the security group of CTSDB 3.0, and add the IP address and port of CVM to the inbound rules for successful connection.

1. On the **Security group rules** page, select the **Inbound rules** tab and click **Add rule**.
2. In the **Add inbound rule** pop-up window, set the rules.

Type: Select the default type **Custom**.

Source: Set the source for accessing the database, namely, the inbound source. The following options are supported.

Source	Description
IP address or CIDR block	Use CIDR blocks. (IPv4: such as 203.0.113.0, 203.0.113.0/24, or 0.0.0.0/0. 0.0.0.0/0 indicates that all IPv4 addresses are matched. IPv6: such as FF05::B5, FF05:B5::/60, ::/0, or 0::0/0. ::/0 or 0::0/0 indicates that all IPv6 addresses are matched.)
Parameter template - IP address	Reference an IP address object in the parameter template.
Parameter template - IP address group	Reference an IP address group object in the parameter template.
Security groups	Select a created security group (the same region and same project) from the drop-down list, and reference the source address bound to the security group ID to the current security group. **Note:** Only the source information on the security group is referenced. The inbound rules will not be added to the current security group.
Current Login IP	Use the public IP address of the current terminal that has logged in to the console. This public IP address will be identified and bypassed.

Protocol port: Fill in the protocol type and port for client access to CTSDB 3.0. You can view the port information in the **private network address** column of the Instance List. The default is 8086.

Policy: Select Allow by default.

Allow: Access requests of this port are allowed.

Reject: Data packets will be discarded without any response.

Remark: It is customized and briefly describes the rules for easier management.

3. Click **OK** to complete adding the security group inbound rules.

Step 3: Binding a Security Group to an Instance

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the right page, select **Version 3.0**.

3. In the Instance list, find the instance to which you want to bind a security group.
4. Click the target instance ID, or click **Manage** in the **Operation** column to enter the **Instance Details** page.
5. Select the **Security Group** tab, and click **Configure Security Group**.

6. In the **Configure Security Group** dialog box, select the created security group and click **OK**.

More Operations

Adjusting the Priority of Bound Security Groups

1. Log in to the CTSDB Console using a Tencent Cloud account.
2. At the top of the right page, select **Version 3.0**.
3. In the Instance list, find the instance to which you want to bind a security group.
4. Click the target instance ID, or click **Manage** in the **Operation** column to enter the **Instance Details** page.
5. Select the **Security Group** tab to view all current security groups of the instance.
6. Click **Edit**. You can click

or

in the **Operation** column to adjust the priority of security groups filtering.

7. Click **Save** to complete the modification.

Adjusting Inbound and Outbound Rules

1. On the **Security Group** tab, you can view all current security groups of the instance.
2. In the security group list, click **Security Group ID** name to jump to Security Group page.
3. Find the security group rule to be modified, and click **Edit** in the **Operation** column to re-edit the security group rules.

Importing Security Group Rules

1. On the Security Group page, select the required security group and click the specific security group ID/name.
2. On the **Inbound rules** or **Outbound rules** tab, click on **Import rule**.
3. In the pop-up dialog box, select the edited inbound/outbound rule template files and click **Import**.

Note:

If there are security group rules under the security groups that need to be imported, it is recommended that you export the existing rules first. Otherwise, when importing new rules, the original rules will be overwritten.

If there is no security group rule under the security group that needs to import rules, it is recommended that you download the template first and then import the file after editing the template file.

Cloning Security Groups

1. On the Security Group page, select **More** > **Clone** in the **Operation** column of the list.
2. In the pop-up dialog box, after selecting the target region and project, click OK.

Deleting Security Groups

1. In Security Group page, select the security group to be deleted, and choose **More** > **Delete** in the operation column.
2. In the pop-up dialog box, click **OK**. If the current security group is associated with a CVM, it is required to disassociate the security group before deletion.

More References

For more information about security groups, see Security Groups Overview.

Public Network Access
Enabling Public Network Services Through CLB

Last updated：2025-04-30 16:33:26

TencentDB for CTSDB 3.0 currently only supports private network addresses for internal access to instances. If necessary, you can use Cloud Load Balancer (CLB) to enable public network services for access. This document introduces how to enable public network services through CLB to connect to instances.

Prerequisites

The backend service feature has been applied, Submit a Ticket to CLB and apply for using the backend service feature.

Step 1: Purchasing a New CLB

Enter the CLB Purchase Page, select the configuration and click **Buy Now**.

