# Content Delivery Network
# Permission Management

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

# Permission Management
# Configure permissions

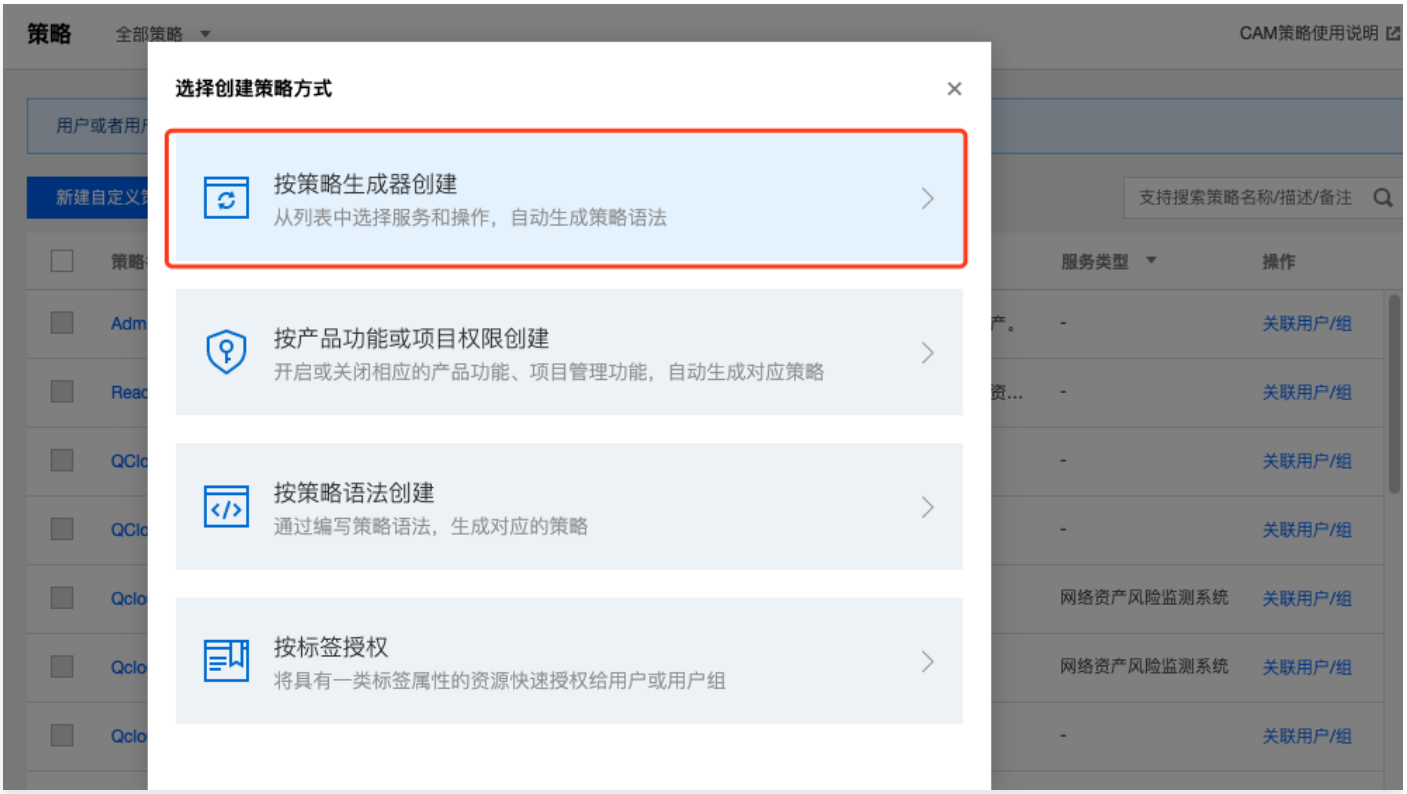
Last updated: 2024-12-31 17:52:23

CDN permission policies have been fully upgraded to facilitate more granular configuration of domain name query and management permissions. Users can achieve domain-level permission allocation through custom policy statements.

