Content Delivery Network

Configuration Guide

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

Configuration Guide
Domain Management
Domain Name Operations

Last updated：2024-12-31 17:29:57

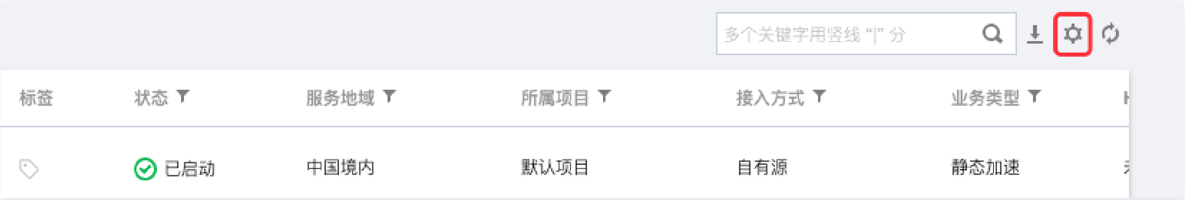
Overview

To manage domain names connected to Tencent Cloud CDN, log in to the CDN console and select **Domain Management** from the left sidebar.
You can customize the domain name list, batch enable/disable acceleration service for domain names, and batch change domain name projects, tags, and configurations, helping you efficiently manage domain names.

Operation Guide

Customizing the List of Adjustments

Click the ⚙ on the right side of the search box, to open the list configuration popup. You can specify which domain configuration items to display or hide, and adjust their display order.



标签	状态	服务地域	所属项目	接入方式	业务类型
	已启动	中国境内	默认项目	自有源	静态加速

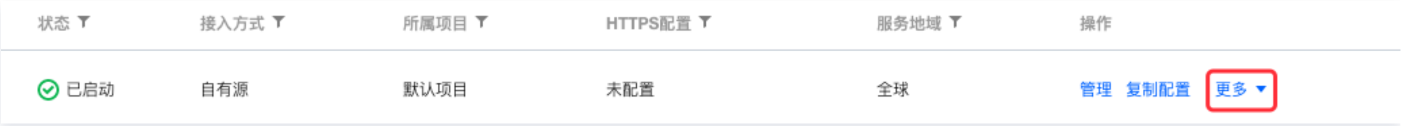
Exporting Domain Configuration

Click the ⤓ icon on the right side of the search bar to export an Excel file of the basic configuration list of domain names. You can export up to 1000 domain names at a time.

Editing Projects

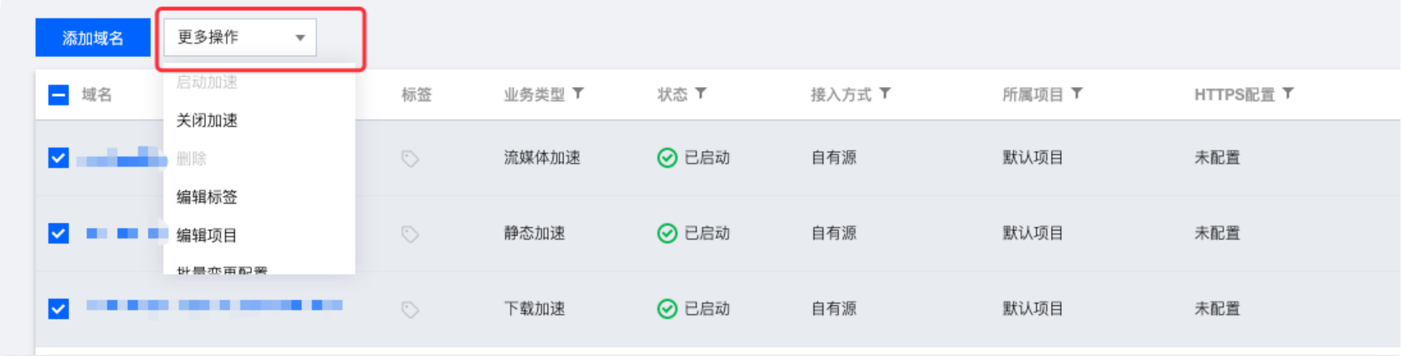
You can change the projects of normally-running domain names.

- Single domain operation: Click **More** on the right side of the domain to change the project the domain belongs to.



状态	接入方式	所属项目	HTTPS配置	服务地域	操作
已启动	自有源	默认项目	未配置	全球	管理 复制配置 更多

- Batch operations: Select multiple domains and click "Edit Project" under **More Operations**. (Note: Up to 50 domains can be selected at a time)



域名	标签	业务类型	状态	接入方式	所属项目	HTTPS配置
[redacted]		流媒体加速	已启动	自有源	默认项目	未配置
[redacted]		静态加速	已启动	自有源	默认项目	未配置
[redacted]		下载加速	已启动	自有源	默认项目	未配置

Editing Tags

- Single domain: Click to enter the domain, and modify the "Tag" in the domain's **Basic info**.
- Batch operations: Select multiple domains, and click "Edit Tag" in **More Operations** above.
  (Note: Maximum quantity per order is 50 domains; changes do not take effect immediately, refresh to see the latest tag content.)

Disabling the acceleration service

When you disable the acceleration service for a domain name, it is deactivated on CDN cache nodes across the entire network. All access requests to the domain name get 404. Therefore, before disabling a domain name, make sure that its CNAME record is resolved to a non-CDN CNAME address.

> **Note**
> Consumption will no longer be generated after the acceleration service is completely disabled.

- Single domain operation: Click **More** on the right to close the domain.
- Batch disable: Select domain names in **Enabled** status, click **More Operations** on the top to disable them in bulk.

Enabling acceleration service

You can re-enable the acceleration service for closed domains, and the domain configuration will be reissued to all acceleration nodes by enabling the acceleration service.

- Single domain: If the domain status is **Disabled**, click **More** on the right to enable the domain.
- Batch enable: Select domain names in **Disabled** status, click **More Operations** on the top to enable them in bulk.

> **Note**
> If an enabled domain name has no operations or consumption for 3 months, it will be considered inactive and CDN will automatically disable its acceleration service.

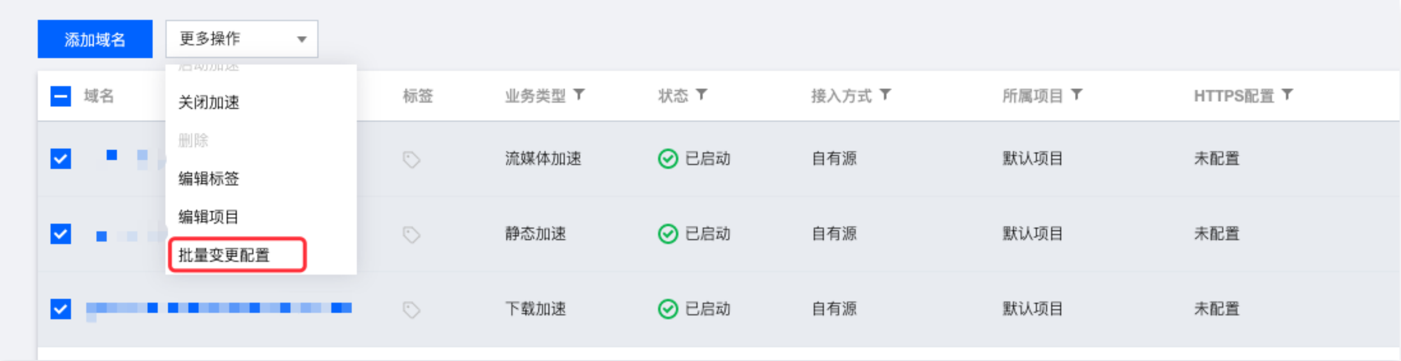
Deleting accelerated domain names

The delete operation can only be performed when the domain status is **Disabled**. After deletion, the domain and its configurations will be cleared and unable to retrieve, and its statistical data will no longer be available. Please proceed with caution:

- Single domain operation: Click **More** on the right to delete the domain.
- Batch operations: Select domains in **Disabled** status and perform batch deletion through **More Operations** above.

Batch changing configurations

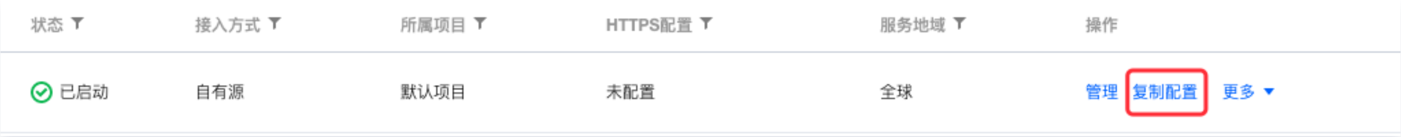
The Batch Change Configuration feature allows you to change a configuration item of multiple domain names at the same time. For more information, please see Batch Changing Configuration.



☑ 域名	标签	业务类型	状态	接入方式	所属项目	HTTPS配置
☑ [redacted]		流媒体加速	✓ 已启动	自有源	默认项目	未配置
☑ [redacted]		静态加速	✓ 已启动	自有源	默认项目	未配置
☑ [redacted]		下载加速	✓ 已启动	自有源	默认项目	未配置

Copying configurations

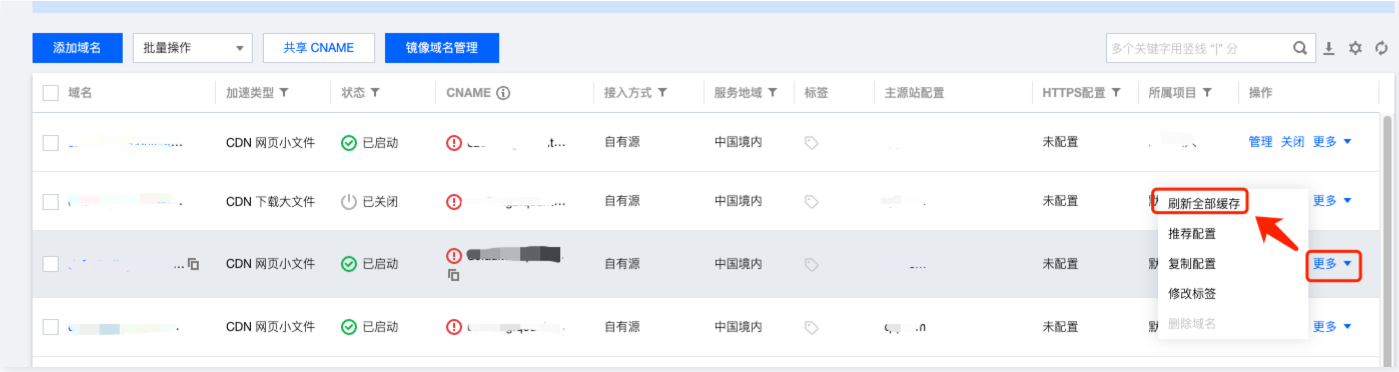
The Copy Configuration feature allows you to duplicate configurations of an existing acceleration domain name to one or multiple new acceleration domain names. For more information, please see Copying Configuration.



状态	接入方式	所属项目	HTTPS配置	服务地域	操作
已启动	自有源	默认项目	未配置	全球	管理 复制配置 更多

Refresh all caches

To purge all cached resources on the CDN nodes under the current domain name, click the **More** button on the right of the domain name, and select **Purge all caches** in the pop-up window. This is used for one-click refresh of all cached resources under the current domain name, suitable for quickly clearing old cached resources on the nodes when there are large-scale resource updates under the domain name.



域名	加速类型	状态	CNAME	接入方式	服务地域	标签	主源站配置	HTTPS配置	所属项目	操作
[redacted]	CDN 网页小文件	已启动	[redacted]	自有源	中国境内		[redacted]	未配置	[redacted]	管理 关闭 更多
[redacted]	CDN 下载大文件	已关闭	[redacted]	自有源	中国境内		[redacted]	未配置		更多
[redacted]	CDN 网页小文件	已启动	[redacted]	自有源	中国境内		[redacted]	未配置	默	更多
[redacted]	CDN 网页小文件	已启动	[redacted]	自有源	中国境内		[redacted]	未配置	默	更多

Domain name search

Last updated：2024-12-31 17:30:08

Retrieval Scenario

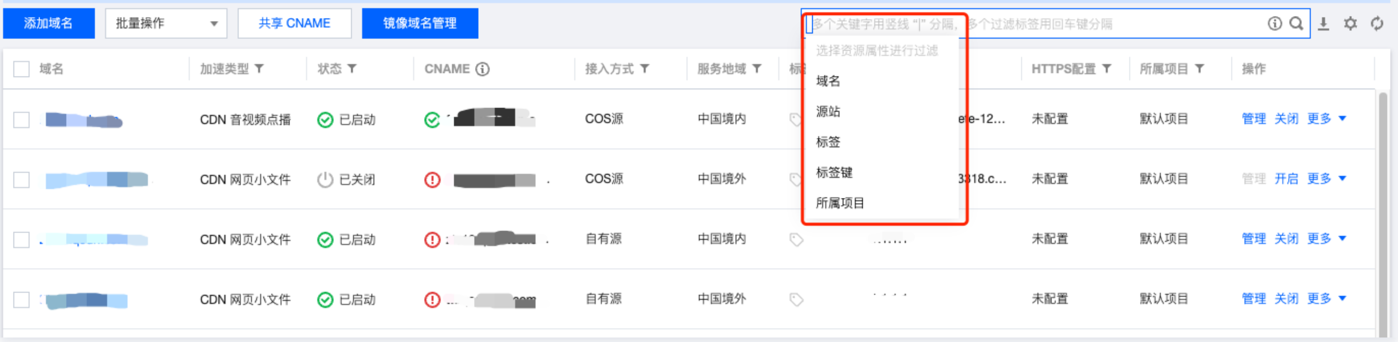
After accessing Tencent Cloud CDN acceleration service, you need to filter the list based on domain names or their specified attributes, or manage cloud resources based on tags, projects, etc.
Tencent Cloud CDN supports multi-condition combination queries through domain names, origin servers, tags, and projects, and supports multiple keyword filtering.
Watch video

> **Note:**
> A tag is provided by Tencent Cloud to identify resources on the cloud. For more information on tags and how to manage it, please see Tag.

Operation Guide

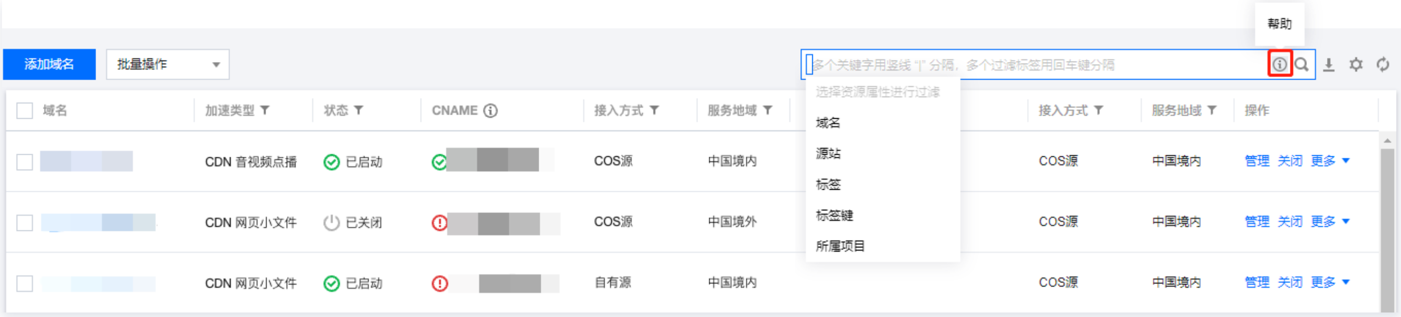
Starting Search

1. Log in to the CDN console, click **Domain Management** on the left menu to enter the management page. (Note: Ordered list content)
2. Click the domain name search box to activate the search feature, select one or more resource attributes such as domain name, origin server, tag, or project, and enter a value to filter domain names.


添加域名
批量操作
共享 CNAME
镜像域名管理
多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔
选择资源属性进行过滤
域名
源站
标签
标签键
所属项目
域名
加速类型
状态
CNAME
接入方式
服务地域
HTTPS配置
所属项目
操作
CDN 音视频点播 已启动 COS源 中国境内 ee-12... 未配置 默认项目 管理 关闭 更多
CDN 网页小文件 已关闭 COS源 中国境外 3318.c... 未配置 默认项目 管理 开启 更多
CDN 网页小文件 已启动 自有源 中国境内 未配置 默认项目 管理 关闭 更多
CDN 网页小文件 已启动 自有源 中国境外 未配置 默认项目 管理 关闭 更多

(Note: Ordered list content)

3. If you have any questions about input resource attributes or input format, you can click the [i] icon to get a search example.


帮助
添加域名
批量操作
多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔
选择资源属性进行过滤
域名
源站
标签
标签键
所属项目
域名
加速类型
状态
CNAME
接入方式
服务地域
接入方式
服务地域
操作
CDN 音视频点播 已启动 COS源 中国境内 COS源 中国境内 管理 关闭 更多
CDN 网页小文件 已关闭 COS源 中国境外 COS源 中国境内 管理 关闭 更多
CDN 网页小文件 已启动 自有源 中国境内 COS源 中国境内 管理 关闭 更多

Search Description

Search Item Description:

- Domain Search: Supports fuzzy matching of complete or partial domain names, and single keyword search.
- Origin Server Search: Supports matching of complete or partial origin server content, fuzzy matching, currently only searches the primary origin server, does not support backup origin server or region-specific origin server configurations, and supports single keyword search.
- Tag Search: Enter a complete tag, and a list of domain names that contain the entered tag will be returned. Tag names **do not support fuzzy search**.

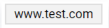
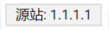
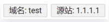
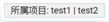
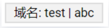
- Project Search: Supports selecting one or multiple projects as a filter.

> **Note**
> When no search item is specified, the default is to search for **domain names**. When entering a single keyword, the search box content is: `Domain name: www.test.com` ; when pasting characters, the search box content is: `Domain name: test|abc` .

Search Capability Description:

- Filter by multiple criteria: You can select one or more criteria such as tag, domain name, origin server, and project for filtering. Use the enter key to separate multiple criteria.
- Filter by multiple keywords: You can enter multiple keywords for each filter criterion, separated by a vertical bar ("|").

Retrieval Example

Category	Input Format	Example	Search Box Example	Description
Single keyword	[Keyword]	`www.test.com`	 www.test.com	Filter domain names containing the character " `www.test.com` ".
Single domain name attribute	[Attribute]:[Keyword]	Origin server:1.1.1.1	 源站: 1.1.1.1	Filter domain names with origin server containing "1.1.1.1".
Multiple domain name attributes	[Attribute]:[Keyword][Enter] [Attribute]:[Keyword]	Domain name:test Origin server:1.1.1.1	 域名: test 源站: 1.1.1.1	Filter domain name containing "test", origin server containing "1.1.1.1".
Single domain name attribute with multiple keywords	[Attribute]:[Keyword]|[Keyword]	Project:test1|test2	 所属项目: test1 | test2	Filter belonging project containing "test1" or "test2". Domain name and origin server attributes do not support multi-keyword search.
Copied character	(Pasted character)	test abc	 域名: test | abc	Filter domain name containing "test" or "abc".

Copying configurations

Last updated：2024-12-31 17:30:26

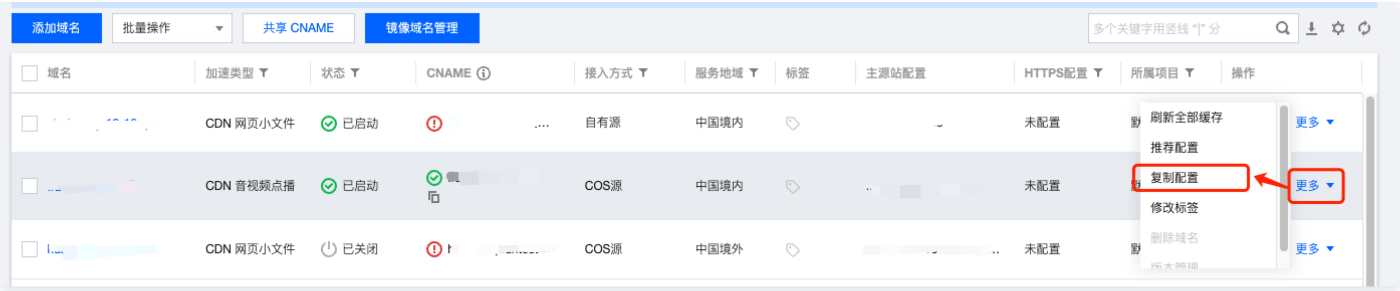
Configuration Scenario

The Copy Configuration feature allows you to duplicate configurations of an existing accelerated domain name to one or more newly added accelerated domain names. You can select an existing domain name as needed and copy its configuration to the new domain names, making it more convenient and faster to connect domains without configuring each new domain individually on the console.

> **Note**
> - This feature is not available for domain names that are disabled or blocked, having expired ICP filing, using external certificates, or with unsupported configurations varying across regions.
> - Note: If the copied domain name has backend-specific configurations (not configured on the console), these configurations cannot be copied.

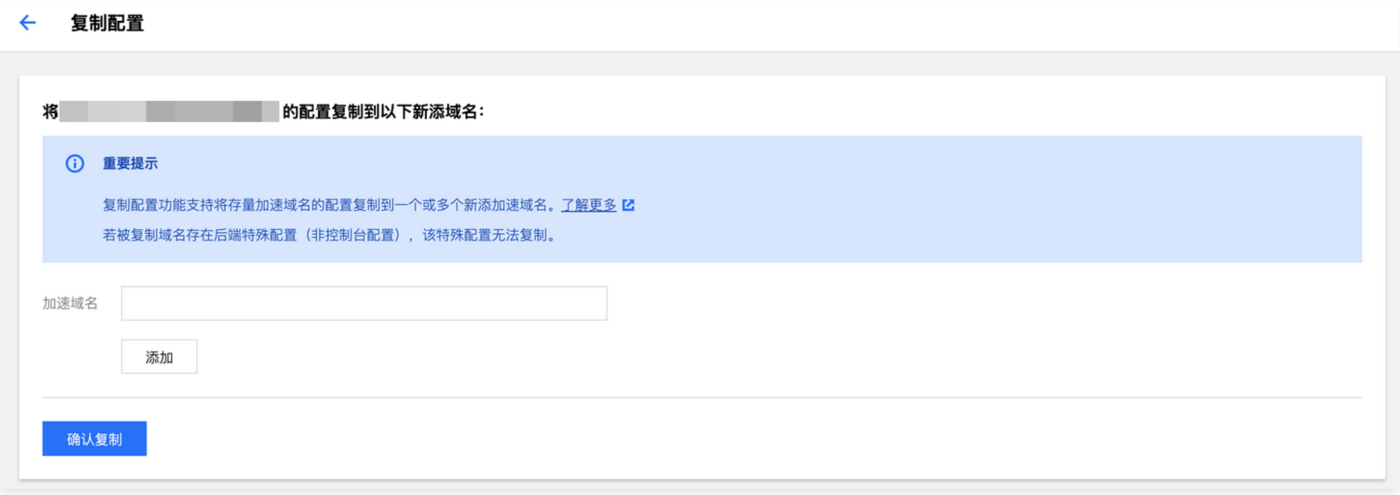
Configuration Guide

Log in to the CDN Console, select **Domain Management** from the left sidebar menu, and click **Copy Configuration** in the domain operation column to enter the copy configuration page.



域名	加速类型	状态	CNAME	接入方式	服务地域	标签	主源站配置	HTTPS配置	所属项目	操作
[redacted]	CDN 网页小文件	已启动	[redacted]	自有源	中国境内		[redacted]	未配置	默	更多
[redacted]	CDN 音视频点播	已启动	[redacted]	COS源	中国境内		[redacted]	未配置	默	更多
[redacted]	CDN 网页小文件	已关闭	[redacted]	COS源	中国境外		[redacted]	未配置	默	更多

You can add new accelerated domain names. After submission, the configuration of the current accelerated domain name will be copied to the new domain names.



复制配置

将[redacted]的配置复制到以下新添域名：

重要提示

复制配置功能支持将存量加速域名的配置复制到一个或多个新添加速域名。了解更多

若被复制域名存在后端特殊配置（非控制台配置），该特殊配置无法复制。

加速域名

> **Note:**
> - The submitting process cannot be interrupted. You can manage the configuration after the new domain name is successfully added.
> - Note: The configurations of a new domain name will be deployed to CDN nodes across the entire network, without affecting your current network business. If you want to officially start acceleration, you need to configure the CNAME. For configuration directions, please see Configure CNAME.

Batch changing configurations

Last updated：2024-12-31 17:30:37

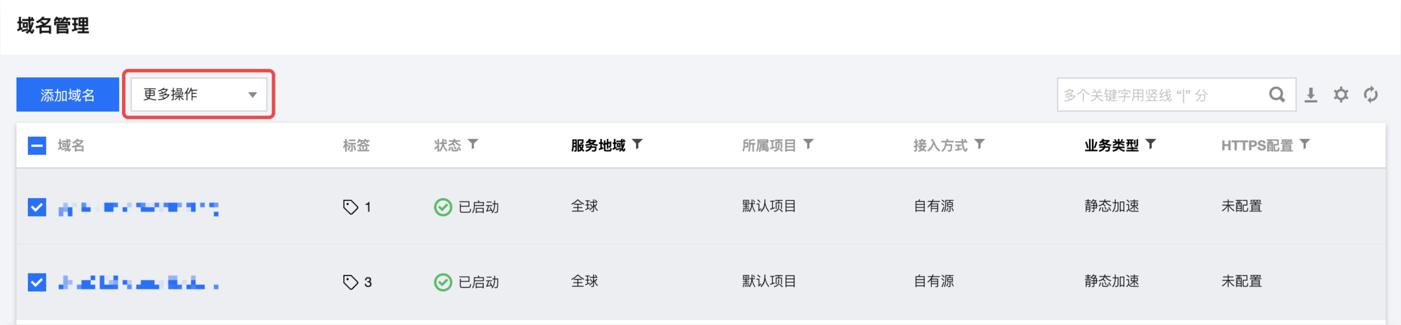
Feature Scenarios

The Batch Change Configuration feature allows you change a configuration item of multiple domain names at the same time.

> **Note**
> This feature does not cover all configuration items of the domain name. Some configuration items are not yet supported and will be gradually updated and released. (Note)

Operation Guide

Log in to the CDN console, select **Domain Management** from the left sidebar menu to enter the domain name management page. When two or more active domain names are selected, choose **More Operations** and then **Batch Change** to enter the batch change configuration page.


域名管理

☐ 域名	标签	状态	服务地域	所属项目	接入方式	业务类型	HTTPS配置
☑ [redacted]	1	✓ 已启动	全球	默认项目	自有源	静态加速	未配置
☑ [redacted]	3	✓ 已启动	全球	默认项目	自有源	静态加速	未配置

> **Note**
> - The new configuration will overwrite the original configuration items of the selected domain names. (Note)
> - Configurations of closed, disabled, blocked, and locked domain names cannot be changed in batches.
> - For domain name configurations that have special backend settings (not configured on the console), these special settings cannot be changed.

More Descriptions

- Configuration changes are irreversible. After the changes are successfully applied, you can manage the domain name configuration normally.
- As some configuration items are associated with acceleration regions/business types/HTTPS certificate configurations, it is recommended to select domain names with the same acceleration regions/business types/HTTPS configuration status for batch changes.
- To batch change the HTTPS certificate configurations, please go to the certificate management page.
- Up to 20 domain names can be changed at a time. It’s not suggested to choose too many domain names as it may take quite a long time for the change to take effect.

Version Management

Last updated：2024-12-31 17:30:49

Note:
The feature is no longer maintained and is about to go offline. If you have similar needs, please contact Online Customer Service for feedback.

Feature Description

Tencent Cloud CDN supports version management for a single domain name, with each version corresponding to a domain name configuration. You can deploy different versions for the domain name. Both production and staging environments are supported:

- Production environment: the live environment where acceleration services are put into operation.
- Staging environment: a sandbox for testing domain name configurations only. This environment is built on a small scale and is only expected for domain name configuration tests in the console. It should not be use for actual business running or performance tests.

Note

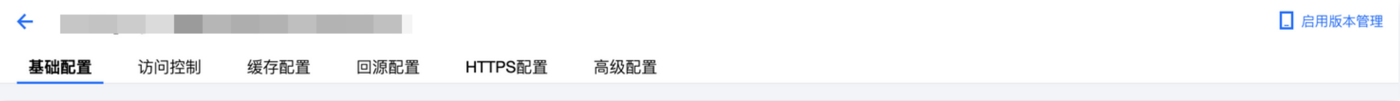
1. Note: Version management is currently only supported for domain names that have not configured a self-owned certificate and have not enabled the Image Optimization feature.
2. Only one version can be deployed at a time in each environment.
3. Note: URL refresh is supported in both the production environment and staging environment, while directory refresh and URL prefetch are only allowed in the production environment. For more information, see Purge and Prefetch.
4. Note: Usage cap and other data/usage monitoring features are only available in the production environment.

Application Scenarios

- Domain name configuration grayscale testing.

Enabling Version Management

Log in to the CDN console, select **Domain Management** in the menu bar to enter the domain list. Click the domain name for which you want to enable version management to enter the domain configuration page. You can see **Enable Version Management** in the top right corner.

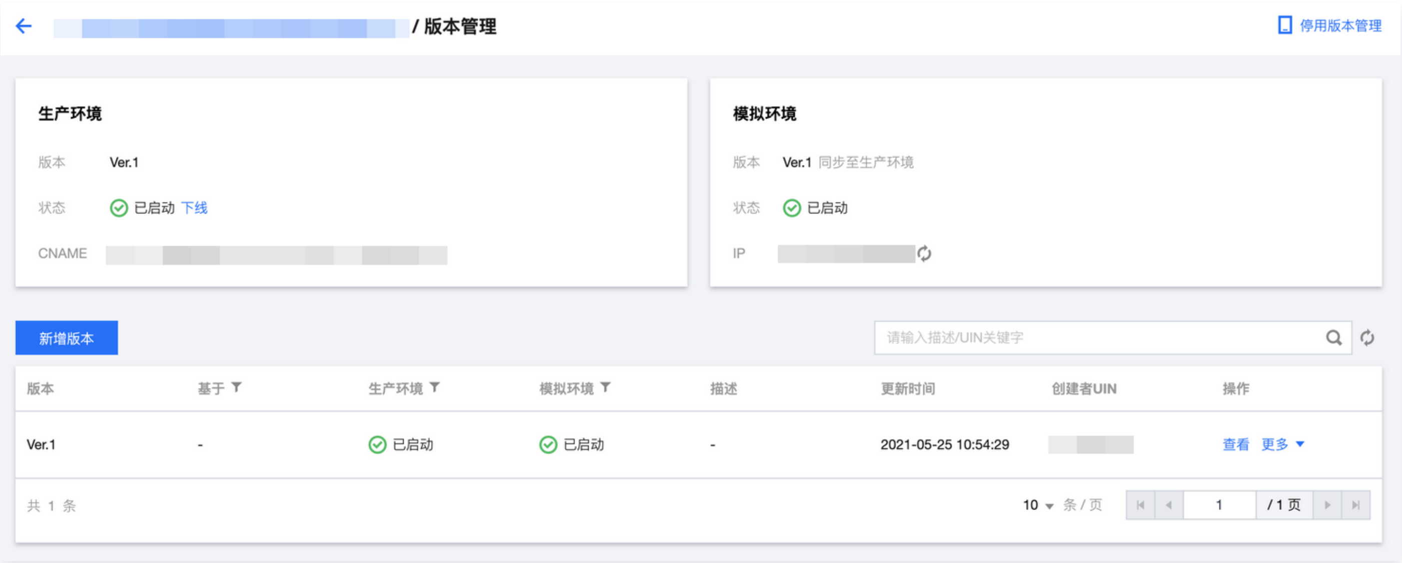


After version management is enabled, Ver.1 will be created with the current domain name configuration and deployed to both the production environment and staging environment.

Version Management

After enabling version management, you can enter the **version management page** to view and manage versions. Different versions are distinguished by version numbers **Ver.n (n=1,2,3,...)**.
You can access the version management page through the domain list page > domain operation bar > **More** > **Managing Versions**, or by clicking on the domain name and entering the **version management page** through the version management option in the top

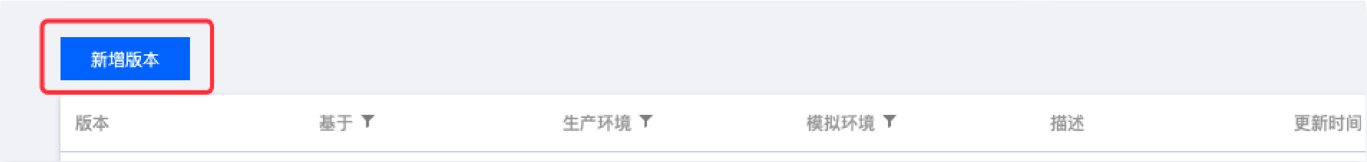
right corner of the domain configuration page.



版本	基于	生产环境	模拟环境	描述	更新时间	创建者UIN	操作
Ver.1	-	已启动	已启动	-	2021-05-25 10:54:29	[redacted]	查看 更多

Adding versions

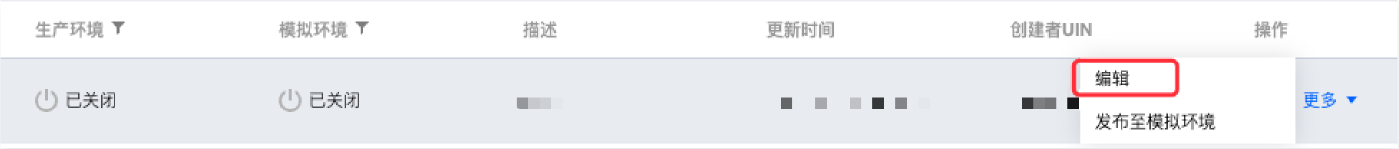
Click **New Version**: The version configuration for the new version defaults to the configuration in the current production environment. You can adjust and submit it to generate a new version.



> **Note**
> If you' re prompted with an error message after submitting the new version (possibly due to a configuration item not being successfully submitted), the version will still be generated (the configuration item with the error will default to its original content), and you don' t need to create a new one. You can go back to the version management page, edit the version, and continue adjusting the configuration.

Editing versions

When the latest version in the version list is not released to the staging environment, it can be edited: click **More** in the version operation column > **Edit**.



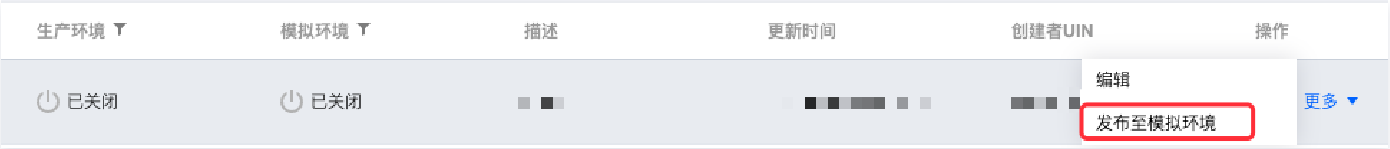
Historical versions (all versions before the latest version), whether released to the staging environment or not, cannot be edited and can only be viewed.

> **Note**
> Before adding a new version, please make sure all the existing versions are released. Otherwise, the version not released will become a historical version that cannot be edited and released to the staging environment.

Publish version

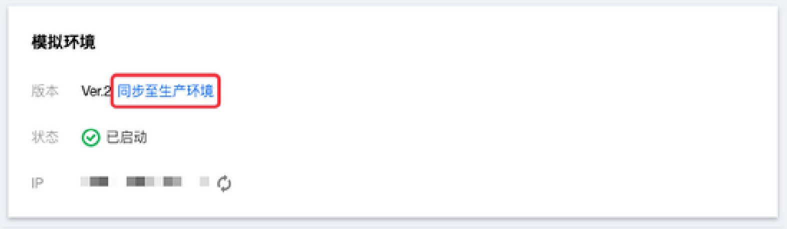
For domain names with version management enabled, release versions as follows:

1. To go live for testing or release a version in the staging environment: click **More** in the version operation column > **Release to Staging Environment**.



生产环境	模拟环境	描述	更新时间	创建者UIN	操作
已关闭	已关闭	[redacted]	[redacted]	[redacted]	编辑 发布至模拟环境 更多

2. CDN will assign an IPv4 IP to the domain name. To test the version deployed in the staging environment, modify the client HOSTS, and point the domain name to the IP.
3. If you want to adjust the configuration and test again, you need to add and submit a new version, and then repeat step 1 and 2.
4. After passing the test, sync the version to the production environment, and the configuration will be released to the network, effective across the network: click **sync to production environment** next to the version number in the staging environment card.



模拟环境

版本 Ver.2 同步至生产环境

状态 已启动

IP [redacted]

5. If you need to change the version in the production environment, repeat steps 1 through 4.

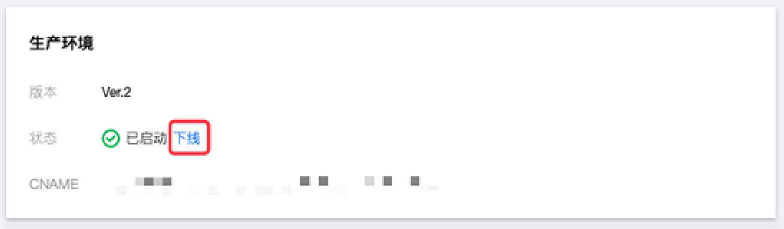
> **Note**
> - You are only allowed to release the latest version (the one with the largest version number) to the staging environment. Historical versions are only available for viewing.
> - Special backend configuration or platform updates will be released to the production environment directly and take effect immediately.
> - If the domain currently has manual configuration or platform upgrade optimization, there may be conflicts when syncing the version from the staging environment to the production environment. The console will display an error message indicating that the domain has special backend configuration. Please create a new version and then publish it.
> - The IP of the staging environment is not suppose to be changed frequently. But to ensure accuracy, it is recommended to get a new IP by clicking the refresh button before testing each time.

Viewing a version

Click **Viewing** in the corresponding version operation column to view the configuration content of that version.

Taking Down/Bringing Up the Version

Click **Going Offline** in the production environment to take down the versions in both the production and staging environments, i.e., take down the domain and close the acceleration service.



生产环境

版本 Ver.2

状态 已启动 下线

CNAME [redacted]

After going offline, you can bring up the domain again by clicking **Bringing Up** in the same position in the production environment. The displayed version in both the production and staging environments will be brought up simultaneously.

Disabling Version Management

For domains operating normally with enabled version management, you can also disable version management. After disabling, it will revert to the basic current network configuration mode, using the online version of the current production environment as the current network configuration. All other existing versions will disappear and be irreversible.
You can click Enable Version Management to enable it again as needed.

Notes

For domain names with version management enabled:

- Batch configuring features, like copying configurations and batch changing configuration, are not supported.
- You cannot configure a certificate for a domain name on the certificate management page in the console.
- When you stop/start the acceleration service, the versions in both the production and staging environments will be taken offline/online simultaneously.
- The tag and project of the domain name are editable.
- To change the acceleration region and service type of an immutable domain, you should disable version management first.

Configuration Management
Configuration Overview

Last updated：2024-12-31 17:31:11

Configuration Overview

CDN supports various custom configurations at different stages of the request, and you can adjust them based on your business needs.

Basic Configuration

Basic configurations include the basic information of the acceleration service, such as acceleration region and service type, as well as origin server configurations, which are required for CDN acceleration.

Configuration Name	Feature Description
Basic Info	Modifies basic information such as the domain name's project, acceleration region, and service type, etc.
Origin Server Configuration	Supports multi-IP round-robin origin-pull configuration, domain name origin retrieval, weighted back to origin, origin host settings, and origin-pull protocol settings. Supports hot backup origin server configuration. **Global acceleration domain names support separate configuration for in and outside the Chinese mainland.**
Advanced Origin-Pull Configuration	Supports more granular origin-pull configuration, retrieving from different origin server addresses based on different rules.
Regional Access Control	Identify the location of end users through client IP, allowing customers to set access privileges for end users in each region for all content or specified directories.

