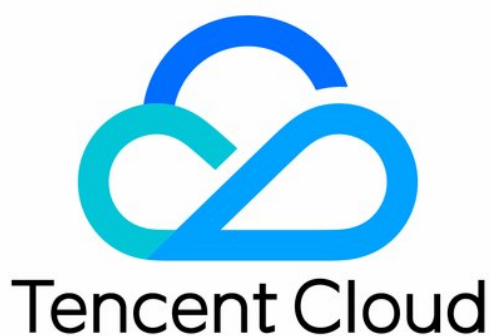


Content Delivery Network Permission Management Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

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.

Contents

Permission Management

Permission Configuration

Console Permissions

Activate Real-time Logging as Sub-account/Collaborator

Permission Management

Permission Configuration

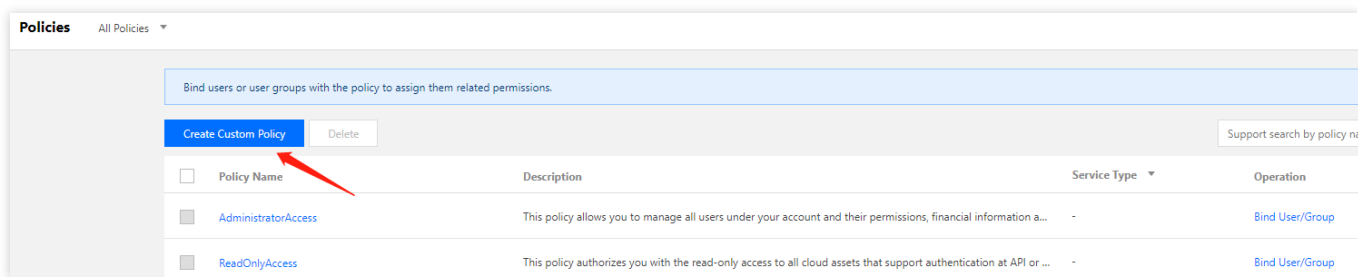
Last updated : 2024-12-30 21:53:33

CDN allows you to configure query and management policies for domain names at a fine granularity. You can grant permissions at the domain name level through custom policy statements.

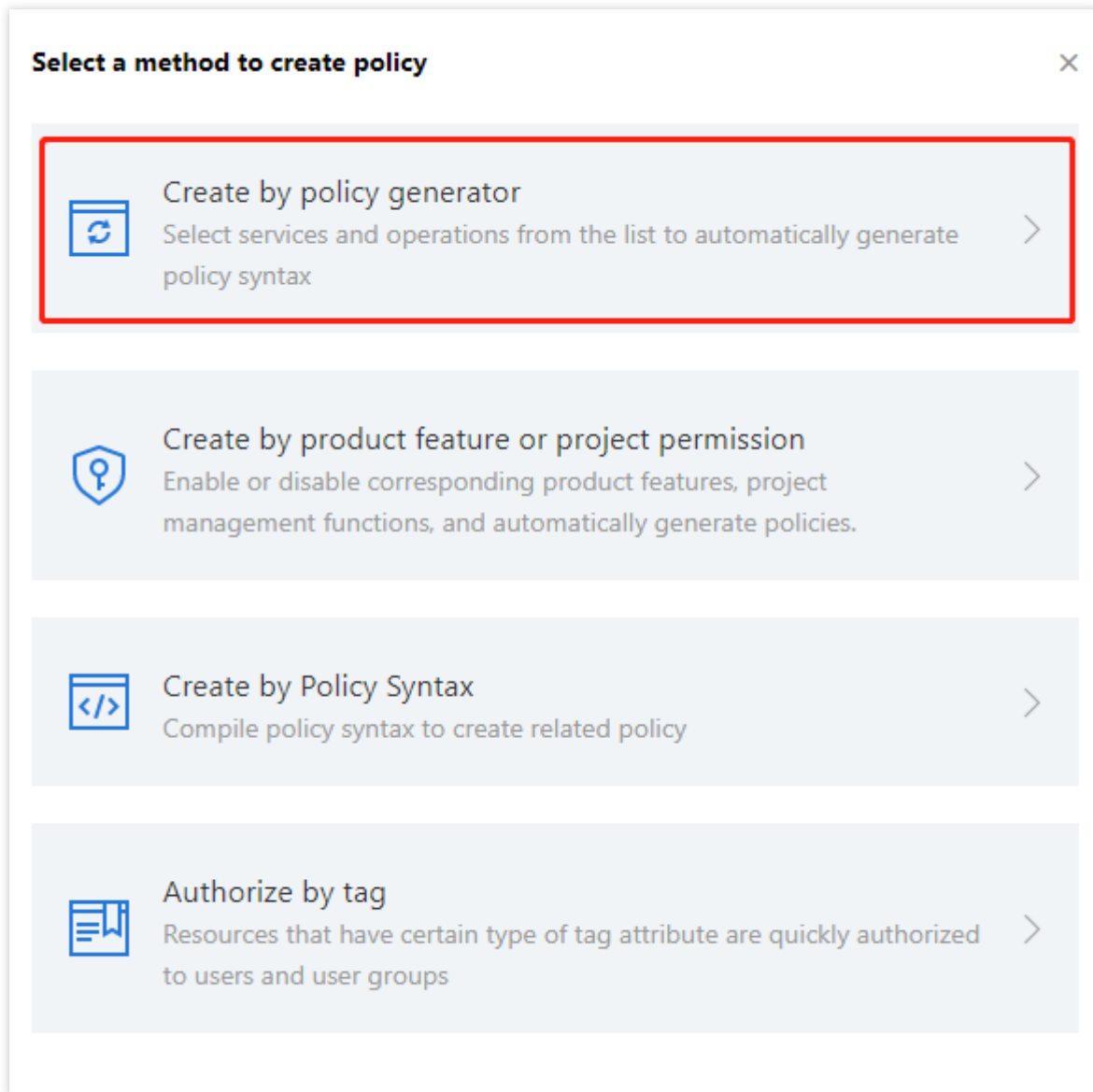
Note:

As the support for CDN API 2.0 has been ended, please choose **Create by Policy Generator** or **Authorize by Tag** to create new policies. The **Create by Product Feature** or **Project Permission** is not recommended.

1. Log in to the [CAM console](#) and click **Policies** to enter the policy management page. Click **Create Custom Policy**:



2. Select **Create by Policy Generator**:



3. Select **CDN** in the service drop-down list and select the actions to be authorized. If you want to grant full read/write permission, check **All actions**. To map specific actions with console features, please see [Console Permissions](#).

1 Select service and operation > 2 Edit Policy

Effect * Allow Reject

Service * CDN

Action * **Action (38 in total)**

Search Action name/description (multiple keywords separated by space)

Action Name	Description
<input type="checkbox"/> All	All Services
<input type="checkbox"/> AddCdnDomain	AddCdnDomain
<input type="checkbox"/> CreateScdnDomain	CreateScdnDomain
<input type="checkbox"/> CreateScdnFailedLogTask	CreateScdnFailedLogTask
<input type="checkbox"/> CreateScdnLogTask	CreateScdnLogTask
<input type="checkbox"/> DeleteCdnDomain	DeleteCdnDomain

(0) selected

Action Name	Description
-------------	-------------

Resource * [Note](#)

Condition

[Add Statement](#)

4. Enter the domain name to be authorized as the resource:

For all domain names: check **All resources** and click **Confirm**.

For specific domain names: check **Specific Resources** and click **Add a 6-segment resource description**.

In the pop-up window on the right, enter a domain name and click **Confirm**. You can repeat the operation to add multiple domain names.

5. After the configuration is completed, click **Confirm** and **Next**. Associate the created policy with existing users or user groups, and finally click **Done** to grant them the permissions.

Console Permissions

Last updated : 2024-12-30 21:53:48

When you have specified both `Action` and `Resource` to create a custom policy, you can call APIs to perform operations for desired resources. This document describes the mappings between console features and `Action`.

Note:

Tencent Cloud CDN can authorize resources by domain name. Authorization does not distinguish between service regions in and outside the Chinese mainland under the same domain name.

When you migrate ECDN services to the CDN console, the ECDN API permission policies will be automatically mapped to corresponding CDN API permission policies. However for resource-level permission policies, you need to set them again in CDN after the migration.

Service Overview

Service overview can categorized as follows based on the displayed content:

Feature	Authorized Action	Notes
Service usage	DescribeCdnData DescribeBillingData	If not all domain names are authorized, each domain name's usage will have to be queried separately
Domain name statistics	DescribeDomains	The total number of authorized domain names will be returned
Billing status	DescribePayType	The permission to change the billing mode cannot be granted to sub-accounts currently
Traffic package statistics	DescribeTrafficPackages	Traffic package status is account-level data, and any associated resources can be queried

Domain Name Management

Feature	Authorized Action	Notes
Domain name list and query	DescribeDomains	Basic configuration items of a domain name can be queried, displayed, and downloaded To get all detailed configuration items, <code>DescribeDomainsConfig</code> should be authorized
Adding domain name	DescribeDomains	Domain names can be added in any acceleration

		service region
Disabling domain name	StopCdnDomain	-
Enabling domain name	StartCdnDomain	-
Deleting domain name	DeleteCdnDomain	-
Modifying domain name project	UpdateDomainConfig	The domain name project is in the domain name configuration All configuration items of a domain name can be modified after authorization
Domain name configuration management	UpdateDomainConfig DescribeDomainsConfig	All configuration items of a domain name can be viewed/modified after authorization