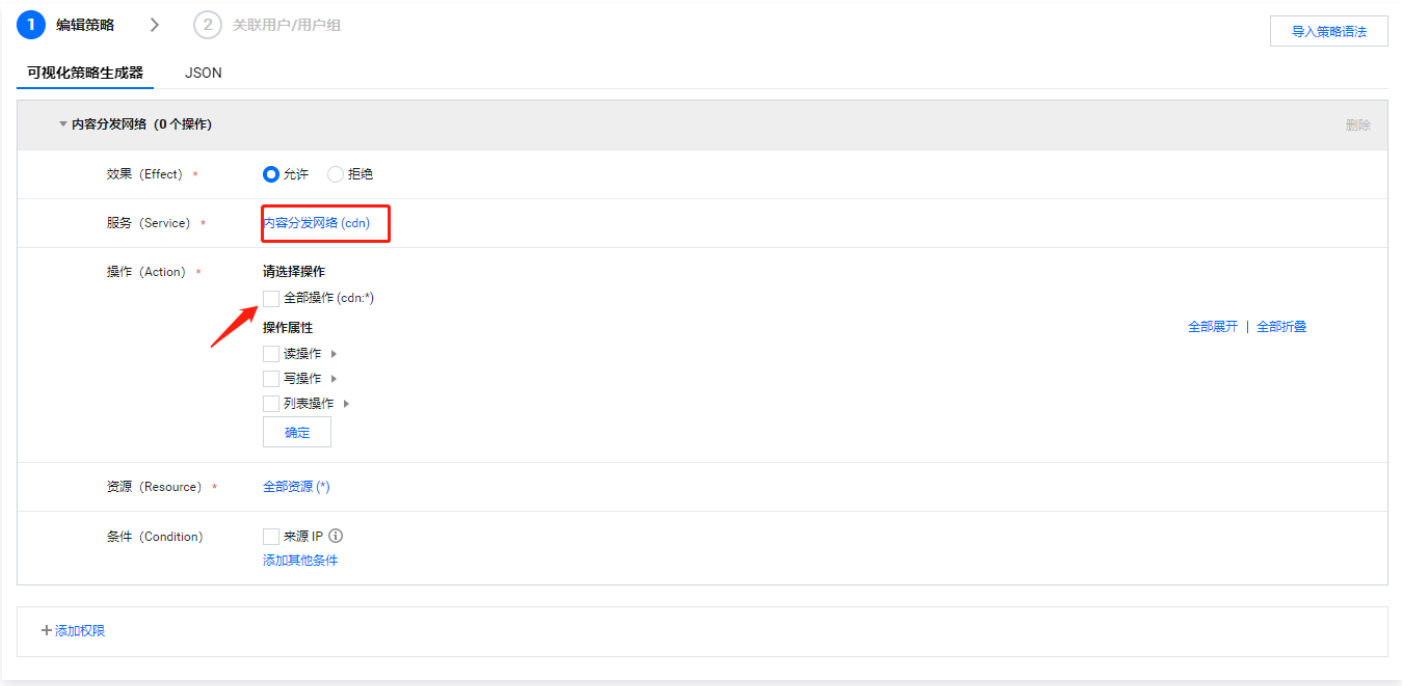
> **Note:**
> Note: As the CDN 2.0 API is no longer updated or maintained, it is not recommended to create new policies using **Create by Product Feature or Project Permission**. Instead, users are advised to use the more comprehensive and convenient **Create Using Policy Generator** or **Tag-based Authorization**.

1. Log in to the CAM Console, click the **Policies** menu to enter the policy management page, and click **Create Custom Policy**:

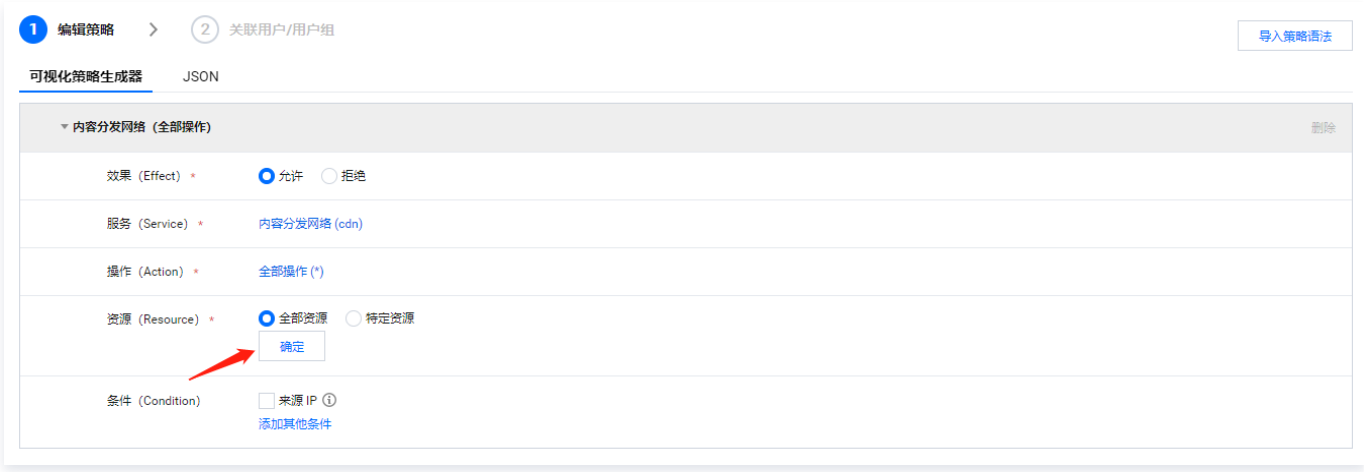

2. Select **Create Using Policy Generator**:




3. In the product selection box, choose **CDN** and select the feature set to be authorized. To grant full read and write permissions, check **All Operations**. For the mapping relationship between features and the console, see the Action Mapping Table.

