Database Audit

Authorizing Sub-account to Use Database Audit

Product Documentation

Copyright Notice

Trademark Notice

Tencent Cloud

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Authorizing Sub-account to Use Database Audit

Last updated：2023-12-21 17:17:55

By default, sub-accounts have no permission to use TencentDB for MySQL Database Audit. Therefore, you need to create policies to allow sub-accounts to use it.

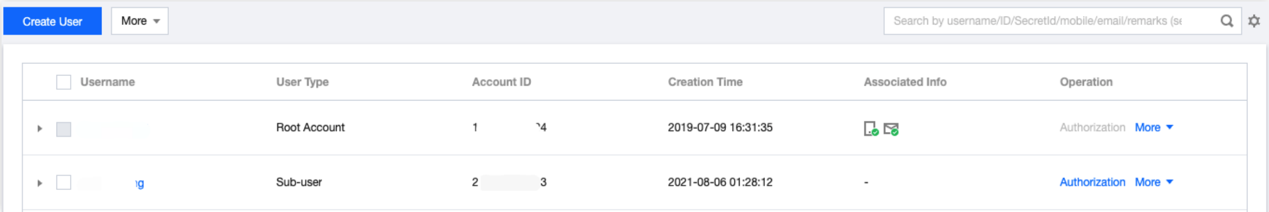
If you don't need to manage sub-accounts' access to resources related to TencentDB for MySQL Database Audit, you can ignore this document.

Cloud Access Management (CAM) is a web-based Tencent Cloud service that helps you securely manage and control access to your Tencent Cloud resources. By using CAM, you can create, manage, and terminate users and user groups. You can manage identities and policies to allow specific users to access your Tencent Cloud resources.

