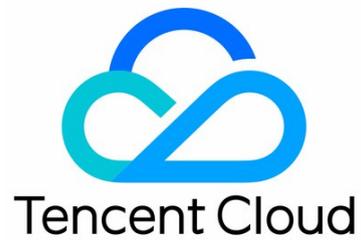


Content Delivery Network Permission Management



Copyright Notice

©2013–2024 Tencent Cloud. All rights reserved.

The complete copyright of this document, including all text, data, images, and other content, is solely and exclusively owned by Tencent Cloud Computing (Beijing) Co., Ltd. ("Tencent Cloud"); Without prior explicit written permission from Tencent Cloud, no entity shall reproduce, modify, use, plagiarize, or disseminate the entire or partial content of this document in any form. Such actions constitute an infringement of Tencent Cloud's copyright, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

Trademark Notice

 Tencent Cloud

This trademark and its related service trademarks are owned by Tencent Cloud Computing (Beijing) Co., Ltd. and its affiliated companies ("Tencent Cloud"). The trademarks of third parties mentioned in this document are the property of their respective owners under the applicable laws. Without the written permission of Tencent Cloud and the relevant trademark rights owners, no entity shall use, reproduce, modify, disseminate, or copy the trademarks as mentioned above in any way. Any such actions will constitute an infringement of Tencent Cloud's and the relevant owners' trademark rights, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

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

- Console Permission Description

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

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.

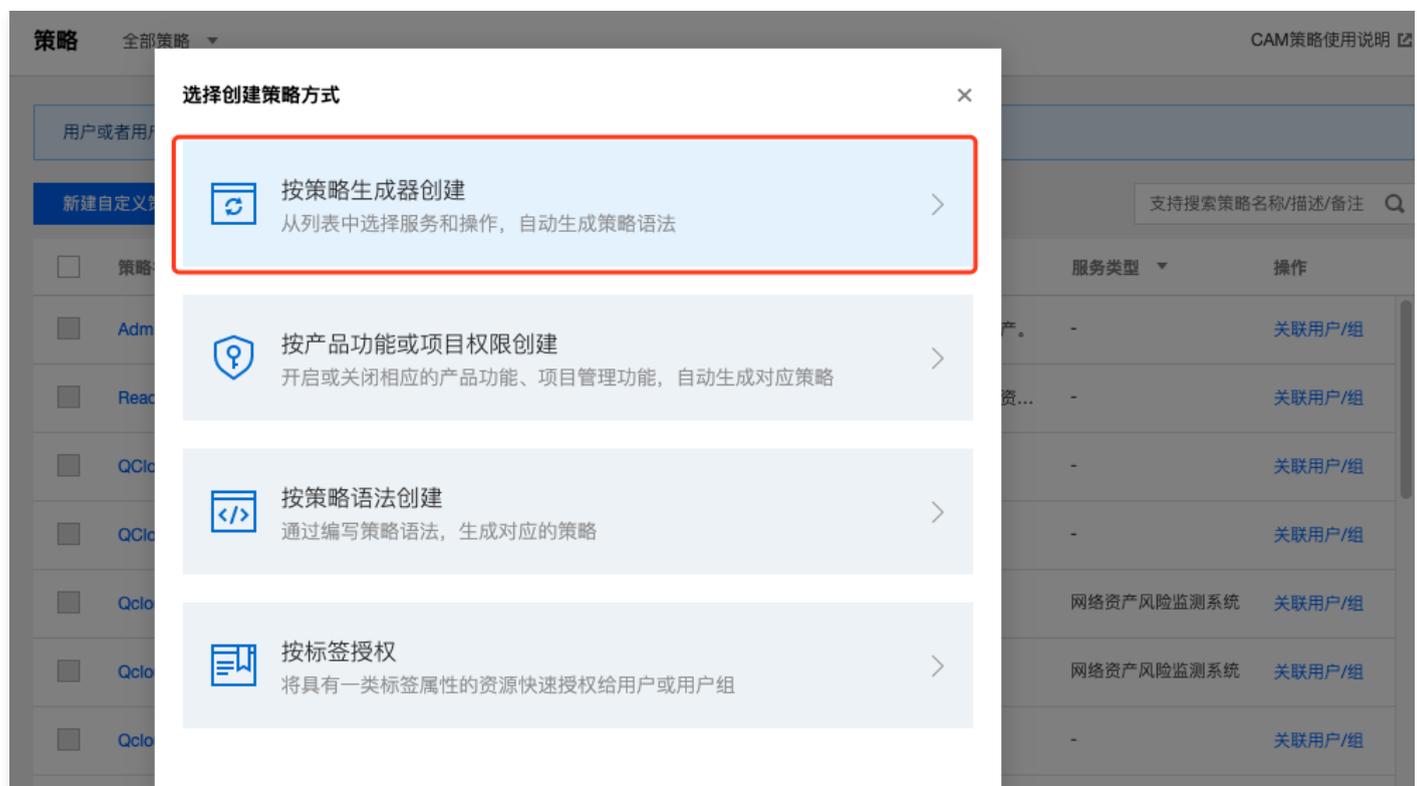
Note:

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](#).

1 编辑策略 > 2 关联用户/用户组 导入策略语法

可视化策略生成器 JSON

▼ 内容分发网络 (0 个操作) 删除

效果 (Effect) * 允许 拒绝

服务 (Service) * 内容分发网络 (cdn)

操作 (Action) * 请选择操作

全部操作 (cdn:*)

操作属性 全部展开 | 全部折叠

读操作 ▶

写操作 ▶

列表操作 ▶

资源 (Resource) * 全部资源 (*)

条件 (Condition) 来源 IP ①

[添加其他条件](#)

[+ 添加权限](#)

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**.

1 编辑策略 > 2 关联用户/用户组 导入策略语法

可视化策略生成器 JSON

▼ 内容分发网络 (全部操作) 删除

效果 (Effect) * 允许 拒绝

服务 (Service) * 内容分发网络 (cdn)

操作 (Action) * 全部操作 (*)

资源 (Resource) * 全部资源 特定资源

条件 (Condition) 来源 IP ①

[添加其他条件](#)

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

1 编辑策略 > 2 关联用户/用户组 导入策略语法

可视化策略生成器 JSON

内容分发网络 (全部操作) 删除

效果 (Effect) * 允许 拒绝

服务 (Service) * 内容分发网络 (cdn)

操作 (Action) * 全部操作 (*)

资源 (Resource) * 全部资源 特定资源

domain 为 DescribeBotRecordData 外加 38 个操作指定 domain 资源六段式①
[添加资源六段式 来限制访问](#)

条件 (Condition) 来源 IP ①
[添加其他条件](#)

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.

按策略生成器创建

1 编辑策略 > 2 关联用户/用户组

可视化策略生成器 JSON

内容分发网络 (全部操作)

效果 (Effect) * 允许 拒绝

服务 (Service) * 内容分发网络 (cdn)

操作 (Action) * 全部操作 (*)

资源 (Resource) * 全部资源 特定资源

[收起](#)

只授权支持特定资源的接口 ①

domain [编辑](#) [删除](#) 此类型任意资源

[添加资源六段式 来限制访问](#)

[添加自定义资源六段式 来限制访问](#)

条件 (Condition) 来源 IP ①
[添加其他条件](#)

+ 添加权限

字符数: 160 (最多6144)

添加资源六段式 ×

资源六段式 [?](#) 用于唯一描述腾讯云的资源对象

服务 *

地域 *

账户 *

资源前缀 *

资源 *

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

← 按策略生成器创建

1 编辑策略 > 2 关联用户/用户组

基本信息

策略名称 *

描述

关联用户/用户组

将此权限授权给用户 [选择用户](#)

将此权限授权给用户组 [选择用户组](#)

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 be categorized as follows based on the displayed content:

Functional Module	Authorized Action	Must-Knows
Service Usage Display	DescribeCdnData 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 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 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

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 Top Domain Ranking Query Domain Status Code Ranking Query Domestic Province Usage Ranking Query Domestic ISP Usage Ranking Query 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 Top Domain Ranking Query Domain Status Code Ranking Query Domestic Province Usage Ranking Query Domestic ISP Usage Ranking Query 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.