Access Control

You can configure various rules based on the actual content of user requests to allow or block access.

Configuration Name	Feature Description
Hotlink Protection Configuration	Supports setting referer allowlists and blocklists to determine whether to allow or deny HTTP access requests based on the request referer headers. **Global acceleration domain names support separate configuration for in and outside the Chinese mainland.**
IP Blocklist/Allowlist Configuration	IP allowlist and blocklist configuration determines whether to deny or allow requests based on the client IP of the access HTTP request. **Global acceleration domain names support separate configuration for in and outside the Chinese mainland.**
IP Access Limit Configuration	Limits the frequency that a single IP can access a single node to deny the access requests from client IPs exceeding the limit.
Authentication Configuration	Supports various timestamp signature algorithms and rules for hotlink protection configuration. **Global acceleration domain names support separate configuration for in and outside the Chinese mainland.**
Video Dragging	Used for streaming media on-demand acceleration scenarios. After enabling the video dragging feature, the video start playback position can be specified using the start parameter.
UA Blocklist/Allowlist	UA allowlist/blocklist configuration determines whether to allow or deny requests based on the User-Agent header of the HTTP access request.

Configuration	
Downstream Speed Limit Configuration	Controls the CDN access bandwidth by setting the downstream speed limit on a URL.
Access Port Configuration	Supports disabling port 80, 8080, and 443 as needed.

Cache configuration

Cache configuration controls the caching behavior of CDN nodes.

Configuration Name	Feature Description
Cache Key Rule Configuration	When setting node cache resources, should the access URL be ignored? And the subsequent parameters. **If the parameters after the URL in your business represent different content, it is recommended not to enable the ignore parameter configuration.**
Node Cache Expiration Configuration	Supports configuring the cache validity of files on nodes based on file path and type.
Status Code Cache	Supports configuring the cache validity of status codes, allowing CDN nodes to directly respond with non-2XX codes, reducing the load on the origin server.
HTTP Header Cache Configuration	It can be disabled as needed. CDN nodes cache all origin server response headers by default.
Ignore Cache Letter Case Configuration	CDN node cache does not ignore letter case by default. Letter case can be ignored as needed.
Access URL Rewrite Configuration	Supports customizing URL rewrite configuration to redirect requests from URLs with 302 status code to target URLs.
Browser Cache Validity Configuration	Supports customizing client browser cache policies to reduce origin-pull rate.

Origin-pull configuration

The origin-pull configuration controls the behavior of CDN nodes when sending requests to the origin server.

Configuration Name	Feature Description
Range GETs Configuration	By default, CDN nodes use sharding origin. If the origin server does not support it, this configuration can be disabled.
Origin HTTP Request Header Configuration	Adds specified headers during origin-pull such as the real client IP.
Follow 301/302 configuration	Supports enabling follow 301/302 configuration.
Origin-pull timeout configuration	Configures the TCP connection timeout period (which defaults to 5 seconds) and loading period (which defaults to 10 seconds) of origin-pull.
Origin URL Rewrite Configuration	Supports modifying the origin request URL to match the origin server.

Origin-pull SNI Configuration	If an origin server IP is bound with multiple domain names, you can set the origin-pull SNI to specify a domain name for CDN nodes to access the origin server via HTTPS.

HTTPS acceleration configuration

The HTTPS acceleration configuration module supports various HTTPS-related configurations.

Configuration Name	Feature Description
HTTPS Configuration	Supports uploading a self-owned certificate or a hosted certificate to enable HTTPS acceleration.
HTTP2.0 Configuration	With it enabled, CDN edge servers can support HTTP2.0. **Please first configure a certificate to enable HTTP2.0.**
Forced Redirection Configuration	Forced redirection from HTTPS to HTTP requests can be achieved with or without a certificate. When a certificate is configured, HTTP can be forcibly redirected to HTTPS requests.
OCSP Stapling Configuration	With it enabled, OCSP stapling is supported. **Before enabling OCSP stapling, certificate configuration must be completed first.**
HSTS Configuration	After enabling, add the strict-transport-security header. **Before enabling HSTS configuration, certificate configuration must be completed first.**
TLS Version Configuration	Support enabling/disabling specified TLS versions as needed.
QUIC	Support enabling QUIC protocol to ensure data transmission security when clients access CDN nodes and improve access efficiency.

Advanced Configuration

Configuration Name	Feature Description
Usage Limit Configuration	Support setting bandwidth or traffic cap for acceleration in and outside the Chinese mainland, and stopping acceleration service as needed after exceeding. **Global domain names support separate configurations for domestic and overseas.**
SEO Configuration	Supports automatically recognizing whether an access IP belongs to a search engine. Automatically return to the source after confirmation to ensure the stability of the search engine's weight.
HTTP Response Header Configuration	Sets HTTP response headers as needed and adds them to the response requests to clients.
Smart Compression Configuration	Performs Gzip or Brotli compression on specified files based on the file type and range.
Custom Error Page Configuration	support redirecting requests with specified error status codes to specified target addresses as needed
Offline Cache Configuration	When the origin server fails and resources cannot be pulled from it normally, support enabling offline cache to use the content cached in CDN.
POST Request Size Configuration	support adjusting the post request size limit based on actual business conditions

Basic Configurations
Basic Information

Last updated：2024-12-31 17:31:32

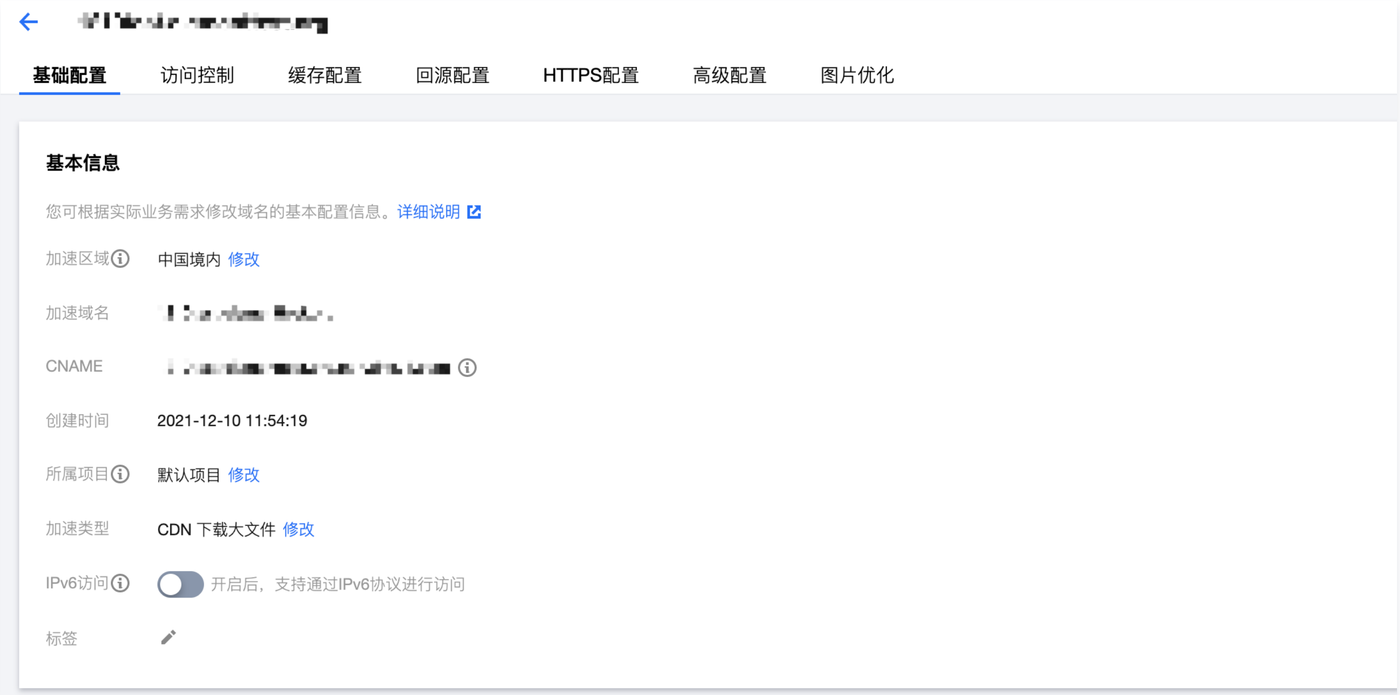
Configuration Scenario

For businesses that have been connected to Tencent Cloud CDN, you can view information such as domain name creation time, corresponding CNAME domain name, acceleration region, project, acceleration type, and supported protocols on the basic information module of the domain name. You can also modify information such as acceleration region, acceleration type, project, and tags as needed.

Configuration Guide

Viewing basic information

Log in to the CDN console, select **Domain Management** from the menu bar, click **Management** on the right side of the domain to enter the domain configuration page, and the first column display is the basic information of the domain name.



← [redacted]

基本信息

您可根据实际业务需求修改域名的基本配置信息。详细说明

加速区域 中国境内 修改

加速域名 [redacted]

CNAME [redacted]

创建时间 2021-12-10 11:54:19

所属项目 默认项目 修改

加速类型 CDN 下载大文件 修改

IPv6访问 开启后，支持通过IPv6协议进行访问

标签

Modifying domain name acceleration region

Click **Modify** on the right side of the acceleration region to adjust the domain name's acceleration region:

- If a domain name is configured for global acceleration, requests will be scheduled to the nearest global CDN cache node. In general, nodes in and outside the Chinese mainland serve users in and outside the Chinese mainland respectively.
- If a domain name is configured for acceleration in the Chinese mainland, access requests from global users will be served by cache nodes in the Chinese mainland.
- If a domain name is configured for acceleration outside the Chinese mainland, access requests from global users will be served by cache nodes outside the Chinese mainland.

> **Note**
> - Acceleration services within and outside the Chinese mainland are billed separately at different prices. For more information, please click here.

- When modifying from the Chinese mainland/overseas to global, the domain name configuration will be synchronized to overseas/the Chinese mainland. If the domain name has special backend configurations, there may be some delay in the synchronization process. Please be patient.

Modifying the Associated Project

Click **Modify** on the right side of the associated project to adjust the domain's associated project.

> ⚠ Note
> - Please note that adjusting the domain's associated project will affect project-based data statistics and sub-user permissions. Please modify with caution.
> - To create or manage existing projects, go to Project Management.

Modifying the Acceleration Type

Tencent Cloud CDN optimizes acceleration performance based on different acceleration types. For better acceleration effect, it is recommended to select the type closer to your business. If adjustment is needed, delete the domain and re-access.

> ⚠ Note
> Note: Before access, pay attention to the acceleration type that best fits your own business. If you need to change the acceleration type after access, you need to delete the current domain and re-access.
> - CDN acceleration of small webpage file downloads: applicable to e-commerce, websites, UGC communities, and other business scenarios that mainly involve small static resources, such as webpage styles, images, and small files.
> - CDN acceleration of large file downloads: applicable to business scenarios where large files, such as game installation packages, application updates, and application program packages, are downloaded.
> - CDN audio and video on demand acceleration: applicable to audio and video on-demand scenarios that require acceleration, such as online on-demand audio and video streaming.
> - ECDN dynamic and static content acceleration: applicable to business scenarios where dynamic and static data is integrated, such as various website homepages.
> - ECDN dynamic acceleration: applicable to scenarios such as account login, order transactions, API calls, and real-time queries.

Modifying IPv6 access

Toggle the IPv6 access switch to enable or disable it. CDN nodes can be accessed over IPv6 protocol after IPv6 access is enabled.

> ⚠ Note
> - Some platforms are being upgraded, IPv6 access is currently not supported. Please stay tuned for the official launch.
> - IPv6 access is only available in the Chinese mainland. For global acceleration domain names, if IPv6 access is enabled, it will take effect only in the Chinese mainland. For domain names with acceleration outside the Chinese mainland, it cannot be enabled.
> - If the domain acceleration region is set to "Global" and the IPv6 access switch is enabled, switching the acceleration region to "Outside Chinese Mainland" will automatically disable the IPv6 access switch, and it cannot be enabled.

Modifying Domain Name Tags

Changing the current domain name tags is supported. Changes do not take effect immediately; refresh to see the latest tag content.

> ⓘ **Note:**
> If you need to modify tags for multiple domain names in bulk, you can perform batch operations on the domain management page. For details, see Domain Name Operations.

Origin Server Configuration

Last updated：2024-12-31 17:31:44

Configuration Scenario

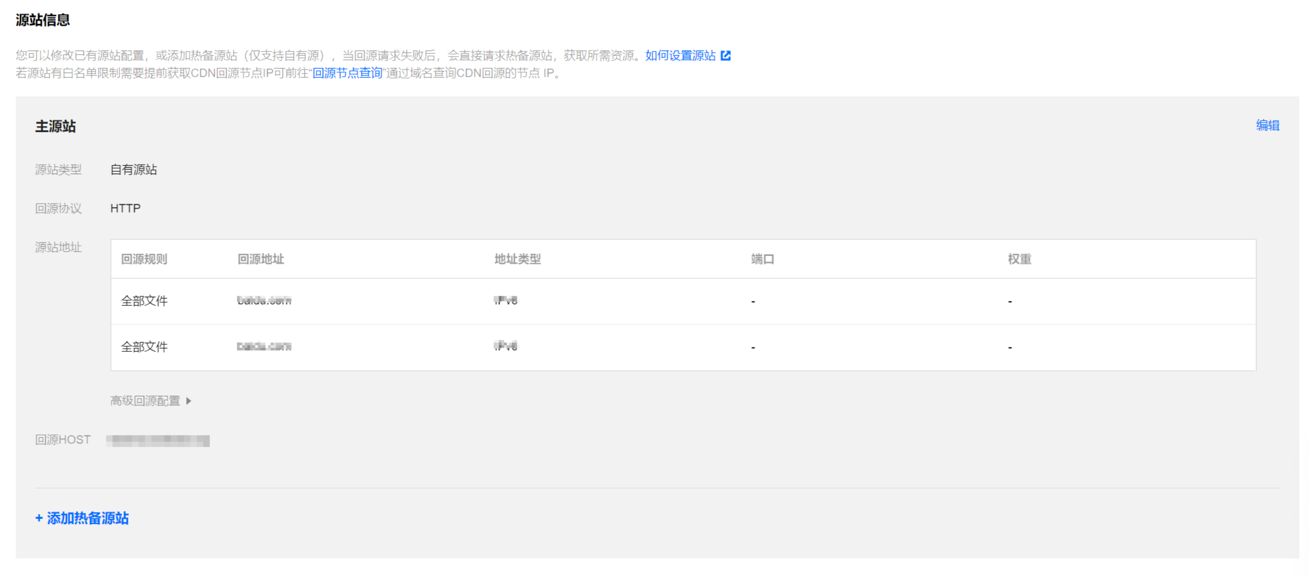
You can modify the domain name's origin server basic information, origin-pull protocol, origin domain, and other information in the origin server configuration module.

> **Note**
> - Note: We recommend that you configure your origin server in the same region as the acceleration region. For example, if the acceleration region resides in the Chinese mainland, configure your origin server in the Chinese mainland. If you configure the origin server in Hong Kong (China) or outside the Chinese mainland, cross-border access is required during origin-pull. In this case, the origin-pull effect may not be ensured.
> - Note: If your acceleration domain name is configured for global acceleration, you can configure independent origin servers respectively for different regions in the origin server configuration module of the domain name. This way, origin-pull requests that are initiated in and outside the Chinese mainland are sent to different origin servers. This ensures the origin-pull effect.

Configuration Guide

Primary origin server configuration

Log in to the CDN console, select **Domain Management** from the menu bar, click **Manage** on the right side of the domain name to enter the domain configuration page. The origin server configuration module is located under the basic information in the first column:



源站信息

您可以修改已有源站配置，或添加热备源站（仅支持自有源），当回源请求失败后，会直接请求热备源站，获取所需资源。如何设置源站
若源站有白名单限制需要提前获取CDN回源节点IP可前往“回源节点查询”通过域名查询CDN回源的节点 IP。

主源站

源站类型 自有源站

回源协议 HTTP

源站地址

回源规则	回源地址	地址类型	端口	权重
全部文件	[redacted]	[redacted]	-	-
全部文件	[redacted]	[redacted]	-	-

回源HOST [redacted]

Origin server type

Self-owned origin server	An existing server with stable performance (i.e., origin server) supports IPV4 addresses or domain names as origin server addresses. IPV6 origin servers are not supported.
COS Origin	You can select a bucket in cloud storage as the origin server, and private bucket access is supported.
IGTM Origin	Create a high availability service domain that can proactively isolate origin server failures or switch traffic based on health check results.
Third-party storage	You can use a bucket of a third-party object storage service other than Tencent Cloud COS as the origin server. Currently, the supported third-party object storage services include Amazon S3, Alibaba Cloud OSS, Huawei Cloud OBS, Qiniu Cloud KODO, and other object storage services compatible with the AWS signature algorithm (refer to General Configuration for Using Tencent Cloud COS in S3-Compatible Third-Party Applications).

	Note: ECDN does not support third-party object storage.

Origin-pull Protocol

The protocol used when a CDN cache node forwards requests to the origin server for origin-pull. You can select HTTP or HTTPS.

HTTP Origin-pull	HTTP/HTTPS requests will use HTTP for origin-pull.
HTTPS Origin-pull	CDN pulls HTTP or HTTPS content from the origin server over HTTPS to prevent theft and tampering of origin-pull data with low CPU usage. Make sure that the origin server is accessible over HTTPS.
Follow Protocol	HTTP requests will use HTTP for origin-pull, and HTTPS requests will use HTTPS for origin-pull. If you only need to use HTTPS for transmitting some key sensitive data and use HTTP for other services, it is recommended to select "Follow Protocol" (the origin server needs to support HTTPS).

> **Note**
>
> If you select HTTPS, make sure your origin server supports HTTPS. Otherwise VOD will fail to pull data from it.

Origin-pull from multiple origin IPs in round robin mode: You can enter multiple origin IPs to pull content from these IPs in round robin mode. CDN checks the availability of each origin IP by default. If content fails to be pulled from an IP or if more than five origin-pull requests that are sent to the origin IP time out within one minute, no more origin-pull requests are sent to the origin IP. The origin IP is blocked for 600 seconds and automatically resumed later.

Origin-pull from a domain name: You can configure a domain name as the origin server address. The domain name must be different from the acceleration domain name. IPv6 domain names are not supported.

Note: You cannot enter a domain name that is connected to CDN and points to the acceleration domain name. Otherwise, resolution loop occurs, which leads to origin-pull failures.

- You can add a port that ranges from 0 to 65535 and a weight that ranges from 1 to 100.
- The weights are sorted based on the size of the number. The larger the number, the higher the weight, and the higher the priority of the origin IP or domain name.
- The origin server address can contain up to 511 characters.
- IPv6 origin servers are not supported.

> **Notes:**
>
> As of November 23, 2023, the option to configure IPv6 origin server addresses has been suspended. Existing users with configured IPv6 origin server types will continue to retain IPv6 origin retrieval services without modifying the origin server configuration.

Origin server address

Self-owned origin server	**Origin-pull from multiple origin IPs in round robin mode:** You can enter multiple origin IPs to pull content from these IPs in round robin mode. CDN checks the availability of each origin IP by default. If content fails to be pulled from an IP or if more than five origin-pull requests that are sent to the origin IP time out within one minute, no more origin-pull requests are sent to the origin IP. The origin IP is blocked for 600 seconds and automatically resumed later. **Origin-pull from a domain name:** You can configure a domain name as the origin server address. The domain name must be different from the acceleration domain name. You cannot use IPv6 domain names. **Note:** You cannot enter a domain name that is connected to CDN and points to the acceleration domain name. Otherwise, resolution loop occurs, which leads to origin-pull failures. • Supports adding ports (0 - 65535) and weights (1 - 100) • Weights are sorted based on the size of the number. The larger the number, the higher the weight, and the higher the origin priority. • The origin server address can contain up to 511 characters.
COS Origin	• Select a COS bucket as the origin server. • Select the default domain name, static website domain name, or global acceleration domain name as the bucket address based on the bucket configuration and your actual business needs. For example, if the static website configuration is enabled for the selected bucket, select the static website domain name.

	• If the read/write permission of your COS bucket is set to private read access, authorize CDN and enable origin-pull authentication to allow private bucket access.
IGTM Origin	• Select a service domain from Tencent Cloud Intelligent Global Traffic Management (IGTM) as the origin server. • The origin protocol only supports HTTP origin-pull on port 80 and HTTPS origin-pull on port 443. Other ports cannot be specified for origin-pull.
Third-party storage	• If your resources are stored in a bucket of a third-party object storage service, enter a valid bucket address as the origin server address. Currently, the supported third-party object storage services include Amazon S3, Alibaba Cloud OSS, Huawei Cloud OBS, Qiniu Cloud KODO, and other object storage services compatible with the AWS signature algorithm (refer to the general configuration for using Tencent Cloud COS in third-party applications compatible with S3). **Example:** `my-bucket.s3.ap-east-1.amazonaws.com` or `my-bucket.oss-cn-beijing.aliyuncs.com` , do not include http:// or https:// protocol headers. • If you use a private bucket of a third-party object storage service as the origin server, enter a valid key and enable origin-pull authentication to allow private bucket access.

Host Header

It refers to the domain name accessed on the origin server by a CDN node during origin-pull. If only one website runs on the origin server and it matches the acceleration domain name, the acceleration domain name is used as the origin domain by default. If the origin server type is COS or a third-party object storage service, the host header cannot be modified and defaults to the origin address in the console.

> **Notes:**
> **What is CDN origin domain configuration?**
> The origin HOST refers to the site domain name that the acceleration domain name points to during the back-to-origin process on a CDN node. If you have deployed several web sites on the origin server, configuring the correct origin HOST can help you successfully access the specified site domain name.

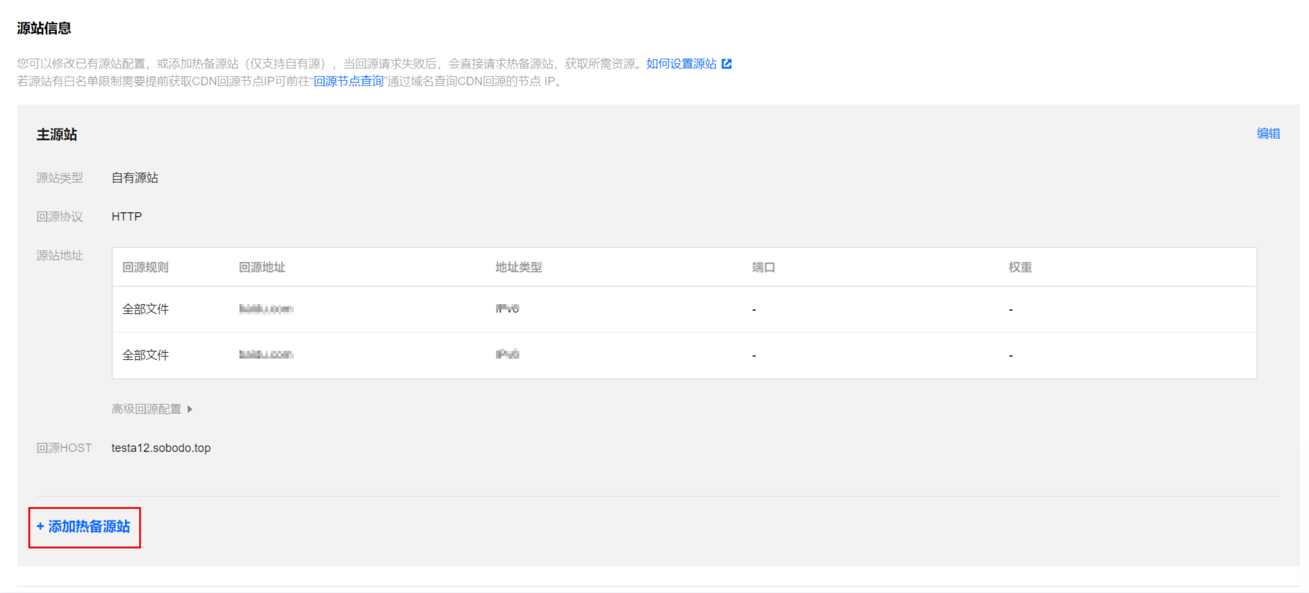
Self-owned origin server	The acceleration domain name is used as the origin domain by default. If a wildcard domain name is connected, the origin domain is the actual access domain name by default and can be customized.
COS Origin	The bucket access address is used as the origin domain by default, which is the same as the origin server address and cannot be modified.
IGTM Origin	The acceleration domain name is used as the origin domain by default. If a wildcard domain name is connected, the origin domain is the actual access domain name by default and can be customized.
Third-party storage	The bucket access address is used as the origin domain by default, which is the same as the origin server address and cannot be modified.

Hot backup origin server configuration

You can add a hot backup origin server for your primary origin server. All origin-pull requests will be forwarded to the primary origin server first. If a 4XX or 5XX error code is returned or an exception such as connection timeout or protocol incompatibility occurs, requests will be forwarded to the hot backup origin server to pull resources, ensuring the high availability of origin-pull.

> **Note**
> Non-idempotent requests retried by CDN nodes can cause unexpected issues. When the primary source anomaly occurs, POST requests will not be retried to the origin. (Note)

The hot backup origin server can be configured with its own origin server address and origin host.



源站信息

您可以修改已有源站配置，或添加热备源站（仅支持自有源），当回源请求失败后，会直接请求热备源站，获取所需资源。如何设置源站
若源站有白名单限制需要提前获取CDN回源节点IP可前往"回源节点查询"通过域名查询CDN回源的节点 IP。

主源站 编辑

源站类型 自有源站

回源协议 HTTP

源站地址

回源规则	回源地址	地址类型	端口	权重
全部文件	[redacted]	[redacted]	-	-
全部文件	[redacted]	[redacted]	-	-

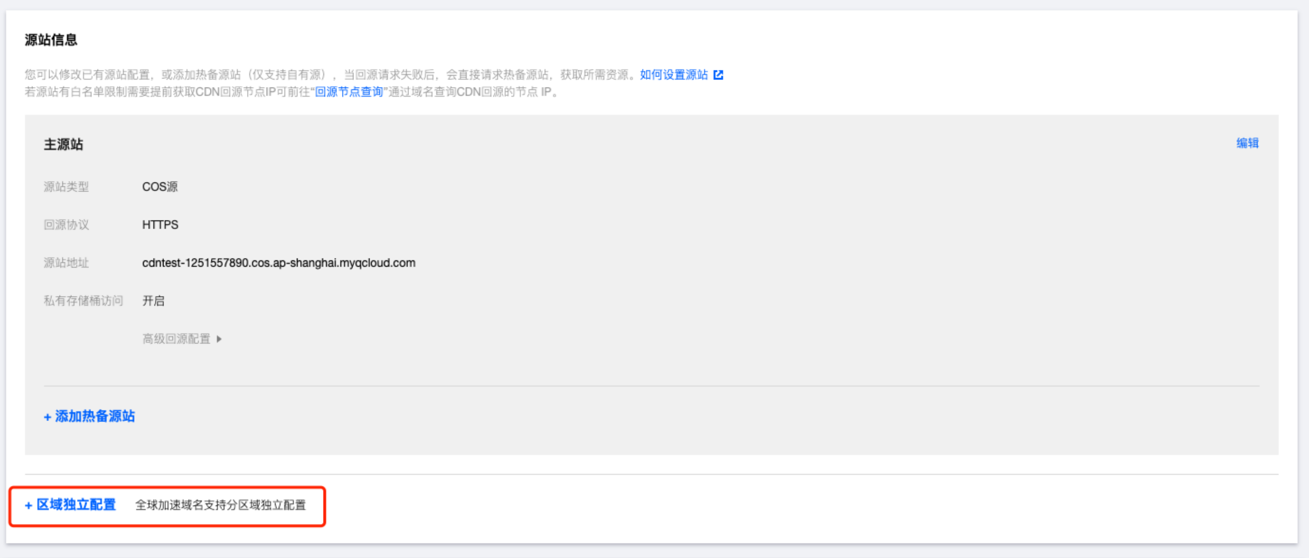
高级回源配置 ▸

回源HOST testa12.sobodo.top

> ⚠ **Note**
> - The primary origin server and hot backup origin server only allow the same origin protocol. To modify the origin protocol, you need to change it in the primary origin server's **origin-pull protocol** section. Once modified, the hot backup origin server's protocol will be updated accordingly. (Note)
> - The hot backup origin server type does not support COS origin and third-party object storage. If you need to use COS origin or third-party object storage as a hot backup, you can enter the public network access address in the private source. (Note)

Region-specific configuration

If your acceleration domain name is configured for global acceleration and you want to avoid cross-border traffic, click **Region-specific configuration** below to configure different origin servers for different service regions of the acceleration domain name.



源站信息

您可以修改已有源站配置，或添加热备源站（仅支持自有源），当回源请求失败后，会直接请求热备源站，获取所需资源。如何设置源站
若源站有白名单限制需要提前获取CDN回源节点IP可前往"回源节点查询"通过域名查询CDN回源的节点 IP。

主源站 编辑

源站类型 COS源

回源协议 HTTPS

源站地址 cdntest-1251557890.cos.ap-shanghai.myqcloud.com

私有存储桶访问 开启

高级回源配置 ▸

全球加速域名支持分区域独立配置

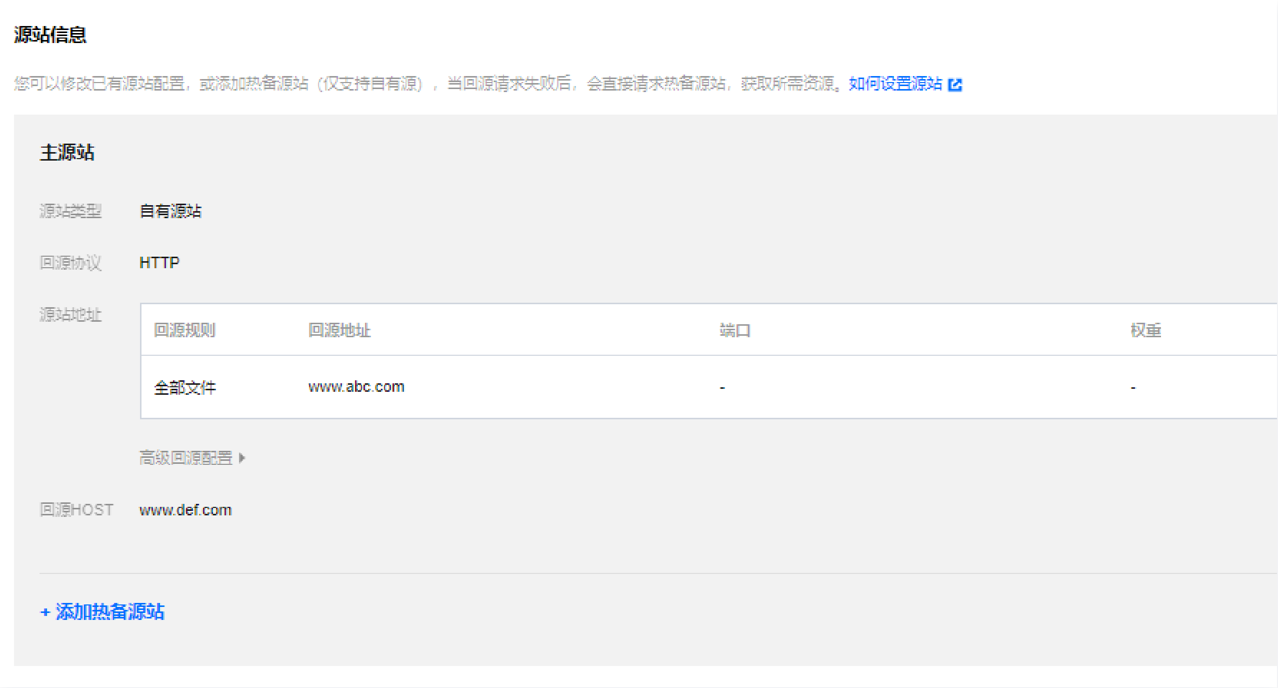
Select regions that need different origin-pull policies and enter the corresponding origin server information. For more information, see Region-specific configuration.

> ⚠ **Note**
> You cannot add a region-specific configuration if you use a bucket of a third-party object storage service as the origin server.

Configuration Example

Origin domain configuration

If the CDN origin server is configured as follows and the acceleration domain name `www.test.com` is configured as follows:



源站信息

您可以修改已有源站配置，或添加热备源站（仅支持自有源），当回源请求失败后，会直接请求热备源站，获取所需资源。如何设置源站

主源站

源站类型 自有源站

回源协议 HTTP

源站地址

回源规则	回源地址	端口	权重
全部文件	www.abc.com	-	-

高级回源配置

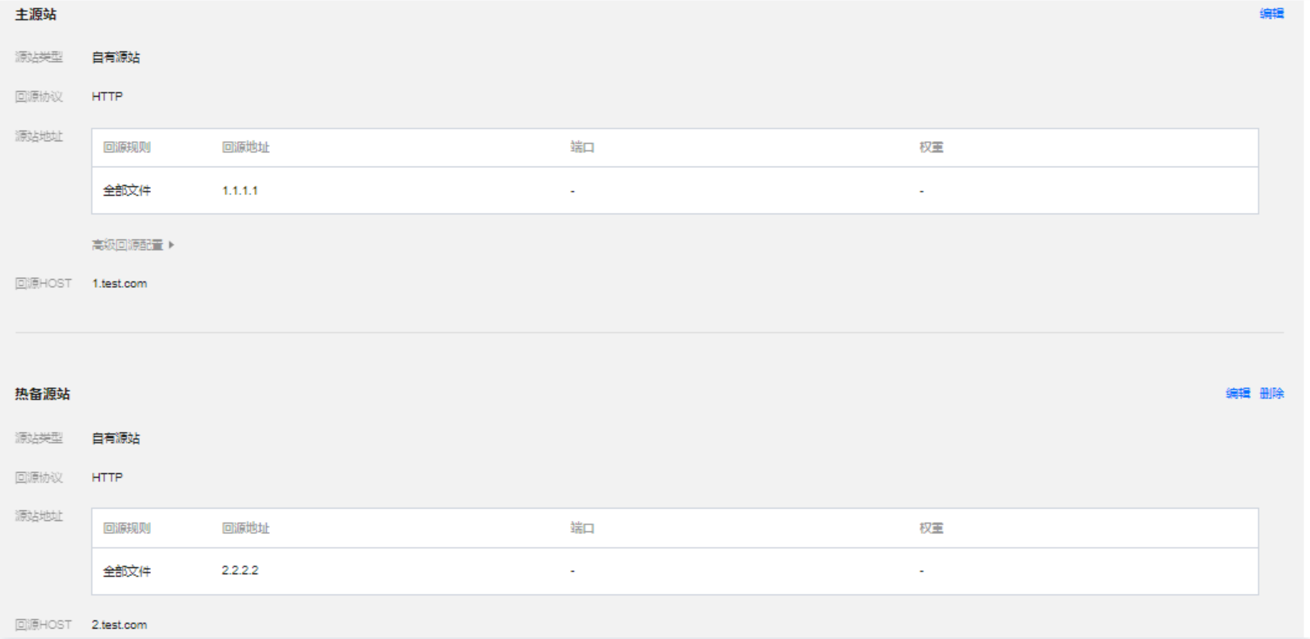
回源HOST www.def.com

+ 添加热备源站

Then the user access path is as follows:
When a user accesses the resource `http://www.test.com/test.txt` , and the CDN node has not cached the resource, the CDN node will resolve the domain name `www.abc.com` to obtain the origin server address, assumed to be `1.1.1.1` . It will then access the server at `1.1.1.1` and find the test.txt file under the Web site `www.def.com` path, and return it to the user.

Region-specific configuration

If the Tencent Cloud CDN origin server is configured as follows and the acceleration domain name `www.test.com` is configured as follows:



主源站 编辑

源站类型 自有源站

回源协议 HTTP

源站地址

回源规则	回源地址	端口	权重
全部文件	1.1.1.1	-	-

高级回源配置

回源HOST 1.test.com

热备源站 编辑 删除

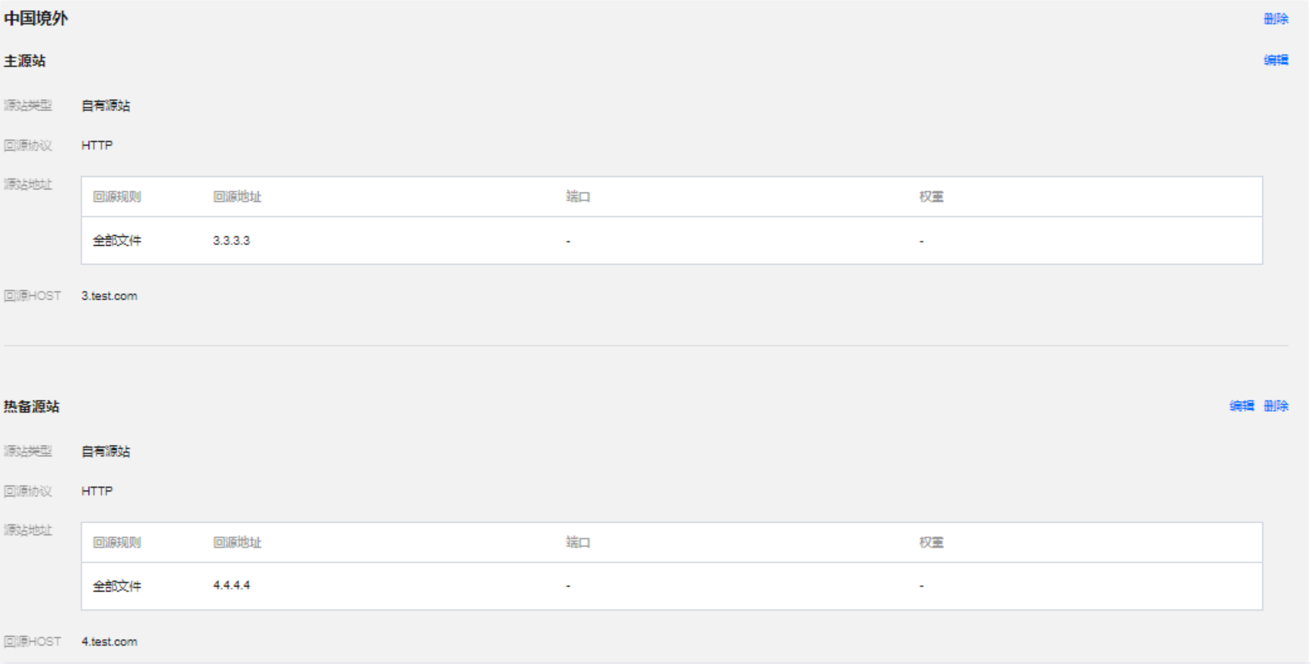
源站类型 自有源站

回源协议 HTTP

源站地址

回源规则	回源地址	端口	权重
全部文件	2.2.2.2	-	-

回源HOST 2.test.com



中国境外 删除

主源站 编辑

源站类型 自有源站

回源协议 HTTP

源站地址

回源规则	回源地址	端口	权重
全部文件	3.3.3.3	-	-

回源HOST 3.test.com

热备源站 编辑 删除

源站类型 自有源站

回源协议 HTTP

源站地址

回源规则	回源地址	端口	权重
全部文件	4.4.4.4	-	-

回源HOST 4.test.com

The actual origin scenario will be:

1. When users within China access the file `http://www.test.com/test.txt` , and the domestic node has not cached the resource, the origin pull request will reach the server `1.1.1.1` to find the test.txt file under the Web site `1.test.com` . If the resource is available, it will be returned to the customer directly. If not, proceed to step 2.
2. If the CDN domestic node fails to pull from the primary origin server and the resource is not found, the origin pull request will reach the server `2.2.2.2` to find the test.txt file under the Web site `2.test.com` , return it to the user, and cache it.
3. At this point, overseas users also access the file `http://www.test.com/test.txt` . If the overseas node has not cached the resource, the origin pull request will reach the server `3.3.3.3` to find the test.txt file under the Web site `3.test.com` . If the resource is available, it will be returned to the customer directly. If not, proceed to step 4.
4. If the CDN overseas node fails to pull from the overseas primary origin server and the resource is not found, the origin pull request will reach the server `4.4.4.4` to find the test.txt file under the Web site `4.test.com` , return it to the overseas user, and cache it.