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

Authorizing Sub-account

1. Log in to the CAM console as a root account, select the target sub-user in the user list, and click **Authorize**.

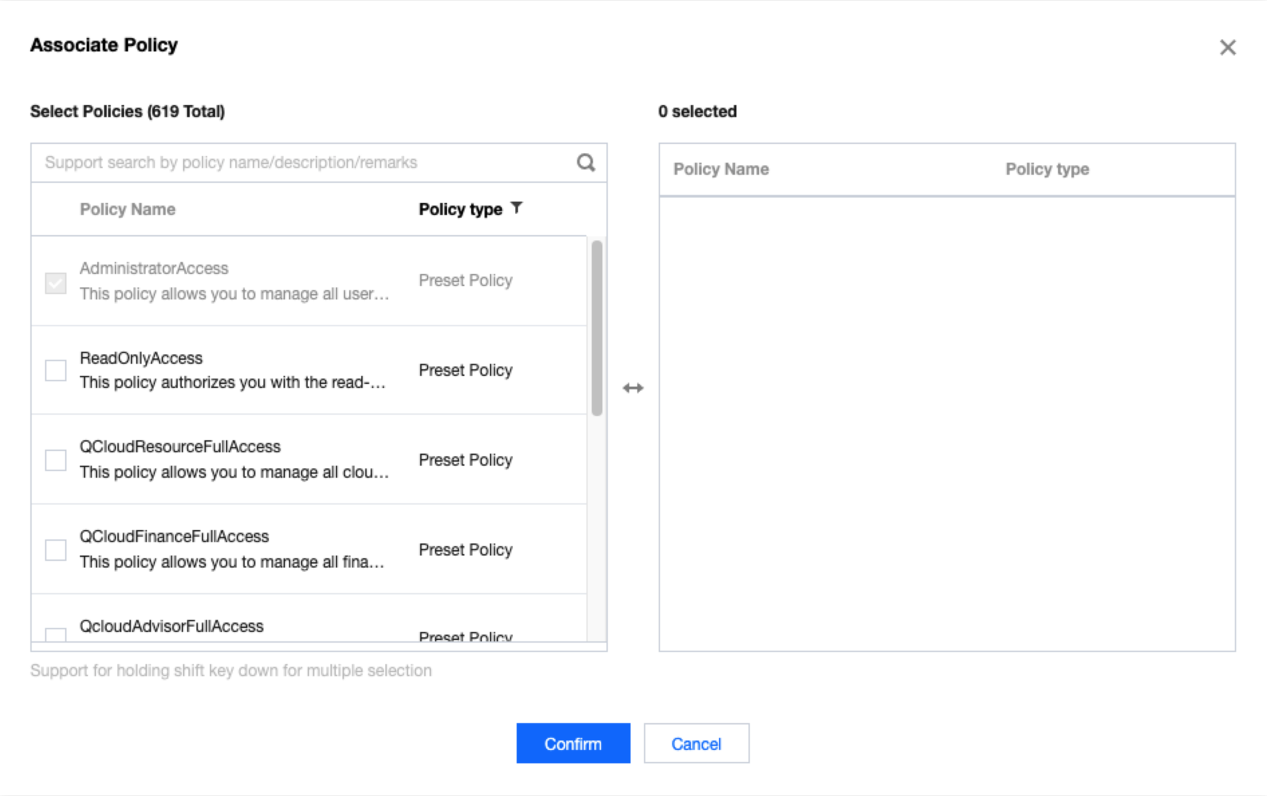


Username	User Type	Account ID	Creation Time	Associated Info	Operation
	Root Account	1 ˋ4	2019-07-09 16:31:35		Authorization More
ıg	Sub-user	2 3	2021-08-06 01:28:12	-	Authorization More

2. In the pop-up window, select the **QcloudCDBFullAccess** or **QcloudCDBInnerReadOnlyAccess** preset policy and click **OK** to complete the authorization.

Note:

MySQL Database Audit is a module in TencentDB for MySQL, so the above two preset policies of TencentDB for MySQL already cover the permission policies required by it. If the sub-user only needs the permission to use this module, please see Custom MySQL Database Audit Policy.



Associate Policy

Select Policies (619 Total)

Support search by policy name/description/remarks

	Policy Name	Policy type
☑	AdministratorAccess This policy allows you to manage all user…	Preset Policy
□	ReadOnlyAccess This policy authorizes you with the read-…	Preset Policy
□	QCloudResourceFullAccess This policy allows you to manage all clou…	Preset Policy
□	QCloudFinanceFullAccess This policy allows you to manage all fina…	Preset Policy
□	QcloudAdvisorFullAccess	Preset Policy

Support for holding shift key down for multiple selection

0 selected

Policy Name	Policy type

Policy Syntax

The CAM policy for MySQL Database Audit is described as follows:

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

version is required. Currently, only the value "2.0" is allowed.

statement describes the details of one or more permissions. It contains a permission or permission set of multiple other elements such as `effect` , `action` , and `resource` . One policy has only one `statement` .

effect is required. It describes the result of a statement. The result can be "allow" or an "explicit deny".

action is required. It describes the allowed or denied action (operation). An operation can be an API (prefixed with "name") or a feature set (a set of specific APIs prefixed with "permid").

resource is required. It describes the details of authorization.

API Operation

In a CAM policy statement, you can specify any API operation from any service that supports CAM. APIs prefixed with `name/cdb:` should be used for Database Audit. To specify multiple operations in a single statement, separate them with commas as shown below:

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

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

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

Resource Path

Resource paths are generally in the following format:

```
qcs::service_type::account:resource
```

service_type: describes the product abbreviation, such as `cdb` here.

account: describes the root account of the resource owner, such as `uin/326xxx46` .

resource: describes the detailed resource information of the specific service. Each TencentDB for MySQL instance (instanceId) is a resource.

Example:

```
"resource": ["qcs::cdb::uin/326xxx46:instanceId/cdb-kf291vh3"]
```

Here, `cdb-kf291vh3` is the ID of the TencentDB for MySQL instance resource, i.e., the `resource` in the CAM policy statement.

Example

The following example only shows the usage of CAM.