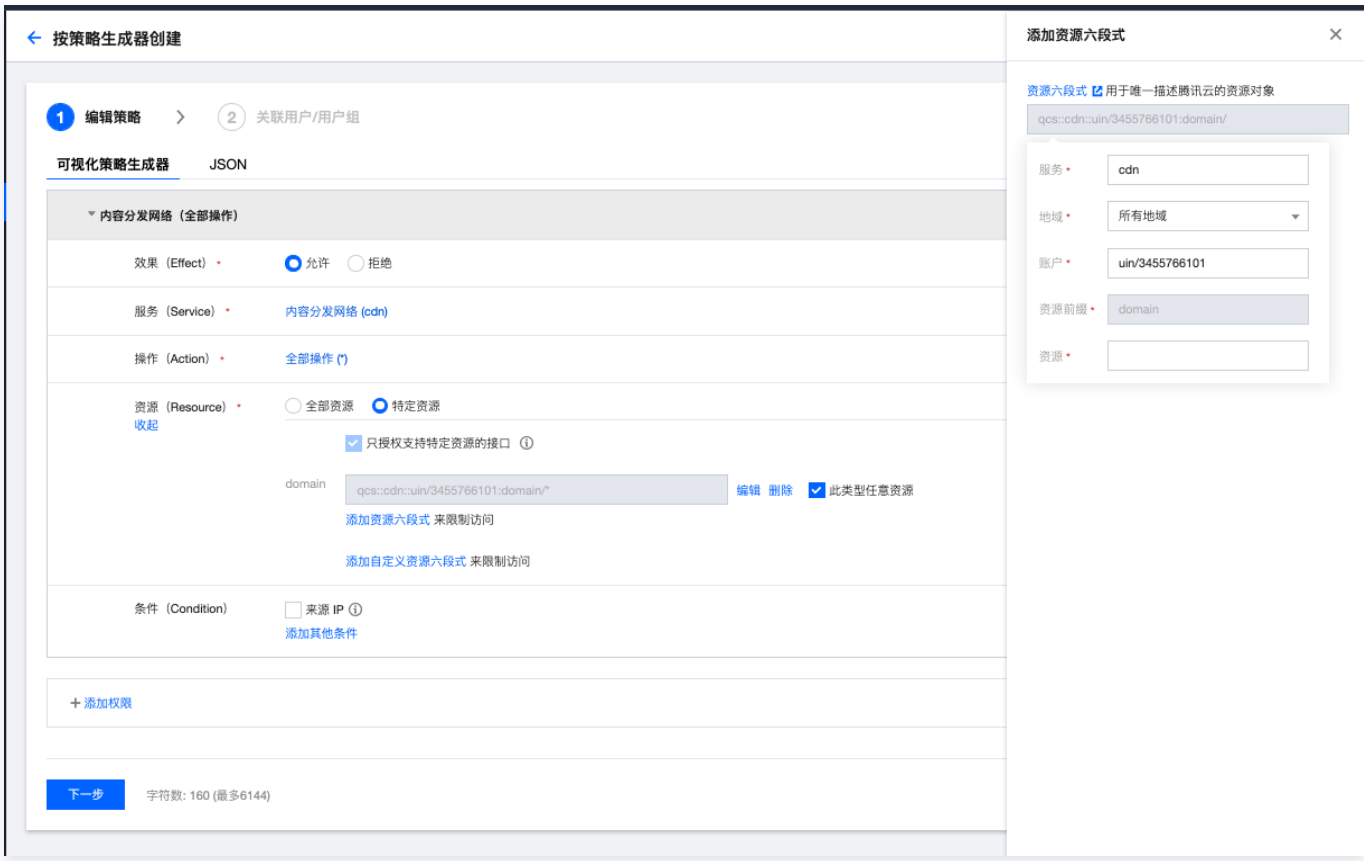



4. Fill in the domain name to be authorized in the resource section. After completing the filling, click **Yes** and click **Next** to create the policy. Associate the created policy with existing users/user groups to authorize.
   - All domain names: Check **all resources** in the resource section, click **Yes**.

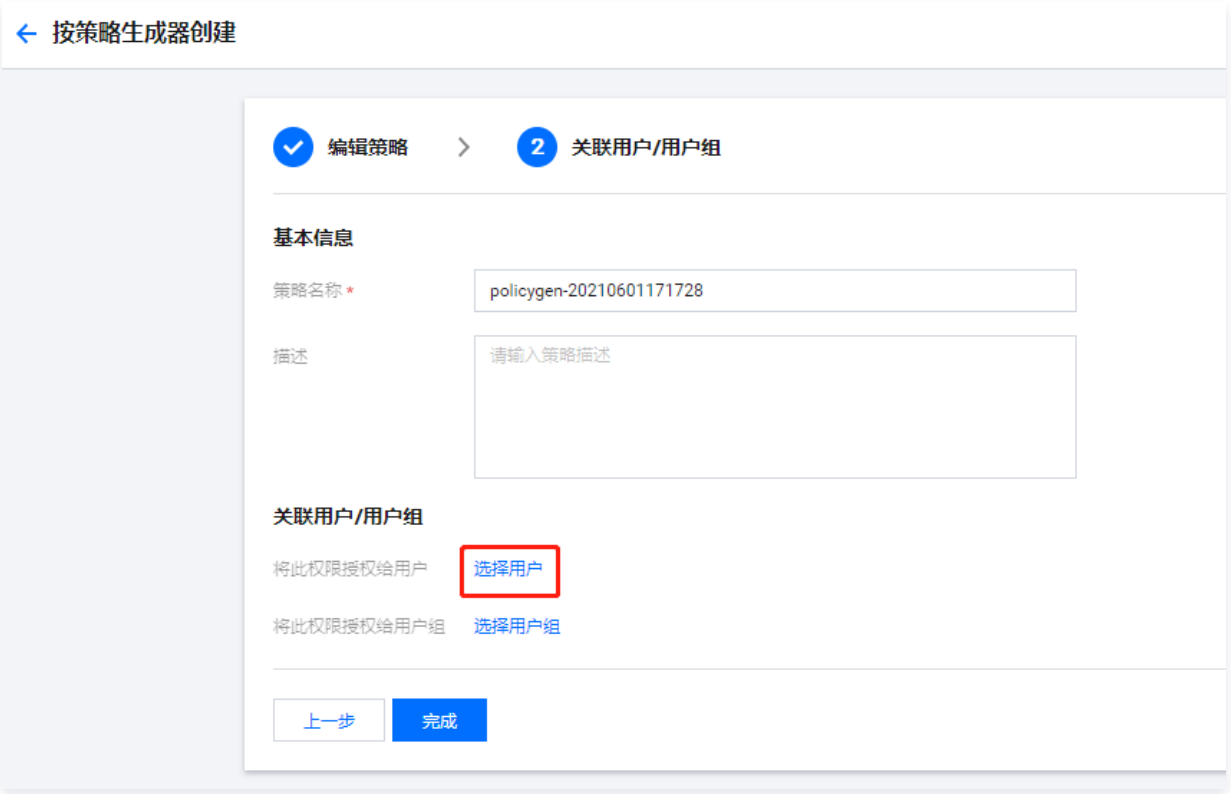



   - Single/Multiple domain names: Check **specific resources**, click **Add a custom six-segment resource description**.