Certificate Management

Feature	Authorized Action	
Querying certificate list	DescribeDomainsConfig	
Configuring certificate	UpdateDomainConfig	
Batch configuring certificates	UpdateDomainsHttps	

Statistical Analysis

Feature	Authorized Action	Notes
Querying detailed access data	DescribeCdnData	All access data metrics under a domain name can be queried after authorization
Querying detailed origin-pull data	DescribeOriginData	All origin-pull data metrics under a domain name can be queried after authorization

Querying top traffic/requests Querying top domain names Querying rankings of domain name status codes Querying usage rankings by province in the Chinese mainland Querying usage rankings by ISP in the Chinese mainland Querying usage rankings outside the Chinese mainland	ListTopData	Rankings of different data metrics and dimensions can be queried after authorization
Querying number of unique IPs	DescribeIpVisit	-

Purge and Prefetch

Feature	Authorized Action
Submitting URLs for purge	PurgeUrlsCache
Submitting directories for purge	PurgePathCache
Querying purge records	DescribePurgeTasks
Submitting prefetch tasks	PushUrlsCache
Querying prefetch records	DescribePurgeTasks

Log Service

Feature	Authorized Action
Querying log download link	DescribeCdnDomainLogs

Network Status Overview

The entire network status monitoring page in the console can be viewed by all sub-accounts with no authorization required.

Operational Report

Features	Authorized Action	Notes
Querying detailed access data	DescribeCdnData	All access data metrics under a domain name can be queried after authorization
Querying detailed origin-pull data	DescribeOriginData	All origin-pull data metrics under a domain name can be queried after authorization
Querying top traffic/requests Querying top domain names Querying rankings of domain name status codes Querying usage rankings by province in the Chinese mainland Querying usage rankings by ISP in the Chinese mainland Querying usage rankings outside the Chinese mainland	ListTopData	Rankings of different data metrics and dimensions can be queried after authorization
Querying number of unique IPs	DescribeIpVisit	-

Traffic Package Management

Feature	Authorized Action	Notes
Querying traffic package list	DescribeTrafficPackages	The content returned by the API is irrelevant to the <code>Resource</code> . The list can be queried with any authorized resource

Note:

Currently, the traffic package renewal and renewal cancellation logics cannot be authorized.

IP Ownership Query

Feature	Authorized Action	Notes
Querying whether IP belongs to Tencent Cloud CDN	DescribeCdnIp	The content returned by the API is irrelevant to the <code>Resource</code> . The list can be queried with any authorized resource

Self-Diagnosis Tool

Currently, the self-diagnosis tool cannot be authorized for sub-accounts.

Activate Real-time Logging as Sub-account/Collaborator

Last updated : 2024-12-30 21:54:02

To activate real-time logging as a sub-account or collaborator, you need to ask the root account or sub-account with administrator permissions to grant access to the following:

1. Preset policy: `QcloudCamSubaccountsAuthorizeRoleFullAccess`
2. Custom policy: `cdn_PassRole`

Directions

1. Associate the preset policy `QcloudCamSubaccountsAuthorizeRoleFullAccess` to the sub-account or collaborator.

The root account/sub-account with administrator permissions needs to log in to the CAM console, and select **Policy** on the left sidebar. Search the preset policy `QcloudCamSubaccountsAuthorizeRoleFullAccess`, and click **Associate Users/Groups** on the right of the policy. In the pop-up dialog, select a sub-account/collaborator to be associated.

2. Create a custom policy `cdn_PassRole` and associate the policy to the sub-account or collaborator.

2.1 The root account/sub-account with administrator permissions needs to log in to the CAM console, select **Policy** on the left sidebar, and then click **Create Custom Policy**. In the pop-up dialog, select **Create by Policy Syntax**.

2.2 On the **Create by Policy Syntax** page, select **Blank Template**, and click **Next**. On the **Edit Policy** page, enter the policy name and content as shown below before clicking **Done**.

The policy syntax is as follows:

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "cam:PassRole"
      ],
      "resource": [
        "qcs::cam::uin/${OwnerUin}:roleName/CDN_QCSRole"
      ]
    }
  ]
}
```

`${OwnerUin}` should be replaced with the root account ID, which can be obtained from the CAM console.

3. Associate the custom policy `cdn_PassRole` to the sub-account or collaborator.

On the Policy page, the custom policy `cdn_PassRole` created is displayed, or search the policy by its name. Click Associate Users/Groups on the right of the policy. In the pop-up dialog, select a sub-account/collaborator to be associated.

4. After all the policy associations are complete, the sub-account/collaborator can activate real-time logging as prompted in the console.