Advanced Origin-Pull Configuration

Last updated：2024-12-31 17:31:57

Feature Introduction

Tencent Cloud CDN allows you to configure fine-grained origin-pull based on origin-pull rules, such as path-based rules (i.e., specifying a file type, folder, full file path, or homepage for origin-pull) and client IP region-based rules.

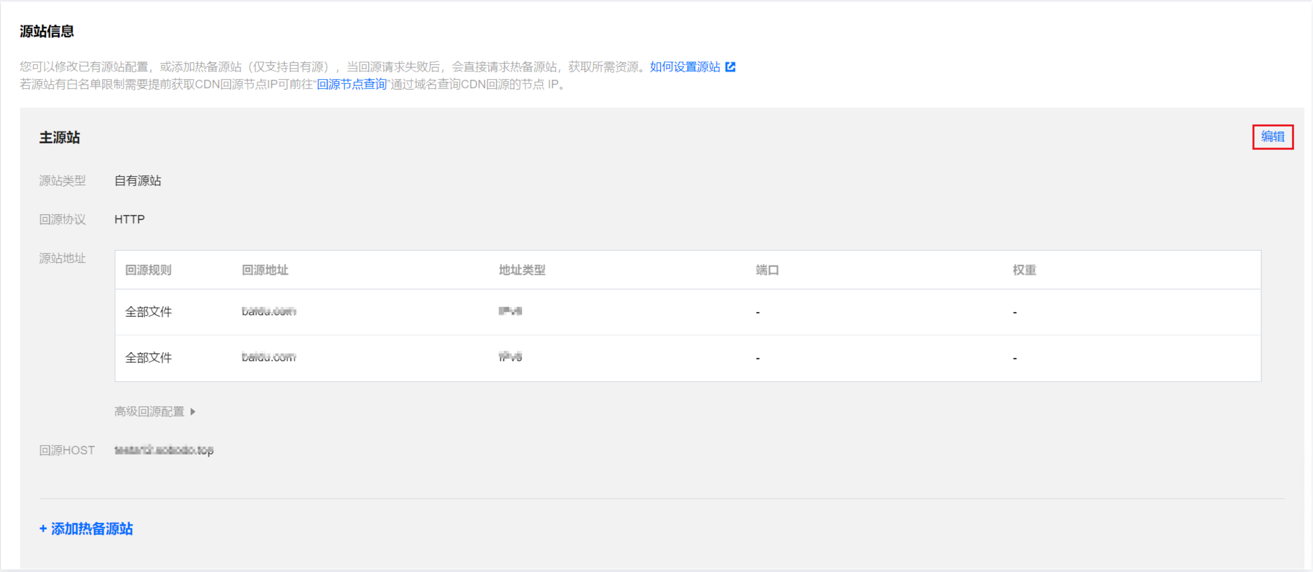
Notes

1. Only domain names with the acceleration type of CDN web page small files, CDN large file download, or CDN audio/video on demand support advanced origin-pull configuration.
2. By default, the origin-pull protocol and origin host are inherited from the primary origin server and cannot be modified based on different rules.
3. Advanced origin-pull configuration only supports origin-pull using IPv4 addresses or domain names, and does not support IPv6 addresses or domain names.

Configuration Instructions

Configuration in domain management

1. Log in to the CDN Console.
2. Click **Domain Management** in the left menu to enter the domain management list;
3. Select the domain to configure and click **Management** to enter the domain configuration page;
4. Within basic information, find the origin server information and click the **Edit** button in the upper right corner;



源站信息

您可以修改已有源站配置，或添加热备源站（仅支持自有源），当回源请求失败后，会直接请求热备源站，获取所需资源。如何设置源站
若源站有白名单限制需要提前获取CDN回源节点IP可前往"回源节点查询"通过域名查询CDN回源的节点 IP。

主源站

编辑

源站类型 自有源站

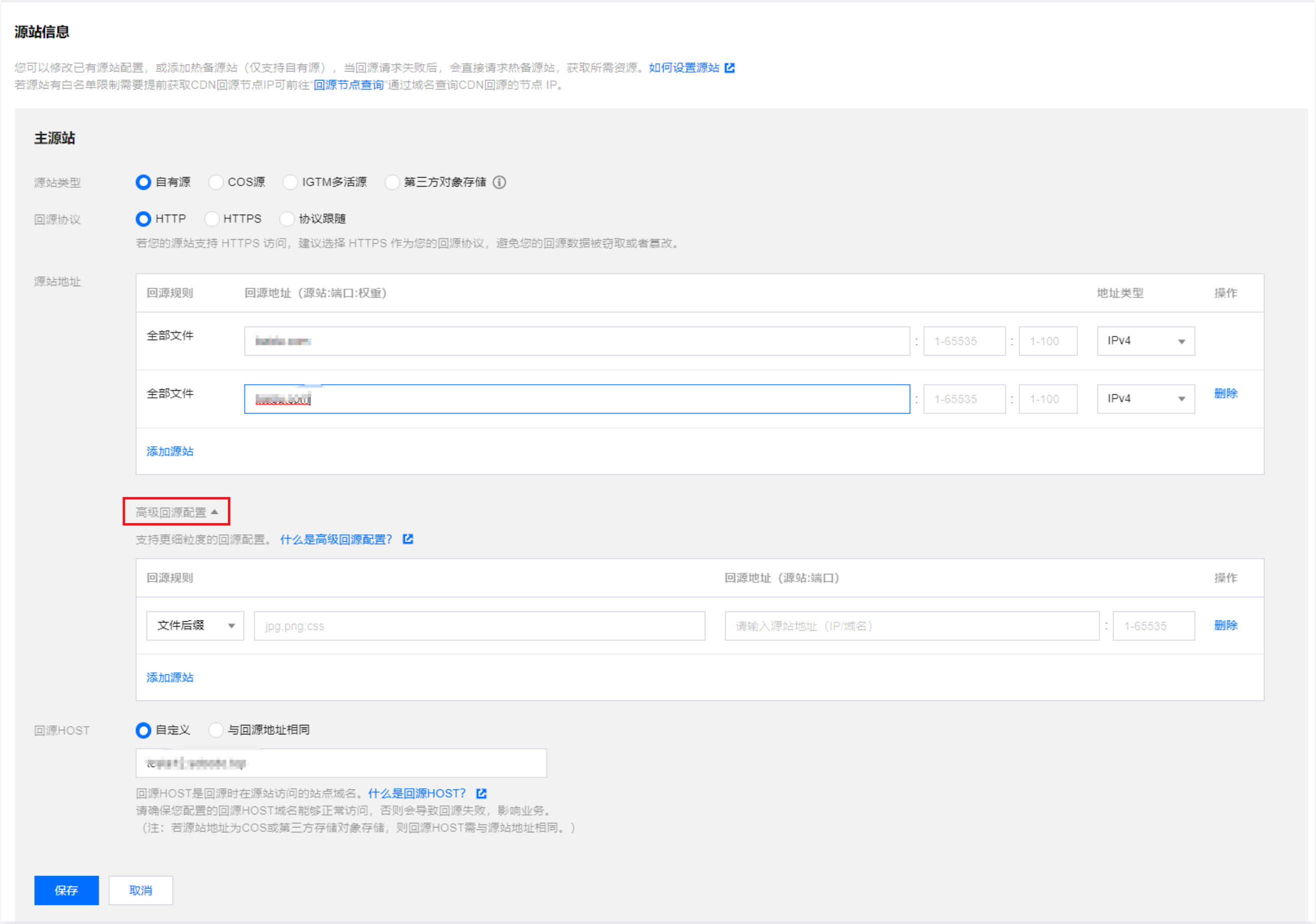
回源协议 HTTP

源站地址

回源规则	回源地址	地址类型	端口	权重
全部文件	baidu.com	IPv4	-	-
全部文件	baidu.com	IPv6	-	-

回源HOST [illegible]

5. Click **Advanced Origin-Pull Configuration** to expand the advanced origin-pull configuration;



源站信息

您可以修改已有源站配置，或添加热备源站（仅支持自有源），当回源请求失败后，会直接请求热备源站，获取所需资源。如何设置源站
若源站有白名单限制需要提前获取CDN回源节点IP可前往"回源节点查询"通过域名查询CDN回源的节点 IP。

主源站

源站类型 ● 自有源 ○ COS源 ○ IGTM多活源 ○ 第三方对象存储

回源协议 ● HTTP ○ HTTPS ○ 协议跟随
若您的源站支持 HTTPS 访问，建议选择 HTTPS 作为您的回源协议，避免您的回源数据被窃取或者篡改。

源站地址

回源规则	回源地址（源站:端口:权重）			地址类型	操作
全部文件	[redacted]	1-65535	1-100	IPv4	
全部文件	[redacted]	1-65535	1-100	IPv4	删除
添加源站					

高级回源配置 ▲
支持更细粒度的回源配置。什么是高级回源配置？

回源规则		回源地址（源站:端口）		操作
文件后缀	jpg;png;css	请输入源站地址（IP/域名）	1-65535	删除
添加源站				

回源HOST ● 自定义 ○ 与回源地址相同
[redacted]
回源HOST是回源时在源站访问的站点域名。什么是回源HOST？
请确保您配置的回源HOST域名能够正常访问，否则会导致回源失败，影响业务。
（注：若源站地址为COS或第三方存储对象存储，则回源HOST需与源站地址相同。）

保存 取消

6. In Advanced Origin-pull Configuration

Configuration Item	Description
Origin-Pull Rules	Support matching user requests according to the following rules: • Client IP: Based on the user's access location, users belonging to or not belonging to the specified region can be specified, and the origin-pull request will be directed to the specified origin server address; • File Suffix: Support matching according to the specified file suffix, case-sensitive. Only requests that match the file suffix will have the origin-pull request directed to the specified origin server address. Support input of multiple suffixes, separated by ;. • File directory: Supports matching based on the specified file directory. File directory matching is case-sensitive. Only requests that match the file directory will have their origin pull requests directed to the specified origin server address. Supports input of multiple suffixes, with multiple directories separated by a semicolon. • Full path file: Supports specifying files. File path and file matching are case-sensitive, e.g., /a/1.jpg. The origin pull request for this file will be directed to the specified origin server address. Supports input of multiple full path files, with multiple files separated by a semicolon. • Homepage: For homepage files, supports specifying that the origin pull request for the homepage file is directed to the specified origin server address.
Origin-pull Address	Supports input of IP/domain. Each origin rule corresponds to an origin-pull address. The origin host will inherit the origin host information from the origin server and perform origin-pull based on this host information.
Port	Supports custom origin port number. If not configured, the default ports will be HTTP port 80 and HTTPS port 443 based on the origin protocol. The origin protocol will follow the settings in the origin server information. For example, if the origin protocol in the origin server information is configured as HTTPS, then when the advanced origin rule is matched, the origin pull will be performed using HTTPS.

Configuration limitations

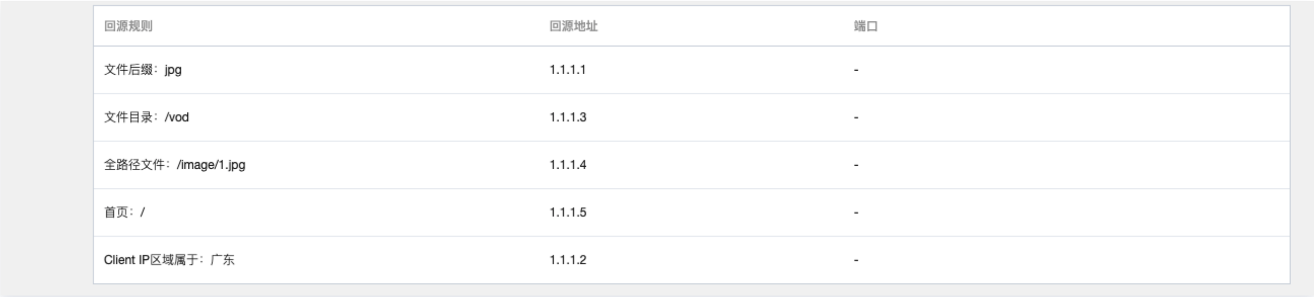
- Each single domain name can add up to 20 rules.
- An individual rule's origin address supports entering one IP/domain name origin server and port (0 – 65535), with the port being optional. If the origin protocol is selected as HTTPS or protocol follow, the port can only be set to 443 or left unconfigured.
- More actions: you can adjust rule priority and edit or delete multiple rules in batches.

Rule priorities

Rule priority is determined first by path–based origin rules (including specified file types, folders, full–path files (e.g., /test/1.jpg), and homepage origin–pull) > Client IP. Among multiple path–based origin and Client IP origin rules, bottom priority is higher than top priority.
For example, if a Client IP from Jiangsu is configured to origin–pull from 1.1.1.1 and a file path containing /test to origin–pull from 2.2.2.2, the priority sequence will first match the path–based origin rule. Thus, a Client IP from Jiangsu accessing /test will origin–pull from 2.2.2.2.

Configuration Example

Examples:
For instance, if the user configures the CDN acceleration domain name as `www.example.com` and sets the following rules in the advanced origin rule, the user requests will be directed to the origin server as follows:



回源规则	回源地址	端口
文件后缀：jpg	1.1.1.1	-
文件目录：/vod	1.1.1.3	-
全路径文件：/image/1.jpg	1.1.1.4	-
首页：/	1.1.1.5	-
Client IP区域属于：广东	1.1.1.2	-

Access scenario one: The user request URL is `http://www.example.com/vod/` , and the user IP belongs to Shanghai. The origin request rule matches the directory rule, and the request will be directed to the origin server at 1.1.1.3;
Access scenario two: The user request URL is `http://www.example.com/` , and the user IP belongs to Guangdong. The origin request rule matches both the home page origin rule and the client IP–based rule. Since the path–based origin rule has a higher priority than the client IP–based rule, the request will be directed to the origin server at 1.1.1.5;
Access scenario three: The user request URL is `http://www.example.com/image/1.jpg` , and the user IP belongs to Guangdong. The origin request rule matches the file suffix, full path file, and client IP–based rules. Since the path–based origin rule has a higher priority than the client IP–based rule, and the bottom priority is higher than the top priority, meaning the full path file rule has a higher priority than the file suffix rule, the request will be directed to the origin server at 1.1.1.4.

HTTPS Origin-pull algorithm description

Last updated：2024-12-31 17:32:09

HTTPS origin-pull currently supports the following algorithms (in no particular order):

ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA384	ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA	ECDHE-ECDSA-AES256-SHA384	ECDHE-ECDSA-AES256-GCM-SHA384
SRP-AES-256-CBC-SHA	SRP-RSA-AES-256-CBC-SHA	SRP-DSS-AES-256-CBC-SHA
DH-RSA-AES256-SHA	DH-RSA-AES256-SHA256	DH-RSA-AES256-GCM-SHA384
DH-DSS-AES256-SHA	DH-DSS-AES256-SHA256	DH-DSS-AES256-GCM-SHA384
DHE-RSA-AES256-SHA	DHE-RSA-AES256-SHA256	DHE-RSA-AES256-GCM-SHA384
DHE-DSS-AES256-SHA	DHE-DSS-AES256-SHA256	DHE-DSS-AES256-GCM-SHA384
CAMELLIA256-SHA	DH-RSA-CAMELLIA256-SHA	DHE-RSA-CAMELLIA256-SHA
PSK-3DES-EDE-CBC-SHA	DH-DSS-CAMELLIA256-SHA	DHE-DSS-CAMELLIA256-SHA
ECDH-RSA-AES256-SHA	ECDH-RSA-AES256-SHA384	ECDH-RSA-AES256-GCM-SHA384
ECDH-ECDSA-AES256-SHA	ECDH-ECDSA-AES256-SHA384	ECDH-ECDSA-AES256-GCM-SHA384
AES256-SHA	AES256-SHA256	AES256-GCM-SHA384
ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA256	ECDHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA	ECDHE-ECDSA-AES128-SHA256	ECDHE-ECDSA-AES128-GCM-SHA256
SRP-AES-128-CBC-SHA	SRP-RSA-AES-128-CBC-SHA	SRP-DSS-AES-128-CBC-SHA
DH-RSA-AES128-SHA	DH-RSA-AES128-SHA256	DH-RSA-AES128-GCM-SHA256
DH-DSS-AES128-SHA	DH-DSS-AES128-SHA256	DH-DSS-AES128-GCM-SHA256
DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA256	DHE-RSA-AES128-GCM-SHA256
DHE-DSS-AES128-SHA	DHE-DSS-AES128-SHA256	DHE-DSS-AES128-GCM-SHA256
ECDH-RSA-AES128-SHA	ECDH-RSA-AES128-SHA256	ECDH-RSA-AES128-GCM-SHA256
ECDH-ECDSA-AES128-SHA	ECDH-ECDSA-AES128-SHA256	ECDH-ECDSA-AES128-GCM-SHA256
CAMELLIA128-SHA	DH-RSA-CAMELLIA128-SHA	DHE-RSA-CAMELLIA128-SHA
PSK-RC4-SHA	DH-DSS-CAMELLIA128-SHA	DHE-DSS-CAMELLIA128-SHA
AES128-SHA	AES128-SHA256	AES128-GCM-SHA256
SEED-SHA	DH-RSA-SEED-SHA	DH-DSS-SEED-SHA
DES-CBC3-SHA	DHE-RSA-SEED-SHA	DHE-DSS-SEED-SHA
IDEA-CBC-SHA	PSK-AES256-CBC-SHA	PSK-AES128-CBC-SHA
EDH-RSA-DES-CBC3-SHA	ECDH-RSA-DES-CBC3-SHA	ECDHE-RSA-DES-CBC3-SHA
EDH-DSS-DES-CBC3-SHA	ECDH-ECDSA-DES-CBC3-SHA	ECDHE-ECDSA-DES-CBC3-SHA
RC4-SHA	ECDH-RSA-RC4-SHA	ECDHE-RSA-RC4-SHA
RC4-MD5	ECDH-ECDSA-RC4-SHA	ECDHE-ECDSA-RC4-SHA

SRP-3DES-EDE-CBC-SHA	SRP-RSA-3DES-EDE-CBC-SHA	SRP-DSS-3DES-EDE-CBC-SHA
DH-DSS-DES-CBC3-SHA	DH-RSA-DES-CBC3-SHA	-

Access Control
Traffic Anti-Fraud Configuration

Last updated：2024-12-31 17:32:49

Notes:
The high-risk IP feature database may be inaccurate or not updated in a timely manner, leading to the risk of false positives or false negatives. You need to bear these risks yourself. It is recommended to use it after thorough evaluation and confirmation.

Traffic Anti-Fraud Configuration

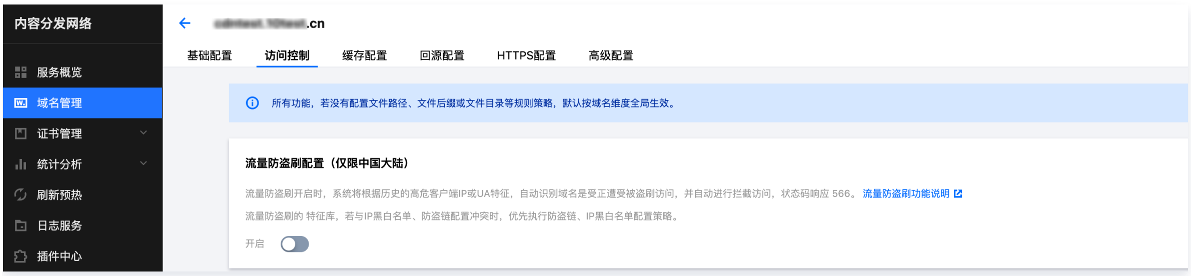
Traffic anti-fraud supports one-click activation of the automatic interception feature. Tencent Cloud automatically identifies suspicious Client IP requests and intercepts them to prevent malicious user fraud and abnormal business bills.

Note:
- Traffic anti-scraping currently only supports blocking access from the Chinese mainland.
- When the Client IP matches the IP feature database, the system will automatically block it and respond with a 566 status code to reduce abnormal business request traffic. However, if it is an HTTPS request service, HTTPS request billing will still occur.
- If you find an IP misjudgment causing normal customer requests to be blocked, please promptly disable the anti-scraping feature.
- When you configure the IP allowlist and blocklist feature, if there is a conflict between the IP and the suspicious IP database of the anti-scraping, the IP allowlist and blocklist you configured will take precedence.

Configuration Guide

Viewing Configuration

Log in to the CDN Console, select **Domain Management** from the menu bar, click **Management** on the right side of the domain name to enter the domain configuration page. In the second column **Access Control**, you can see the hotlink protection configuration, which is disabled by default:



[redacted].cn

所有功能，若没有配置文件路径、文件后缀或文件目录等规则策略，默认按域名维度全局生效。

流量防盗刷配置（仅限中国大陆）

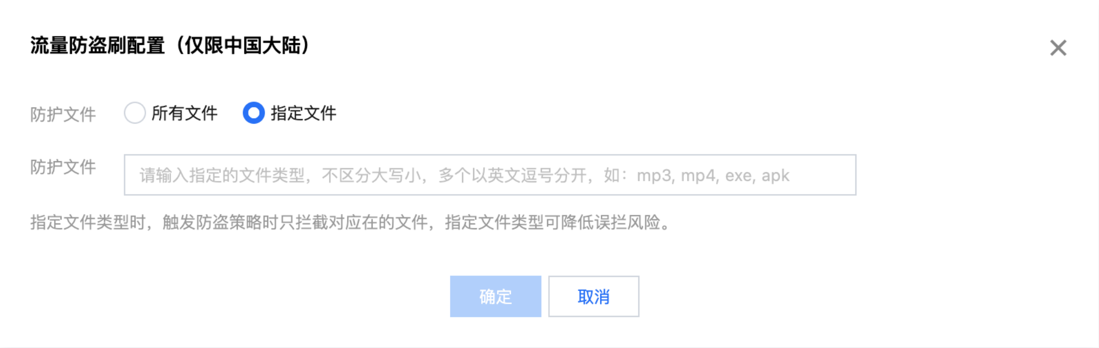
流量防盗刷开启时，系统将根据历史的高危客户端IP或UA特征，自动识别域名是受正遭受被盗刷访问，并自动进行拦截访问，状态码响应 566。流量防盗刷功能说明

流量防盗刷的 特征库，若与IP黑白名单、防盗链配置冲突时，优先执行防盗链、IP黑白名单配置策略。

开启

Enabling the configuration

Click to enable, and you can activate the automatic interception feature with one click. The system will identify all requests under the domain by default. If the customer's IP is in the system's suspicious feature database, the request will be directly intercepted, responding with a 566 status code.
Specified File Type Configuration:
Specified file type protection configuration allows targeted anti-theft protection for specific files while reducing false interceptions. When enabling the configuration, you can specify the file type. The configuration is as follows:



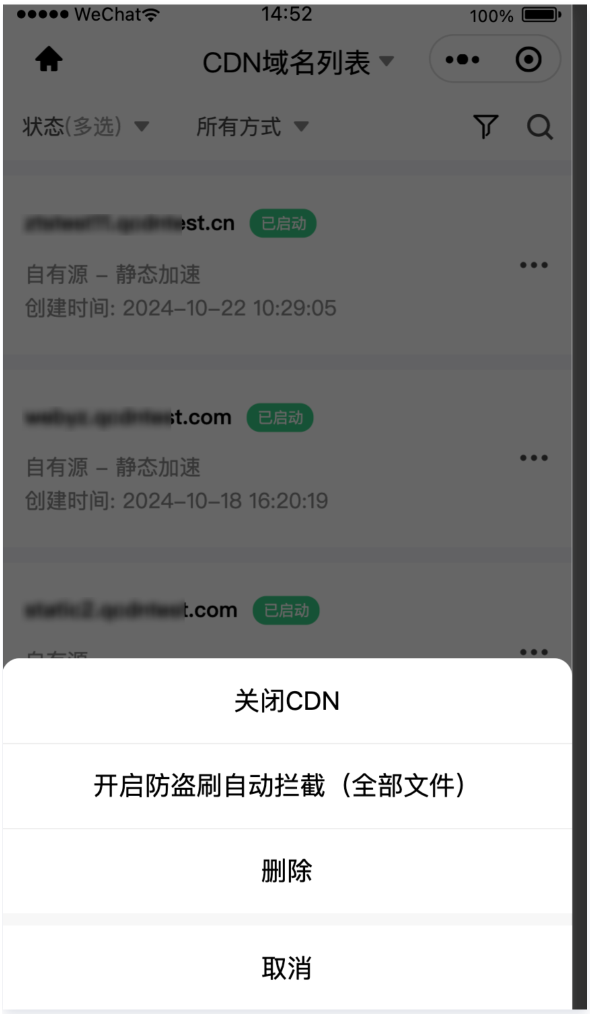
流量防盗刷配置（仅限中国大陆）

防护文件 ○ 所有文件 ● 指定文件

防护文件 请输入指定的文件类型，不区分大写小，多个以英文逗号分开，如：mp3, mp4, exe, apk

指定文件类型时，触发防盗策略时只拦截对应在的文件，指定文件类型可降低误拦风险。

Quick Configuration for Mini Programs:
You can also quickly access the CDN domain list through WeChat mini programs and enable the anti-scraping interception feature for all files with one click, as shown below:



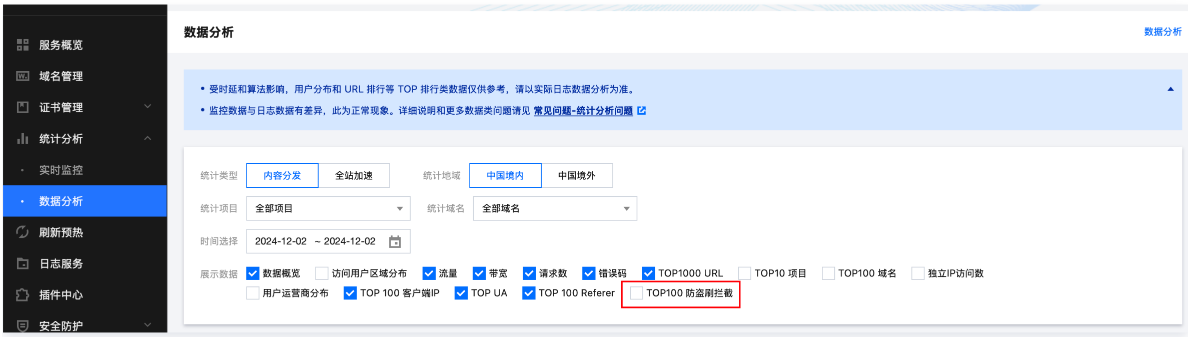
[redacted]st.cn 已启动
自有源 – 静态加速
创建时间: 2024–10–22 10:29:05

[redacted]st.com 已启动
自有源 – 静态加速
创建时间: 2024–10–18 16:20:19

[redacted].com 已启动

Querying Automatic Interception

Click the menu in the CDN Console: Data Analysis , and check the "TOP 100 Hotlink Protection" query option, as shown below:



数据分析

数据分析

- 受时延和算法影响，用户分布和 URL 排行等 TOP 排行类数据仅供参考，请以实际日志数据分析为准。
- 监控数据与日志数据有差异，此为正常现象。详细说明和更多数据类问题请见 常见问题-统计分析问题

统计类型 内容分发 全站加速

统计地域 中国境内 中国境外

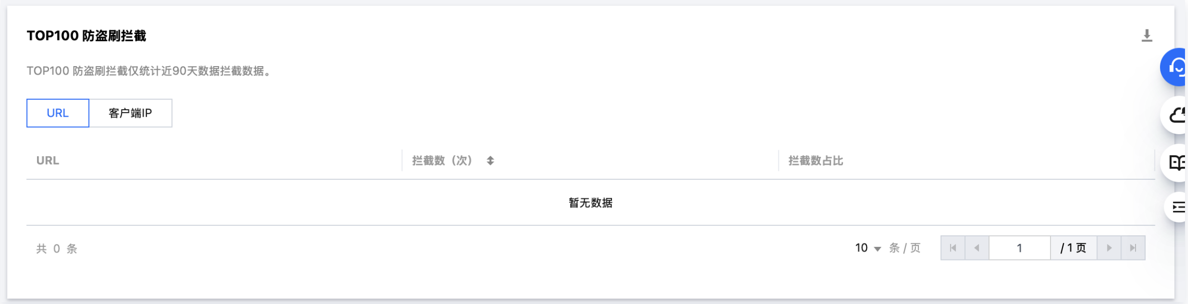
统计项目 全部项目

统计域名 全部域名

时间选择 2024-12-02 ~ 2024-12-02

展示数据 ☑ 数据概览 □ 访问用户区域分布 ☑ 流量 ☑ 带宽 ☑ 请求数 ☑ 错误码 ☑ TOP1000 URL □ TOP10 项目 □ TOP100 域名 □ 独立IP访问数
□ 用户运营商分布 ☑ TOP 100 客户端IP ☑ TOP UA ☑ TOP 100 Referer □ TOP100 防盗刷拦截

After selecting, scroll down to view the top URLs and Client IPs automatically blocked.



TOP100 防盗刷拦截

TOP100 防盗刷拦截仅统计近90天数据拦截数据。

URL	拦截数（次）	拦截数占比
暂无数据		

共 0 条

10 条 / 页 1 / 1 页

Downloading the top blocked data is also supported.

Hotlink Protection

Last updated：2024-12-31 17:33:01

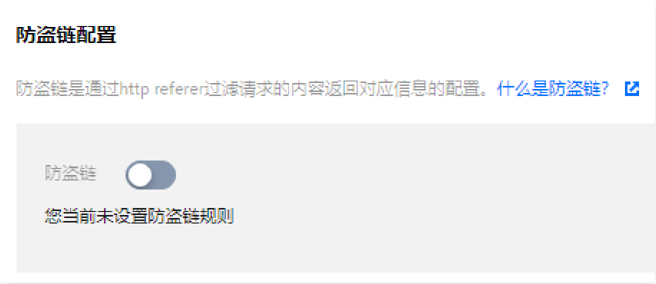
Hotlink Protection

To control the source of access to your business resources, you can use the referer hotlink protection feature in Tencent Cloud CDN.
By configuring an access control policy on the value of the referer field in the HTTP request header, you can restrict the access source to prevent malicious users from unauthorized access.

Configuration Guide

View Configuration

Log in to the CDN Console, select **Domain Management** in the menu bar, click **Management** on the right side of the domain to enter the domain configuration page. In the second column, **Access Control**, you can see the hotlink protection configuration. By default, hotlink protection is in closed status:



防盗链配置

防盗链是通过http referer过滤请求的内容返回对应信息的配置。什么是防盗链?

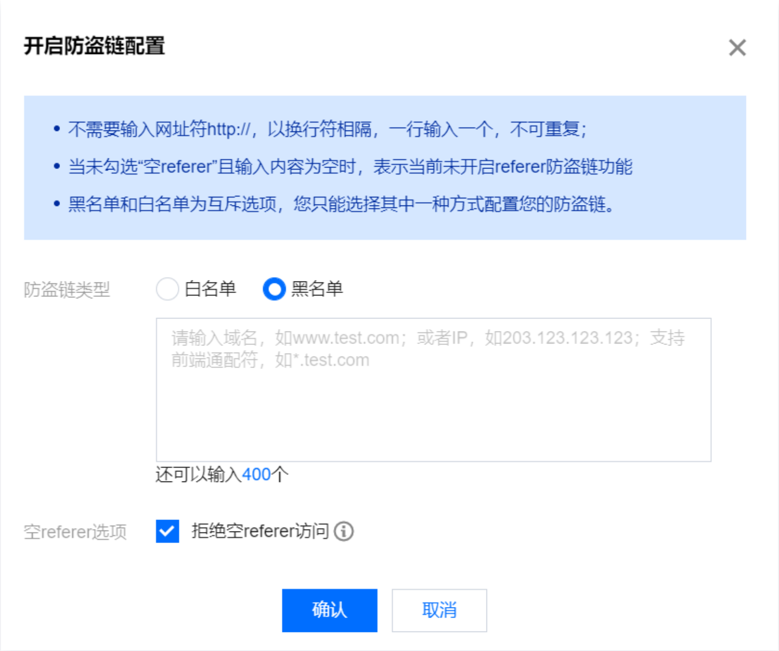
防盗链

您当前未设置防盗链规则

Enabling the configuration

Click the switch, select the Hotlink protection type, and fill in the list to enable the Hotlink protection configuration:
referer blocklist:

- If the referer field of a request matches the string configured in the blocklist, CDN node will not return the requested information and a 403 status code will be returned.
- If the referer field of a request does not match the string configured in the blocklist, CDN node will return the requested information.
- If the empty referer option is ticked **reject empty referer access**, CDN node will not return the requested information and a 403 status code will be returned if the referer field is empty or does not exist in a request (such as a browser request).



开启防盗链配置

- 不需要输入网址符http://，以换行符相隔，一行输入一个，不可重复；
- 当未勾选"空referer"且输入内容为空时，表示当前未开启referer防盗链功能
- 黑名单和白名单为互斥选项，您只能选择其中一种方式配置您的防盗链。

防盗链类型 ○ 白名单 ● 黑名单

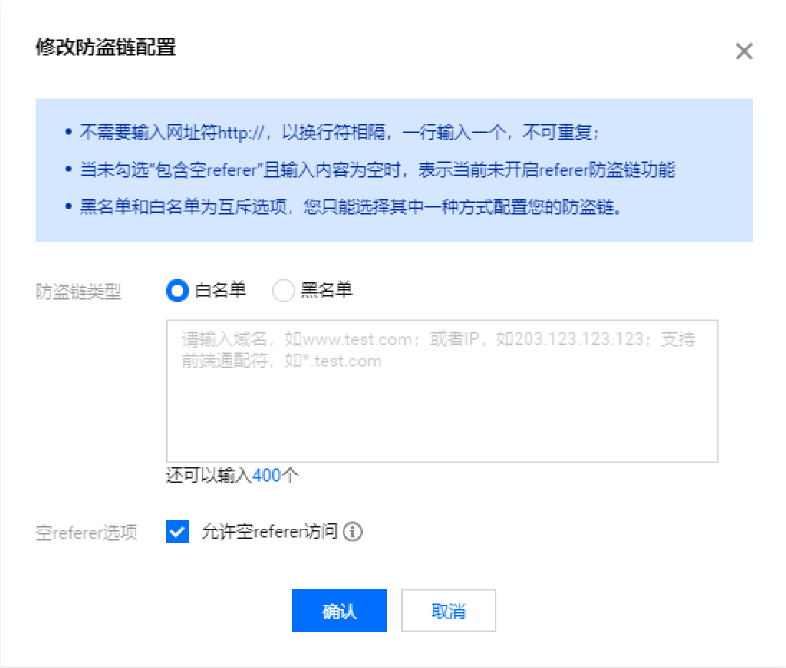
请输入域名，如www.test.com；或者IP，如203.123.123.123；支持前端通配符，如*.test.com

还可以输入400个

空referer选项 ☑ 拒绝空referer访问

referer allowlist:

- If the referer field of a request matches the string configured in the allowlist, CDN node will return the requested information.
- If the referer field of a request does not match the string configured in the allowlist, CDN node will not return the requested information and a 403 status code will be returned.
- Once the allowlist is configured, CDN node can only return requests that match the string configured in the allowlist.
- If the empty referer option **allow empty referer access** is ticked, CDN node will return the requested information if the referer field is empty or does not exist in a request (such as a browser request).



修改防盗链配置

- 不需要输入网址符http://，以换行符相隔，一行输入一个，不可重复；
- 当未勾选"包含空referer"且输入内容为空时，表示当前未开启referer防盗链功能
- 黑名单和白名单为互斥选项，您只能选择其中一种方式配置您的防盗链。

防盗链类型 ● 白名单 ○ 黑名单

请输入域名，如www.test.com；或者IP，如203.123.123.123；支持前端通配符，如*.test.com

还可以输入400个

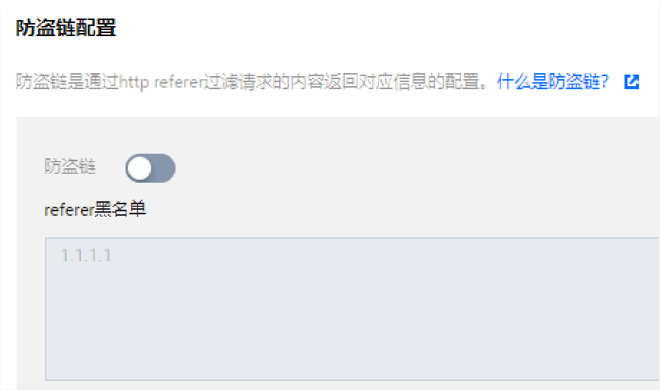
空referer选项 ☑ 允许空referer访问

Configuration limitations:

- Hotlink protection supports domain name/IP rules (if an IP rule is used, prefix matching is available; if a domain name rule is used, prefix matching is not supported). For example, if `www.abc.com` is configured, then `www.abc.com/123` will be matched, but `www.abc.com.cn` will not; if `127.0.0.1` is configured, then `127.0.0.1/123` will be matched.
- Hotlink protection supports wildcard matching. If the assumed list is `*.qq.com`, then `www.qq.com` and `a.qq.com` will be matched. However, `qq.com` will not be matched because its domain level is different from `*.qq.com`.

Disabling the Configuration

You can toggle off the switch to disable this feature. When the switch is off, this feature does not take effect in the production environment even if there is an existing configuration. If you toggle the switch on, the configuration will take effect across the entire network after the action is confirmed:



防盗链配置

防盗链是通过http referer过滤请求的内容返回对应信息的配置。什么是防盗链？

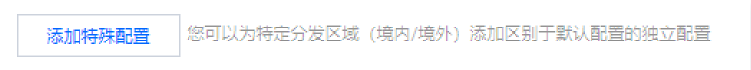
防盗链

referer黑名单

1.1.1.1

Region-specific configuration

If your acceleration domain name is configured for global acceleration and you want to configure different referer hotlink protection for acceleration in and outside the Chinese mainland, you can click **Add Special Configuration** to set it up:

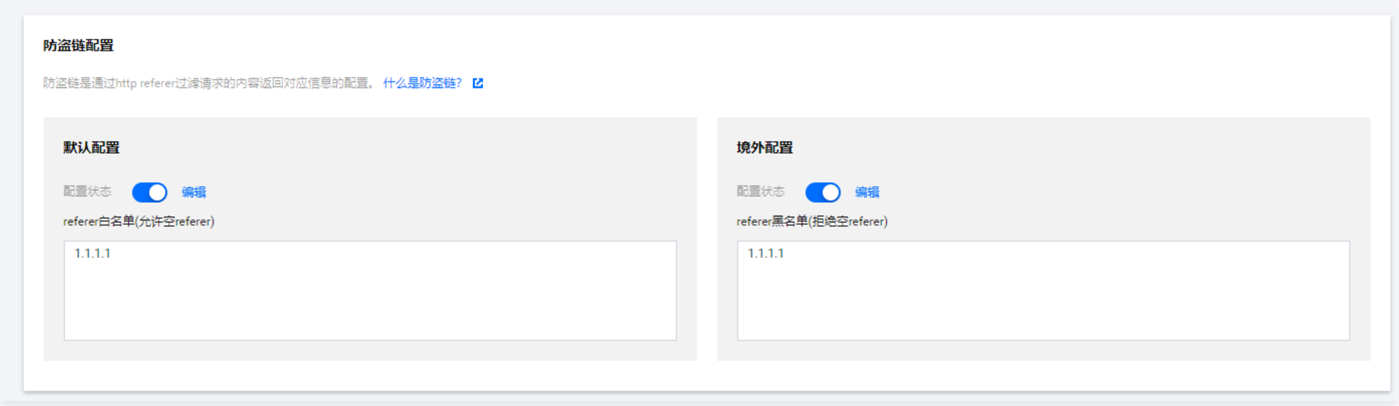


添加特殊配置 您可以为特定分发区域（境内/境外）添加区别于默认配置的独立配置

Note
Currently, an added region-specific configuration can only be disabled but not deleted.