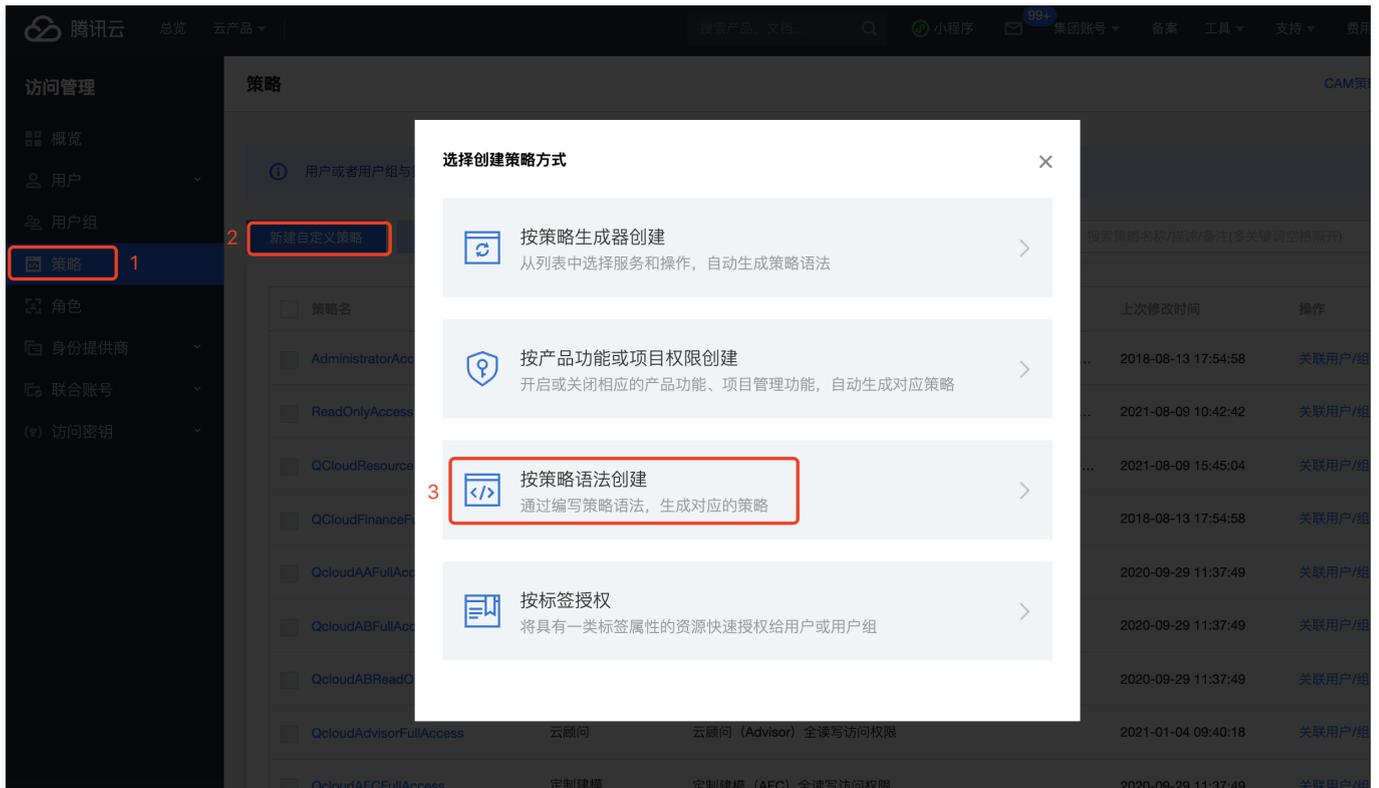
1. Preset policy QcloudCamSubaccountsAuthorizeRoleFullAccess
2. Custom policy cdn_PassRole

