SSL 证书

访问管理

产品文档

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

访问管理
访问控制概述

最近更新时间：2021-08-03 14:54:32

访问控制（CAM）用于管理腾讯云账户下资源访问权限，通过 CAM，您可以根据身份管理和策略管理控制哪些子账号有哪些资源的操作权限。

例如，您的账户下有多个证书部署在不同项目中，为了加强权限控制，您需要对资源进行授权，您可以给项目 A 的管理员绑定一个授权策略，该策略规定：只有该管理员可操作项目 A 下的负载均衡资源。SSL 证书大部分接口支持资源级授权，详情请参考 可授权资源类型。

如果您不需要对子账户进行 SSL 证书相关资源的访问控制，您可以跳过此章节。

> ⚠ 注意：
> 目前仅有控制台支持 CAM 访问授权。

CAM 基本概念

主账户通过给子账户绑定策略实现授权，策略设置可精确到[API，资源，用户/用户组，允许/拒绝，条件]维度。

1. **账户**
   - **主账号**：腾讯云资源归属、资源使用计量计费的基本主体，可登录腾讯云服务。
   - **子账号**：由根账号创建账号，有确定的身份 ID 和身份凭证，且能登录到腾讯云控制台。根账号可以创建多个子账号（用户）。**子账号默认不拥有资源，必须由所属根账号进行授权**。
   - **身份凭证**：包括登录凭证和访问证书两种，**登录凭证**是指用户登录名和密码，**访问证书**是指云 API 密钥（SecretId 和 SecretKey）。
2. **资源与权限**
   - **资源**：资源是云服务中被操作的对象，例如一个云服务器实例，COS 存储桶，VPC 实例等。
   - **权限**：权限是指允许或拒绝某些用户执行某些操作。默认情况下，**根账号拥有其名下所有资源的访问权限，而子账号没有根账号下任何资源的访问权限**。
   - **策略**：策略是定义和描述一条或多条权限的语法规范。**根账号**通过将**策略关联**到用户/用户组完成授权。

更多相关信息，请参见 CAM 概述。

相关文档

目标	链接

目标	链接
了解策略和用户之间关系	策略管理
了解策略的基本结构	策略语法
了解还有哪些产品支持 CAM	支持 CAM 的云服务列表

可授权资源类型

最近更新时间：2021-08-02 17:18:16

资源级权限指的是能够指定用户对一些资源具有执行操作的能力。SSL 大部分接口支持资源级授权，即表示针对支持资源级权限的 SSL 操作，能控制并允许用户使用一些特定资源。

SSL 在访问管理中支持的授权类型

资源类型	资源六段式格式
证书	qcs::ssl::$accountid:certificate/$certid

其中：

- 所有 $accountid 应为资源拥有者的 AccountId，或者留空。
- 所有 $certid 应为某个证书的 ID，或者 “*” 。

SSL 在访问管理支持授权的操作

> 说明：
> 目前 SSL 只有 certificate 这一种资源类型。

API操作	资源描述	接口说明
ApplyCertificate	申请免费证书，重新申请证书	* 只对接口进行鉴权
CommitCertificateInformation	提交证书资料	qcs::ssl::$accountid:certificate/$certid
DeleteCertificate	删除证书	qcs::ssl::$accountid:certificate/$certid
DescribeCertificate	获取证书信息	qcs::ssl::$accountid:certificate/$certid
DescribeCertificateDetail	获取证书详情	qcs::ssl::$accountid:certificate/$certid

API操作	资源描述	接口说明
DescribeCertificateOperateLogs	获取证书操作日志列表	qcs::ssl::$accountid:certificate/$certid
DescribeCertificates	获取证书列表	qcs::ssl::$accountid:certificate/$certid
ModifyCertificateAlias	修改证书别名	qcs::ssl::$accountid:certificate/$certid
ModifyCertificateProject	修改证书项目	qcs::ssl::$accountid:certificate/$certid
ReplaceCertificate	重颁发证书	qcs::ssl::$accountid:certificate/$certid
SubmitCertificateInformation	补充证书资料	qcs::ssl::$accountid:certificate/$certid
UploadCertificate	上传证书	* 只对接口进行鉴权

授权策略语法

最近更新时间：2021-08-02 17:17:29

策略语法

CAM 策略：

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

- **版本 version** 是必填项，目前仅允许值为 “2.0”。
- **语句 statement** 是用来描述一条或多条权限的详细信息。该元素包括 effect、action、resource，condition 等多个其他元素的权限或权限集合。一条策略有且仅有一个 statement 元素。
  - **操作 action** 用来描述允许或拒绝的操作。操作可以是 API（以 name 前缀描述）或者功能集（一组特定的 API，以 permid 前缀描述）。该元素是必填项。
  - **资源 resource** 描述授权的具体数据。资源是用六段式描述。每款产品的资源定义详情会有所区别。有关如何指定资源的信息，请参阅您编写的资源声明所对应的产品文档。该元素是必填项。
  - **生效条件 condition** 描述策略生效的约束条件。条件包括操作符、操作键和操作值组成。条件值可包括时间、IP 地址等信息。有些服务允许您在条件中指定其他值。该元素是非必填项。
  - **影响 effect** 描述声明产生的结果是 “允许” 还是 “显式拒绝”。包括 allow（允许）和 deny（显式拒绝）两种情况。该元素是必填项。

SSL 的操作

在 CAM 策略语句中，您可以从支持 CAM 的任何服务中指定任意的 API 操作。对于 SSL，请使用 `name/ssl:` 为前缀指定 action。
您可以在 action 中指定单个或者多个 action。

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

您也可以使用通配符指定多项操作。例如，您可以指定名字以单词 “Describe” 开头的所有操作，如下所示：

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

如果您要指定 ssl 中所有操作，请使用 “*” 通配符，如下所示：

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

SSL 的资源路径

每个 CAM 策略语句都有适用于自己的资源。 资源路径的一般形式如下：

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

- **project_id**：描述项目信息，仅为了兼容 CAM 早期逻辑，无需填写。
- **service_type**：产品简称，例如 ssl。
- **region**：ssl 无地区区分，因此留空。
- **account**：资源拥有者的根帐号信息，例如 uin/164256472，可以不填写，不填写的情况下默认为主账号 ownerUin。
- **resource**：资源详情，例如 certificate/{CertId} 或者 certificate/*，其中 certificate 为前缀，{CertId} 为证书ID。

您可以在资源描述中指定单个或者多个资源，如下所示：

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

您还可以使用 * 通配符指定属于特定账户的所有实例，如下所示：

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

您要指定所有资源，或者如果特定 API 操作不支持资源级权限，请在 Resource 元素中使用 “*” 通配符，如下所示：

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

访问控制策略示例

最近更新时间：2021-08-02 17:16:59

SSL 的全读写策略

- 为子用户或协作者授权完全读写权限（创建、管理等全部操作）。
- 策略名称：QcloudSSLFullAccess

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

SSL 的只读策略

- 授权一个子用户只读访问 SSL 证书的权限（即可以查看所有 SSL 下面所有资源的权限），但用户无法创建、更新或删除它们。 在控制台，操作一个资源的前提是可以查看该资源，所以建议您为子账户开通 SSL 全读权限。
- 策略名称： QcloudSSLReadOnlyAccess

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

```
]
}
```