Configuration Example

If the hotlink protection configuration of the acceleration domain name `www.test.com` is as follows:



防盗链配置

防盗链是通过http referer过滤请求的内容返回对应信息的配置。什么是防盗链？

默认配置

配置状态 编辑

referer白名单(允许空referer)

1.1.1.1

境外配置

配置状态 编辑

referer黑名单(拒绝空referer)

1.1.1.1

The actual access is as follows:

1. If a user in the Chinese mainland initiates a request with the referer field being `1.1.1.1`, which matches the allowlist configured for the Chinese mainland, then the requested content will be directly returned.
2. If a user outside the Chinese mainland initiates a request with a blank referer, which matches the blocklist configured for regions outside the Chinese mainland due to **rejecting empty referer access**, then a 403 status code will be returned.

IP Blocklist/Allowlist Configuration

Last updated：2024-12-31 17:33:14

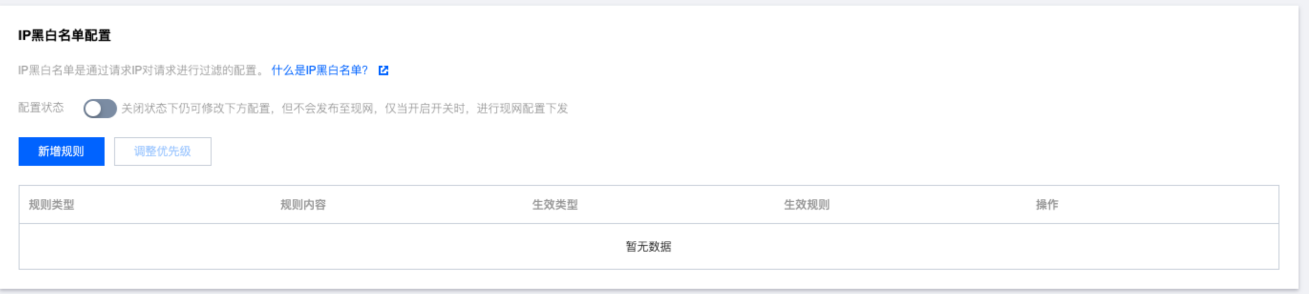
Configuration Scenario

To control the source of access to your business resources, you can use the IP blocklist/allowlist feature in Tencent Cloud CDN. By configuring an access control policy on IPs of user requests, you can effectively control the source of access to prevent hotlinking by malicious IPs, attacks, etc.

Configuration Guide

View Configuration

Log in to the CDN console, select **Domain Management** in the menu bar, click **Management** on the right side of the domain to enter the domain configuration page. In the second column **Access Control**, you can see the IP allowlist and blocklist configuration, which is disabled by default:



IP黑白名单配置

IP黑白名单是通过请求IP对请求进行过滤的配置。 什么是IP黑白名单?

配置状态 关闭状态下仍可修改下方配置，但不会发布至现网，仅当开启开关时，进行现网配置下发

规则类型	规则内容	生效类型	生效规则	操作
暂无数据				

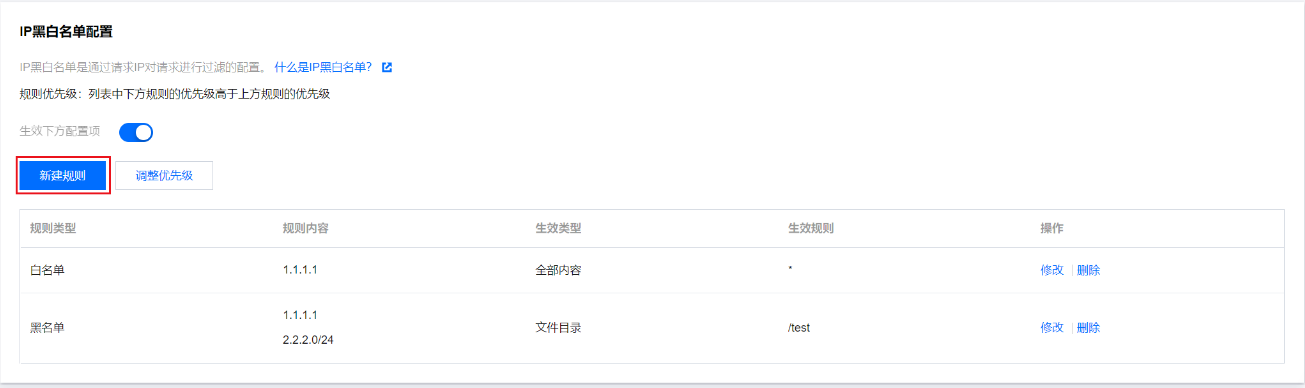
Enabling the configuration

Click the switch to enable the configuration. When enabling for the first time, if no rule exists, the new rule page will pop up by default. After enabling, the IP blocklist/allowlist will take effect according to the rule priority, with the bottom rule having the highest priority.

> **Note**
> If your acceleration domain name is configured for global acceleration, the IP blocklist/allowlist configuration takes effect globally. This configuration does not distinguish between requests from regions in and outside the Chinese mainland.

Adding or modifying a rule

You can click the **new rule** button in the IP blocklist to add one IP blocklist/allowlist rule.



IP黑白名单配置

IP黑白名单是通过请求IP对请求进行过滤的配置。 什么是IP黑白名单?

规则优先级：列表中下方规则的优先级高于上方规则的优先级

生效下方配置项

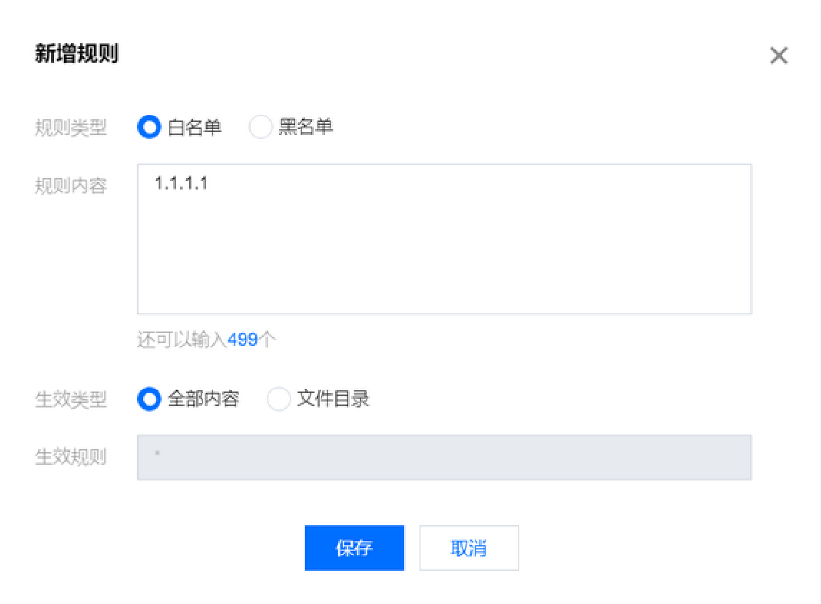
规则类型	规则内容	生效类型	生效规则	操作
白名单	1.1.1.1	全部内容	*	修改 | 删除
黑名单	1.1.1.1 2.2.2.0/24	文件目录	/test	修改 | 删除

IP Blocklist

When the user-end IP matches an IP or IP segment in the blocklist, accessing the CDN node will directly return a 514 status code.

IP Allowlist

When the user-end IP does not match an IP or IP segment in the allowlist, accessing the CDN node will directly return a 514 status code.



新增规则

规则类型 ● 白名单 ○ 黑名单

规则内容

```
1.1.1.1
```

还可以输入499个

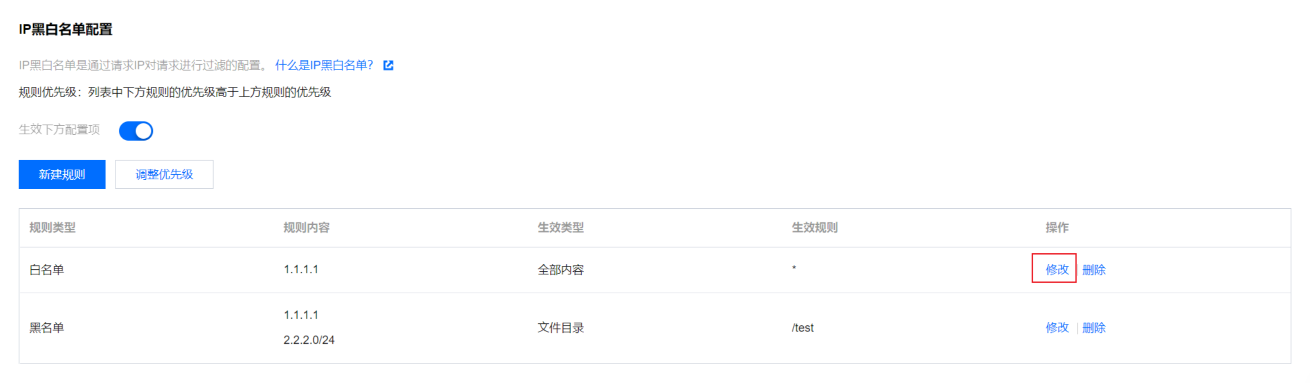
生效类型 ● 全部内容 ○ 文件目录

生效规则 *

Configuration limitations

- In a single rule, the IP blocklist and allowlist are mutually exclusive and cannot be configured at the same time.
- You can configure up to 20 rules.
- Across all rules, the IP allowlist can support 500 IPs/IP segments, and the blocklist can support 200 IPs/IP segments.
- Configuring reserved IPv4 and IPv6 addresses and segments as IP blocklist/allowlist is not supported.
- Supports IPv4, IPv6 addresses and segment formats /X (IPv4: 1⩽X⩽32; IPv6: 1⩽X⩽128), does not support IP:port format.
- Does not support parameterized file directories.

To modify a rule, click the **Modify** button in the action list on the right side of the rule.



IP黑白名单配置

IP黑白名单是通过请求IP对请求进行过滤的配置。 什么是IP黑白名单?

规则优先级：列表中下方规则的优先级高于上方规则的优先级

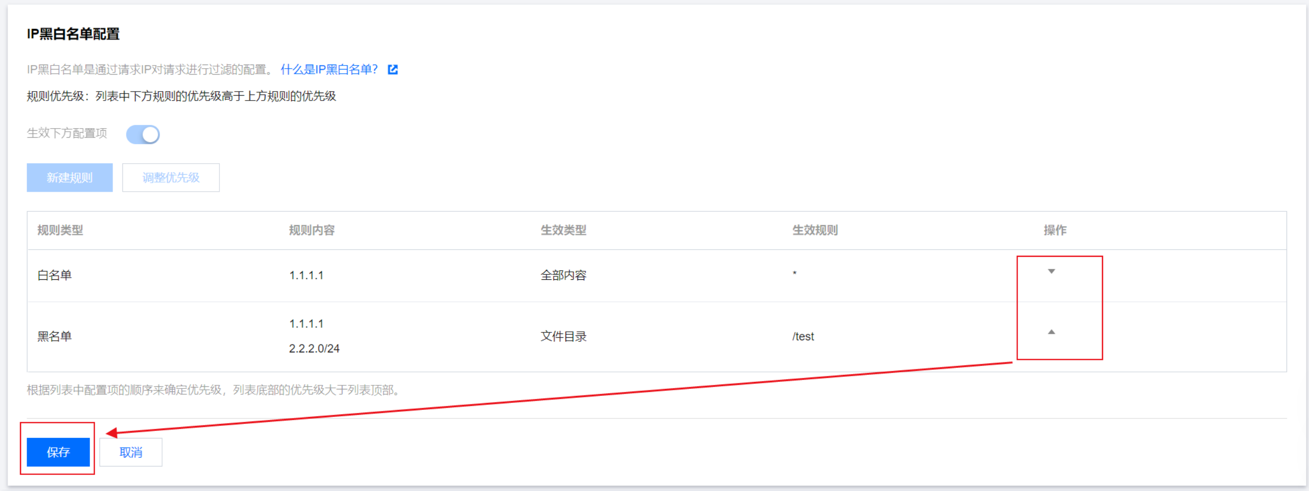
生效下方配置项

规则类型	规则内容	生效类型	生效规则	操作
白名单	1.1.1.1	全部内容	*	修改 删除
黑名单	1.1.1.1 2.2.2.0/24	文件目录	/test	修改 | 删除

Adjusting the priority of a rule

To adjust the priority of a rule, click **Adjust Priority** at the top of the rule list to enter priority adjustment mode. The page will appear as shown below. You can adjust the rule priority in the action column. The up arrow represents moving the rule up, and the down arrow represents moving the rule down. After adjustment, click **Save** to save the current rule priority order.

> **Note**
> Note: The priority at the bottom of the list is higher than that at the top.



IP黑白名单配置

IP黑白名单是通过请求IP对请求进行过滤的配置。 什么是IP黑白名单?

规则优先级：列表中下方规则的优先级高于上方规则的优先级

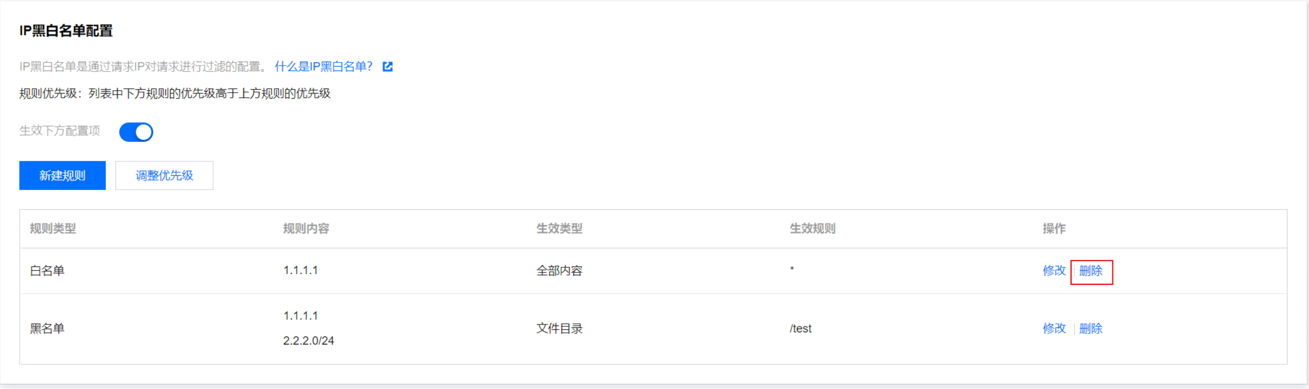
生效下方配置项

规则类型	规则内容	生效类型	生效规则	操作
白名单	1.1.1.1	全部内容	*	▾
黑名单	1.1.1.1 2.2.2.0/24	文件目录	/test	▴

根据列表中配置项的顺序来确定优先级，列表底部的优先级大于列表顶部。

Delete Rule

To delete a rule, click the **Delete** button in the action column of the rule. A popup for confirmation will appear. After confirmation, the rule will be permanently deleted.



IP黑白名单配置

IP黑白名单是通过请求IP对请求进行过滤的配置。 什么是IP黑白名单?

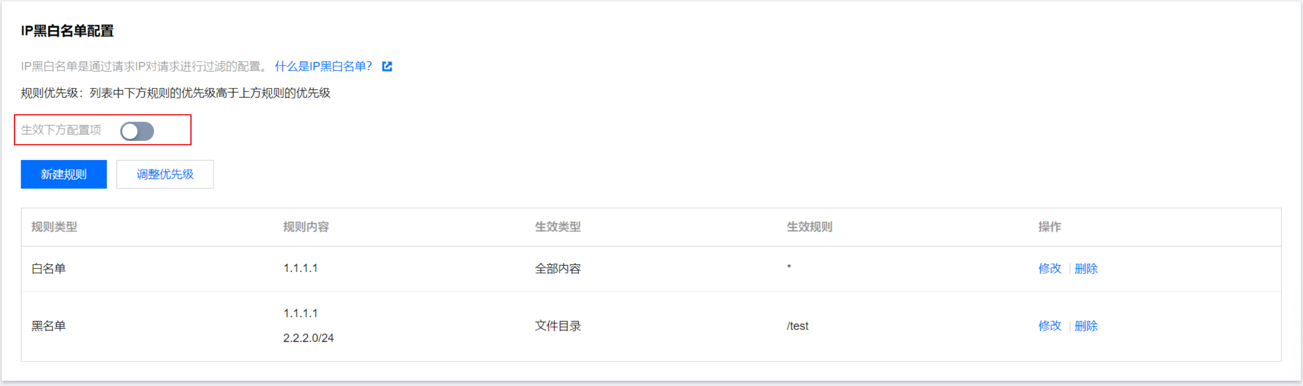
规则优先级：列表中下方规则的优先级高于上方规则的优先级

生效下方配置项

规则类型	规则内容	生效类型	生效规则	操作
白名单	1.1.1.1	全部内容	*	修改 | 删除
黑名单	1.1.1.1 2.2.2.0/24	文件目录	/test	修改 | 删除

Disabling the Configuration

Click the switch on the right side of the configuration status to disable the configuration. When the configuration is disabled, you can still modify the IP blocklist and allowlist rules, but they will not be immediately published to the current network. The rules will only take effect when the configuration is enabled.



IP黑白名单配置

IP黑白名单是通过请求IP对请求进行过滤的配置。 什么是IP黑白名单?

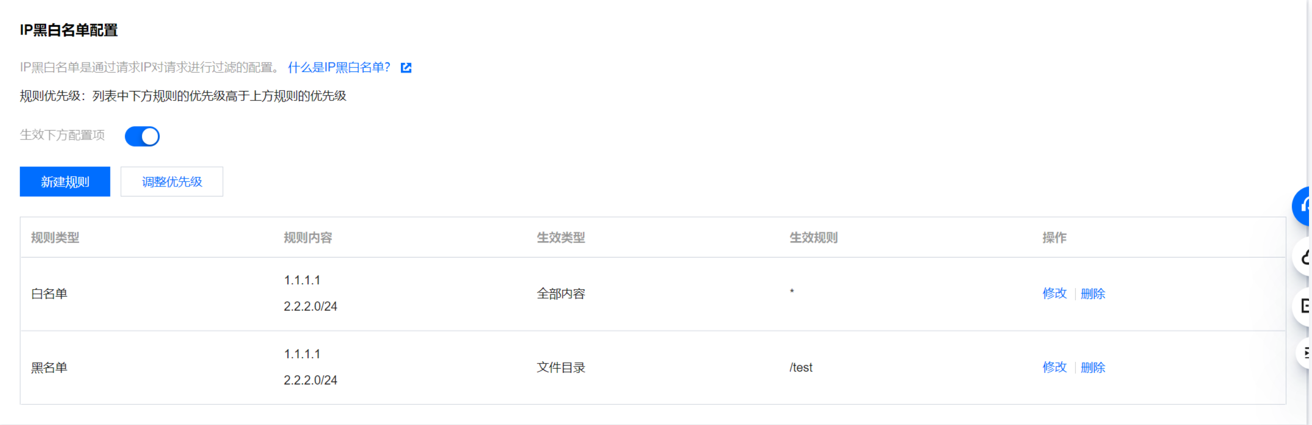
规则优先级：列表中下方规则的优先级高于上方规则的优先级

生效下方配置项

规则类型	规则内容	生效类型	生效规则	操作
白名单	1.1.1.1	全部内容	*	修改 | 删除
黑名单	1.1.1.1 2.2.2.0/24	文件目录	/test	修改 | 删除

Configuration Example

If the IP blocklist/allowlist configuration of the acceleration domain name `www.test.com` is as follows:



IP黑白名单配置

IP黑白名单是通过请求IP对请求进行过滤的配置。 什么是IP黑白名单？

规则优先级：列表中下方规则的优先级高于上方规则的优先级

生效下方配置项

规则类型	规则内容	生效类型	生效规则	操作
白名单	1.1.1.1 2.2.2.0/24	全部内容	*	修改 | 删除
黑名单	1.1.1.1 2.2.2.0/24	文件目录	/test	修改 | 删除

Then the actual access will be as follows:

1. If a user whose IP is 1.1.1.1 requests to access `https://www.test.com/test/vod.mp4` , the request matches the bottom blocklist rule, and the user is not allowed to access, returning 514.
2. If a user whose IP is 1.1.1.2 requests to access `https://www.test.com/test/vod.mp4` , the IP is not in the blocklist rule, so the blocklist rule is not matched. However, the request matches the allowlist rule, which only allows access for IP 1.1.1.1. Since the user's IP does not match, the user is not allowed to access, returning 514.
3. If a user whose IP is 1.1.1.1 requests to access `https://www.test.com/vod.mp4` , the blocklist rule is not matched, but the allowlist rule is matched. In this case, the access request is allowed, and the user can access the resource as expected.
4. If a user whose IP is 2.2.2.1 requests to access `https://www.test.com/vod.mp4` , the blocklist rule is not matched. Since 2.2.2.1 belongs to the 2.2.2.0/24 IP range, the allowlist rule is matched. In this case, the access request is allowed, and the user can access the resource as expected.

IP Access Frequency Configuration

Last updated：2024-12-31 17:33:24

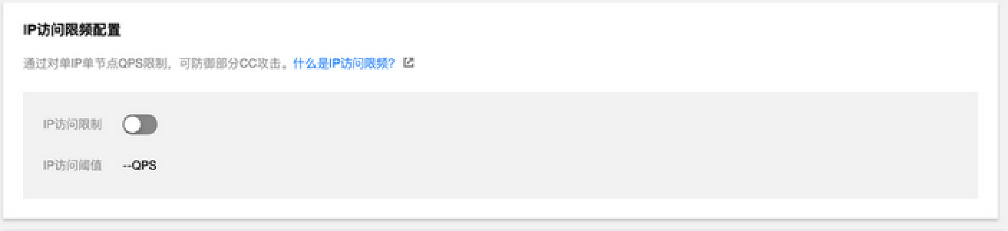
Configuration Scenario

To control the source of access to your business resources, you can use the IP access limit feature in CDN. By limiting the number of access requests to a node per second from a single IP, you can defend against high-frequency CC attacks and prevent hotlinking by malicious users.

Configuration Guide

Viewing Configuration

Log in to the cdn console, select **Domain Management** from the menu bar, click **Management** on the right side of the domain to enter the domain configuration page. In the second column **Access Control**, you can see the IP access limit configuration. By default, the configuration is disabled and the threshold is empty:



IP访问限频配置

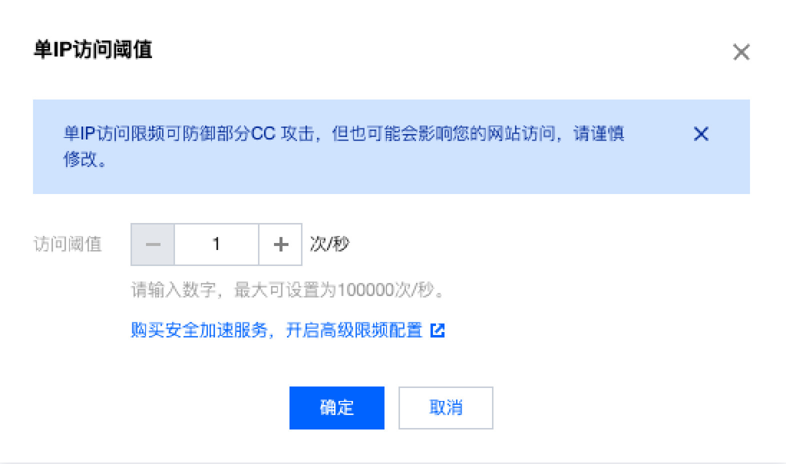
通过对单IP单节点QPS限制，可防御部分CC攻击。什么是IP访问限频？

IP访问限制

IP访问阈值 --QPS

Enabling the configuration

Click the switch, fill in the frequency control threshold, and click **OK** to enable IP access limit control:



单IP访问阈值

单IP访问限频可防御部分CC 攻击，但也可能会影响您的网站访问，请谨慎修改。

访问阈值 1 次/秒

请输入数字，最大可设置为100000次/秒。

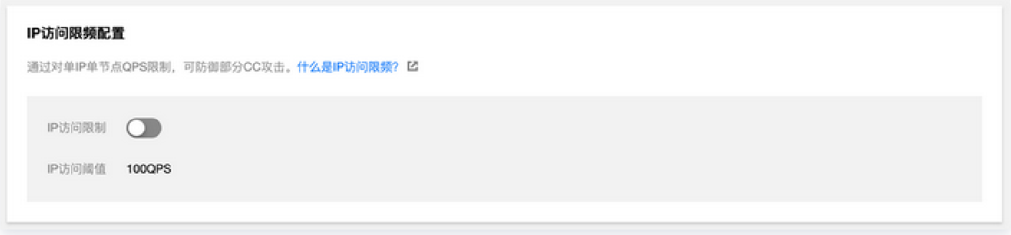
购买安全加速服务，开启高级限频配置

Configuration Note

- After the configuration is enabled, a 514 error will be returned for requests that exceed the QPS limit. A low access frequency limit may impact the normal use of your business by high-frequency users. Configure the proper threshold according to your actual business conditions and use cases.
- IP access limit is effective for attacks from a single IP to a single node. If a malicious user uses a high number of IPs to attack nodes on your entire network, this feature is no longer applicable. For stronger CC attack defense, it is recommended to purchase the Tencent Cloud EdgeOne.
- Under the same domain, if multiple different URLs are requested simultaneously, any URL that exceeds the threshold from a single IP to a single node will directly return a 514 error.

Disabling the Configuration

You can switch to disable this feature. When the switch is off, this feature does not take effect in the production environment even if there is an existing configuration. When the switch is on, this configuration will take effect across the entire network:



IP访问限频配置

通过对单IP单节点QPS限制，可防御部分CC攻击。什么是IP访问限频？

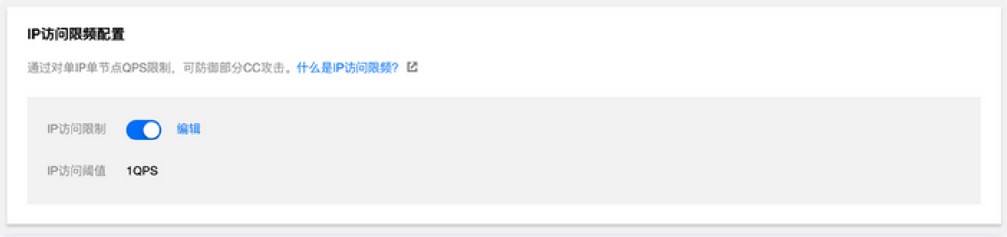
IP访问限制 ○

IP访问阈值 100QPS

> ⚠ **Note**
> If your acceleration domain name is configured for global acceleration, the IP access limit configuration takes effect globally. This configuration does not distinguish between requests from regions in and outside the Chinese mainland. (Note)

Configuration Example

Suppose the IP access limit for the acceleration domain name `www.test.com` is as follows:



IP访问限频配置

通过对单IP单节点QPS限制，可防御部分CC攻击。什么是IP访问限频？

IP访问限制 ● 编辑

IP访问阈值 1QPS

The actual access status will be as follows:

1. A user with the client IP `1.1.1.1` requests the resource `http://www.test.com/1.jpg` 10 times in one second, all accessing a server in CDN cache node A. This generates 10 access logs on that server, with 9 logs showing status code 514 due to exceeding the QPS limit.
2. A user with the client IP `2.2.2.2` requests the resource `http://www.test.com/1.jpg` twice in one second, and the access requests may be distributed to two CDN cache nodes for processing due to network conditions. Each node will return the content normally.

Video dragging configuration

Last updated：2024-12-31 17:34:16

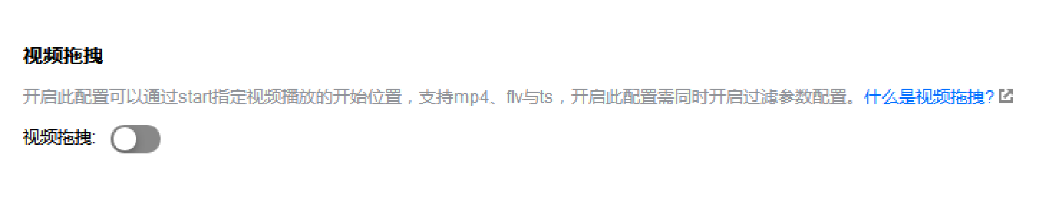
Configuration Scenario

- Video dragging generally happens in VOD scenarios. When a user drags the video progress bar, a request similar to the one as shown below will be sent to the server:
  `http://www.test.com/test.flv?start=10`
  In this case, data will be returned starting from the 10th byte. Video files in VOD scenarios are all cached on various CDN nodes; therefore, the nodes can directly respond to such requests once this configuration is enabled.
- To enable video dragging, the ignore parameter configuration must also be enabled. That is, the ignore parameter configuration for all rules in the cache key rules must be "ignore all", and the origin server must support range requests. Supported file formats are: mp4, flv, ts.

File Type	Meta Information	Parameter Description (start)	Request Sample
MP4	The meta information of the origin server video must be in the file header; videos with meta information in the tail are not supported.	The start parameter represents time in seconds and supports decimals to indicate milliseconds (e.g., start = 1.01 means the start time is 1.01s). The CDN will locate the key frame before the time indicated by start (if the current start is not a key frame).	`http://www.test.com/demo.mp4?start=10` means to start playing from the 10th second.
FLV	The origin server video must contain meta information.	The start parameter represents bytes. CDN will automatically locate the key frame before the byte indicated by the start parameter (if start is not currently a key frame).	`http://www.test.com/demo.flv?start=10` means to start playing from the 10th byte.
TS	No special requirements	The start parameter represents bytes. CDN will automatically locate the byte indicated by the start parameter.	`http://www.test.com/demo.ts?start=10` means to start playing from the 10th byte.

Viewing Configuration

Log in to the CDN console, select **Domain Management** from the left sidebar menu, choose the domain name with the business type of streaming media on-demand acceleration, and enter the domain configuration page. In the Tab **Access Control** page, you can find **Video Dragging**, which is in closed status by default. You can enable **Video Dragging** by default through the recommended configuration of CDN audio and video on-demand domain name.



视频拖拽

开启此配置可以通过start指定视频播放的开始位置，支持mp4、flv与ts，开启此配置需同时开启过滤参数配置。什么是视频拖拽?

视频拖拽: ○

Authentication Configuration Configuration Instructions

Last updated：2024-12-31 17:34:31

Configuration Scenario

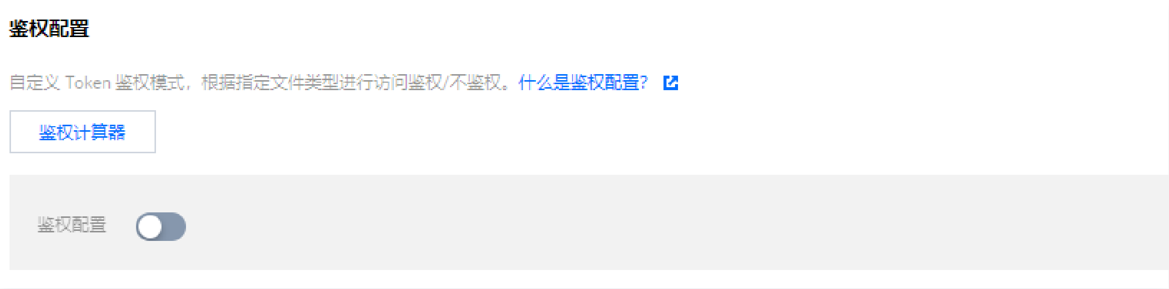
Generally, contents delivered over CDN are public resources by default, which can be accessed by users with URLs. To prevent malicious users from hotlinking your content for profit, you can configure advanced timestamp authentication in addition to access control policies such as referer blocklist/allowlist, IP blocklist/allowlist, and IP access frequency limit.

> **Note**
> After timestamp hotlink protection is configured, the client needs to calculate the signature as configured and carry it to the server when initiating a request. The CDN node will authenticate the signature on the server, which will pass only after successful authentication.

Configuration Guide

Viewing Configuration

Log in to the CDN console, select **Domain Management** from the menu bar, click **Management** on the right side of the domain name to enter the domain configuration page. In **Access Control**, you can see the authentication configuration, which is in closed status by default:



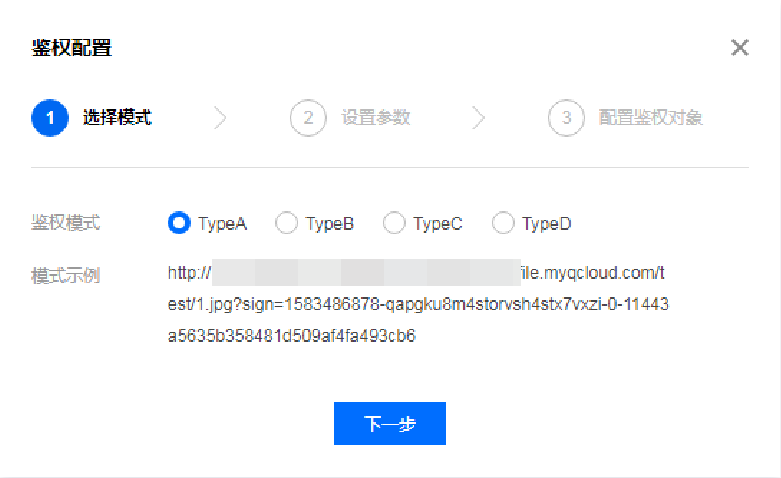
鉴权配置

自定义 Token 鉴权模式，根据指定文件类型进行访问鉴权/不鉴权。什么是鉴权配置？

Modify

1. Modify the configuration

CDN provides four authentication signature calculation methods for you to choose from. You can also use the **authentication calculator** above to view different authentication modes and the final effect after configuration. For specific algorithm descriptions, please refer to the algorithm documentation for TypeA, TypeB, TypeC, and TypeD:



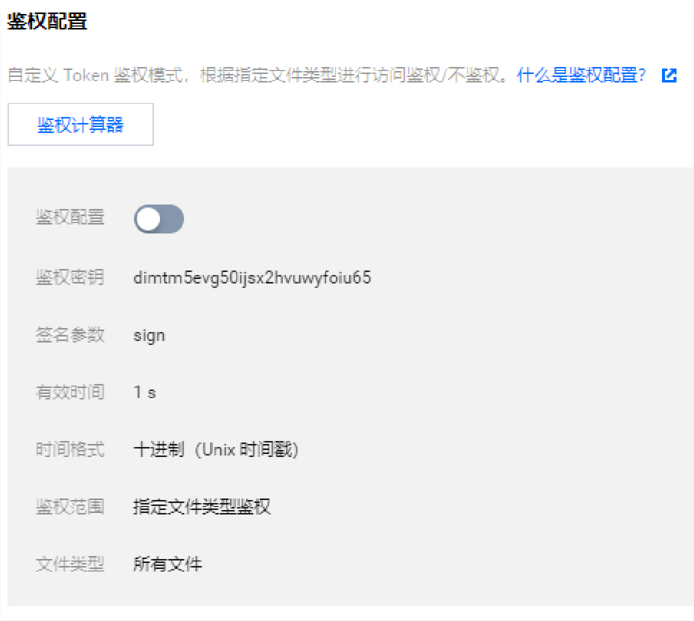
鉴权配置

鉴权模式 ● TypeA ○ TypeB ○ TypeC ○ TypeD

模式示例 http://[redacted]ile.myqcloud.com/test/1.jpg?sign=1583486878-qapgku8m4storvsh4stx7vxzi-0-11443a5635b358481d509af4fa493cb6

2. Disable the configuration

You can toggle the authentication configuration switch to disable this feature. When the switch is off, any existing configuration will not take effect in the production environment. If you toggle the switch on, a message will be displayed asking for your confirmation before the configuration takes effect across the entire network:



鉴权配置

自定义 Token 鉴权模式，根据指定文件类型进行访问鉴权/不鉴权。什么是鉴权配置？

鉴权计算器

鉴权配置

鉴权密钥 dimtm5evg50ijsx2hvuwyfoiu65

签名参数 sign

有效时间 1 s

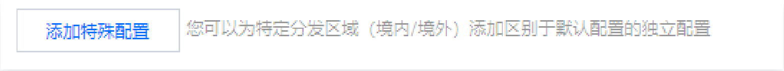
时间格式 十进制（Unix 时间戳）

鉴权范围 指定文件类型鉴权

文件类型 所有文件

3. Add a region-specific configuration

If your acceleration domain name is configured for global acceleration and you want to configure different authentication settings for acceleration in and outside the Chinese mainland, you can click [Add Special Configuration] below the configuration to set it up.

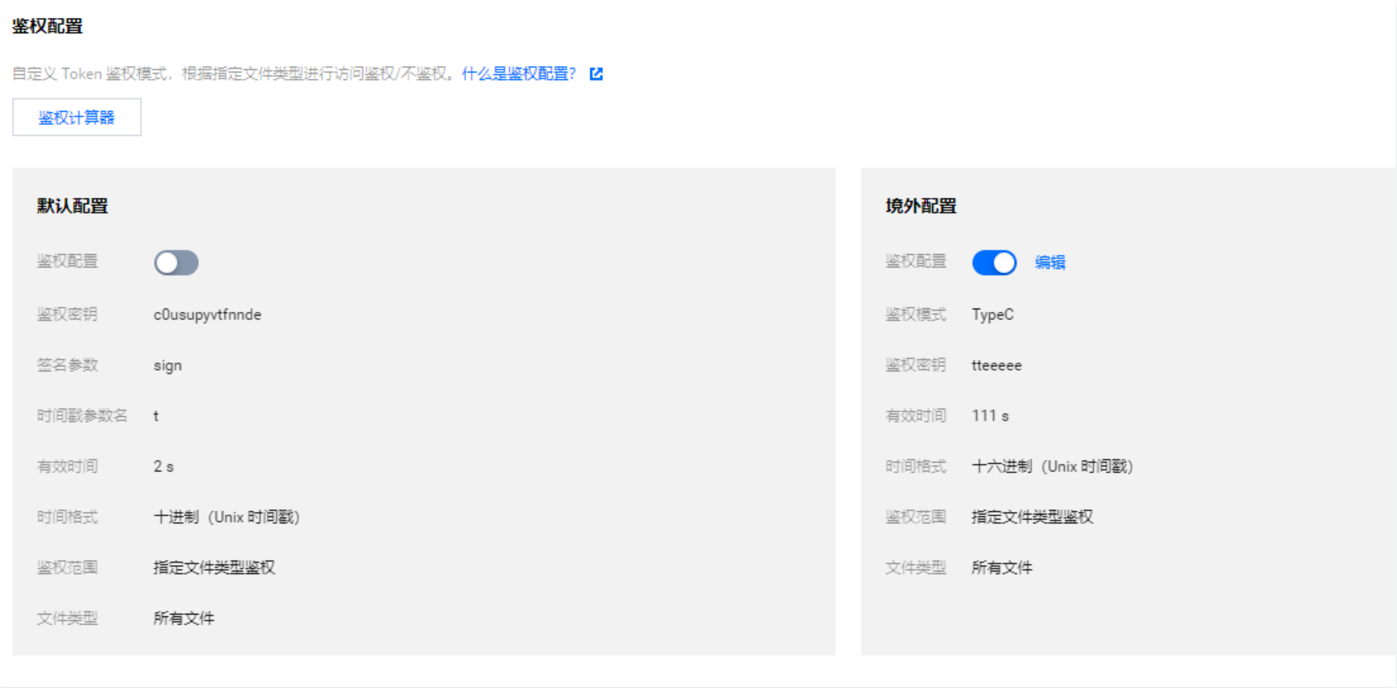


添加特殊配置 您可以为特定分发区域（境内/境外）添加区别于默认配置的独立配置

> ⚠ **Note**
> Currently, an added region-specific configuration can only be disabled but not deleted.

