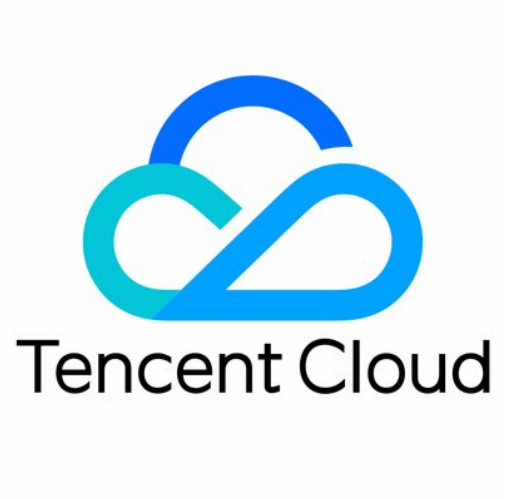
Content Delivery Network

Permission Description

Product Documentation



Permission Description

Last updated：2019-08-12 19:04:10

Tencent Cloud CDN has been integrated with Cloud Access Management (CAM), so that you can manage user groups, users, roles, and polices in the CAM Console.

As the permission control system of CDN is currently being upgraded, you can assign management permissions of CDN to your sub-users and roles in the following ways.

Default Policies

Default policies applicable to CDN include:

- AdministratorAccess: A sub-user associated with this policy can manage the assets, financial information, users, and permissions of all Tencent Cloud services (including CDN) under their account.
- QCloudResourceFullAccess: A sub-user associated with this policy can manage the assets of all Tencent Cloud services (including CDN) under their account.

Project Permissions

Project Management Authorization

CDN supports assigning permissions by project, i.e., configuring project admins. By creating a **project management** policy in the following steps and assigning a project, you can grant a sub-user permissions to manage all CDN resources of the project.

1. Click **Create by Product Feature or Project Permission**.
2. Name the policy and click **Project Management** in Service Type.
3. Enable **Manage CDN Resources in the Project**.
4. Associate the specified project.

After the policy above is created and associated with a sub-user, the sub-user can manipulate all resources of Tencent Cloud services (including CDN) within the project.

Feature-specific Project Authorization

CDN supports project-level authorization by preset feature set. By creating a **CDN** service policy in the following steps, you can grant a sub-user permissions to use specified features in the project:

1. Click **Authorize by Product Feature or Project Permission**.

2. Name the policy and click **CDN** in Service Type.
3. Enable the desired feature set, such as **View usage data and statistics**.
4. Associate the specified project.

After the policy above is created and associated with a sub-user, the sub-user can query the statistics of the resources (domain names) in the project through the following APIs.

Notes on APIs

Sub-users that have resource-specific permissions at the project level can only call the following APIs for related operations.

Permission Set	API 3.0	Authorization Required
Query usage data and statistics	DescribeCdnData DescribeOriginData ListTopData DescribeIpVisit	Yes
Query domain name information	Not available yet	Yes
Query a CDN log download link	Not available yet	Yes
Add a domain name	Not available yet	Yes
Launch/deactivate a domain name	Not available yet	Yes
Delete a domain name	Not available yet	Yes
Modify domain name configuration	Not available yet	Yes
Purge and prefetch	Not available yet	Yes
Query a service	Not available yet	No

Notes on the Console

- View usage data and statistics: If **View usage data and statistics** is enabled in the policy and associated with a project, the sub-user can view the following modules in the console:
  - Overview page
  - Statistical analysis: Real-time monitoring

  - Statistical analysis: Data analysis
  - Internet-wide data monitoring

- Query domain name information: If the policy enables **Query domain name information** and is associated with a project, the sub-user can view the domain name list and detailed configuration information of the authorized project on the **Domain Name Management** page in the console.

- Query a CDN log download link: If the policy enables **Query a CDN log download link** and is associated with a project, the sub-user can query a log download link on the **Log Management** page in the console.