Fill in the corresponding single domain in the **Resources** section of the right popup window, then click **Yes**. To add multiple domains, click **Add a custom six-segment resource description** multiple times.



5. After completing the above operations, click **Next**, select the sub-account user to be authorized, and click **Finish**.



# Console Permission Description

Last updated: 2024-12-31 17:52:31

After specifying action and resource to create a custom policy, you can directly call the API for operations on related resources. The mapping between console features and actions is explained below.

> **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:

| Functional Module | Authorized Action | Must-Knows |
|---|---|---|
| Service Usage Display | DescribeCdnData<br>DescribeBillingData | If only part of the domains are authorized, you can only independently query the usage of each domain name. |
| 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 Management

| Functional Module | Authorized Action | Must-Knows |
|---|---|---|
| Domain name list and query | DescribeDomains | Query / Display / Download basic domain configuration<br>Full detailed configuration requires authorization DescribeDomainsConfig |
| Adding domain name | DescribeDomains | Domain names can be added in any acceleration service region |
| Disabling domain name | StopCdnDomain | - |
| Enabling domain name | StartCdnDomain | - |
| Deleting a domain name | DeleteCdnDomain | - |
| Modifying domain name project | UpdateDomainConfig | The domain's associated project is part of the domain configuration<br>All configuration items of a domain name can be modified after authorization |
| Domain name configuration management | UpdateDomainConfig<br>DescribeDomainsConfig | All configuration items of a domain name can be viewed/modified after authorization |

## Certificate Management

| Functional Module | Authorized Action | Must-Knows |
| --- | --- | --- |
| Querying certificate list | DescribeDomainsConfig | All configuration items of a domain name can be viewed after authorization |
| Configuring Certificates | UpdateDomainConfig | All configuration items of a domain name can be modified after authorization |
| Batch configuring certificates | UpdateDomainsHttps | It is used to configure certificates in batches |

## Statistical Analysis

| Functional Module | Authorized Action | Must-Knows |
| --- | --- | --- |
| 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 |
| Top Traffic/Request Query<br>Top Domain Ranking Query<br>Domain Status Code Ranking Query<br>Domestic Province Usage Ranking Query<br>Domestic ISP Usage Ranking Query<br>Overseas Region Usage Ranking | ListTopData | Rankings of different data metrics and dimensions can be queried after authorization |
| Unique IP Count Query | DescribeIpVisit | - |

## Purge and Prefetch

| Functional Module | Authorized Action |
| --- | --- |
| Submitting URL purge | PurgeUrlsCache |
| Submitting directory refresh | PurgePathCache |
| Query purge records | DescribePurgeTasks |
| Submitting preheating task | PushUrlsCache |
| Querying prefetch records | DescribePushTasks |

## Cloud Log Service

| Functional Module | Authorized Action |
| --- | --- |
| Querying log download link | DescribeCdnDomainLogs |

## Entire Network Status Monitoring

The console global network status monitoring page supports viewing by all sub-accounts without authorization.

## Operational Report

| Functional Module | Authorized Action | Must-Knows |
| --- | --- | --- |

| | | |
|---|---|---|
| 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 |
| Top Traffic/Request Query<br>Top Domain Ranking Query<br>Domain Status Code Ranking Query<br>Domestic Province Usage Ranking Query<br>Domestic ISP Usage Ranking Query<br>Overseas Region Usage Ranking | ListTopData | Rankings of different data metrics and dimensions can be queried after authorization |
| Unique IP Count Query | DescribeIpVisit | - |

## Traffic Package

| Functional Module | Authorized Action | Must-Knows |
|---|---|---|
| Querying traffic package list | DescribeTrafficPackages | The API response is unrelated to the Resource; any resource authorization can query |

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

## IP Ownership Query

| Functional Module | Authorized Action | Must-Knows |
|---|---|---|
| Querying whether IP belongs to Tencent Cloud CDN | DescribeCdnIp | The API response is unrelated to the Resource; any resource authorization can query |

