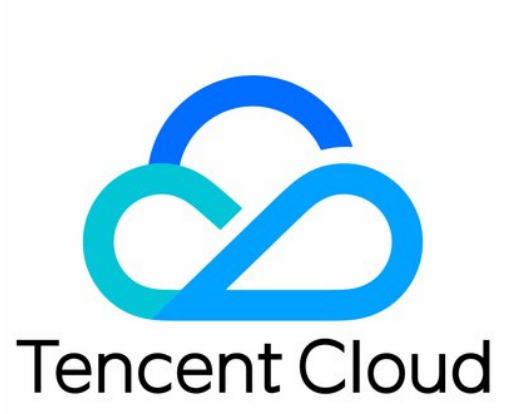
SSL Certificates

Cloud Access Management



Copyright Notice

Trademark Notice

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

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

Cloud Access Management Access Control Overview

Last updated: 2023-10-09 11:31:46

Access Control (CAM) is utilized for managing access permissions to resources under Tencent Cloud accounts. Through CAM, you can dictate which sub-accounts have operational permissions for specific resources, based on identity management and policy management.
For instance, if there are multiple certificates deployed under your account across various projects, to enhance access control, you need to authorize these resources. You can bind an authorization policy to the administrator of Project A, stipulating that only this administrator can operate the load balancing resources under Project A. Most SSL certificate interfaces support resource-level authorization. For more details, please refer to Types of Authorizable Resources.
If you do not require access control over SSL certificate-related resources for sub-accounts, you may bypass this section.

> **Note**
> Currently, CAM-based access authorization is only supported in the console.

Basic CAM Concepts

A root account authorizes sub-accounts by binding policies. The policy settings can be specific to the level of **API, Resource, User/User Group, Allow/Deny, and Condition**.

1. **Account**
   - **Root account**: The primary entity to which Tencent Cloud resources belong and are measured for usage and billing. This account can log into Tencent Cloud services.
   - **Sub-account**: A sub-account is created by a root account, possessing a distinct identity ID and credentials, and has the ability to log into the Tencent Cloud console. A root account can create multiple sub-accounts (users). **By default, sub-accounts do not own any resources and must be authorized by their respective root accounts.**
   - **Identity Credentials**: These include login credentials and access certificates. **Login credentials** refer to the user's login name and password, while **Access certificates** pertain to the Cloud API keys (SecretId and SecretKey).
2. **Resources and Permissions**
   - **Resource**: A resource is an object that is operated within cloud services, such as a cloud server instance, a COS storage bucket, a VPC instance, and so on.

- **Permission**: Permission refers to the authorization that allows or denies certain users to perform specific operations. By default, the **root account possesses access rights to all resources under its purview, while a sub-account does not have access to any resources under the root account**.
- **Policy**: It is a syntax rule that defines and describes one or more permissions. The **root account** performs authorization by **associating policies** with users/user groups.

For more information, please refer to CAM Overview.

Documentation

Content	Document
Understand the relationship between policies and users	Policy Management
Understand the basic structure of policies	Policy Syntax
Check CAM-enabled products	List of CAM-Supported Cloud Services

Authorizable Resource Types

Last updated: 2023-10-09 11:32:54

Resource-level permission refers to the ability to designate which resources a user has the capacity to manipulate. Most SSL interfaces support resource-level authorization, implying that for SSL operations that support resource-level permissions, control can be exerted and users can be permitted to utilize certain specific resources.

Authorization types supported by SSL in access management

ResourceType	Six-Segment Resource Description Format
Certificate	`qcs::ssl::$accountid:certificate/$certid`

In the description:

- All `$accountid` should be the AccountId of the resource owner, or left blank.
- All `$certid` should be an ID of a certain certificate, or "*".

Operations authorized by SSL in access management

> **Note**
> Currently, SSL only has one type of resource, which is the certificate.