Note:

If there is already a CLB instance in the same region as CTSDB 3.0, you do not need to purchase it.

The region should be the same as the **region where CTSDB 3.0 is located**.

The CLB instance and CTSDB 3.0 instance should be in the same VPC.

Step 2: Configuring a CLB

1. Enable cross-VPC access (CLB supports binding to other private IP addresses after it is enabled).

1.1 Log in to the CLB Console, select a region, and click **Instance ID** in the Instance Management list to enter the instance management page.

1.2 In the **Backend Service** area of the **Basic Information** tab, click **Configure**.

1.3 In the pop-up dialog box, click **Submit** to enable it.

2. Configure the public network listening port.

2.1 Log in to the CLB Console, select a region, and click **Instance ID** in the Instance Management list to enter the instance management page.

2.2 On the instance management page, select the **Listener Management** page and click **Create** under **TCP/UDP/TCP SSL/QUIC Listener**.
2.3 In the pop-up dialog box, complete the settings step by step, and then click **Submit** to complete the creation.

Step 3: Binding a CTSDB 3.0 Instance

1. After creating the listener, on the **Listener Management** page, click the created listener, and then click **Bind** that appears on the right.
2. In the pop-up dialog box, select **Target Type** as **IP Type**, enter the IP address and port of the CTSDB 3.0 instance in the IP and Port input boxes respectively, and click **Confirm** to complete the binding.

Note:

The logged-in account should be a standard account (bandwidth migrated). If it cannot be bound, Submit a Ticket for assistance.

Step 4: Configuring the CTSDB 3.0 Security Group

After the public network service is enabled, configure security group rules for CLB and its CTSDB 3.0 instances on time to control the access source and ensure the security of data access.
1. Log in to the security group page of Security groups Console, **Create security group**, and set **Inbound Rule** to allow the IP address of the CTSDB 3.0 client and the listening protocol port of the CTSDB 3.0 instances you specified. For specific operations, see Creating Security Groups.

2. Log in to the CLB Console, find the CLB instance bound to CTSDB 3.0 in the Instance List of Instance Management, click its **Instance ID**, enter the instance's **Basic Information** tab, select the **Security group** tab, and click **Bind** in the **Bound Security Group** area. In the pop-up **Configure Security Group** window, select the created security group and click **Confirm**. For specific operations, see Configuring A CLB Security Group.

3. Log in to the CTSDB Console, select **3.0** at the top of the right page, and find the instance that needs to be bound to the security group in the Instance List. Click the target **Instance ID**, select the **Security Group** tab, and click **Configure Security Group**. In the **Configure Security Group** dialog box, select the security group to be bound and click **Confirm**. For specific operations, see Configuring Security Groups.

Step 5: Connecting to CTSDB Through influx CLI Client

Enter the influx CLI path and execute the following command to connect to the CTSDB 3.0 instance.

-username: a created user account.

-password: password corresponding to the user account.

-host: Configure it as the public network address of CLB.

-port: Configure it as the listening protocol port of CLB.

```
./influx -host <DB_HOST> -port <DB_PORT> -username <USERNAME> -password <PASSWORD>
```

Iptable Forwarding

Last updated：2025-04-29 22:44:25

Overview

If a user needs to access TencentDB for CTSDB 3.0 on the public network, the user can also perform port forwarding through a Cloud Virtual Machine (CVM) with a public IP address to achieve public network access.

Note:

The iptable forwarding has a stability risk. It is not recommended to use public network access in production environments.

Directions

1. Log in to CVM and enable the IP forwarding feature of CVM.

Note:

The CVM and CTSDB should be in the same account and in the same VPC (ensuring the same region), or in the same basic network.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

2. Configure forwarding rules. The following example shows how to forward the access to 26.xx.x.2:10001 (public network address of CVM, and the port can be selected manually) to a CTSDB 3.0 instance with a private network address of 10.0.0.5:8086.

```
iptables -t nat -A PREROUTING -p tcp --dport 10001 -j DNAT --to-destination
10.0.0.5:8086
iptables -t nat -A POSTROUTING -d 10.0.0.5 -p tcp --dport 8086 -j MASQUERADE
```

3. Configure CVM Security Group, allow access to the public network port of the CVM. It is recommended that the security group rule only allow access from the source addresses that need to access.

4. Connect to the CTSDB 3.0 instance in the private network via the public network address (which is 26.xx.xx.2:10001 in this example) on the access side. The connection command is the same as the private network connection command. See influx CLI Client for the command.