Configuration Example

Suppose the domain name `cloud.tencent.com` is configured for global acceleration and the authentication configuration is as follows:



鉴权配置

自定义 Token 鉴权模式，根据指定文件类型进行访问鉴权/不鉴权。什么是鉴权配置？

鉴权计算器

默认配置

鉴权配置 ○

鉴权密钥 c0usupyvtfnnde

签名参数 sign

时间戳参数名 t

有效时间 2 s

时间格式 十进制（Unix 时间戳）

鉴权范围 指定文件类型鉴权

文件类型 所有文件

境外配置

鉴权配置 ● 编辑

鉴权模式 TypeC

鉴权密钥 tteeeee

有效时间 111 s

时间格式 十六进制（Unix 时间戳）

鉴权范围 指定文件类型鉴权

文件类型 所有文件

The actual effect will be as follows:

1. When users within China access the resource `http://cloud.tencent.com/1.jpg` , if the global default configuration is off and the special configuration for the region is only on for outside China, the configuration within China will not have an authentication effect. Users can directly initiate the request, the current request will be effective, and the correct file will be returned.
2. When users outside China access the resource `http://cloud.tencent.com/1.jpg` , since the current authentication mode for outside China is TypeC, the correct format of the request URL should be `http://cloud.tencent.com/509301d10da7b862052927ed7a947f43/5e561139/1.jpg` . If users request using this URL, the correct file content will be returned; otherwise, the access request will be denied.

Sample code

The following is the authentication calculation method with the Demo for Python as an example:

```
import requests
import json
import sys
import time
import hashlib

def generate_url(category, ts=None):
    url = 'http://www.test.com'              # Test domain name
    path = '/1.txt'                                     # Access path
    suffix = '?a=1&b=2'                                 # URL parameter
    key = 'abc123456789'                                # authentication key
    now = int(time.mktime(time.strptime(ts, "%Y%m%d%H%M%S")) if ts else time.time())                # If a
ts is entered, it will be used; otherwise, the current ts will be used
    sign_key = 'key'                                    # URL signature field
    time_key = 't'                                      # URL time field
    ttl_format = 10                                     # Time format. Valid values: 10, 16. This is
supported only for type D
    if category == 'A':                                 #Type A
        ts = now
        rand_str = '123abc'
        sign = hashlib.md5('%s-%s-%s-%s-%s' % (path, ts, rand_str, 0, key)).hexdigest()
        request_url = '%s%s?%s=%s' % (url, path, sign_key, '%s-%s-%s-%s' % (ts, rand_str, 0, sign))
        print(request_url)
    elif category == 'B':                               #Type B
```

```
        ts = time.strftime('%Y%m%d%H%M', time.localtime(now))
        sign = hashlib.md5('%s%s%s' % (key, ts, path)).hexdigest()
        request_url = '%s/%s/%s%s%s' % (url, ts, sign, path, suffix)
        print(request_url)
    elif category == 'C':                               #Type C
        ts = hex(now)[2:]
        sign = hashlib.md5('%s%s%s' % (key, path, ts)).hexdigest()
        request_url = '%s/%s/%s%s%s' % (url, sign, ts, path, suffix)
        print(request_url)
    elif category == 'D':                               #Type D
        ts = now if ttl_format == 10 else hex(now)[2:]
        sign = hashlib.md5('%s%s%s' % (key, path, ts)).hexdigest()
        request_url = '%s%s?%s=%s&%s=%s' % (url, path, sign_key, sign, time_key, ts)
        print(request_url)


if __name__ == '__main__':
    if len(sys.argv) == 1:
        print('usage: python generate_url.py A 20200501000000')
    args = sys.argv[1:]
    generate_url(*args)
```

TypeA

Last updated：2024-12-31 17:34:42

To protect your site resources from being downloaded or stolen by unauthorized users, you can choose an authentication method from Types A, B, C, and D as needed. This document describes parameter fields and their purposes in Type A authentication.

Algorithm Description

- **Access URL Format**
  `http://DomainName/Filename?sign=timestamp-rand-uid-md5hash`

> **Note**
> - The access URL cannot contain any Chinese characters. If the URL contains Chinese characters, please encode them in advance.
> - Does not support authentication for URLs with parameters containing ?.
> - Supports minimum time unit in seconds (s), maximum valid time can be entered is 630720000s.

- **Description of authentication fields**

Field	Description
DomainName	CDN domain.
Filename	Resource access path. During authentication, `Filename` must start with a slash (/).
timestamp	The time when the server generates the authentication URL. It is a positive hex integer Unix timestamp, which is the total number of seconds between 00:00:00, January 1, 1970, UTC time and the URL generation time. Its definition is irrelevant to the time zone.
rand	A random string consisting 0-100 characters ([0-9], [a-z], [A-Z]).
uid	User ID, not used yet, set it to `0` .
md5hash	A fixed-length string of 32 characters calculated using the MD5 algorithm. The specific calculation formula for md5hash is as follows: • md5hash = md5sum(uri-timestamp-rand-uid-pkey) • `uri` : It is the resource access path and must start with a slash (/). • timestamp: value is one of the above timestamps • rand: value is one of the above rands • uid: value is one of the above uids • pkey: custom key: consists of 6 - 40 uppercase and lowercase letters and numbers. The key must be strictly confidential and known only to the client and server.

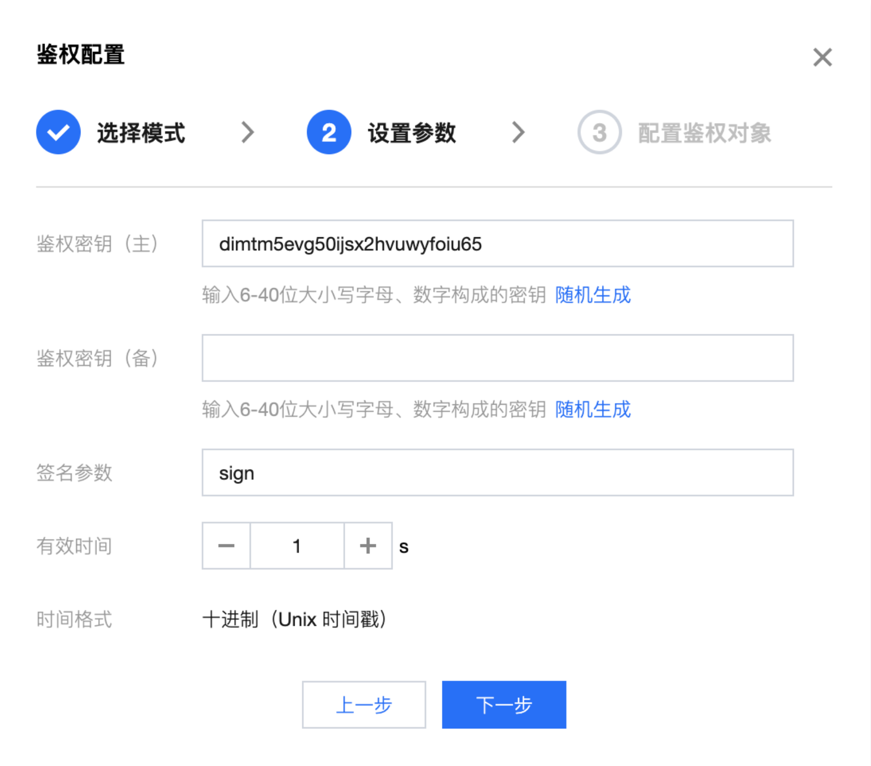
- **Authentication logic description**
  After the CDN server receives the client request, it parses the timestamp parameter in the URL and compares the authentication URL validity duration with the current time.
  - If timestamp + authentication URL duration is less than the current time, the server judges it as expired and invalid, and returns an HTTP 403 error.
  - If timestamp + authentication URL duration is greater than the current time, use the MD5 algorithm to calculate the md5hash value, then compare the calculated md5hash value with the md5hash value passed in the URL. If they match, it is allowed; if not, an HTTP 403 error is returned.

Configuration Guide

Taking the configuration of Type-A authentication as an example, the parameters and console configuration items are configured as follows:

- **Field configuration**
  - Authentication key: dimtm5evg50ijsx2hvuwyfoiu65

  - Signature parameter: sign
  - Validity period of the authentication URL: 1s



鉴权密钥（主） dimtm5evg50ijsx2hvuwyfoiu65

输入6-40位大小写字母、数字构成的密钥

鉴权密钥（备）

输入6-40位大小写字母、数字构成的密钥

签名参数 sign

有效时间 1 s

时间格式 十进制（Unix 时间戳）

  - Time when the signature server generates the authentication URL: February 27, 2020, 16:10:32 (UTC+8), converted to a decimal integer value is 1582791032 (timestamp)
  - Requested origin address: `http://cloud.tencent.com/test.jpg`

- **Generation process**
  - Get authentication parameters:

Parameter	Value.
uri	The resource access path is /test.jpg
timestamp	1582791032
rand	Generate a random string: im1acp76sx9sdqe601v
uid	Set it to `0`
pkey	dimtm5evg50ijsx2hvuwyfoiu65

  - Concatenate the signature string: /test.jpg-1582791032-im1acp76sx9sdqe601v-0-dimtm5evg50ijsx2hvuwyfoiu65
  - Calculate the MD5 value of the signature string: md5hash = md5sum(uri-timestamp-rand-uid-pkey) = md5sum(/test.jpg-1582791032-im1acp76sx9sdqe601v-0-dimtm5evg50ijsx2hvuwyfoiu65) = 3fbb88382c9356b6faaf9d68c7b2ae3a
- **Generate authentication URL:**
  `http://cloud.tencent.com/test.jpg?sign=1582791032-im1acp76sx9sdqe601v-0-3fbb88382c9356b6faaf9d68c7b2ae3a`
  When the client accesses through the encrypted URL, if the md5hash value calculated by the CDN server matches the md5hash value in the access request, both being 3fbb88382c9356b6faaf9d68c7b2ae3a, the authentication succeeds; otherwise, the authentication fails.

Notes

Cache hit rate

For domain names using TypeA authentication mode, the access URL will carry the authentication parameter. When a CDN node caches the resource, the corresponding parameter will be ignored and thus will not affect the cache hit rate.

> **Note**
> Since the corresponding parameters will be automatically ignored after configuration, the configured authentication parameters will be ignored, affecting the cache key of files within the authentication range. This priority is higher than the cache key rules in **Cache Configuration - Cache Key Rule Configuration**.
> For example, if the TypeA configuration here is: authentication parameter: sign - authentication range: jpg, then the "sign" parameter for jpg files will be automatically ignored, even if **Cache Configuration - Cache Key Rule Configuration** is configured: all files - do not ignore parameters.

Origin-pull policy

The access format of a domain name with Type A authentication mode enabled is as follows:

```
http://DomainName/Filename?sign=timestamp-rand-uid-md5hash
```

After authentication is passed, if the CDN node is not hit, the node will initiate an origin-pull request, **the format is consistent with the access request and the signature parameter will be retained**. The origin server can ignore or re-verify as needed.

TypeB

Last updated：2024-12-31 17:35:20

To protect your site resources from being downloaded or stolen by unauthorized users, you can choose an authentication method from Types A, B, C, and D as needed. This document describes parameter fields and their purposes in Type B authentication.

Algorithm Description

- **Access URL Format**
  `http://DomainName/timestamp/md5hash/FileName`

  > **Note**
  > - The access URL cannot contain any Chinese characters. If the URL contains Chinese characters, please encode them in advance.
  > - Does not support authentication for URLs with parameters containing ?.
  > - Supports minimum time unit in seconds (s), maximum valid time can be entered is 630720000s.

- **Description of authentication fields**

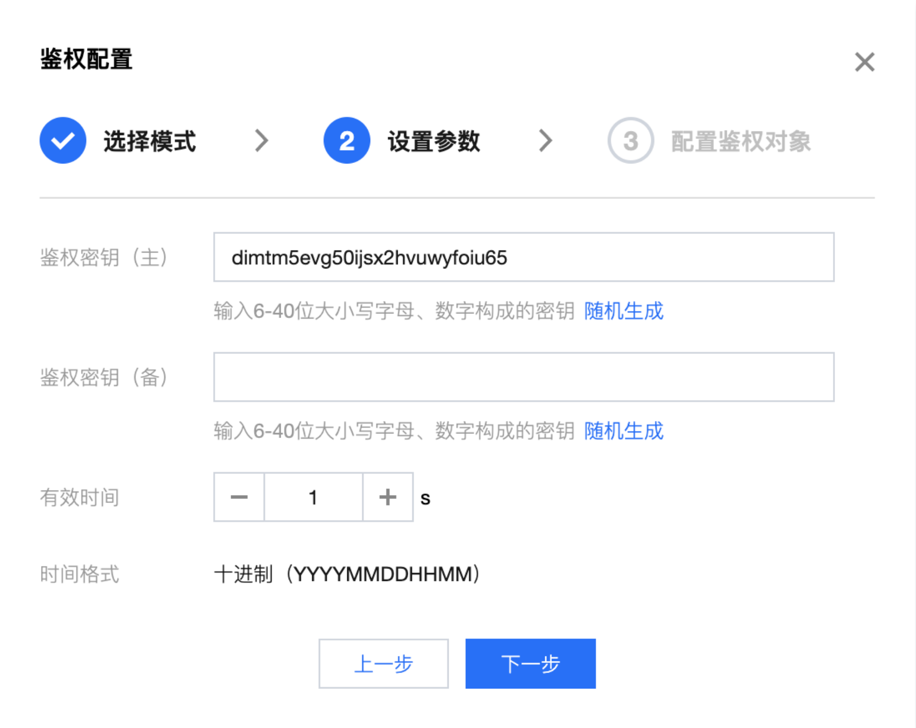
Field	Description
DomainName	CDN domain.
Filename	Resource access path. During authentication, `Filename` must start with a forward slash (`/`).
timestamp	The time to generate the authenticated URL by the signature calculation server, together with the validity period, controls the expiration time of the authenticated URL. The format is: YYYYMMDDHHMM (the time point is based on the UTC+8 time of the signature calculation server), for example: 201807301000.
md5hash	A string containing 32 characters calculated based on the MD5 algorithm. The specific calculation formula is as follows: • md5hash = md5sum(pkeytimestampuri) No symbols between parameters • pkey: custom key: consists of 6 - 40 uppercase and lowercase letters and numbers. The key must be strictly confidential and known only to the client and server. • uri resource access path starts with a forward slash (/). • timestamp: the value is the timestamp mentioned above.

- **Authentication logic description**
  After the CDN server receives the client request, it parses the timestamp parameter in the URL and compares the timestamp + authentication URL duration with the current time.
  - If timestamp + authentication URL duration is less than the current time, the server judges it as expired and invalid, and returns an HTTP 403 error.
  - If timestamp + authentication URL duration is greater than the current time, the MD5 algorithm is used to calculate the value of md5hash. Then, the calculated md5hash value is compared with the md5hash value passed in the URL. If they match, the request is allowed; if not, an HTTP 403 error is returned.

Configuration Guide

Taking the configuration of Type-B authentication as an example, the parameters and console configuration items are configured as follows:

- **Field configuration**
  - Authentication key: dimtm5evg50ijsx2hvuwyfoiu65
  - Validity period of the authentication URL: 1s



鉴权配置

✓ 选择模式 > 2 设置参数 > 3 配置鉴权对象

鉴权密钥（主） dimtm5evg50ijsx2hvuwyfoiu65

输入6-40位大小写字母、数字构成的密钥 随机生成

鉴权密钥（备）

输入6-40位大小写字母、数字构成的密钥 随机生成

有效时间 1 s

时间格式 十进制（YYYYMMDDHHMM）

  - Time when the signature server generates the authentication URL: February 27, 2020, 16:10:32 (UTC+8)
  - Requested origin address: `http://cloud.tencent.com/test.jpg`
- **Generation process**
  - Get authentication parameters:

Parameter	Value.
uri	The resource access path is /test.jpg
timestamp	202002271610
pkey	dimtm5evg50ijsx2hvuwyfoiu65

  - Concatenate the signature string: dimtm5evg50ijsx2hvuwyfoiu65202002271610/test.jpg
  - Calculate the MD5 value of the signature string: md5hash = md5sum(pkeytimestampuri) =md5sum(dimtm5evg50ijsx2hvuwyfoiu65202002271610/test.jpg) = 2e03a07cfa55a47768226d3e5ea82a8d
- **generate authentication url**

  `http://cloud.tencent.com/202002271610/2e03a07cfa55a47768226d3e5ea82a8d/test.jpg` When the client accesses through the encrypted URL, if the md5hash value calculated by the CDN server matches the md5hash value in the access request, both being 2e03a07cfa55a47768226d3e5ea82a8d, the authentication succeeds; otherwise, the authentication fails.

Notes

Cache hit rate

For domain names using TypeB authentication mode, the access URL path will carry the signature and timestamp. When a CDN node caches the resource, the fields in the path will be automatically ignored and thus will not affect the cache hit rate.

Origin-pull policy

The access format of a domain name with TypeB authentication mode enabled is as follows:

`http://DomainName/timestamp/md5hash/FileName`

After authentication is passed, if the CDN node is not hit, the node will initiate an origin server request, **the origin server request will remove the md5hash and timestamp from the path**, and the origin server does not need special handling.

TypeC

Last updated：2024-12-31 17:35:34

To protect your site resources from being downloaded or stolen by unauthorized users, you can choose an authentication method from Types A, B, C, and D as needed. This document describes parameter fields and their purposes in Type C authentication.

Algorithm Description

- **Access URL Format**
  `http://DomainName/md5hash/timestamp/FileName`

> **Note**
> - The access URL cannot contain any Chinese characters. If the URL contains Chinese characters, please encode them in advance.
> - Does not support authentication for URLs with parameters containing ?.
> - Supports minimum time unit in seconds (s), maximum valid time can be entered is 630720000s.

- **Description of authentication fields**

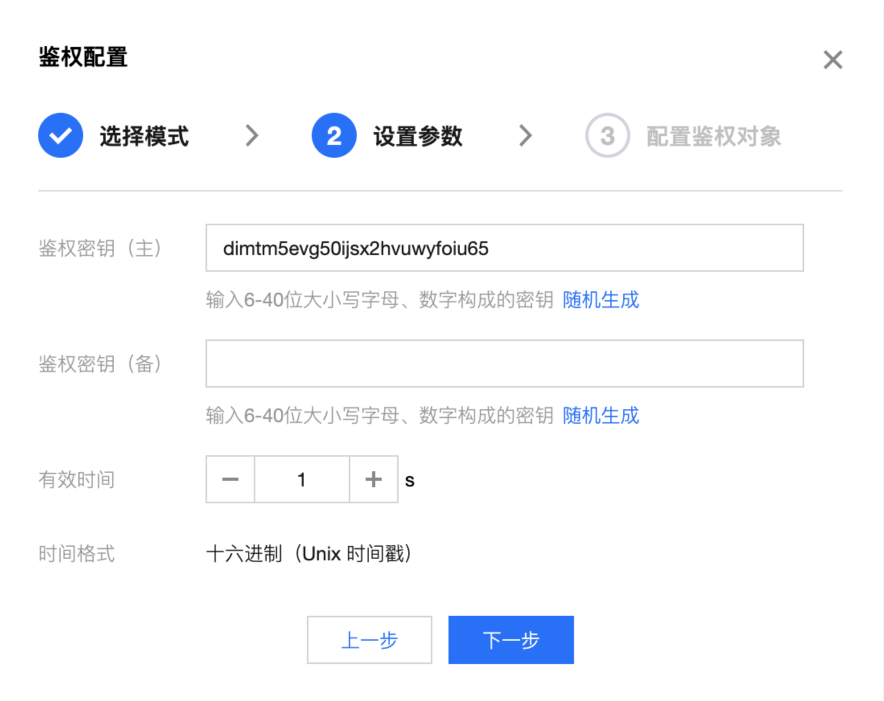
Field	Description
DomainName	CDN domain.
Filename	Resource access path. During authentication, `Filename` must start with a slash (/).
timestamp	The time when the server generates the authentication URL. It is a positive hex integer Unix timestamp, which is the total number of seconds between 00:00:00, January 1, 1970, UTC time and the URL generation time. Its definition is irrelevant to the time zone.
md5hash	A string containing 32 characters calculated based on the MD5 algorithm. The specific calculation formula is as follows: • md5hash = md5sum(pkeyuritimestamp) no symbols between parameters • pkey: Custom key: consists of 6-40 uppercase and lowercase letters and numbers. The key must be kept strictly confidential and known only to the client and server. • uri resource access path starts with a forward slash (/). • timestamp: The value is the timestamp mentioned above.

- **Authentication logic description**
  After the CDN server receives the client request, it parses the timestamp parameter in the URL and compares the timestamp + authentication URL duration with the current time.
  - If timestamp + authentication URL duration is less than the current time, the server judges it as expired and invalid, and returns an HTTP 403 error.
  - If timestamp + authentication URL duration is greater than the current time, the MD5 algorithm is used to calculate the value of md5hash. Then, the calculated md5hash value is compared with the md5hash value passed in the URL. If they match, the request is allowed; if not, an HTTP 403 error is returned.

Configuration Guide

Taking the configuration of TypeC authentication as an example, the parameters and console configuration items are configured as follows:

- **Field configuration**
  - Authentication key: dimtm5evg50ijsx2hvuwyfoiu65
  - Validity period of the authentication URL: 1s



鉴权密钥（主） dimtm5evg50ijsx2hvuwyfoiu65

输入6-40位大小写字母、数字构成的密钥 随机生成

鉴权密钥（备）

输入6-40位大小写字母、数字构成的密钥 随机生成

有效时间 1 s

时间格式 十六进制（Unix 时间戳）

- Time when the signature server generates the authentication URL: February 27, 2020, 16:10:32 (UTC+8), converted to a hexadecimal integer value from the decimal Unix timestamp as 5e577978 (timestamp).
- Requested origin address: `http://cloud.tencent.com/test.jpg`

- Generation process
  - Get authentication parameters:

Parameter	Value.
uri	The resource access path is /test.jpg
timestamp	5e577978
pkey	dimtm5evg50ijsx2hvuwyfoiu65

  - Concatenate the signature string: dimtm5evg50ijsx2hvuwyfoiu65/test.jpg5e577978
  - Calculate the MD5 value of the signature string: md5hash = md5sum(pkeyuritimestamp)=md5sum(dimtm5evg50ijsx2hvuwyfoiu65/test.jpg5e577978)=7913fc0c5c9e92dd3633b7895152bbb2
- **Generate authentication URL:**
  `http://cloud.tencent.com/7913fc0c5c9e92dd3633b7895152bbb2/5e577978/test.jpg` When the client accesses via the encrypted URL, if the md5hash value calculated by the CDN server matches the md5hash value in the access request, both being 7913fc0c5c9e92dd3633b7895152bbb2, the authentication succeeds; otherwise, it fails.

Notes

Cache hit rate If you have enabled TypeC authentication for a domain, the signature and timestamp will be carried in the access URL path. When a CDN node caches the resource, it will automatically ignore the authentication path and thus not affect the cache hit rate.
Origin-pull policy The access format of a domain name with TypeC authentication mode enabled is as follows:
`http://DomainName/md5hash/timestamp/FileName`
After authentication is passed, if the CDN node is not hit, the node will initiate an origin pull request. **The origin pull request will remove the md5hash and timestamp from the path**, so the origin server does not need special handling.

TypeD

Last updated：2024-12-31 17:35:45

To protect your site resources from being downloaded or stolen by unauthorized users, you can choose an authentication method from Types A, B, C, and D as needed. This document describes parameter fields and their purposes in Type D authentication.

Algorithm Description

- **Access URL Format**
  `http://DomainName/FileName?sign=md5hash&t=timestamp`

> **Note**
> - The access URL cannot contain any Chinese characters. If the URL contains Chinese characters, please encode them in advance.
> - Does not support authentication for URLs with parameters containing ?.
> - Supports minimum time unit in seconds (s), maximum valid time can be entered is 630720000s.

- **Description of authentication fields**

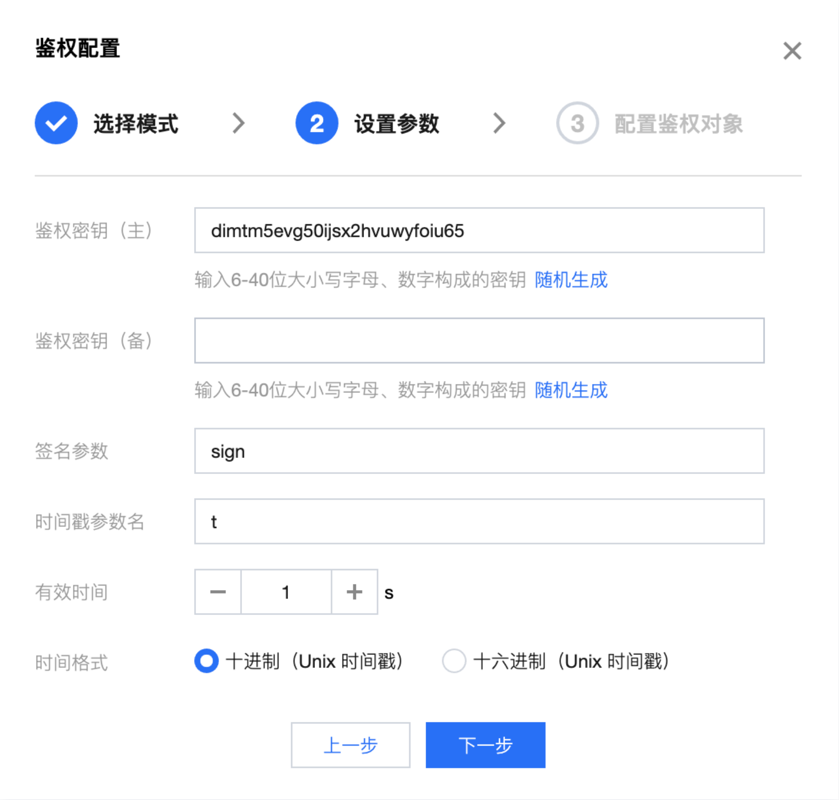
Field	Description
DomainName	CDN domain.
Filename	Resource access path. During authentication, `Filename` must start with a slash (/).
timestamp	The time when the server generates the authentication URL. It is a positive hex integer Unix timestamp, which is the total number of seconds between 00:00:00, January 1, 1970, UTC time and the URL generation time. Its definition is irrelevant to the time zone.
md5hash	A string containing 32 characters calculated based on the MD5 algorithm. It is calculated as follows: `md5hash = md5sum(pkeyuritimestamp)` . There are no symbols between the parameters. `pkey` : It can contain 6 to 40 letters and digits. It should be kept private and disclosed to only the client and server. `uri` : It is the resource access path and must start with a slash (/).

- **Authentication logic description**
  After the CDN server receives the client request, it parses the timestamp parameter in the URL and compares the timestamp + authentication URL duration with the current time.
  - If timestamp + authentication URL duration is less than the current time, the server judges it as expired and invalid, and returns an HTTP 403 error.
  - If timestamp + authentication URL duration is greater than the current time, the MD5 algorithm is used to calculate the value of md5hash. Then, the calculated md5hash value is compared with the md5hash value passed in the URL. If they match, the request is allowed; if not, an HTTP 403 error is returned.

Configuration Guide

Taking the configuration of Type-D authentication as an example, the parameters and console configuration items are configured as follows:

- **Field configuration**
  - Authentication key: dimtm5evg50ijsx2hvuwyfoiu65
  - Validity period of the authentication URL: 1s



鉴权配置

✓ 选择模式 > 2 设置参数 > 3 配置鉴权对象

鉴权密钥（主） dimtm5evg50ijsx2hvuwyfoiu65

输入6-40位大小写字母、数字构成的密钥 随机生成

鉴权密钥（备）

输入6-40位大小写字母、数字构成的密钥 随机生成

签名参数 sign

时间戳参数名 t

有效时间 − 1 + s

时间格式 ● 十进制（Unix 时间戳） ○ 十六进制（Unix 时间戳）

  - The time when the signature calculation server generated the authentication URL: February 27, 2020, 16:10:32 (UTC+8), converted to a decimal integer value is 1582791032 (timestamp)
  - Requested origin address: `http://cloud.tencent.com/test.jpg`
- **Generation process**
  - Get authentication parameters:

Parameter	Value.
uri	The resource access path is /test.jpg
timestamp	1582791032
pkey	dimtm5evg50ijsx2hvuwyfoiu65

  - Concatenate the signature string: dimtm5evg50ijsx2hvuwyfoiu65/test.jpg1582791032
  - Calculate the MD5 value of the signature string: md5hash = md5sum(pkeyuritimestamp) =md5sum(dimtm5evg50ijsx2hvuwyfoiu65/test.jpg1582791032) =900a5049aa8ac1ab144527d9c2be4cea
- **generate authentication url**
  `http://cloud.tencent.com/test.jpg?sign=900a5049aa8ac1ab144527d9c2be4cea&t=1582791032`
  When the client accesses through the encrypted URL, if the md5hash value calculated by the CDN server matches the md5hash value in the access request, both being 900a5049aa8ac1ab144527d9c2be4cea, the authentication is successful; otherwise, the authentication fails.

Notes

Cache hit rate

If you have enabled the TypeD authentication mode for a domain name, the access URL will carry the authentication parameter. When a CDN node caches the resource, it will automatically ignore the parameter and thus will not affect the cache hit rate.

> ⚠ **Note**
> Since the configuration will automatically ignore the parameter, it will ignore the configured authentication parameter and timestamp parameter, affecting the cache key of files within the authentication scope. This priority is higher than the **Cache Configuration – Cache Key Rule Configuration**.

> For example, if the TypeD configuration is: authentication parameter: sign – timestamp parameter: t – authentication scope: jpg, then jpg files will automatically ignore the "sign" and "t" parameters, even if **Cache Configuration – Cache Key Rule Configuration** is configured: all files – do not ignore parameters.

Origin-pull policy

The access format of a domain name with TypeD authentication mode enabled is as follows:

`http://DomainName/FileName?sign=md5hash&t=timestamp`

After authentication is passed, if the CDN node is not hit, the node will initiate an origin return request, **the format is consistent with the access request and will retain the sign/t parameters**. The origin server can ignore or re-verify them as needed.

UA Blocklist/Allowlist Configuration

Last updated：2024-12-31 17:35:58

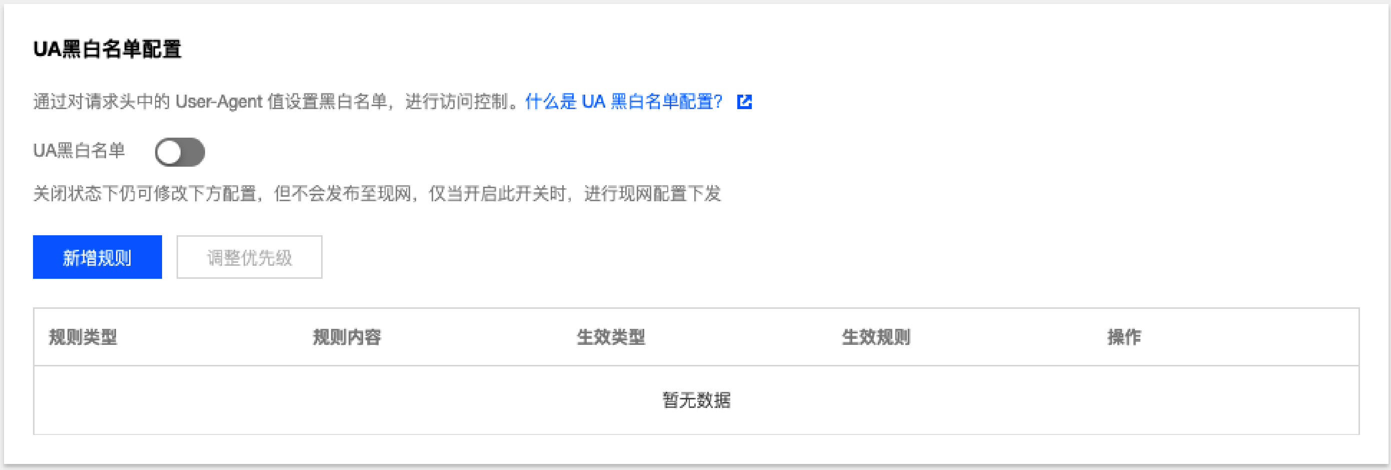
Configuration Scenario

Tencent Cloud CDN supports access control by configuring User-Agent blocklist and allowlist rules. By performing rule judgment on the User-Agent in the user HTTP request header, user access can be allowed or denied as needed.

Configuration Guide

Viewing Configuration

Log in to the CDN console, select **Domain Management** from the menu bar, and click **Management** on the right side of the domain to enter the domain configuration page. In the second column **Access Control**, you can see the UA blocklist and allowlist configuration, which is disabled by default:



UA黑白名单配置

通过对请求头中的 User-Agent 值设置黑白名单，进行访问控制。什么是 UA 黑白名单配置?

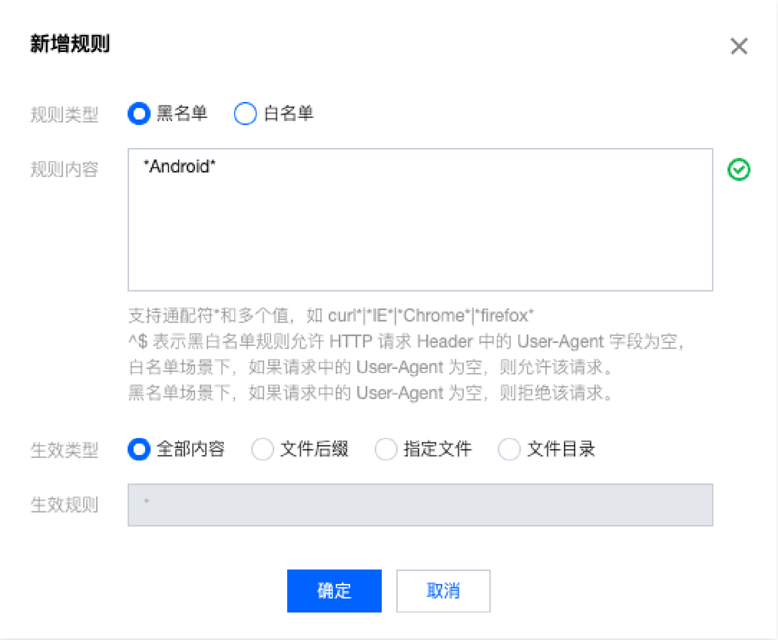
UA黑白名单 ○

关闭状态下仍可修改下方配置，但不会发布至现网，仅当开启此开关时，进行现网配置下发

规则类型	规则内容	生效类型	生效规则	操作
暂无数据				

Adding rules

Click **Adding rules** to add blocklist (allowlist) entries one by one as needed:



新增规则

规则类型 ● 黑名单 ○ 白名单

规则内容 *Android*

支持通配符*和多个值，如 curl*|*IE*|*Chrome*|*firefox*
^$ 表示黑白名单规则允许 HTTP 请求 Header 中的 User-Agent 字段为空，
白名单场景下，如果请求中的 User-Agent 为空，则允许该请求。
黑名单场景下，如果请求中的 User-Agent 为空，则拒绝该请求。

生效类型 ● 全部内容 ○ 文件后缀 ○ 指定文件 ○ 文件目录

生效规则 *

Configuration limitations

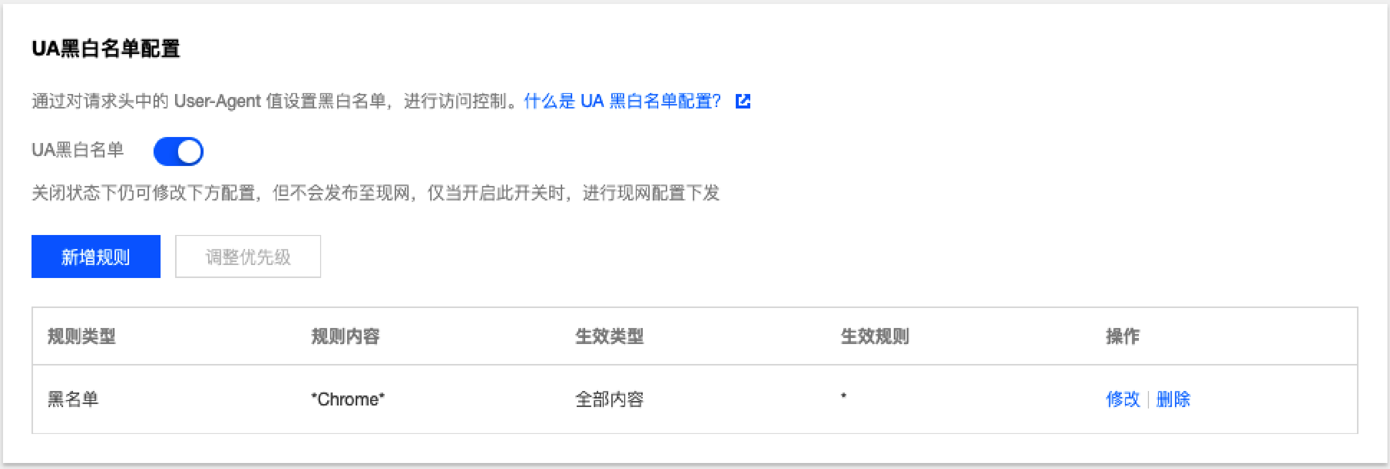
- Only support setting all to blocklist or all to allowlist, and do not support setting both blocklist and allowlist rules simultaneously.

- Up to 10 blocklist or allowlist rules can be configured.
- Rules support the wildcard `*`. Please separate multiple values with `|`.
- Supported effect types: all content, file extension, file directory, and specified file. Regular matching is currently not supported.

> ⚠ **Note**
>
> 1. Supports wildcard * and multiple values, such as curl*|*IE*|*Chrome*|*firefox*.
>   ^$ represents an empty User-Agent. If the rule content includes an empty User-Agent, handle it as follows:
>   In the allowlist scenario, if the User-Agent in the request is empty, the request is allowed.
>   In the blocklist scenario, if the User-Agent in the request is empty, the request is denied.
> 2. If there is no `*`, all characters will be used for exact match.

Configuration Example

If the UA allowlist/blocklist configuration of the acceleration domain name `cloud.tencent.com` is as follows:



UA黑白名单配置

通过对请求头中的 User-Agent 值设置黑白名单，进行访问控制。什么是 UA 黑白名单配置?

UA黑白名单

关闭状态下仍可修改下方配置，但不会发布至现网，仅当开启此开关时，进行现网配置下发

规则类型	规则内容	生效类型	生效规则	操作
黑名单	*Chrome*	全部内容	*	修改 | 删除

When the User-Agent in the HTTP Request Header is as follows:

```
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
```

The blocklist will be hit and a 403 error will be directly returned.

Downstream Speed Limit Configuration

Last updated：2024-12-31 17:36:09

Configuration Scenario

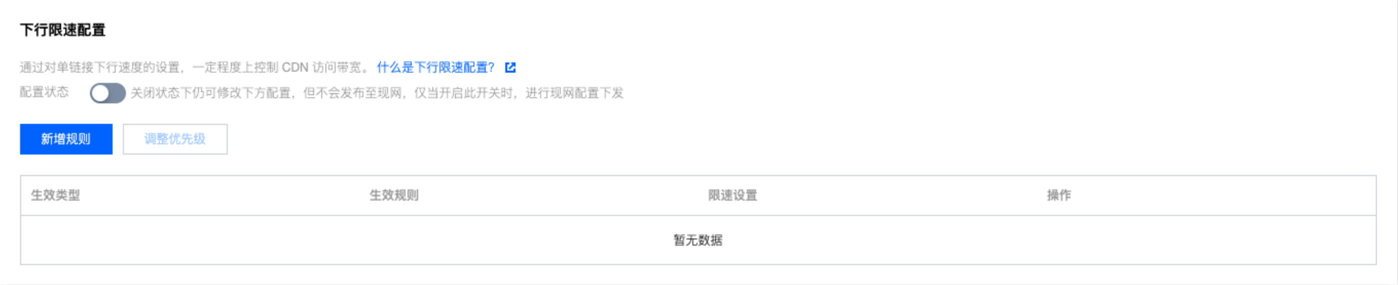
Tencent Cloud CDN supports downstream speed limit configuration for setting the maximum downstream throughput speed over one single URL on the node. The downstream speed limit configuration can control the peak bandwidth of CDN to a certain degree. It is frequently used in scenarios such as e-commerce promotions and new game version releases and updates.