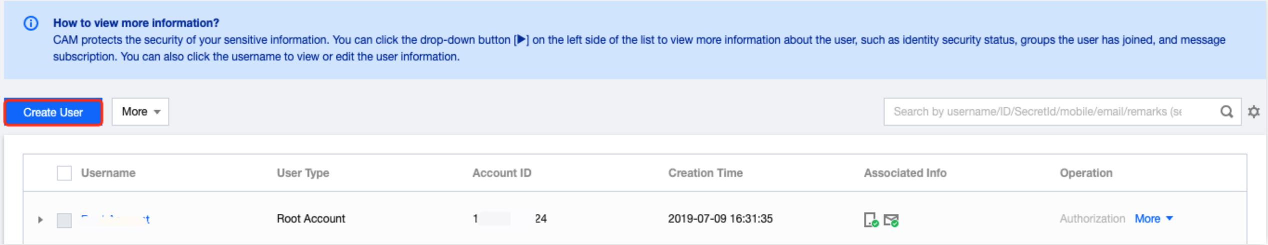
```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "name/cdb: DescribeAuditRules"
            ],
            "resource": [
                "*"
            ]
```

```
          },
          {
              "effect": "allow",
              "action": [
                  "name/cdb: CreateAuditPolicy"
              ],
              "resource": [
                  "*"
              ]
          },

          {
              "effect": "allow",
              "action": [
                  "name/cdb: DescribeAuditLogFiles"
              ],
              "resource": [
                  "qcs::cdb::uin/326xxx46:instanceId/cdb-kf291vh3"
              ]
          }
      ]
  }
```

Custom MySQL Database Audit Policy

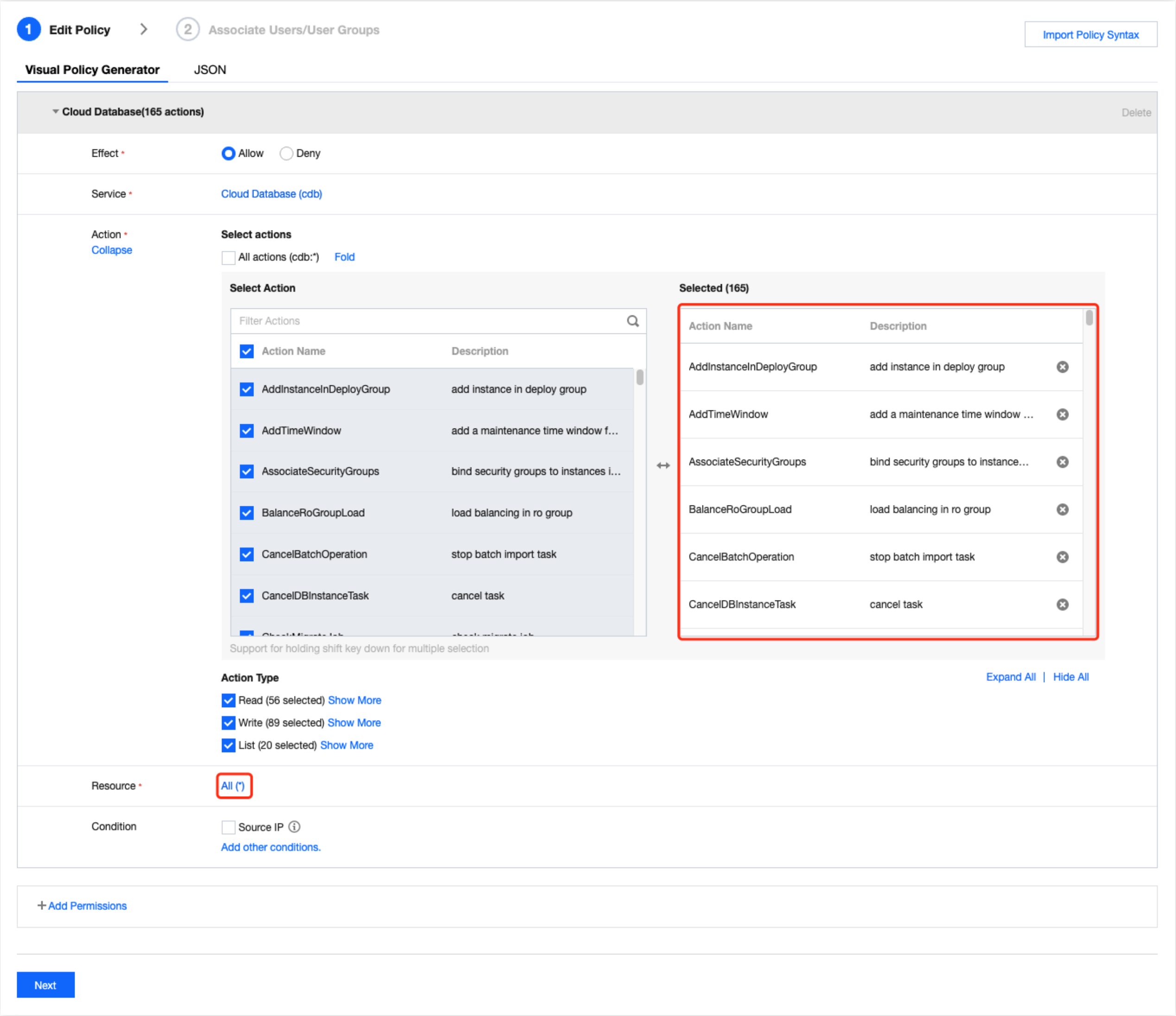
1. Log in to the CAM console as the root account and click **Create Custom Policy** in the policy list.