- Add a domain name: If the policy enables **Add a domain name** and is associated with a project, the sub-user can add a domain name to the specified project.

- Launch/deactivate a domain name: If the policy enables **Launch/deactivate a domain name** and is associated with a project, the sub-user can launch/deactivate an accelerated domain name in the specified project.

- Delete a domain name: If the policy enables **Delete a domain name** and is associated with a project, the sub-user can delete an accelerated domain name in the specified project. As only deactivated domain names can be deleted, if the sub-user wants to delete a launched domain name, they need to have the permission to **launch/deactivate a domain name**.

- Modify domain name configuration: If the policy enables **Modify domain name configuration** and is associated with a project, the sub-user can modify the configuration of an accelerated domain name in the specified project.

  > Note:
  >
  > On the **Certificate Management** page in the console, the sub-user can modify the corresponding HTTPS configuration (API 2.0 is not supported at this time).

- Purge and prefetch: If **Purge and prefetch** is enabled in the policy and associated with a project, the sub-user can submit corresponding purge or prefetch tasks and query their execution status on the **Cache Purge** page.

  > Note:

The prefetch feature is in trial period and only open to whitelist users.

Domain Name Permissions

To make it easier for you to configure domain name queries and manage permissions in a more refined manner, the CDN system is currently upgrading the permission policy section and will gradually support policy syntax, so that you can grant permissions at the domain name level through custom policy statements.

The new v3.0 APIs and statistical analysis-enabled console fully support policy syntax with the corresponding actions as below:

- DescribeCdnData: It queries the domain name access monitoring data, including real-time metrics such as bandwidth, traffic, traffic hit rate, requests, status codes, and response time, which supports a granularity of 1 minute. This corresponds to the data on the real-time monitoring page and access monitoring page in **Statistical Analysis** in the console.
- DescribeOriginData: It queries domain name origin-pull monitoring data, including real-time metrics such as origin-pull bandwidth, origin-pull traffic, origin-pull requests, origin-pull failure rate, and origin-pull status codes, which support a granularity of 1 minute. This corresponds to the data on the real-time monitoring page and origin-pull monitoring page in **Statistical Analysis** in the console.
- ListTopData: It supports queries where results can be sorted by multiple criteria, such as sorting traffic data entries by domain name or by URL in the specified time period in descending order, which corresponds to the related list section in **Statistical Analysis** in the console.
- DescribeIpVisit: It queries active IPs with a granularity of 5 minutes and daily active users data, which corresponds to the related module in **Statistical Analysis** in the console.

Policy Syntax

The following policy syntax can be used to grant domain name-level permissions:

- ```
  {
  "version": "2.0",
  "statement": [
  {
  "action": [
  "*"
  ],
  "resource": [
  "qcs::cdn::uin/987654321:domain/www.test.com"
  ],
  ```
  ```

```
"effect": "allow"
}
]
}
```

Syntax description

- action: It indicates the action that needs to be authorized. Only four actions are supported, i.e., DescribeCdnData, DescribeOriginData, ListTopData, and DescribeIpVisit. For more information, see Domain Name Permissions.
- resource: It indicates the object that needs to be authorized. For the CDN service, only domain name-level authorization is supported, and the format in the example must be used.
- effect: It can be configured as "allow" to allow calling "action" for "resource" or "deny" to prohibit calling "action" for "resource".
- Multiple statements can be configured. If both "deny" and "allow" are configured for a domain name, "deny" takes precedence.

Note:

- The policy syntax only supports authorizing the 4 actions as describes above, i.e., DescribeCdnData, DescribeOriginData, ListTopData, and DescribeIpVisit. For more information, see Domain Name Permissions. If `action` is set to "*", all those actions are authorized.
- Domain name-level permissions can be granted by project and through policy syntax at the same time. If a sub-user is granted the data access permission in project A, but denied the data query permission for domain name a in project A by the policy syntax, then the sub-user has no permissions for project A.