## Self-Diagnostic Tool

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

# Activate Real-time Logging as Sub-account/Collaborator

Last updated: 2024-12-31 17:52:48

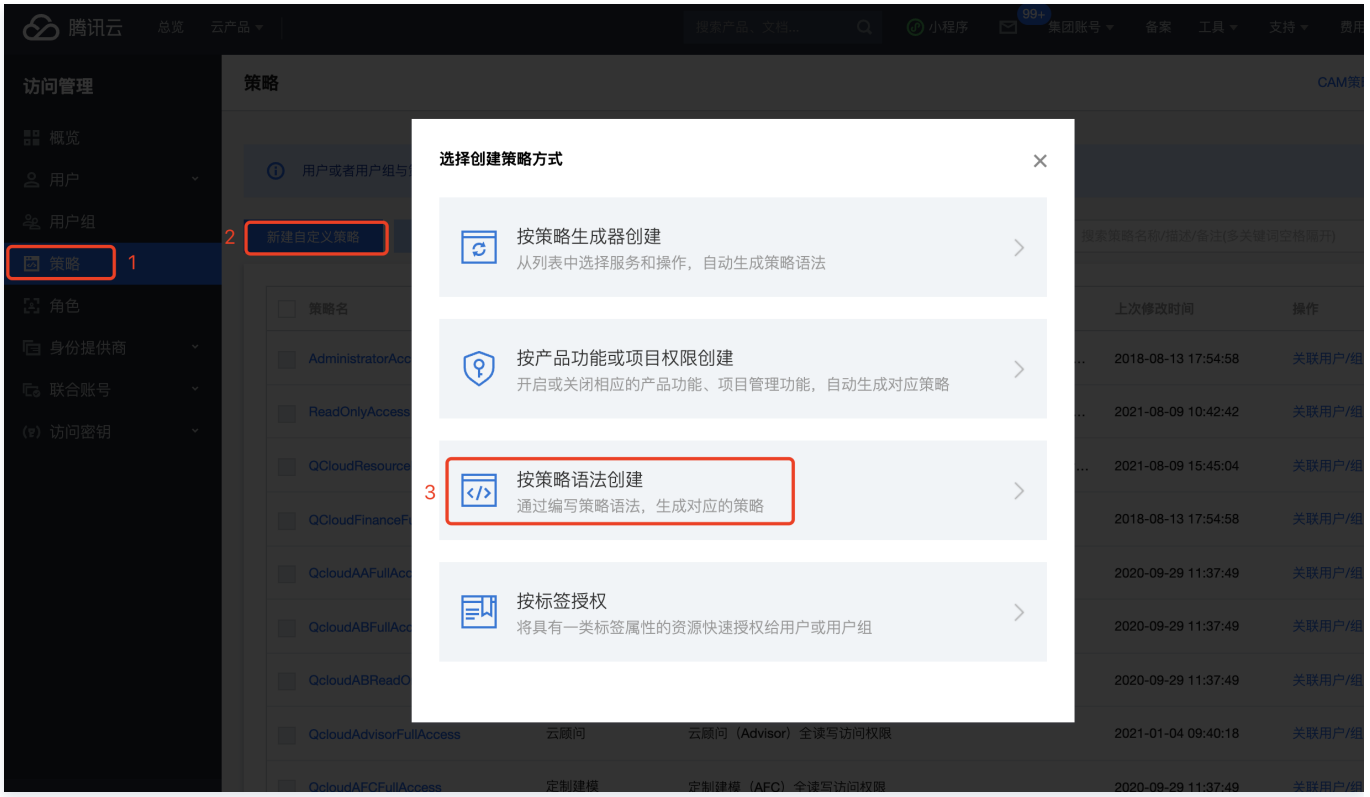
When a sub-account/collaborator activates real-time logging, the main account or a sub-account/collaborator with management permissions needs to grant the following two authorizations to the sub-account/collaborator executing the activation, and then proceed with the activation of real-time logging.