How to view more information?
CAM protects the security of your sensitive information. You can click the drop-down button [▶] on the left side of the list to view more information about the user, such as identity security status, groups the user has joined, and message subscription. You can also click the username to view or edit the user information.

Username	User Type	Account ID	Creation Time	Associated Info	Operation
[redacted]	Root Account	1 [redacted] 24	2019-07-09 16:31:35		Authorization More

2. In the pop-up window, select **Create by Policy Generator**.
3. On the **Select Service and Action** page, select configuration items, click **Add Statement**, and click **Next**.
Service: select **TencentDB for MySQL**.
Action: select all APIs of MySQL Database Audit.
Resource: for more information, please see Resource Description Method. You can enter `*` to indicate that the audit logs of all TencentDB for MySQL instances can be manipulated.



Cloud Database(165 actions) Delete

Effect * ● Allow ○ Deny

Service * Cloud Database (cdb)

Action * Collapse

Select actions

□ All actions (cdb:*) Fold

Select Action

Filter Actions

☑	Action Name	Description
☑	AddInstanceInDeployGroup	add instance in deploy group
☑	AddTimeWindow	add a maintenance time window f...
☑	AssociateSecurityGroups	bind security groups to instances i...
☑	BalanceRoGroupLoad	load balancing in ro group
☑	CancelBatchOperation	stop batch import task
☑	CancelDBInstanceTask	cancel task

Support for holding shift key down for multiple selection

Selected (165)

Action Name	Description
AddInstanceInDeployGroup	add instance in deploy group
AddTimeWindow	add a maintenance time window ...
AssociateSecurityGroups	bind security groups to instance...
BalanceRoGroupLoad	load balancing in ro group
CancelBatchOperation	stop batch import task
CancelDBInstanceTask	cancel task

Action Type Expand All | Hide All

☑ Read (56 selected) Show More

☑ Write (89 selected) Show More

☑ List (20 selected) Show More

Resource * All (*)