Operation Steps

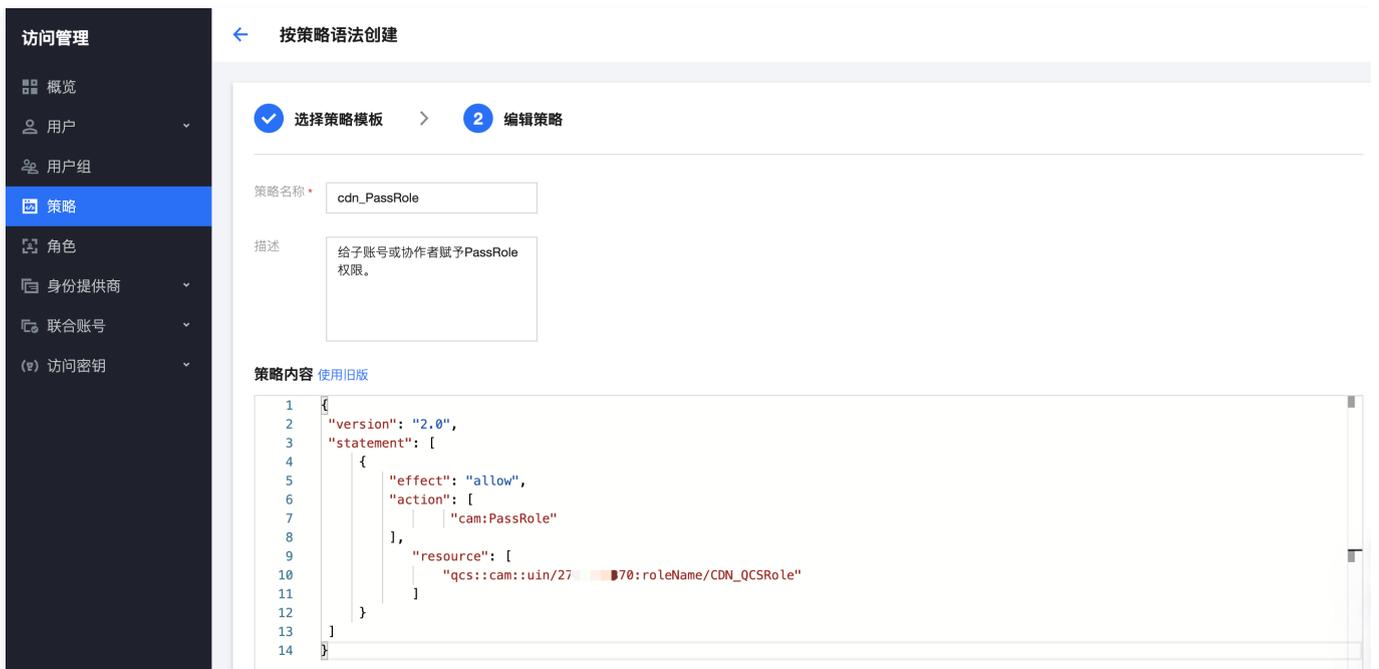
1. Associate the preset policy QcloudCamSubaccountsAuthorizeRoleFullAccess with sub-account/Collaborator. The root account or sub-account/Collaborator with administrative privileges should select **Policy** from the left sidebar. After entering the **Policy** page, search for QcloudCamSubaccountsAuthorizeRoleFullAccess 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.

The screenshot shows the Tencent Cloud console interface for managing policies. The left sidebar is titled '访问管理' (Access Management) and includes options like '概览' (Overview), '用户' (Users), '用户组' (User Groups), '策略' (Policies), '角色' (Roles), '身份提供商' (Identity Providers), and '联合账号' (Federated Accounts). The '策略' (Policies) option is selected and highlighted in red. The main content area is titled '策略' (Policies) and contains a table of policies. The table has columns for '策略名' (Policy Name), '服务类型' (Service Type), '描述' (Description), '上次修改时间' (Last Modified Time), and '操作' (Operations). One policy is listed: 'cdn_PassRole' with a description '给予子账号或协作者赋予PaaRole权限。' (Grant PaaRole permissions to sub-accounts or collaborators). The '操作' column for this policy has a '关联用户组' (Associate User Group) button circled in red. Above the table, there are buttons for '新建自定义策略' (New Custom Policy) and '删除' (Delete), and a search bar for policies.

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.