> **Note**
> The downstream speed limit configuration takes effect globally for all users who access the domain name. After the downstream speed limit is configured, the user access experience and CDN acceleration effect may be affected. Therefore, configure the downstream speed limit with caution.

Configuration Guide

Viewing Configuration

Log in to the CDN console, select **Domain Management** from the menu bar, click **Management** on the right side of the domain to enter the domain configuration page. In the second column **Access Control**, you can see the downstream speed limit configuration, which is in closed status by default:



下行限速配置

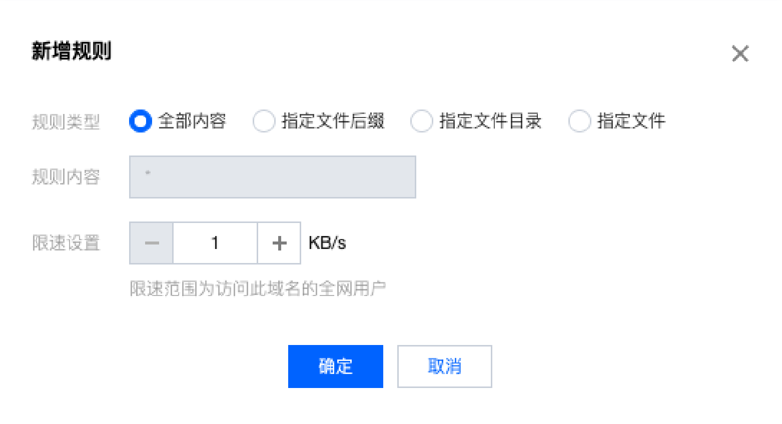
通过对单链接下行速度的设置，一定程度上控制 CDN 访问带宽。什么是下行限速配置?

配置状态 ○ 关闭状态下仍可修改下方配置，但不会发布至现网，仅当开启此开关时，进行现网配置下发

生效类型	生效规则	限速设置	操作
	暂无数据		

Adding rules

Click **Add Speed Limit Rule** to configure a rule:



新增规则

规则类型 ● 全部内容 ○ 指定文件后缀 ○ 指定文件目录 ○ 指定文件

规则内容 *

限速设置 1 KB/s

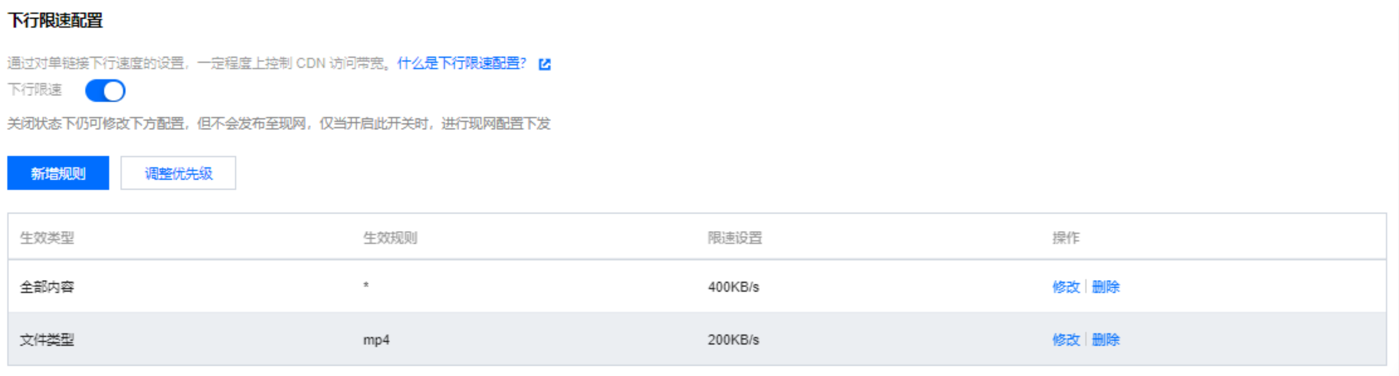
限速范围为访问此域名的全网用户

Configuration limitations

- Up to 10 downstream speed limit rules can be configured.
- The speed limit unit is KB/s, which needs to be filled with a positive integer. The value range is 1 - 1000000.
- Supported effect types: all content, file extension, file directory, and specified file. Regular matching is currently not supported.
- Rules are executed from bottom to top. Rules at the bottom have higher priority.

Configuration Example

If the downstream speed limit configuration of the acceleration domain name `cloud.tencent.com` is as follows:



下行限速配置

通过对单链接下行速度的设置，一定程度上控制 CDN 访问带宽。什么是下行限速配置？

下行限速 ●

关闭状态下仍可修改下方配置，但不会发布至现网，仅当开启此开关时，进行现网配置下发

生效类型	生效规则	限速设置	操作
全部内容	*	400KB/s	修改 | 删除
文件类型	mp4	200KB/s	修改 | 删除

If a user accesses the resource `http://cloud.tencent.com/test.mp4` , the server will return the content at the configured downstream speed of 200 KB/s.

If a user accesses the resource `http://cloud.tencent.com/test.flv` , the server will return the content at the configured downstream speed of 400 KB/s.

Remote Authentication

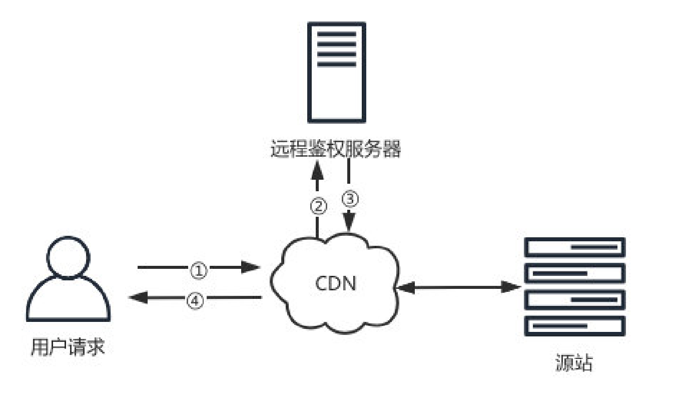
Last updated：2024-12-31 17:36:21

Remote Authentication

Remote authentication is only available to users who have used the remote authentication feature before November 8, 2023. If this feature is not visible in the console, you can access it via EdgeOne. For details, see Tencent Cloud EdgeOne > Edge Functions > Example Functions > Remote Authentication.

Configuration Scenario

To prevent customer resources from being accessed by unauthorized users, Tencent Cloud not only supports advanced timestamp authentication at the CDN edge but also supports forwarding requests to the customer-specified remote authentication server. The authentication server validates user requests, and the CDN decides whether to continue providing services based on the validation results returned by the remote authentication server.
The following describes how remote authentication works:



1. The end user initiates a request for resources.
2. CDN synchronously forwards the request to the remote authentication server, including the request header and authentication parameters.
3. The remote authentication server returns the authentication result.
4. The CDN node decides whether to continue responding to the user's request based on the authentication result.

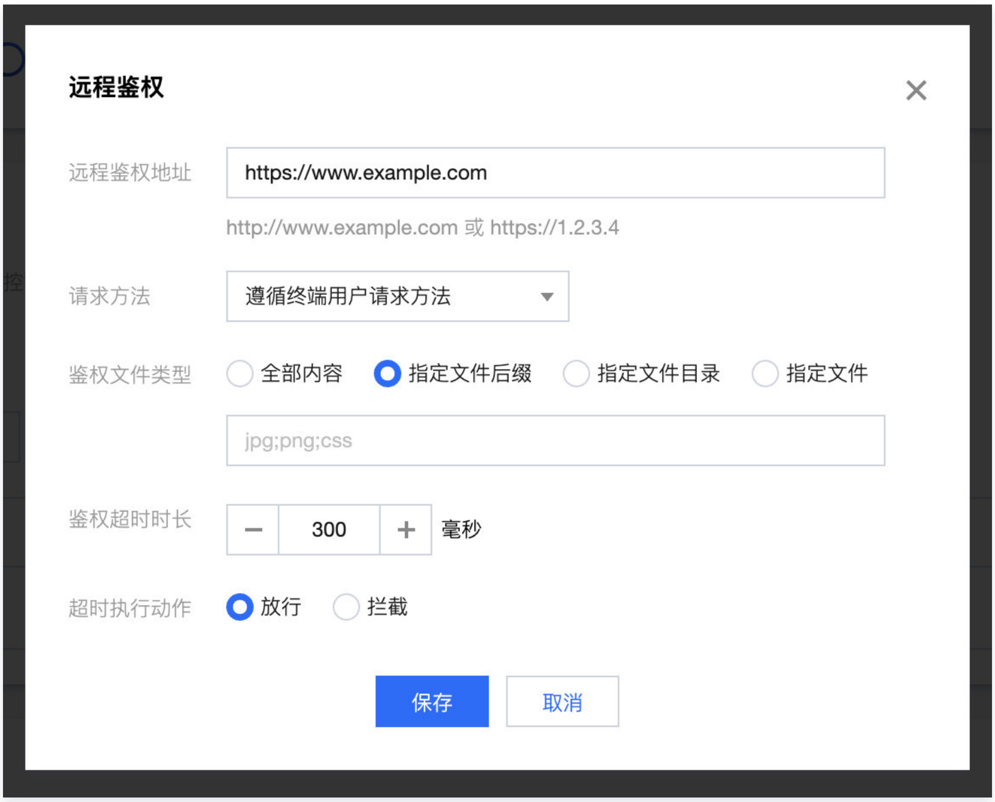
> **Note**
> - The CDN node determines whether the authentication is successful based on the status codes returned by the remote server. The status codes for successful authentication are `200` / `206` / `304` , while other status codes indicate authentication failure. If authentication is successful, the request is allowed (200 returned); if it fails, the request is blocked (403 returned).
> - For now, only synchronized remote authentication is supported, which means that CDN responds after receiving the authentication result from the remote authentication server.
> - Some overseas platforms do not support remote authentication configuration, and modifying the domain acceleration region may cause the remote authentication feature to fail.

Configuration Guide

Log in to the CDN console, select **Domain Management** from the menu bar, click **Manage** on the right side of the domain to enter the domain configuration page, and configure remote authentication in **Access Control**:

- Remote Authentication Address: supports HTTP/HTTPS protocols, and you can fill in the domain or IP address.
- Request Method: the method to initiate a request to the remote server, supports following the terminal user's request method or specifying GET/POST/HEAD request methods.
- Authentication file type: Set the scope of the authentication file, supporting remote authentication for **all content/specified file suffix/specified file directory/specified file.**

- Authentication timeout duration: Set the response timeout for the remote authentication server, with a maximum of 30,000 milliseconds.
- Timeout execution action: Set the action to be taken when remote authentication times out, the default action is to allow.



远程鉴权

远程鉴权地址 https://www.example.com

http://www.example.com 或 https://1.2.3.4

请求方法 遵循终端用户请求方法

鉴权文件类型 ○ 全部内容 ● 指定文件后缀 ○ 指定文件目录 ○ 指定文件

jpg;png;css

鉴权超时时长 300 毫秒

超时执行动作 ● 放行 ○ 拦截

Example

Assume the customer's acceleration domain name is `www.example.com` and its remote authentication is configured as follows:

- Remote authentication address: `www.remoteauth.com` .
- Request method: Follow the end-user request method.
- Authentication file type: All content.
- Authentication timeout duration: 1500 milliseconds.
- Timeout execution action: Intercept.

The example process of user request response at this time is as follows:

1. User initiates a GET request:
```
http://www.example.com/v001/test.txt?
token=Gf6Gq04ymjdSTXusvTmh8yalO82YsuKUQb63ToXOFc&e=1467565695283&sign=854124740723b575a7cfa4fc40f0be30
```
2. CDN receives the request and initiates a GET request to the remote authentication server:
```
http://www.remoteauth.com/v001/test.txt?
token=Gf6Gq04ymjdSTXusvTmh8yalO82YsuKUQb63ToXOFc&e=1467565695283&sign=854124740723b575a7cfa4fc40f0be30
```
3. The remote authentication server returns a status code.
4. CDN responds normally with 200 if the returned status code is 200 (i.e., the authentication passed).

Access Port Configuration

Last updated：2024-12-31 17:36:33

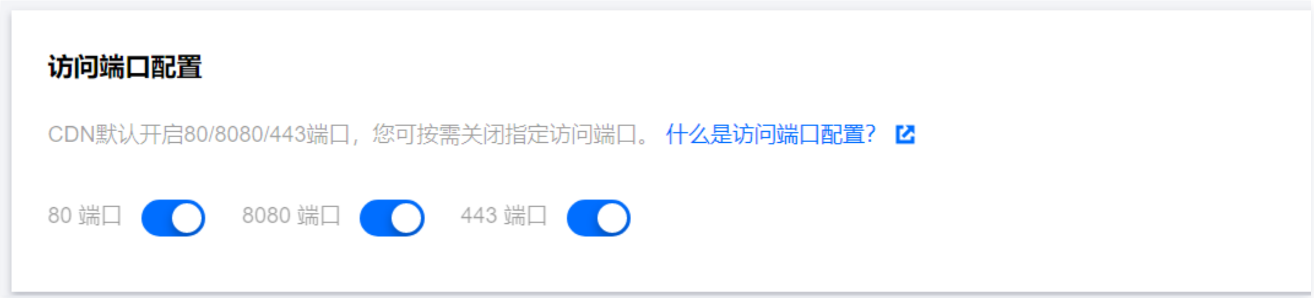
Configuration Scenario

By default, CDN enables access to ports 80, 8080, and 443. You can disable any of these ports as needed based on your business requirements.

Configuration Guide

Viewing Configuration

Log in to the CDN console, select **Domain Management** from the left sidebar menu, click **Management** in the domain operation column to enter the domain configuration page, switch the tab to **Access Control**, and you will find the **Access Port Configuration**. Port 80, 8080, and 443 are enabled by default:



访问端口配置

CDN默认开启80/8080/443端口，您可按需关闭指定访问端口。 什么是访问端口配置？

Modify

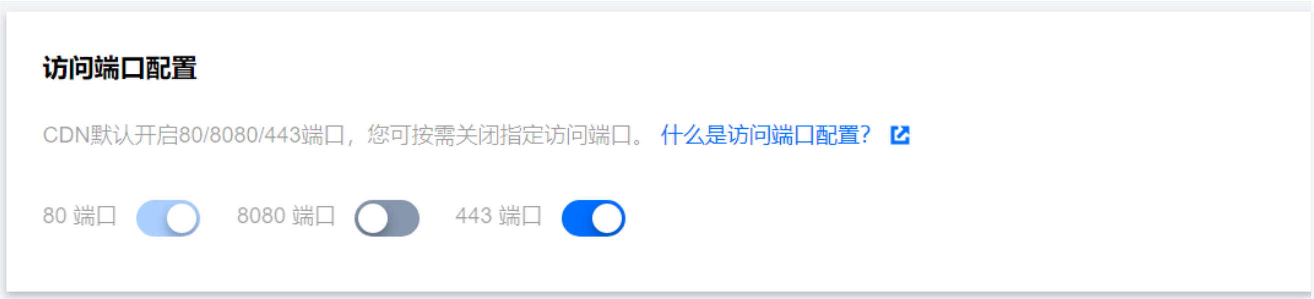
You can disable and enable the ports as needed.

Modify Constraints

- If HTTPS access or forced HTTPS redirection is enabled for a domain name, Port 443 cannot be disabled.
- Port 80 and Port 8080 cannot be closed simultaneously.

Configuration Example

If the access port configuration of the acceleration domain name `www.test.com` is as follows:



访问端口配置

CDN默认开启80/8080/443端口，您可按需关闭指定访问端口。 什么是访问端口配置？

The actual access situation is as follows:
CDN nodes will deny access to port 8080.

Cache configuration
Cache Key Rule Configuration

Last updated：2024-12-31 17:37:00

Configuration Scenario

Tencent Cloud CDN uses a Key-Value format for resource mapping during caching, where the Key is the cache key and the Value is the resource cached in the CDN. You can configure cache key rules to retain only parameters that affect the resource content as cache keys, converting a type of request for the same resource into a unified cache key and hitting the same cache to improve hit rate.

Ignore Parameter

If in your business scenario, the parameters after the question mark in the resource URL path affect the resource content, they need to be retained as cache keys; otherwise, if the parameters do not affect the resource content, they should not be used as cache keys.

Scenario of not ignoring parameters

- When a user accesses the resource through a URL, the access request may carry some parameters for special purposes. For example, the following URLs are used to represent two different images: `http://cloud.tencent.com/1.jpg?version=1` `http://cloud.tencent.com/1.jpg?version=2` In this scenario, you need to select "Do not ignore" and retain all parameters and values in the URL as cache keys to cache images and distinguish between resources.

Scenario of retaining specified parameters or ignoring specified parameters

- If the URL carries other parameters that do not affect the image content, such as the timestamp "time" to record the request time, in addition to the "version" parameter that affects the resource content: `http://cloud.tencent.com/1.jpg?version=1&time=1651752741` `http://cloud.tencent.com/1.jpg?version=1&time=1651752742` `http://cloud.tencent.com/1.jpg?version=2&time=1651752743` In this scenario, you can choose to "retain specified parameters" or "ignore specified parameters", specifying to retain the "version" parameter that affects the image content as the cache key, or specifying to ignore the "time" parameter that does not affect the image content. Both methods can achieve the following caching results:
- For requests with the same version value, ignore the time parameter and its value, sharing a cache.
- For requests with different version values, ignore the time parameter and its value, distinguishing caches.

Scenarios where all parameters are ignored

- If you use the timestamp signature parameter for access authentication in an audio/video scenario: `http://cloud.tencent.com/1.mp4?sign=XXXXXX` In this scenario, you need to choose "Ignore All", using the URL part before "?" `http://cloud.tencent.com/1.mp4` as the cache key. The node will then only cache one resource, and the cache can be directly hit through signature authentication even if the timestamp signature keeps changing.

Ignore case

If case differences in resource URL paths are irrelevant to resource content in your business scenario, you can enable the case ignoring configuration to improve the hit rate.

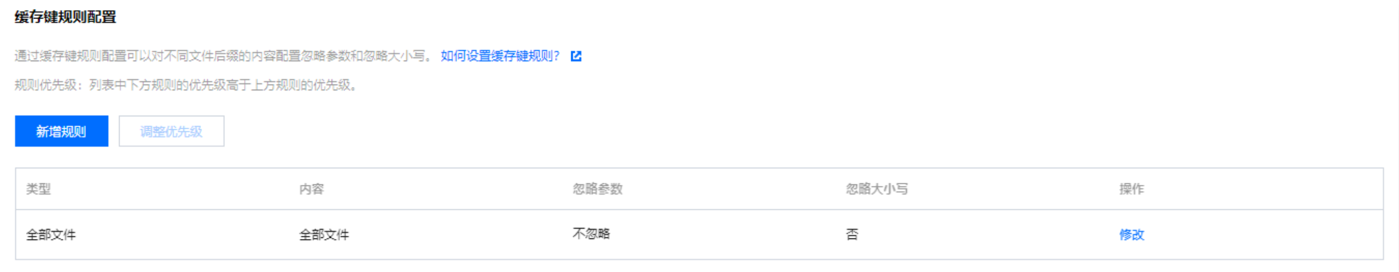
Configuration Guide

View Configuration

Log in to the CDN Console, select **Domain Management** from the left menu, click **Management** in the domain operation column to enter the domain configuration page, switch the tab to **Cache Configuration**, and you will find **Cache Key Rule Configuration**.
When adding an accelerated domain name, the ignore parameters default to off or on based on different business types:

- If the accelerated domain name selects small web file business type, the default does not enable ignore parameters. In the cache key rule configuration, the **ignore parameters** for all file rules are set to "do not ignore."

- If the accelerated domain name selects large file download or audio and video on-demand business type, the default enable ignore parameters. In the cache key rule configuration, the **ignore parameters** for all file rules are set to "ignore all."



缓存键规则配置

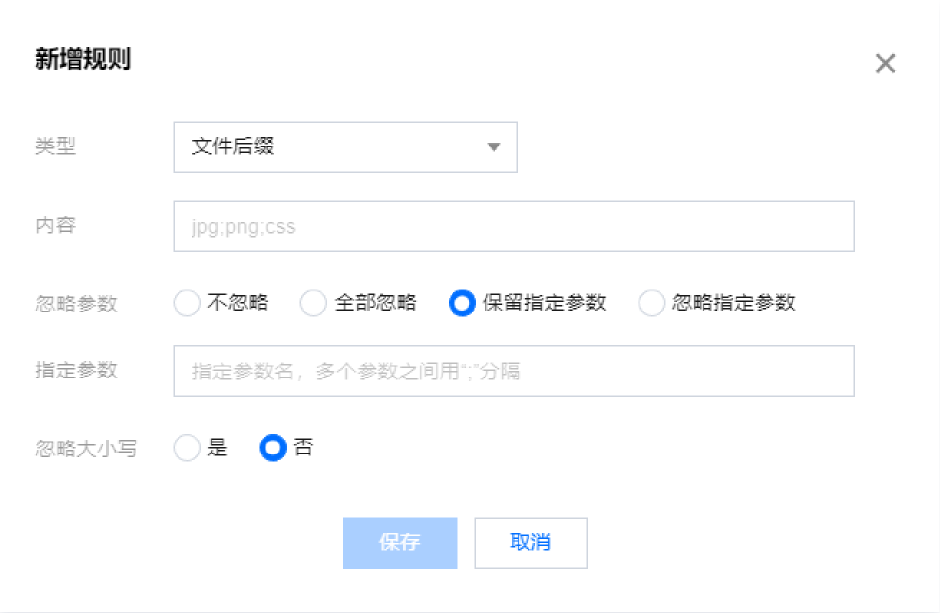
通过缓存键规则配置可以对不同文件后缀的内容配置忽略参数和忽略大小写。如何设置缓存键规则？

规则优先级：列表中下方规则的优先级高于上方规则的优先级。

类型	内容	忽略参数	忽略大小写	操作
全部文件	全部文件	不忽略	否	修改

Adding rules

You can add cache rules as needed.



新增规则

类型：文件后缀

内容：jpg;png;css

忽略参数：○ 不忽略 ○ 全部忽略 ● 保留指定参数 ○ 忽略指定参数

指定参数：指定参数名，多个参数之间用";"分隔

忽略大小写：○ 是 ● 否

Configuration limitations

- Each domain name can be configured with up to 20 cache key rules (including the default ones).
- Rule priority can be adjusted: rules at the bottom of the list have higher priority (the priority of default rules cannot be adjusted).
- In each rule of specified file type, folder, and full-path file, up to 100 groups of contents can be entered. Please use ";" to separate different contents, e.g., "Specified file type - jpg;png".
- Select **Retain Specified Parameters** and **Ignore Specified Parameters**. The constraints for specifying parameters are as follows:
  - All files: up to 30 parameter names can be entered; each one can contain up to 20 characters.
  - Specified file type/folder/full-path file: up to 30 parameter names can be entered; each one can contain up to 20 characters. Separate each parameter name with ";". For example: key1;key2;key3.

Modify Rule

You can modify the added cache key rules. Click **Modify** in the operation column of the cache key rule.

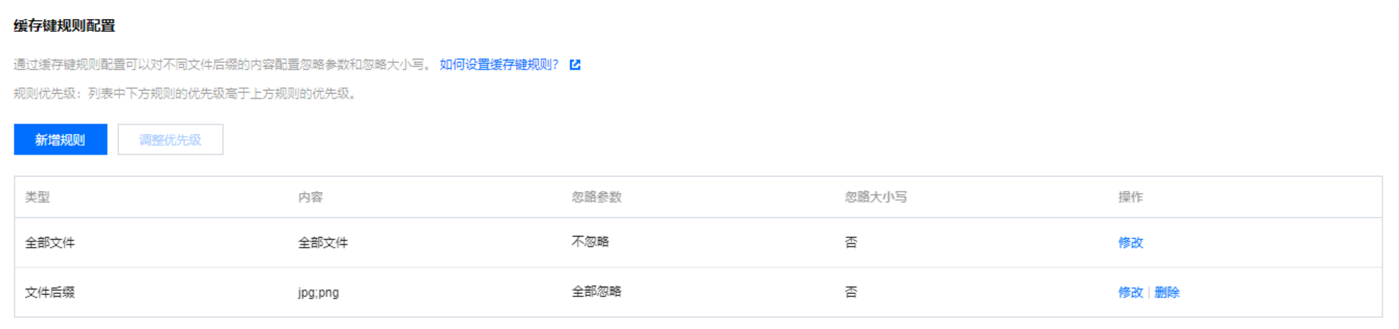
> **Note**
> The default rules support modifying ignore parameters and cache ignore URL case configurations, while the type and content cannot be modified.

Delete Rule

You can delete the added cache key rules. Click **Delete** in the operation column of the cache key rule. (Default rules cannot be deleted)

Configuration Example

If the cache key rule configuration of the acceleration domain name `www.test.com` is as follows:



缓存键规则配置

通过缓存键规则配置可以对不同文件后缀的内容配置忽略参数和忽略大小写。 如何设置缓存键规则？

规则优先级：列表中下方规则的优先级高于上方规则的优先级。

类型	内容	忽略参数	忽略大小写	操作
全部文件	全部文件	不忽略	否	修改
文件后缀	jpg;png	全部忽略	否	修改 | 删除

The actual access is as follows:
The client requests resources `www.test.com/abc.jpg?version=1&colour=red` and `www.test.com/abc.JPG?version=1&colour=red`.
Assuming both requests reach CDN node X, and node X does not have the cache of these two resources:

- The request goes back to the origin server to fetch the image resource `abc.jpg` and caches it on CDN node X. Since ignore parameters: ignore all is enabled, the link before "?" `www.test.com/abc.jpg` is used as the cache key.
- When the client requests `www.test.com/abc.JPG?version=1&colour=red`, because ignore case is not enabled, it cannot hit the previously cached resource `www.test.com/abc.jpg`. The request goes back to the origin server to fetch the image resource `abc.JPG` and caches it on CDN node X, with the corresponding cache key `www.test.com/abc.JPG?version=1&colour=red`.

<Node Cache Expiration Configuration>

Last updated：2024-12-31 17:37:15

The node cache configuration allows you to set the cache expiration time of origin server resources on CDN nodes, adjusting the cache update frequency. You can configure the cache expiration time of resources by directory, file suffix name, or full file path according to your business needs.

Feature Introduction

CDN determines whether the cached resources on CDN nodes have expired based on the cache expiration time set in the node cache configuration.

- If the resource accessed by the user is not expired in the CDN node cache, the CDN node returns the cached resource directly to the user.
- If the resource accessed by the user is not cached or the cache has expired, the CDN node will pull the latest resource from the origin server, cache it on the CDN node, and return it to the user.

After a resource on the origin server is updated, its cache on the CDN node must be updated immediately. You can use the Purge Cache feature to update unexpired caches on the CDN node, ensuring consistency between the resources cached on the CDN node and those stored on the origin server.

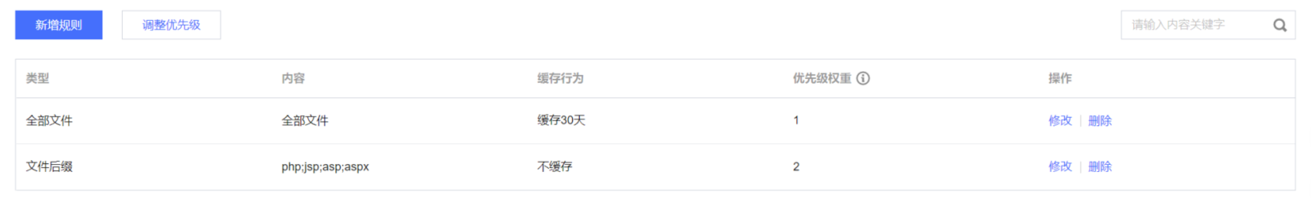
Notes

- The cache validity period will affect the back-to-origin frequency. It is recommended to set the resource cache duration based on actual business needs. If the cache validity period is too short, CDN will frequently pull the content from the origin server, increasing the origin server's bandwidth. If it is too long, the cache will be updated slowly, affecting users' access to the latest resources.
- CDN nodes cache resources according to Tencent Cloud CDN Caching Rules and Priorities. However, the cached resources on CDN nodes may be deleted before the cache validity period expires due to request frequency too low.
- It is recommended to use different names for resources before and after updating the origin server, such as naming resources with version numbers (img-v1.jpg, img-v2.jpg) to avoid CDN nodes returning old resources to users due to unexpired cache after the origin server updates the resource content.
- If you are still using the old version (basic mode) of the node cache validity configuration, it is recommended to upgrade to the latest version by configuring and submitting in advanced mode to support more features. Note that once upgraded to advanced mode, it cannot be reverted to the original basic mode. View the old version of the node cache validity configuration document: Node Cache Validity Configuration (Old).
- The origin server can control the cache validity period of CDN nodes by setting the response header Cache-Control (cache option: follow origin server). At the same time, CDN nodes will pass the Cache-Control response header to users to control the browser's cache time. If you need CDN nodes to set the browser's cache time, you can modify the Cache-Control header returned to users by CDN nodes through Browser Cache Validity Configuration.

Configuration Instructions

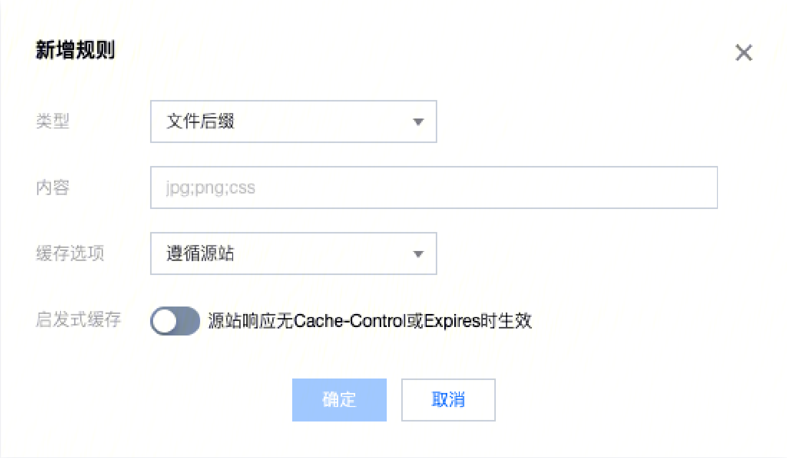
Directions

1. Log in to the CDN Console.
2. Click **Domain Management** in the left menu to enter the domain management list;
3. Select the domain to configure and click **Management** to enter the domain configuration page;
4. Click **Cache Configuration**, switch to the cache configuration tab, where you can view the **Node Cache Configuration**.;



类型	内容	缓存行为	优先级权重 ⓘ	操作
全部文件	全部文件	缓存30天	1	修改 | 删除
文件后缀	php;jsp;asp;aspx	不缓存	2	修改 | 删除

5. Click **Adding rules** to enter the new rule page and add node cache configuration.



新增规则

类型 文件后缀

内容 jpg;png;css

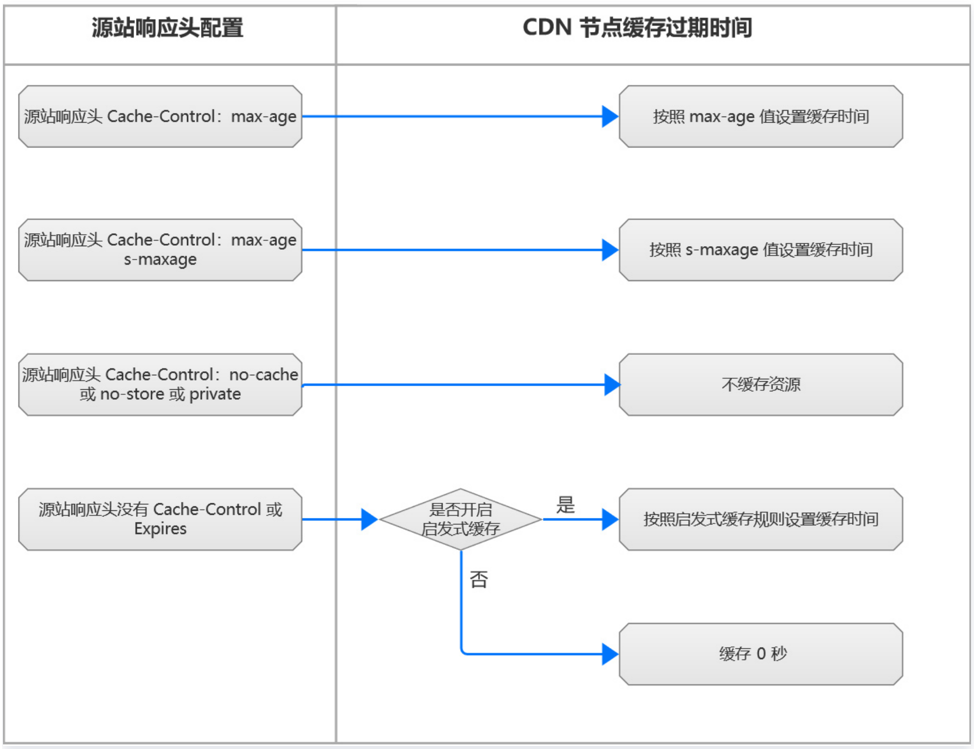
缓存选项 遵循源站

启发式缓存 源站响应无Cache-Control或Expires时生效

Configuration Item	Description
Type	Supports configuration for all files, file suffix, file directory, full path file, and homepage: All files: Set rules for all files, default rule. File suffix: Set rules for file suffix. File directory: Set rules for file directory. Full path file: Set rules for full file path. Homepage: Set rules for domain root directory.
Content	Based on the selected file type, content input constraints: When the type is all files: Fixed as all files. When the type is file suffix: Supports input of file suffix name, separated by ";". For example, jpg;png;css. When the type is file directory: Supports input of file directory, not ending with "/", separated by ";". For example, /test;/a/b/c. When the type is full path file: Supports input of full file path, separated by ";". For example, /index.html;/test/.jpg. Note: Content is case-sensitive, please enter the correct case.
Cache options	Supports configuration according to follow origin server, cache, and no cache rules: Follow origin server: Set CDN node cache time according to the origin server response header Cache-Control, supports setting heuristic cache. Cache: Custom set CDN node cache time, supports setting forced cache. No cache: Set CDN node to not cache resources.

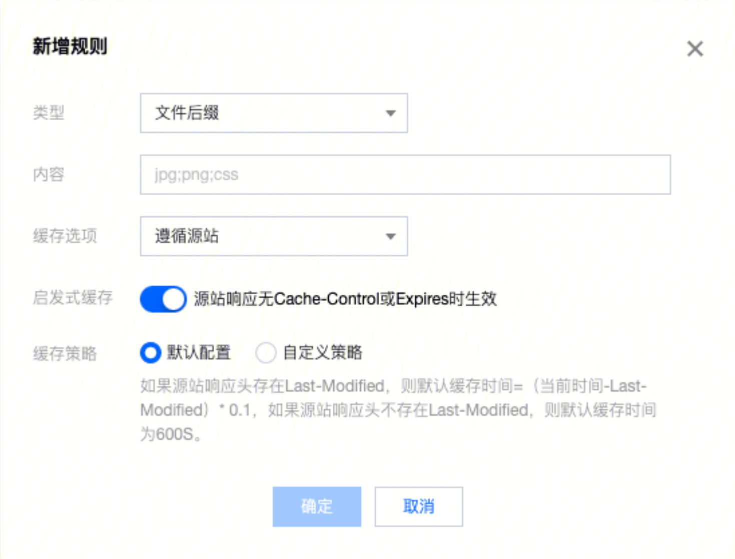
Tencent Cloud CDN Cache Rules and Priorities

Cache option is: follow origin server


源站响应头配置
CDN 节点缓存过期时间
源站响应头 Cache-Control：max-age
按照 max-age 值设置缓存时间
源站响应头 Cache-Control：max-age s-maxage
按照 s-maxage 值设置缓存时间
源站响应头 Cache-Control：no-cache 或 no-store 或 private
不缓存资源
源站响应头没有 Cache-Control 或 Expires
是否开启启发式缓存
是
按照启发式缓存规则设置缓存时间
否
缓存 0 秒

CDN nodes will follow the origin server response header Cache-Control to set cache time

- The origin server response header Cache-Control field is max-age, set CDN node cache time according to the max-age value, such as Cache-Control: max-age=300, then the cache time is 300 seconds;
- The origin server response header Cache-Control field has both max-age and s-maxage, set CDN node cache time according to the s-maxage value, such as Cache-Control: max-age=300 s-maxage=600, then the cache time is 600 seconds;
- The origin server response header Cache-Control field is no-cache or no-store or private, CDN nodes do not cache resources;
- When the origin server's response header lacks Cache-Control or Expires, cache rules are set according to heuristic caching, as follows:
  - Disable heuristic caching: when the origin server's response header lacks Cache-Control or Expires, the cache duration is 0 seconds.
  - Enable heuristic caching: when the origin server's response header lacks Cache-Control or Expires, heuristic cache duration is set according to the following rules:
    i. Automatically configured: If the origin server's response header includes Last-Modified, then cache duration = (current time - Last-Modified) * 0.1. If Last-Modified is absent, the default cache duration is 600 seconds.



新增规则

类型：文件后缀

内容：jpg;png;css

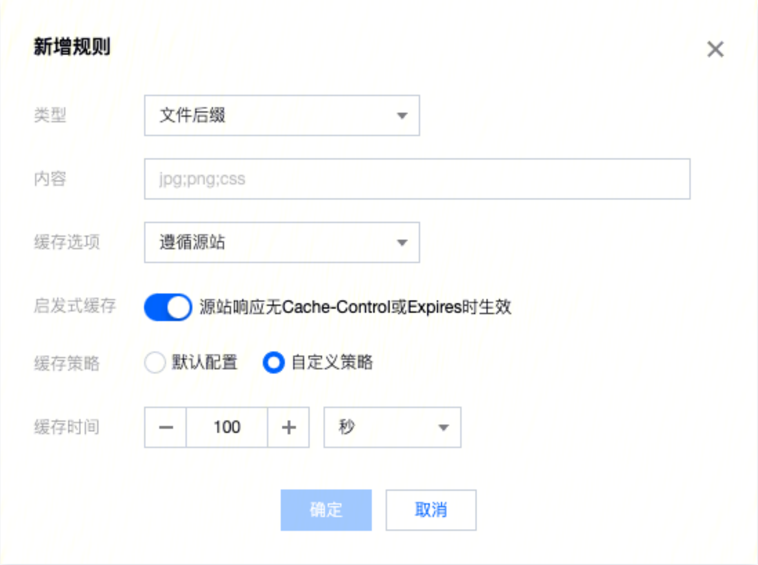
缓存选项：遵循源站

启发式缓存：源站响应无Cache-Control或Expires时生效

缓存策略：● 默认配置 ○ 自定义策略

如果源站响应头存在Last-Modified，则默认缓存时间=（当前时间-Last-Modified）* 0.1，如果源站响应头不存在Last-Modified，则默认缓存时间为600S。

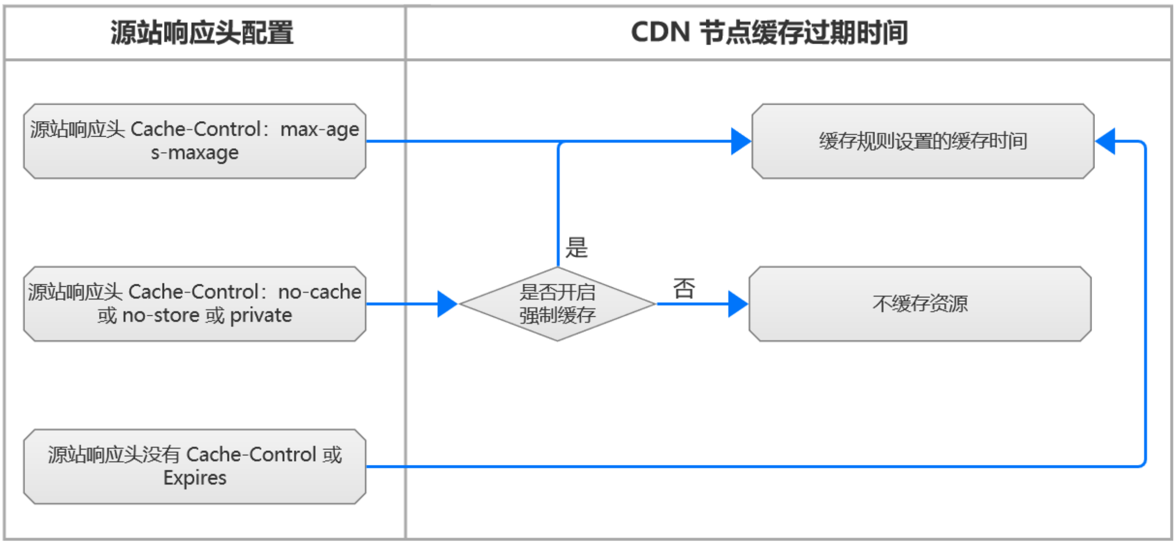
ii. Custom policy: Allows for custom setting of heuristic cache duration.