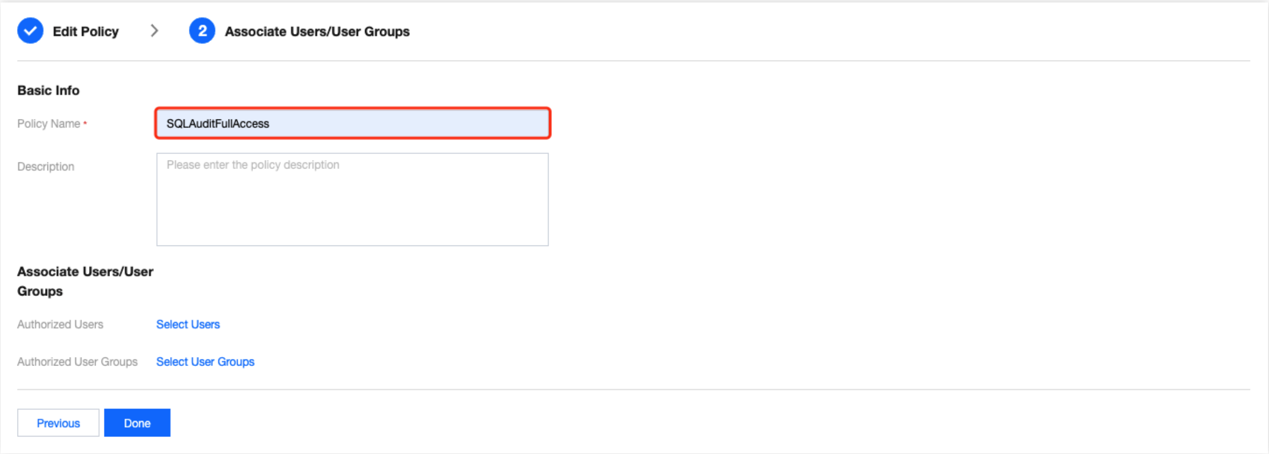
Condition □ Source IP ⓘ

Add other conditions.

+Add Permissions

Next

4. On the **Edit Policy** page, enter the **Policy Name** (such as `SQLAuditFullAccess`) as required and **Description** and click **Done**.



Basic Info

Policy Name * SQLAuditFullAccess

Description Please enter the policy description

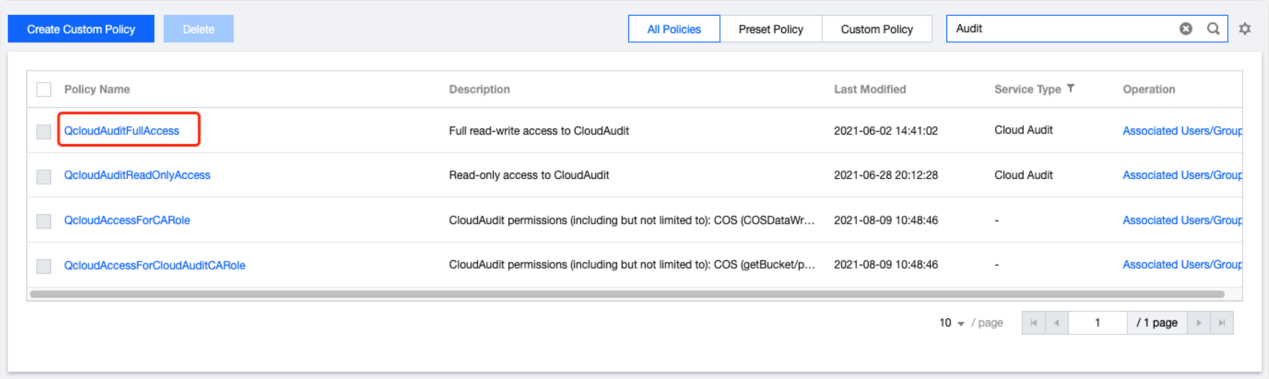
Associate Users/User Groups

Authorized Users Select Users

Authorized User Groups Select User Groups

Previous Done

5. Return to the policy list and you can view the custom policy just created.



□	Policy Name	Description	Last Modified	Service Type	Operation
□	QcloudAuditFullAccess	Full read-write access to CloudAudit	2021-06-02 14:41:02	Cloud Audit	Associated Users/Group
□	QcloudAuditReadOnlyAccess	Read-only access to CloudAudit	2021-06-28 20:12:28	Cloud Audit	Associated Users/Group
□	QcloudAccessForCARole	CloudAudit permissions (including but not limited to): COS (COSDataWr...	2021-08-09 10:48:46	-	Associated Users/Group
□	QcloudAccessForCloudAuditCARole	CloudAudit permissions (including but not limited to): COS (getBucket/p...	2021-08-09 10:48:46	-	Associated Users/Group