1. Preset policy QcloudCamSubaccountsAuthorizeRoleFullAccess
2. Custom policy cdn_PassRole

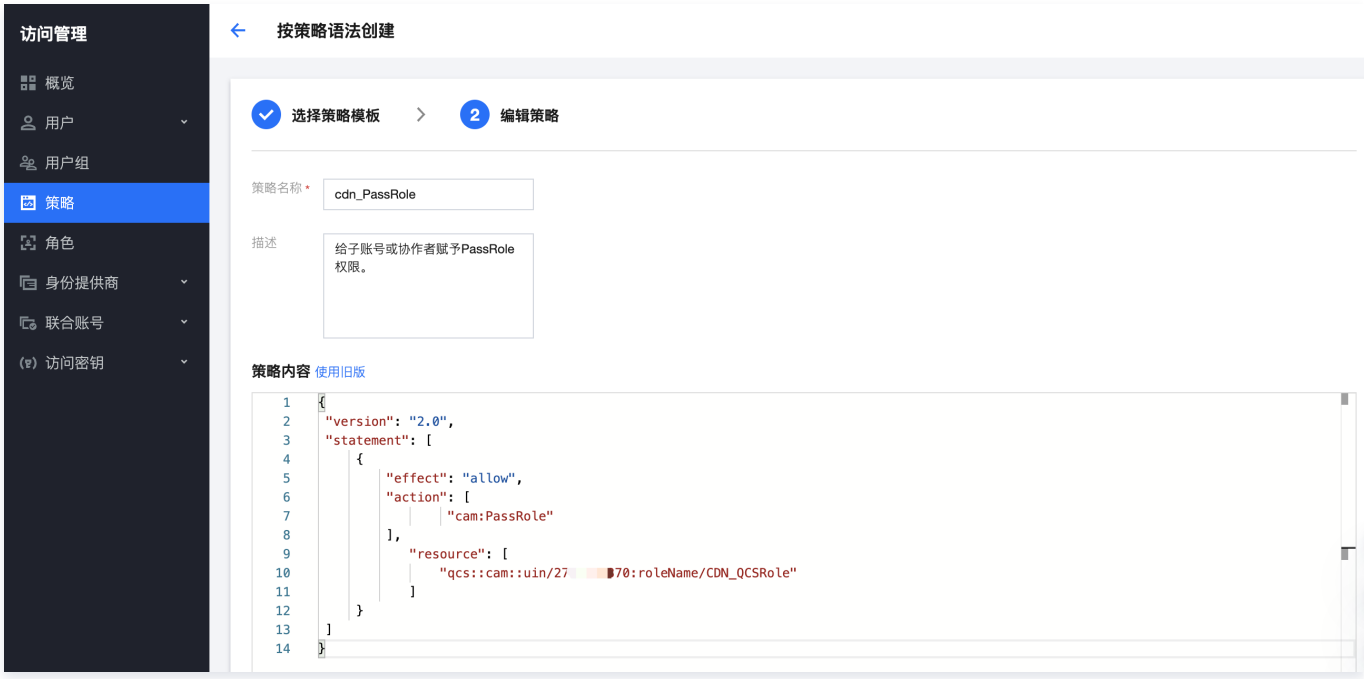
## Operation Steps

1. Associate the preset policy QcloudCamSubaccountsAuthorizeRoleFullAccess with sub-account/Collaborator. The root account or sub-account/Collaborator with administrative privileges should select **Policy** from the left sidebar. After entering the **Policy** page, search for QcloudCamSubaccountsAuthorizeRoleFullAccess to find the policy, click **Associate User/Group** in the operation column on the right, select the sub-account/Collaborator to associate in the pop-up window, and complete the association operation.


2. Create a custom policy cdn_PassRole and associate it with sub-account/Collaborator.
   2.1 The root account or sub-account/Collaborator with administrative privileges 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 box, 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** to create the policy.




The policy syntax is as follows:

```
{
 "version": "2.0",
 "statement": [
  {
   "effect": "allow",
   "action": [
            "cam:PassRole"
   ],
```

```
        "resource": [
            "qcs::cam::uin/${OwnerUin}:roleName/CDN_QCSRole"
        ]
    }
  ]
}
```

Where `${OwnerUin}` needs to be replaced with the main account ID, which can be obtained from the console account information page.

3. Associate the cdn_PassRole policy with the sub-account or collaborator.
   In the left sidebar, select **Policies**. After entering the **Policies** page, you can see the newly created cdn_PassRole policy, or find it by searching names. Click **Associating a Users/Groups** in the right operation column. In the pop-up window, select the sub-account/collaborator to be associated and complete the association operation.


4. After completing the association of the above two permissions, the authorized sub-account/collaborator can activate real-time logging as prompted in the console.