新增规则

类型	文件后缀
内容	jpg;png;css
缓存选项	遵循源站
启发式缓存	● 源站响应无Cache-Control或Expires时生效
缓存策略	○ 默认配置 ● 自定义策略
缓存时间	− 100 + 秒

Caching options: Caching

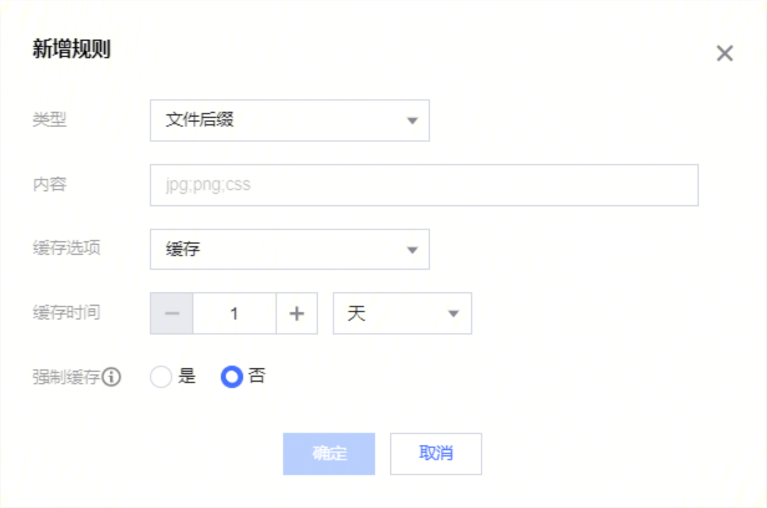


源站响应头配置
CDN 节点缓存过期时间
源站响应头 Cache-Control：max-age s-maxage
源站响应头 Cache-Control：no-cache 或 no-store 或 private
源站响应头没有 Cache-Control 或 Expires
是否开启强制缓存
是
否
缓存规则设置的缓存时间
不缓存资源

Customize the cache time of CDN nodes.

- Disable forced caching:
  - If the origin server's response header Cache-Control field is max-age or both max-age and s-maxage are present, cache according to the custom CDN node caching rules.
  - If the origin server's response header lacks Cache-Control or Expires, cache according to the custom CDN node caching rules.

- If the origin server's response header Cache-Control field is no-cache, no-store, or private, CDN nodes do not cache the resource.



类型 文件后缀

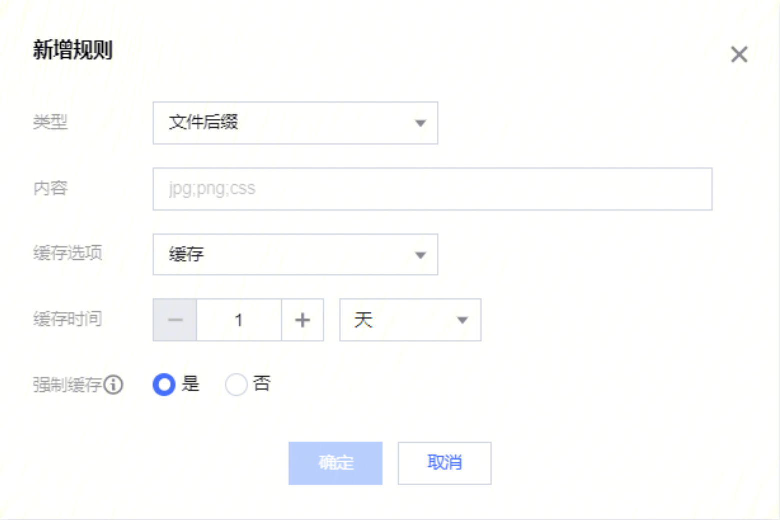
内容 jpg;png;css

缓存选项 缓存

缓存时间 − 1 + 天

强制缓存ⓘ ○ 是 ● 否

- Enable forced caching: Ignore the origin server's response header Cache-Control and cache according to the custom CDN node caching rules.



类型 文件后缀

内容 jpg;png;css

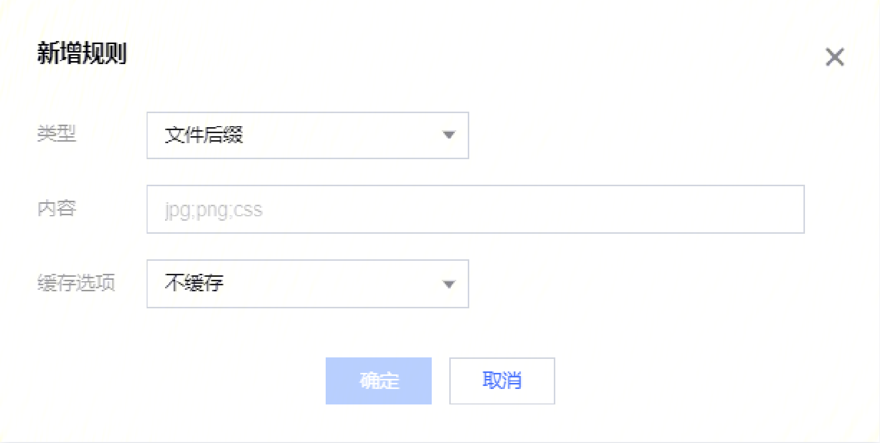
缓存选项 缓存

缓存时间 − 1 + 天

强制缓存ⓘ ● 是 ○ 否

The cache option is: Do not cache

Set CDN nodes to not cache resources. For each user request for this resource, CDN nodes will directly retrieve the resource from the origin server and respond to the user.



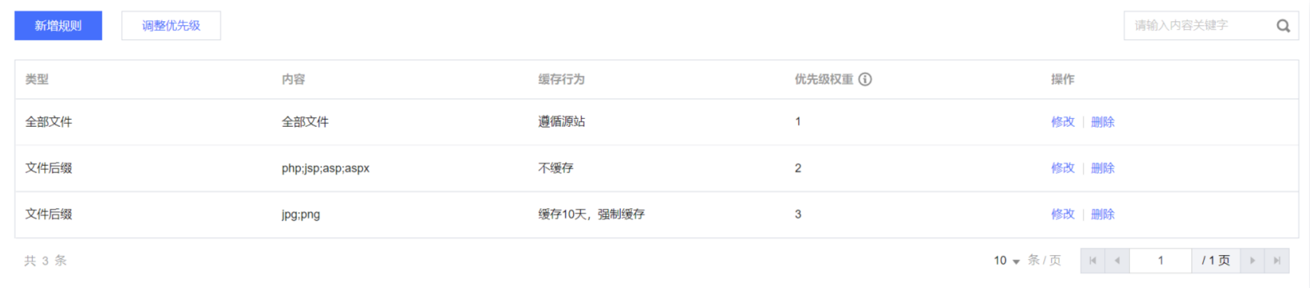
类型 文件后缀

内容 jpg;png;css

缓存选项 不缓存

Priority of multiple cache rules

When configuring multiple cache rules simultaneously, the larger the priority weight number, the higher the priority (the bottom rule has **higher priority than** the top rule). You can adjust the priority by clicking **adjust priority** and dragging the order of cache rules.



类型	内容	缓存行为	优先级权重 ⓘ	操作
全部文件	全部文件	遵循源站	1	修改 | 删除
文件后缀	php;jsp;asp;aspx	不缓存	2	修改 | 删除
文件后缀	jpg;png	缓存10天，强制缓存	3	修改 | 删除

Recommended Configuration

- Infrequently updated static files (e.g., image types, application download types, etc.) are recommended to be set to 30 days.
- Frequently updated static files (e.g., js, css) should have their cache time set according to the business update frequency.
- Dynamic files (e.g., php, jsp, asp, aspx) **should be set to do not cache**.
- Other requests involving **site log-in** (e.g., WordPress backend log-in directory /wp-admin) or **API queries** that need to interact directly with the origin server **should be set to do not cache**, otherwise, it may cause access errors.

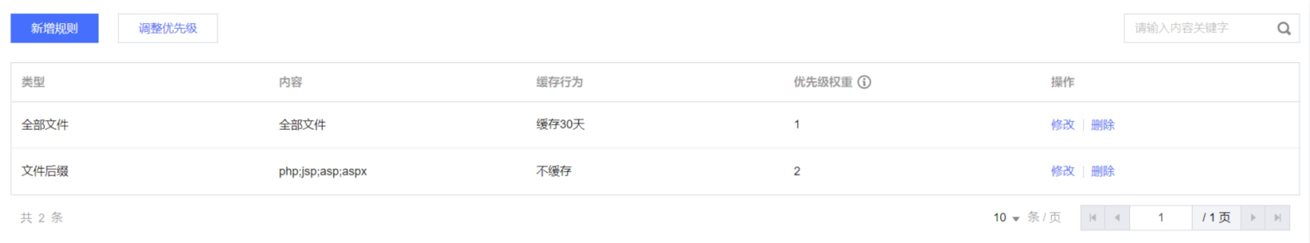
Configuration limitations

- A maximum of 100 caching rules can be added for a single domain name.
- Priority of multiple caching rules: rules at the bottom have higher priority than those at the top.
- In a single file suffix/file directory/full path file rule, up to 100 entries can be input, separated by ";". For example: file suffix jpg;png.
- If you have not configured any rules or the request does not match the configured rules, the CDN node will follow the Cache-Control header settings from the origin server to determine the cache time. If the origin server response header does not have a Cache-Control field, the CDN node will cache the resource for 600 seconds by default.
- CDN nodes only cache the content of GET and HEAD request types. For other request types such as POST and OPTIONS, CDN nodes do not cache the content.

Configuration Example

Sample 1

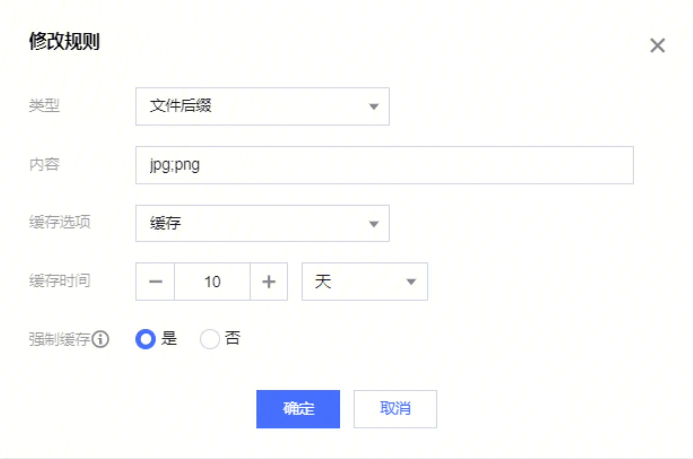
The original cache rule was: resources with php, jsp, asp, and aspx file extensions are not cached, while all other files are cached for 30 days.



类型	内容	缓存行为	优先级权重 ⓘ	操作
全部文件	全部文件	缓存30天	1	修改 | 删除
文件后缀	php;jsp;asp;aspx	不缓存	2	修改 | 删除

Now, it is required to add: resources with jpg and png file extensions are cached for 10 days, and the origin server response header Cache-Control is ignored, i.e., forced caching is enabled. The cache rule for all other files is modified to follow the origin server.

1. Click **Add Rule**, set the type to file suffix, the content to jpg;png, the cache option to cache, the cache time to 10 days, and enable forced caching. Click **Yes**.



修改规则

类型：文件后缀

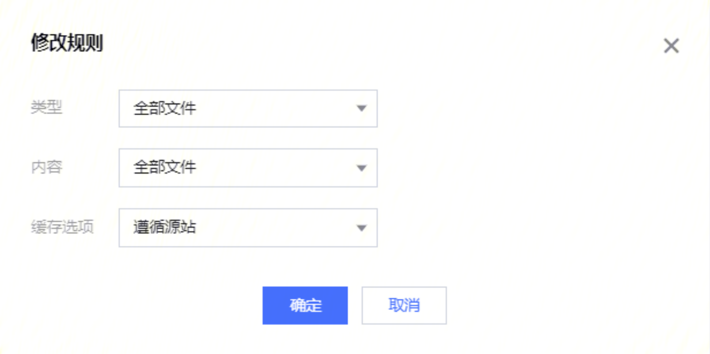
内容：jpg;png

缓存选项：缓存

缓存时间：10 天

强制缓存：● 是 ○ 否

2. Select the cache rule for all files, click **Modify**, change the cache option to follow the origin server, and click **Yes**.



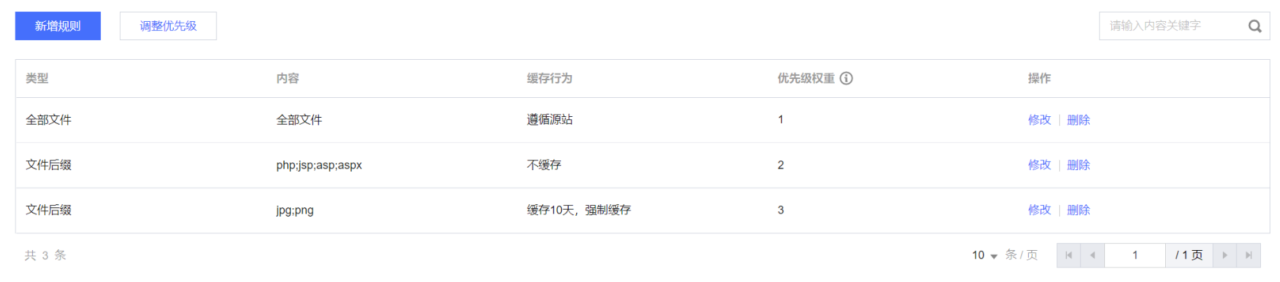
修改规则

类型：全部文件

内容：全部文件

缓存选项：遵循源站

3. The cache rules after the adjustment are:
   - Resources with jpg,png file extensions are cached for 10 days with forced caching;
   - Resources with php;jsp;asp;aspx file extensions are not cached;
   - All other files follow the origin server for caching.



类型	内容	缓存行为	优先级权重	操作
全部文件	全部文件	遵循源站	1	修改 | 删除
文件后缀	php;jsp;asp;aspx	不缓存	2	修改 | 删除
文件后缀	jpg;png	缓存10天，强制缓存	3	修改 | 删除

The actual caching situation is as follows:
   - `www.test.com/abc.jpg` The resource node cache time is 10 days, even if the origin server response header Cache-Control field is no-cache, no-store, or private.
   - `www.test.com/def.php` The resource will not be cached to the node;

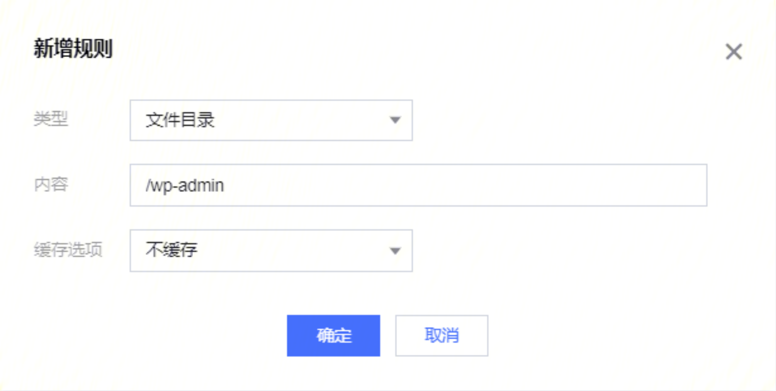
Sample 2

Recommended node cache validity configuration for WordPress sites:

- Resources under the backend login address /wp-admin directory need to be set to no-cache, otherwise, backend login-related resources will be cached, causing login errors. If there are other API-related resources, they also need to be set to no-cache.
- Resources with dynamic file extensions such as php, jsp, asp, and aspx need to be set to no-cache (default CDN caching rules).
- html;js;css file extensions are updated frequently, and the cache time should be set according to the update frequency. It is recommended to set the cache time to 7 days without setting forced cache;
- 30 days for all other files (CDN default cache rule).

Based on the default CDN cache rules, add new rules as follows:

1. Click **add new rule**, type is directory, content is /wp–admin, cache option is no–cache, click **Yes**.



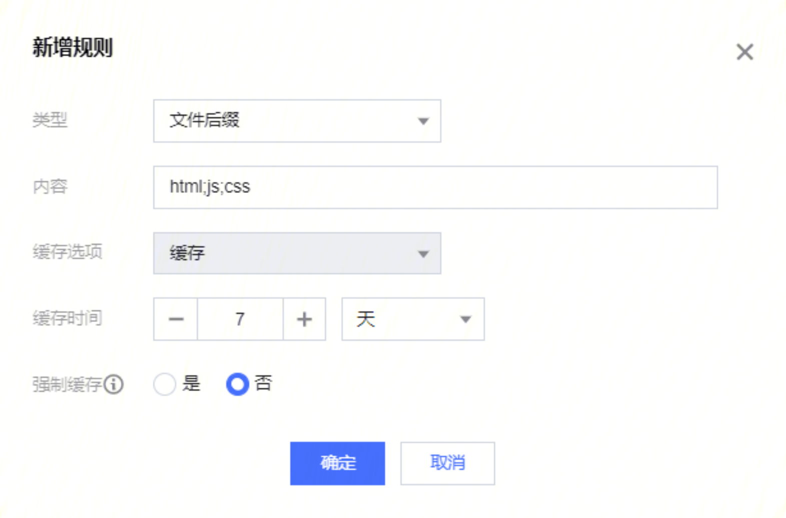
新增规则

类型: 文件目录

内容: /wp-admin

缓存选项: 不缓存

2. Click **add new rule**, type is file extension, content is html;js;css, cache option is cache, cache time is 7 days, forced cache is no, click **Yes**.



新增规则

类型: 文件后缀

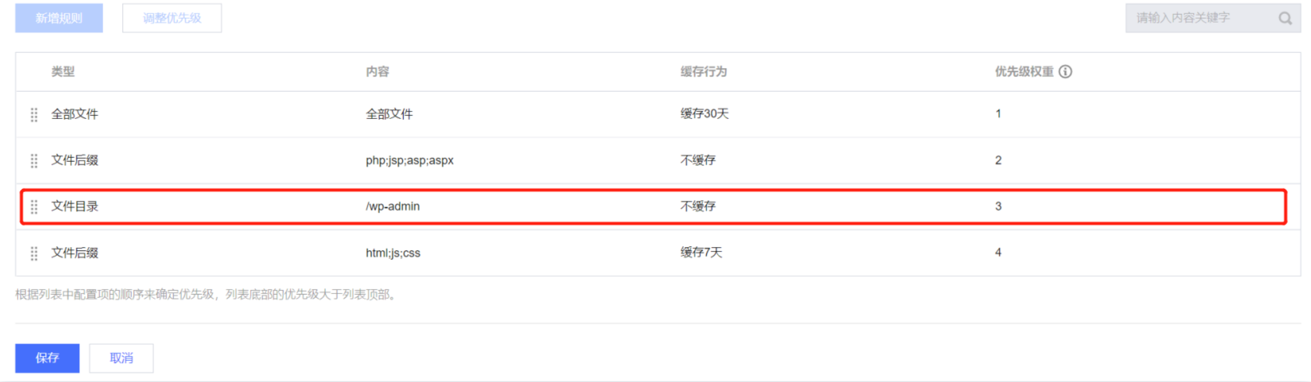
内容: html;js;css

缓存选项: 缓存

缓存时间: 7 天

强制缓存: ○ 是 ● 否

3. According to the priority order, bottom priority higher than top, click **adjust priority**, drag the "/wp–admin directory no–cache rule" to the bottom to make this rule the highest priority.

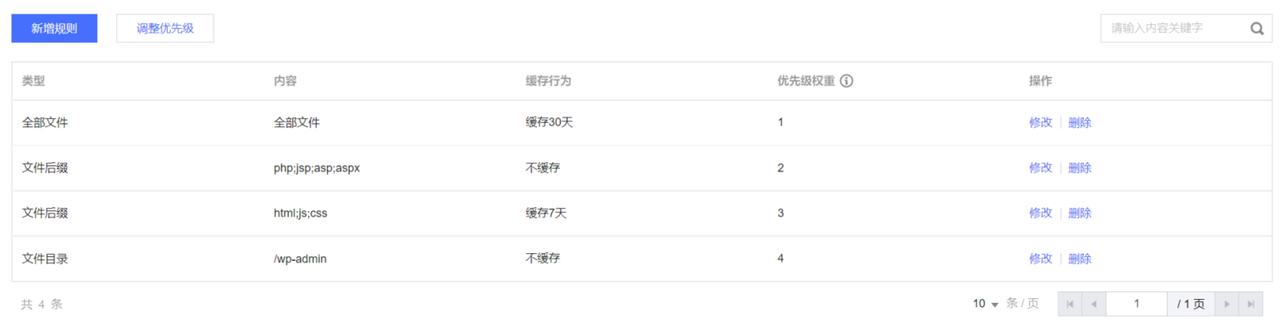


类型	内容	缓存行为	优先级权重
全部文件	全部文件	缓存30天	1
文件后缀	php;jsp;asp;aspx	不缓存	2
文件目录	/wp-admin	不缓存	3
文件后缀	html;js;css	缓存7天	4

根据列表中配置项的顺序来确定优先级，列表底部的优先级大于列表顶部。

4. The adjusted cache rules are:
   - All resources under the /wp–admin directory are not cached;
   - Resources with html;js;css file extensions are cached for 7 days;
   - Resources with php;jsp;asp;aspx file extensions are not cached;

- ○ 30 days for all other files.



类型	内容	缓存行为	优先级权重 ⓘ	操作
全部文件	全部文件	缓存30天	1	修改 | 删除
文件后缀	php;jsp;asp;aspx	不缓存	2	修改 | 删除
文件后缀	html;js;css	缓存7天	3	修改 | 删除
文件目录	/wp-admin	不缓存	4	修改 | 删除

FAQs

- If the file changes on the origin server, will the cache on CDN acceleration nodes be proactively and in real time updated?
- How do I tell whether user access has hit the CDN node cache?

Node Cache Validity Configuration (Old)

Last updated：2024-12-31 17:37:26

The node cache validity configuration is updated with an advanced mode, supporting more refined configurations. For more information, see Node Cache Validity Configuration (New).

Configuration Scenario

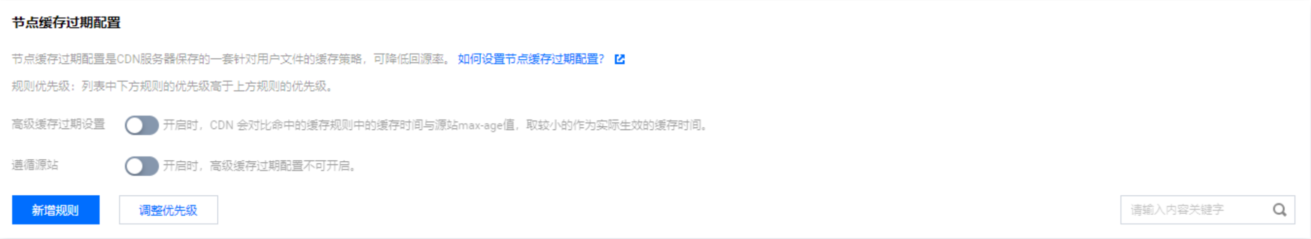
The resource cache in Tencent Cloud CDN is triggered by requests. If the CDN node receiving the user request has not cached the requested resource, it will forward the request to the origin server to pull the resource. After the resource is successfully pulled by the node (with a 2XX status code returned), it will be cached on the node and returned to the user.
You cannot directly manage resources cached on CDN nodes. If you are worried that resources on the origin server change but CDN nodes still cache the legacy resources and return them to users, you can configure node cache rules.
Each resource cached on a CDN node has an "expiration time". If the cached resource is expired, it will be considered invalid and fetched from the origin again, even if the node still has the cache. Node cache rule configuration supports specifying the cache validity time for certain types, directories, and resources of the path on nodes, which can be configured according to actual business scenarios.

> ⚠ **Note**
> Currently, a file up to 32 GB can be cached, otherwise, the resources will be pulled from the origin server.

Configuration Guide

View Configuration

Log in to the CDN console, select **Domain Management** on the left sidebar, click **Management** in the domain operation column, enter the domain configuration page, switch the tab to **Cache Configuration**, and you will find the **Node Cache Configuration**.



节点缓存过期配置

节点缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 如何设置节点缓存过期配置?

规则优先级：列表中下方规则的优先级高于上方规则的优先级。

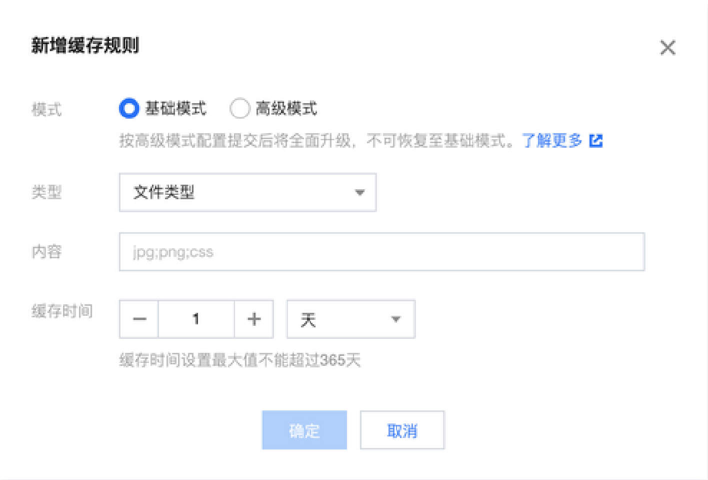
高级缓存过期设置 ○ 开启时，CDN 会对比命中的缓存规则中的缓存时间与源站max-age值，取较小的作为实际生效的缓存时间。

遵循源站 ○ 开启时，高级缓存过期配置不可开启。

Adding rules

CDN currently supports configuring node cache validity rules in the following four types:

- File: the cache validity period can be configured by the entered file extension. Different file extensions should be separated with `;` , i.e., `jpg;css` .
- Folder: the cache validity period can be configured by the entered directory path in the format of `/test` and does not need to end with `/` . Different directories should be separated with `;` .
- Full-path file: the cache validity period can be configured by the entered full file path in the format of `/index.html` . The full file path and file type can be combined for matching, such as `/test/*.jpg` .
- Homepage: the cache validity period can be configured by the root directory.
- Content is case-sensitive, please enter the correct case.



新增缓存规则

模式 ● 基础模式 ○ 高级模式

按高级模式配置提交后将全面升级，不可恢复至基础模式。了解更多

类型 文件类型

内容 jpg;png;css

缓存时间 – 1 + 天

缓存时间设置最大值不能超过365天

Configuration limitations:

- A maximum of 100 caching rules can be added for a single domain name.
- You can adjust the priority for multiple rules. Rules at the bottom of the list have higher priority.
- In each rule of specified file type, folder, and full-path file, up to 100 groups of contents can be entered. Please use ";" to separate different contents, e.g., "Specified file type - jpg;png".
- The cache validity can be set as up to 365 days.

> **Note**
> If "Advanced Mode" is selected in the **Mode** option and rules are submitted, it will be comprehensively upgraded to Advanced Mode. For details, see Node Cache Configuration (New). After the upgrade, it cannot be reverted to the original Basic Mode.

Advanced cache expiration setting switch

When enabled, CDN will compare the cache time in the hit cache rule with the max-age value of the origin server and take the smaller one as the effective cache time:

- The Max-Age of `/index.html` configured by the user's origin server is 200 seconds, and the corresponding cache time configured by CDN is 600 seconds. Therefore, the actual cache time of the file on the node is 200 seconds.
- The Max-Age of `/index.html` configured by the user's origin server is 800 seconds, and the corresponding cache time configured by CDN is 600 seconds. Therefore, the actual cache time of the file on the node is 600 seconds.

> **Note**
> When enabled, if the origin server does not return the Last-Modified field, CDN will add the Last-Modified field by default, changing it every 10 minutes.

Following the origin server switch

After it is enabled, if a request does not match any cache rules, the origin server will be followed.

> **Note**
> The follow origin server switch and the advanced cache validity configuration switch cannot be enabled at the same time.

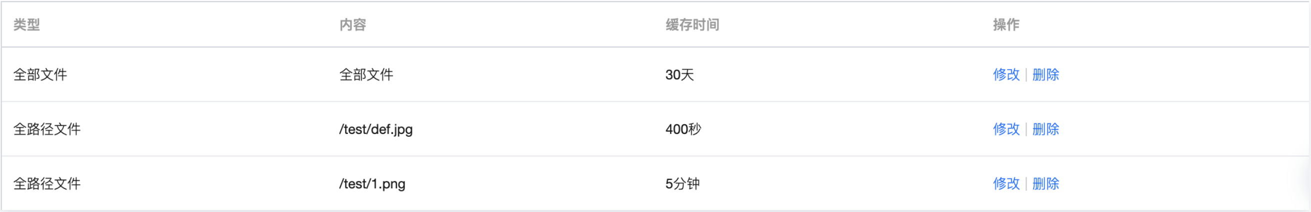
Platform default policies

If no feature is enabled, no rule is configured, or requests do not match the configured rules, the default platform policies will be applied:

- When user requests a business resource, if the HTTP Response Header from the origin server contains the Cache-Control field, follow that Cache-Control.
- If the HTTP Response Header from the origin server does not contain the Cache-Control field, CDN nodes will cache the resource for 600 seconds by default.

Configuration Example

The node cache validity configurations for the acceleration domain name `cloud.tencent.com` are as follows:



类型	内容	缓存时间	操作
全部文件	全部文件	30天	修改 | 删除
全路径文件	/test/def.jpg	400秒	修改 | 删除
全路径文件	/test/1.png	5分钟	修改 | 删除

The actual cache validity will be as follows:

1. `/test/def.jpg` file node cache time is 400 seconds.
2. `/test/1.png` file node cache time is 5 minutes.
3. 30 days for other files.

Status Code Cache Configuration

Last updated：2024-12-31 17:37:35

Configuration Scenario

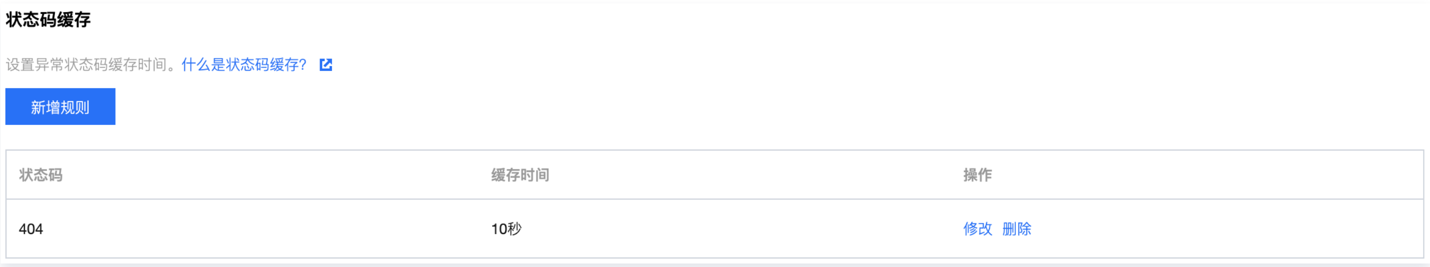
Under normal circumstances, when a CDN node successfully pulls the requested resource (2XX status code) from the origin server, it processes the resource according to the node cache validity configuration. If the origin server cannot quickly respond with a non-2XX status code and you do not want all requests to be passed back to the origin server, you can configure the cache validity time for status codes. This allows the CDN node to directly respond with non-2XX status codes, reducing the load on the origin server.
Currently supported status codes are:

- 4XX: 400, 401, 403, 404, 405, 407, 414, 451
- 5XX: 500, 501, 502, 503, 504, 509, 514

Configuration Guide

View Configuration

Log in to the CDN Console, select **Domain Management** from the menu bar, click **Management** in the domain operation column, enter the domain configuration page, switch tabs to **Cache Configuration**, where you can find **Status Code Cache**.
By default, there is a rule: "404 - Cache for 10 seconds":



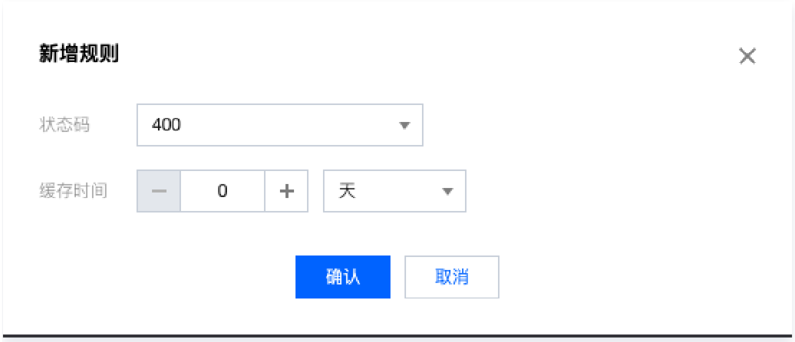
状态码缓存

设置异常状态码缓存时间。什么是状态码缓存？

状态码	缓存时间	操作
404	10秒	修改 删除

Adding rules

You can add status code cache rules as needed, click **Add Status Code Cache**:



新增规则

状态码 400

缓存时间 0 天

Configuration limitations:

- Only one rule can be added for each status code, cannot be added repeatedly.
- When the cache time is 0, it means do not cache.

HTTP Header Cache Configuration

Last updated：2024-12-31 17:37:47

Configuration Scenario

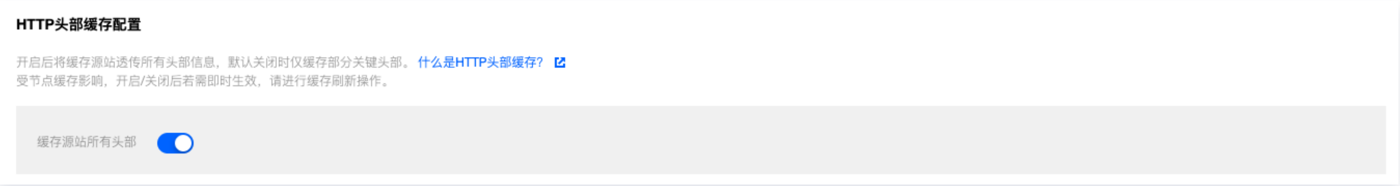
HTTP Header Cache can be configured to determine whether Tencent Cloud CDN caches origin server HTTP headers:

- On: CDN will cache all origin server HTTP headers. If headers are modified through HTTP Response Header Configuration, CDN configuration will take precedence;
- Off: CDN will only cache the following origin server HTTP headers:
  - Access-Control-Allow-Origin
  - Timing-Allow-Origin
  - Content-Disposition
  - Accept-Ranges

Configuration Guide

View Configuration

Log in to the CDN Console, select **Domain Management** from the menu bar, click **Management** on the right side of the domain to enter the domain configuration page. In the third column **Cache Configuration**, you can see HTTP Header Cache, which is enabled by default. You can disable it as needed.



HTTP头部缓存配置

开启后将缓存源站透传所有头部信息，默认关闭时仅缓存部分关键头部。什么是HTTP头部缓存?
受节点缓存影响，开启/关闭后若需即时生效，请进行缓存刷新操作。

缓存源站所有头部 ●

Access URL Rewrite Configuration

Last updated：2024-12-31 17:37:58

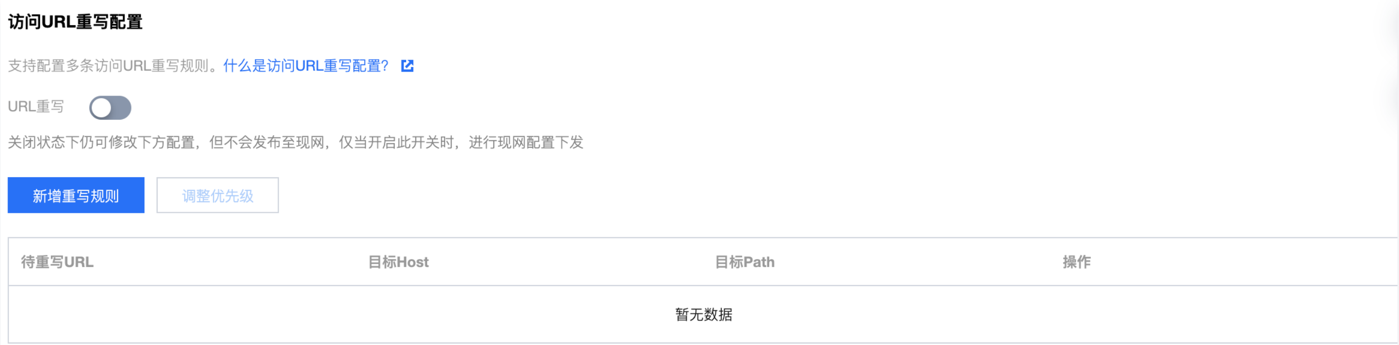
Configuration Scenario

If you need to modify the actual access URL to the URL that matches the origin server, you can use the access URL rewrite configuration in Tencent Cloud CDN.
You can customize the access URL rewrite configuration to redirect 302 URLs to the specified URL.