API Action	Description	Format
ApplyCertificate	Apply for a complimentary certificate, reapply for a certificate.	* Authenticate only the API
CommitCertificateInformation	Submitting certificate information	`qcs::ssl::$accountid:certificate/$certid`
Delete Certificate	Delete Certificate	`qcs::ssl::$accountid:certificate/$certid`
DescribeCertificate	Getting the information of a certificate	`qcs::ssl::$accountid:certificate/$certid`
DescribeCertificateDetail	Getting certificate details	`qcs::ssl::$accountid:certificate/$certid`

DescribeCertificateOperateLogs	Retrieve Certificate Operation Log List	qcs::ssl::$accountid:certificate/$certid
DescribeCertificates	Getting the certificate list	qcs::ssl::$accountid:certificate/$certid
Modify Certificate Alias	Modify Certificate Alias	qcs::ssl::$accountid:certificate/$certid
Modify Certificate Project	Modify Certificate Project	qcs::ssl::$accountid:certificate/$certid
ReplaceCertificate	Reissuing a certificate	qcs::ssl::$accountid:certificate/$certid
SubmitCertificateInformation	Supplement Certificate Information	qcs::ssl::$accountid:certificate/$certid
Upload Certificate	Upload Certificate	* Authenticate only the API

Authorization Policy Syntax

Last updated: 2023-10-09 11:34:41

Policy Syntax

CAM policy:

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

- The **version** is a mandatory field. Currently, only the value "2.0" is permitted.
- The **statement** is used to detail one or more permissions. This element includes a permission or collection of permissions from several other elements such as `effect`, `action`, `resource`, and `condition`. A policy contains only one `statement` element.
- The **action** is used to describe the operations that are permitted or denied. An operation can be an API (described with an "ssl" prefix) or a feature set (a group of specific APIs described with a "permid" prefix). This element is mandatory.
  - The **resource** describes the specific data authorized. A resource is described in a six-segment format. Detailed resource definitions vary by product. For information on specifying resources, please refer to the product documentation corresponding to the resource statement you are writing. This element is required.
  - The **condition** describes the constraints under which the policy takes effect. A condition consists of an operator, operation key, and operation value. The condition value can include information such as time and IP address. Some services allow you to specify other values in the condition. This element is optional.
  - The **effect** describes whether the result of the statement is to "allow" or "explicitly deny". It includes two scenarios: "allow" and "deny" (explicit denial). This element is mandatory.

SSL operations

In a CAM policy statement, you can specify any API operation from any service that supports CAM. For SSL, use the prefix `ssl:` to specify the action. You can specify one or more actions within the `action` field.

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

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

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

To specify all operations within "ssl", please use the wildcard "*" as demonstrated below:

```
"action": ["ssl:*"]
```

SSL resource path

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

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

- **project_id**: Describes project information, included only for compatibility with early CAM logic, and does not need to be filled in.
- **service_type**: Refers to the product abbreviation, such as `ssl`.
- **region**: As SSL does not differentiate by region, this field should be left blank.
- **account**: Refers to the root account information of the resource owner, such as `uin/164256472`. This field is optional and if left blank, it defaults to the primary account `ownerUin`.
- The **resource** refers to the details of a resource, such as `certificate/{CertId}` or `certificate/*`, where 'certificate' is the prefix and `{CertId}` is the certificate ID.

You can specify one or more resources in the resource description, as shown below:

```
"resource":[ "qcs::ssl:: uin/123456789:certificate/AbcdEfG2",
"qcs::ssl:::certificate/AbcdEfG3"]
```

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

```
"resource":[ "qcs::ssl::uin/123456789:certificate/*"]
```

If you wish to specify all resources, or if a particular API operation does not support resource-level permissions, please use the wildcard "*" in the Resource element as demonstrated below:

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

Sample Access Control Policy

Last updated: 2023-10-09 11:35:03

SSL full read-write policy

- Grant full read-write access (including creation and management) to a sub-user or collaborator.
- Policy Name: QcloudSSLFullAccess

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

SSL read-only policy

- Authorize a sub-user with read-only access to SSL certificates (i.e., the ability to view all resources under SSL), but they cannot create, update, or delete them. In the console, the prerequisite for operating a resource is the ability to view it, so it is recommended to grant full read access to SSL for sub-accounts.
- Policy Name: QcloudSSLReadOnlyAccess

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

```
}
```