Configuration Guide

Viewing Configuration

Log in to the CDN console, select **Domain Management** from the left sidebar menu, click **Manage** in the domain operation column to enter the domain configuration page, switch the tab to **Cache Configuration**, and you will find the **Access URL Rewrite Configuration**.
By default, the access URL rewrite configuration is in closed status:



访问URL重写配置

支持配置多条访问URL重写规则。什么是访问URL重写配置？

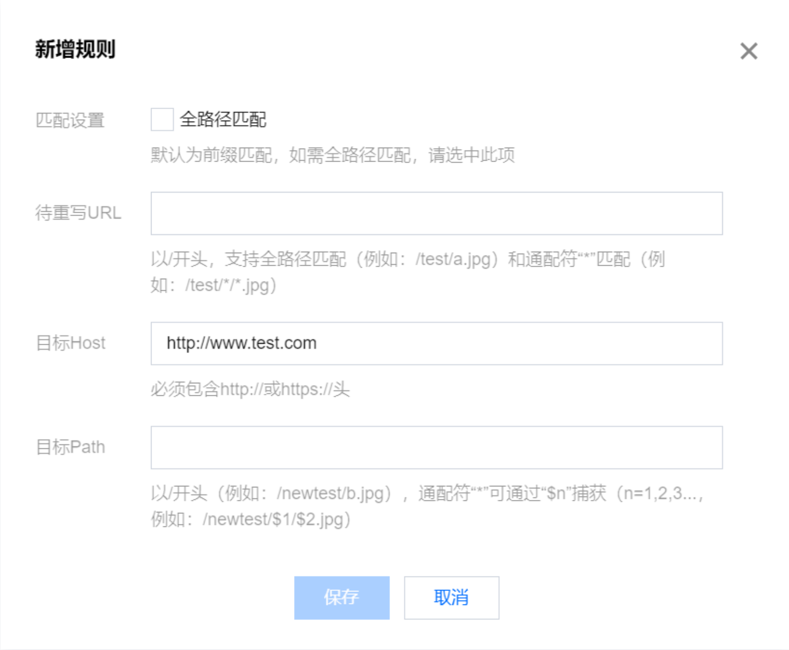
URL重写

关闭状态下仍可修改下方配置，但不会发布至现网，仅当开启此开关时，进行现网配置下发

待重写URL	目标Host	目标Path	操作
暂无数据			

Adding rules

You can add rewrite rules as needed by clicking **Adding rewrite rules:**



新增规则

匹配设置 □ 全路径匹配
默认为前缀匹配，如需全路径匹配，请选中此项

待重写URL
以/开头，支持全路径匹配（例如：/test/a.jpg）和通配符“*”匹配（例如：/test/*/*.jpg）

目标Host http://www.test.com
必须包含http://或https://头

目标Path
以/开头（例如：/newtest/b.jpg），通配符“*”可通过“$n”捕获（n=1,2,3...，例如：/newtest/$1/$2.jpg）

Configuration limitations

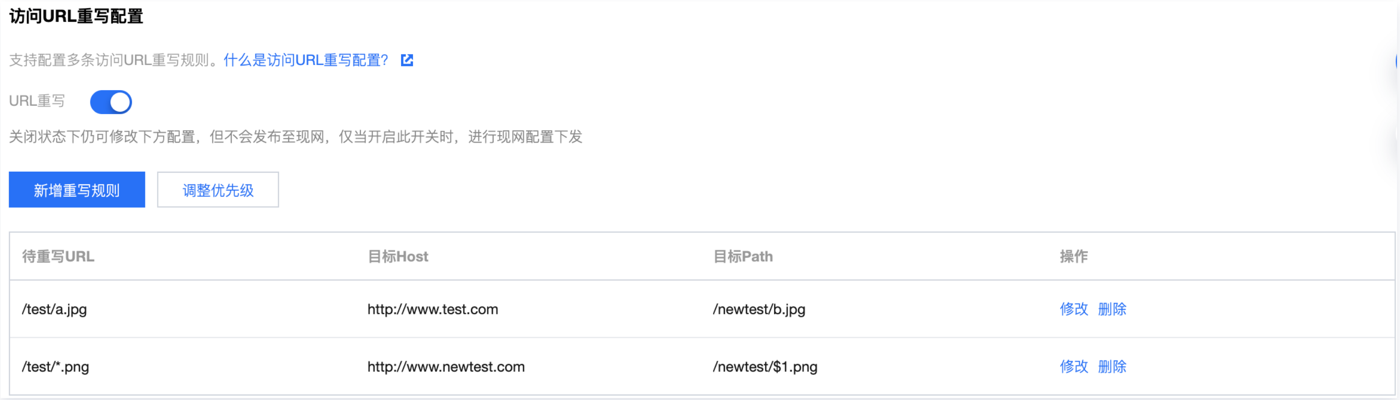
- Each domain name can have up to 100 rewrite rules.
- If a single rule does not select full path matching, it defaults to prefix matching. The more specific the matching rules, the lower they should be configured on the console, while broader directories should be configured at the top. If full path matching is

selected, it will be exact full path matching. When multiple rules have overlapping paths, the full path matching rule should be placed at the bottom.

- You can adjust the priority for multiple rules. Rules at the bottom of the list have higher priority.
- URL to be rewritten: starts with /, supports exact full path matching (e.g., /test/a.jpg) and wildcard `*` matching (e.g., /test/*/*.jpg). If full path matching is required, select full path matching. If specifying a file directory, it should not end with “/” (e.g., /test).
- Target Host: Defaults to the current domain (with http header by default), can be modified to another domain, must include `http://` or `https://` header.
- Target Path: Starts with / (e.g., /newtest/b.jpg), wildcard `*` can be captured by `$n` (n=1,2,3..., e.g., /newtest/$1/$2.jpg). If specifying a file directory, it must not end with "/" (e.g., /test).
- Up to 5 wildcards `*` and 10 capture placeholders `$n` are supported, other regex matching conditions are not supported.
- The content cannot exceed 1,024 characters and Chinese characters are not supported.

Configuration Example

If the Access URL Rewrite Configuration of the acceleration domain name `www.test.com` is as follows:



访问URL重写配置

支持配置多条访问URL重写规则。什么是访问URL重写配置?

关闭状态下仍可修改下方配置，但不会发布至现网，仅当开启此开关时，进行现网配置下发

待重写URL	目标Host	目标Path	操作
/test/a.jpg	http://www.test.com	/newtest/b.jpg	修改 删除
/test/*.png	http://www.newtest.com	/newtest/$1.png	修改 删除

The actual access is as follows:

- A client requests `www.test.com/test/a.jpg` and the CDN node returns the content of `www.test.com/newtest/b.jpg` .
- A client requests `www.test.com/test/a.png` and the CDN node returns the content of `www.newtest.com/newtest/a.png` .

Browser Cache Validity Configuration

Last updated：2024-12-31 17:38:09

Feature Introduction

The origin server can control the cache expiration time of CDN nodes by setting the Cache-Control response header (if the cache option is set to follow the origin). At the same time, the CDN node will pass the Cache-Control header to the user to control the browser's cache time. If you need the CDN node to set the browser's cache time, you can use this feature to modify the Cache-Control header in the CDN node's response to the user to achieve a lower back-to-origin rate.
When a user requests a business resource, if you have configured/hit the console Node Cache Configuration, the Cache-Control header will follow the platform policy by default:

- If the HTTP Response Header from the origin server does not contain a Cache-Control header and does not hit the enabled heuristic cache, it will pass the response without a Cache-Control header to the browser.
- If the HTTP Response Header from the origin server does not contain a Cache-Control header and hits the enabled heuristic cache, it will pass the Cache-Control header of the heuristic cache policy to the browser.
- If the HTTP Response Header from the origin server contains a Cache-Control header, it will pass that Cache-Control header to the browser.

If no rule is configured or matches requests:

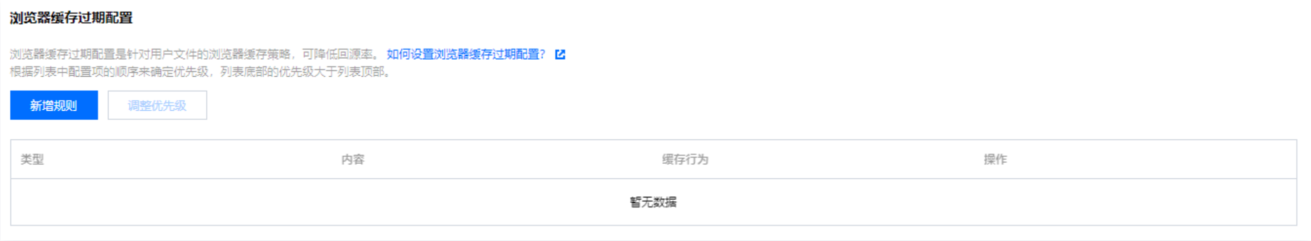
- If the origin server's HTTP Response Header contains a Cache-Control header, follow the Cache-Control header for the browser.
- If the origin server's HTTP Response Header does not contain a Cache-Control header, pass no Cache-Control header to the browser.

> **Note**
> When a request comes, if the requested resource is cached on the browser, it will be returned directly. If no, the request will be forwarded to CDN cache nodes. If the resource still cannot be found on the cache node, the request will be forwarded to the origin server.

Configuration Guide

Viewing Configuration

Log in to the CDN console, select **Domain Management** from the left sidebar menu, click **Management** in the domain operation column, enter the domain configuration page, switch tab to **Cache Configuration**, and you will find the **Browser Cache Validity Configuration**.



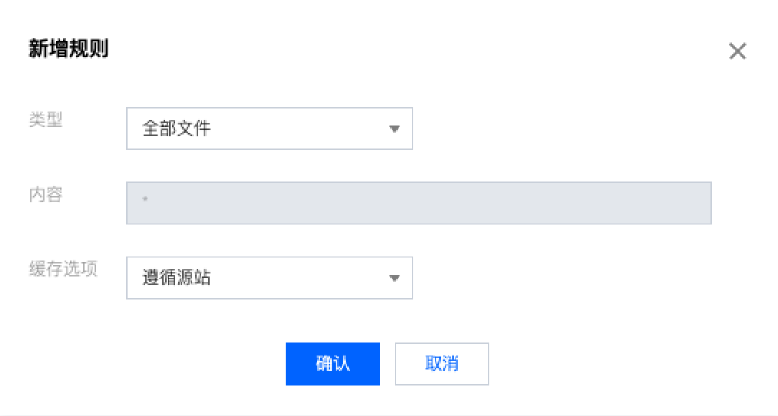
浏览器缓存过期配置

浏览器缓存过期配置是针对用户文件的浏览器缓存策略，可降低回源率。 如何设置浏览器缓存过期配置？
根据列表中配置项的顺序来确定优先级，列表底部的优先级大于列表顶部。

类型	内容	缓存行为	操作
暂无数据			

Adding rules

You can add browser cache validity rules as needed by clicking **Adding rules**. It supports specifying cache behavior for file types/file directory/file path/homepage configuration:



新增规则

类型 全部文件

内容 *

缓存选项 遵循源站

- Follow origin server: Follow the Cache-Control header of the origin server. If the origin server has no Cache-Control header or the Cache-Control header is no-cache/no-store/private, the browser will not cache the resource.
- Cache: Enforce the browser cache configuration rules in the console.
- No cache: no resource is cached in a browser.

Configuration limitations

- Each domain name can be configured with up to 20 rules. For all file and homepage type rules, only one rule can be added.
- Case-sensitive matching, please enter the content with correct case.
- You can adjust the priority for multiple rules. Rules at the bottom of the list have higher priority.
- In each rule of specified file type, file directory, and file path, up to 50 groups of content can be entered. Please use ";" to separate different content, e.g., Specified File Type: jpg;png.

Cache Configuration FAQs

Last updated：2024-12-31 17:38:20

What's node cache validity configuration?

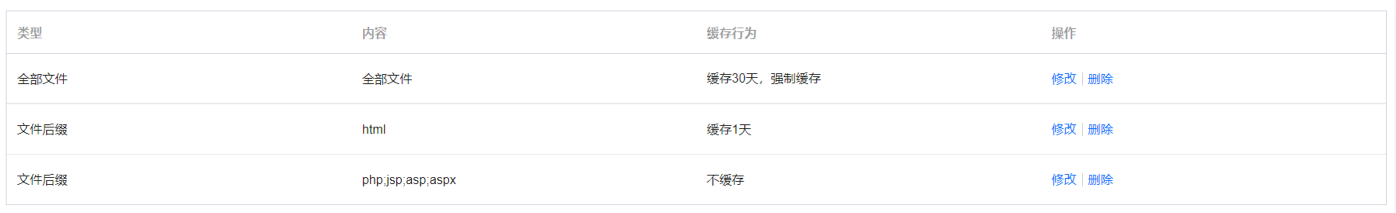
Node cache validity configuration refers to a set of expiration rules followed by CDN acceleration nodes when caching your business content. User resources cached on CDN nodes face the issue of "expiration." If the resource is not expired, the node will directly return the resource to the user upon request, improving access speed. If the resource is expired (i.e., it has exceeded the set validity period), the node will send the request to the origin server. If the origin server content is updated, the node will fetch and cache the new content, then return it to the user. If the origin server content is not updated, the node will only update the cache validity. Properly configuring cache validity can effectively improve hit rate, reduce back-to-origin rate, and save your bandwidth.

How do I control the file cache validity in a browser?

You can configure the browser cache validity on the console. For more information, please see Browser Cache Validity Configuration.

How do I configure CDN to return specific files without caching?

You can set the cache validity based on directory, file path, or file type. For more information, please see Node Cache Configuration. When the cache option is set to no cache, the CDN node will not cache the resource. Each time a user sends a request to the CDN node, the node will directly fetch the corresponding file from the origin server. For example, you need to set dynamic files like php, jsp, asp, aspx to no cache, html files to cache for 1 day, and other files to cache for 30 days. According to the priority rules, where bottom priority is higher than top, the node cache validity configuration is as shown below:



类型	内容	缓存行为	操作
全部文件	全部文件	缓存30天，强制缓存	修改 | 删除
文件后缀	html	缓存1天	修改 | 删除
文件后缀	php;jsp;asp;aspx	不缓存	修改 | 删除

What cache validity configurations supported in CDN?

CDN allows you to set a cache validity period and whether to ignore parameters, ignore case, follow origin server and enable heuristic cache for various file types. By using these cache rules properly, you can effectively improve the hit rate with a lower back-to-origin rate and bandwidth usage. For details, see Cache Configuration and Node Cache Validity Configuration.

What is the default cache configuration of CDN?

When accessing an acceleration domain name, CDN will add default node cache validity rules based on different business types, which you can adjust as needed:

- The following types of resources are not cached by default, including CDN webpage files, large files and audio and video on demand, and ECDN dynamic and static content (such as PHP, JSP, ASP and ASPX dynamic files). Other files are cached for 30 days.
- For ECDN dynamic content acceleration, all files are not cached.

If no rule is configured or matches requests, the default policies will be applied:

- When user requests a business resource, if the HTTP Response Header from the origin server contains the Cache-Control field, follow that Cache-Control.
- If the HTTP Response Header from the origin server does not contain the Cache-Control field, CDN nodes will cache the resource for 600 seconds by default.

What are cache matching rules?

When multiple cache rules are set, there will be overlaps between them, and the ones at the bottom of the list have higher priority than those at the top. For example, if a domain name is configured with the following cache settings:

```
All files - 30 days
```

```
.php .jsp .aspx - 0 seconds
.jpg .png .gif - 300 seconds
/test/*.jpg - 400 seconds
/test/abc.jpg - 200 seconds
```

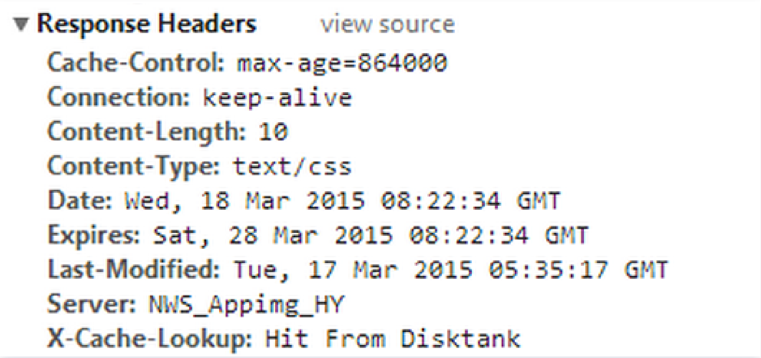
If the domain name is `www.test.com` , and the resource is `www.test.com/test/abc.jpg` , the matching rule will be as follows:

1. Match all files with the first rule. It is hit, so the cache validity is 30 days.
2. Match with the second rule. It is not hit.
3. Match with the third rule. It is hit, so the cache validity is 300 seconds.
4. Match with the fourth rule. It is hit, so the cache validity is 400 seconds.
5. Match with the fifth rule. It is hit, so the cache validity is 200 seconds.

The final cache validity is subject to the last matching result, so it will be 200 seconds.

How to Tell If User Access Hits the CDN Node Cache

You can determine whether the CDN node cache is hit based on the value of the X-Cache-Lookup in the HTTP response header.
Multiple X-Cache-Lookup headers may exist simultaneously to indicate different levels of hit status.
If X-Cache-Lookup returns any of the following values, a cache hit occurs; otherwise, it is a cache miss.
X-Cache-Lookup: Hit From MemCache
X-Cache-Lookup: Hit From Disktank
X-Cache-Lookup: Hit From Inner Cluster
X-Cache-Lookup: Cache Hit



▼ Response Headers view source

```
Cache-Control: max-age=864000
Connection: keep-alive
Content-Length: 10
Content-Type: text/css
Date: Wed, 18 Mar 2015 08:22:34 GMT
Expires: Sat, 28 Mar 2015 08:22:34 GMT
Last-Modified: Tue, 17 Mar 2015 05:35:17 GMT
Server: NWS_Appimg_HY
X-Cache-Lookup: Hit From Disktank
```

Will the cache on CDN cache nodes be actively and in real time updated after the origin server changes files?

No. The cache on CDN cache nodes will not be updated in real time.

- CDN nodes update the cache according to the Node Cache Configuration rules you configure in the console. If there are file changes on the origin server and the cache is still valid, CDN cache nodes will not perform origin-pull to update the cache. As a result, the file on the origin server is different from the cache.
- After a resource on the origin server is updated, its cache on the CDN node must be updated immediately. You can use the Purge Cache feature to update unexpired caches on the CDN node, ensuring consistency between the resources cached on the CDN node and those stored on the origin server.
- If you need to update the cache of a file on a schedule, you can use scheduled refresh preheating to trigger the refresh task on time.

Node Cache Validity (In Internal Testing)

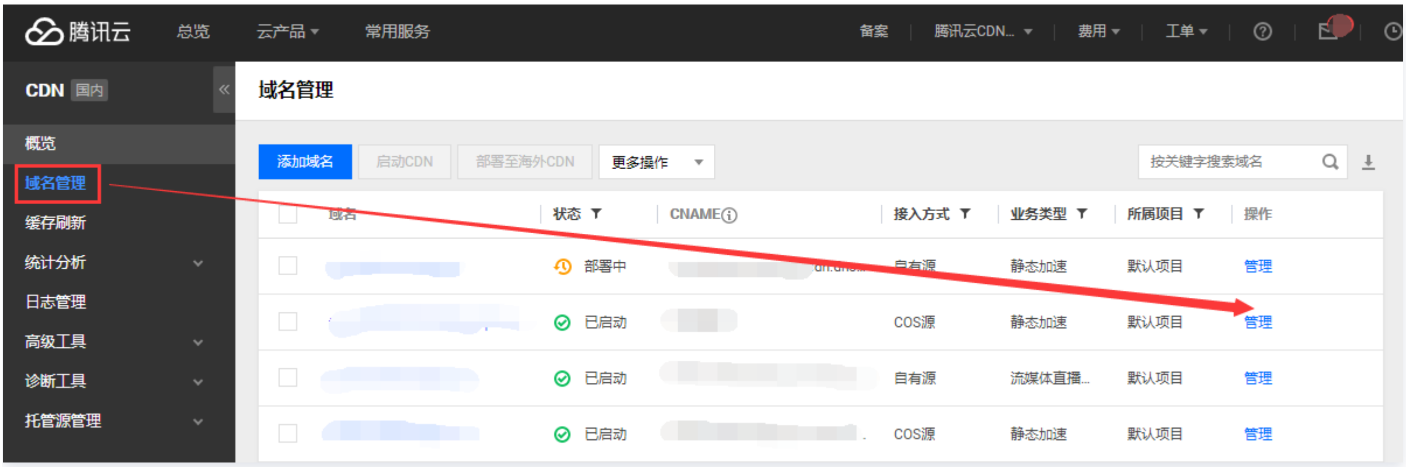
Last updated：2024-12-31 17:38:36

Note:
- Cache expiration configuration refers to a set of expiration rules that CDN acceleration nodes follow when caching your business content. User resources cached on CDN nodes all face the issue of "expiration". If a resource is in a non-expired state, when a user request reaches the node, the node will directly return this resource to the user, improving the retrieval speed; when a resource is in an expired state (i.e., beyond the set validity period), the user request will be sent from the node to the origin server to re-fetch the content and cache it on the node, while also returning it to the user.
- Tencent Cloud CDN supports setting content cache times across various dimensions and supports custom priority adjustments. Properly configuring cache times can effectively improve the hit rate, reduce the back-to-origin rate, and save your bandwidth.
- Tencent Cloud CDN supports setting cache expiration times for 403 and 404 status codes.

Browser Cache Validity Configuration

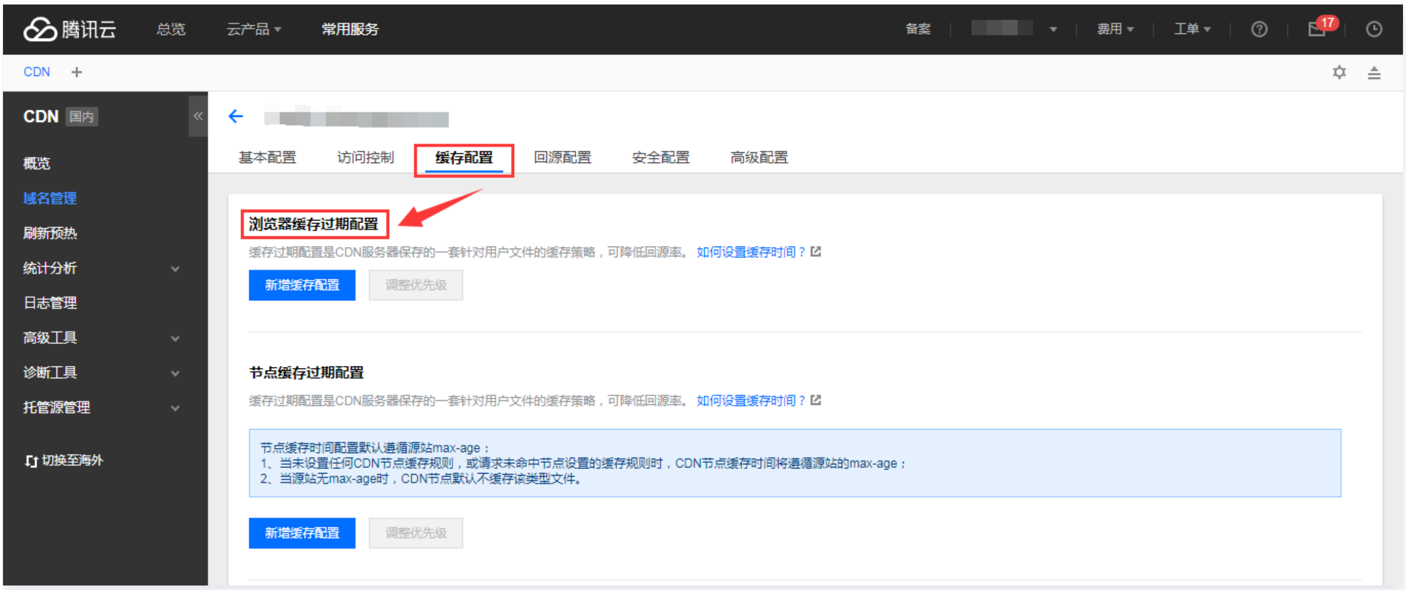
Configuration Guide

Log in to the CDN console, select **Domain Management** from the left menu, and click **Management** on the right side of the domain you want to edit:



域名	状态	CNAME	接入方式	业务类型	所属项目	操作
[redacted]	部署中	[redacted]	自有源	静态加速	默认项目	管理
[redacted]	已启动	[redacted]	COS源	静态加速	默认项目	管理
[redacted]	已启动	[redacted]	自有源	流媒体直播...	默认项目	管理
[redacted]	已启动	[redacted]	COS源	静态加速	默认项目	管理

Click [Cache Configuration], and you will see the **Browser Cache Validity Configuration** module:



浏览器缓存过期配置

缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 如何设置缓存时间？

节点缓存过期配置

缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 如何设置缓存时间？

节点缓存时间配置默认遵循源站max-age：
1、当未设置任何CDN节点缓存规则，或请求未命中节点设置的缓存规则时，CDN节点缓存时间将遵循源站的max-age；
2、当源站无max-age时，CDN节点默认不缓存该类型文件。

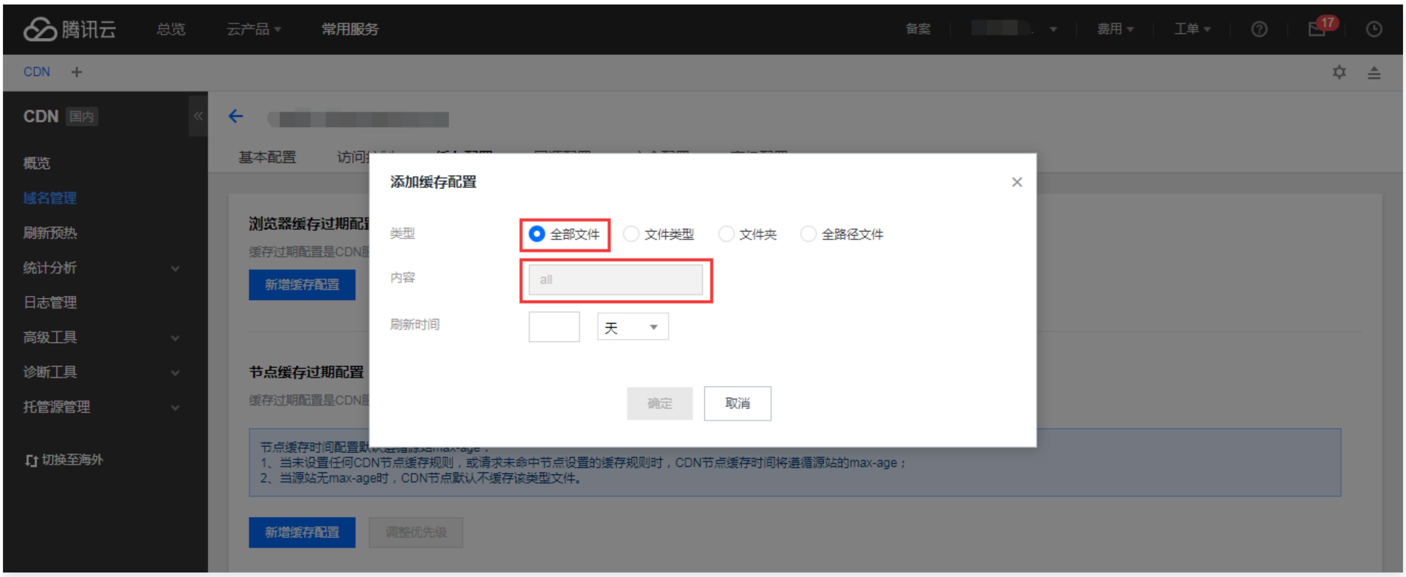
When a domain is accessed, the browser cache validity configuration is not set by default.

Modify

Click [Add Cache Configuration] to add a cache configuration. You can set the browser cache validity period according to your own business needs. CDN supports four methods for setting browser cache validity periods:

1. Setting cache validity period for all files

You can choose to set the cache validity period for all files. The content is fixed as `all` and cannot be changed, as shown below:



添加缓存配置

类型 ● 全部文件 ○ 文件类型 ○ 文件夹 ○ 全路径文件

内容 all

刷新时间 天

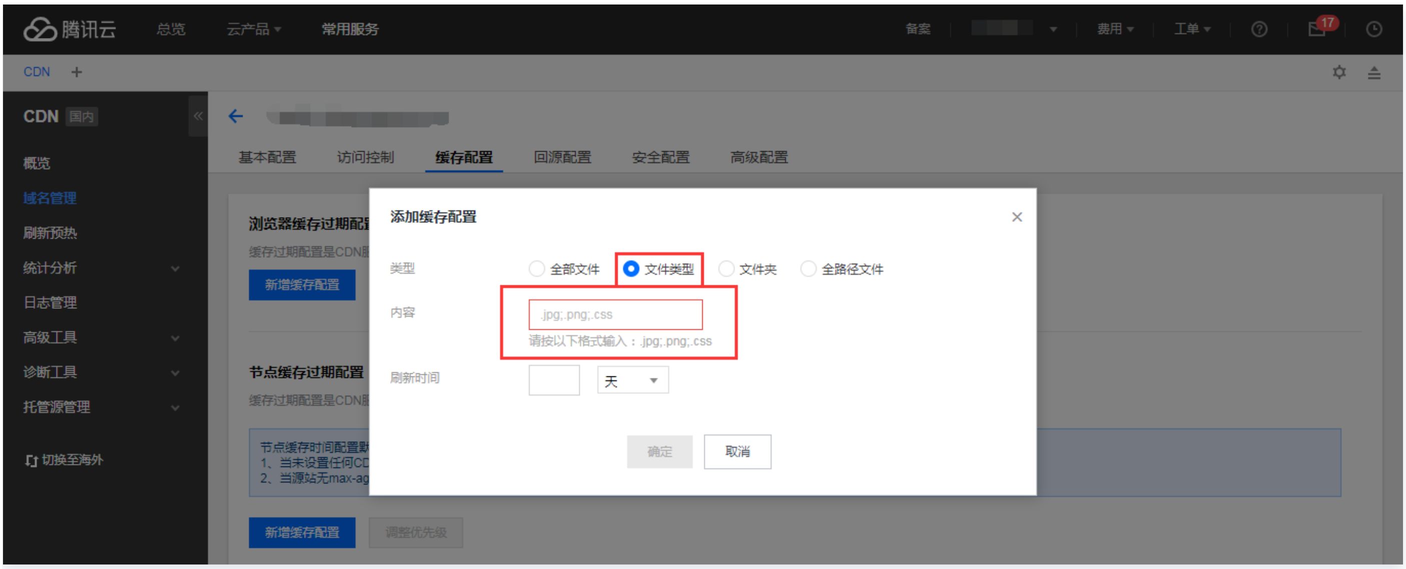
确定 取消

节点缓存时间配置默认遵循源站max-age：
1、当未设置任何CDN节点缓存规则，或请求未命中节点设置的缓存规则时，CDN节点缓存时间将遵循源站的max-age；
2、当源站无max-age时，CDN节点默认不缓存该类型文件。

When the refresh time is set to 0, there is no caching; the cache validity period cannot exceed 365 days.

2. Setting cache validity period by file type

You can fill in the file type suffix to set the cache time based on the type, as follows:



添加缓存配置

类型 ○ 全部文件 ● 文件类型 ○ 文件夹 ○ 全路径文件

内容 .jpg;.png;.css

请按以下格式输入：.jpg;.png;.css

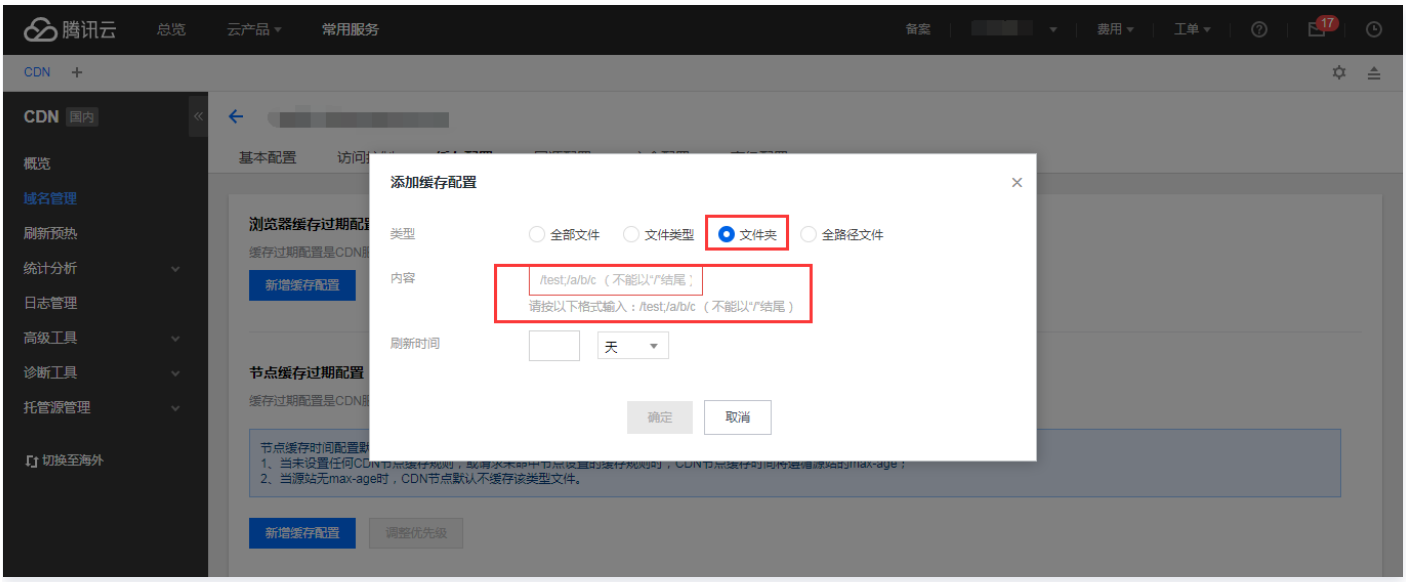
刷新时间 天

确定 取消

When configuring the cache time, multiple items can be entered, separated by `;`. The content is case-sensitive and must start with a `.` file suffix, such as `.png`. When the refresh time is set to 0, it will not be cached; the maximum cache time cannot exceed 365 days.

3. Setting the cache validity period by folder

You can fill in the folder path to set the cache time based on the folder, as follows:



添加缓存配置

类型 ○ 全部文件 ○ 文件类型 ● 文件夹 ○ 全路径文件

内容 /test;/a/b/c（不能以"/"结尾；

请按以下格式输入：/test;/a/b/c（不能以"/"结尾）

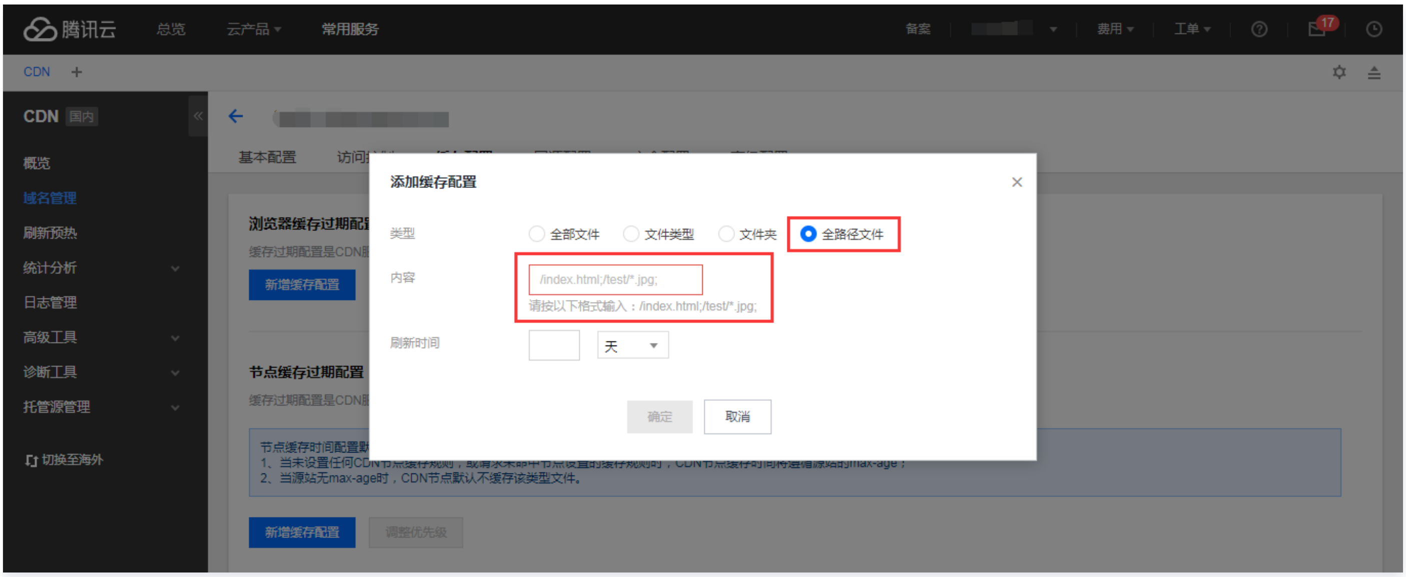
刷新时间 天

确定 取消

When configuring the cache time, multiple items can be entered, separated by `;`. The content is case-sensitive and must start with a `/` folder. When the refresh time is set to 0, it will not be cached; the maximum cache time cannot exceed 365 days.

4. Setting cache expiration time for a full-path file

You can set the cache time for a specific file as follows:



添加缓存配置

类型 ○ 全部文件 ○ 文件类型 ○ 文件夹 ● 全路径文件

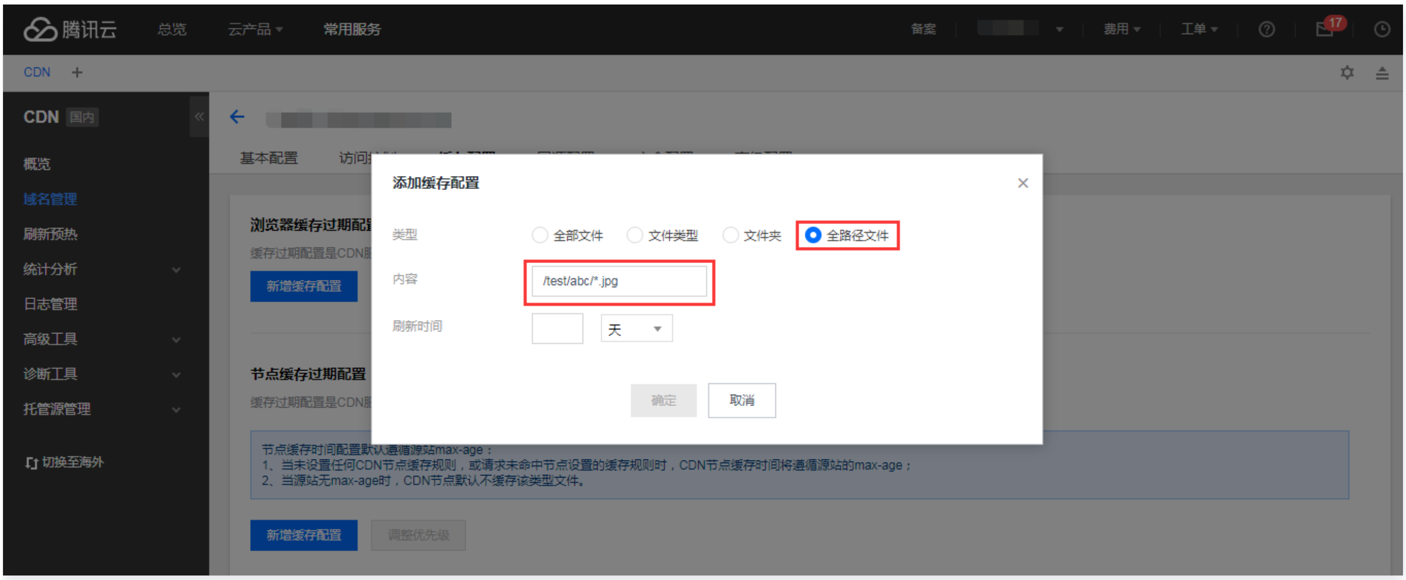
内容 /index.html;/test/*.jpg;

请按以下格式输入：/index.html;/test/*.jpg;

刷新时间 天

确定 取消

When configuring the cache time, multiple items can be entered, separated by `;`. The content is case-sensitive and supports `*` to match a specific type of file, such as `/test/abc/*.jpg`:



添加缓存配置

类型 ○ 全部文件 ○ 文件类型 ○ 文件夹 ● 全路径文件

内容 /test/abc/*.jpg

刷新时间 天

确定 取消

节点缓存时间配置默认遵循源站max-age：
1、当未设置任何CDN节点缓存规则，或请求未命中节点设置的缓存规则时，CDN节点缓存时间将遵循源站的max-age；
2、当源站无max-age时，CDN节点默认不缓存该类型文件。

Priority

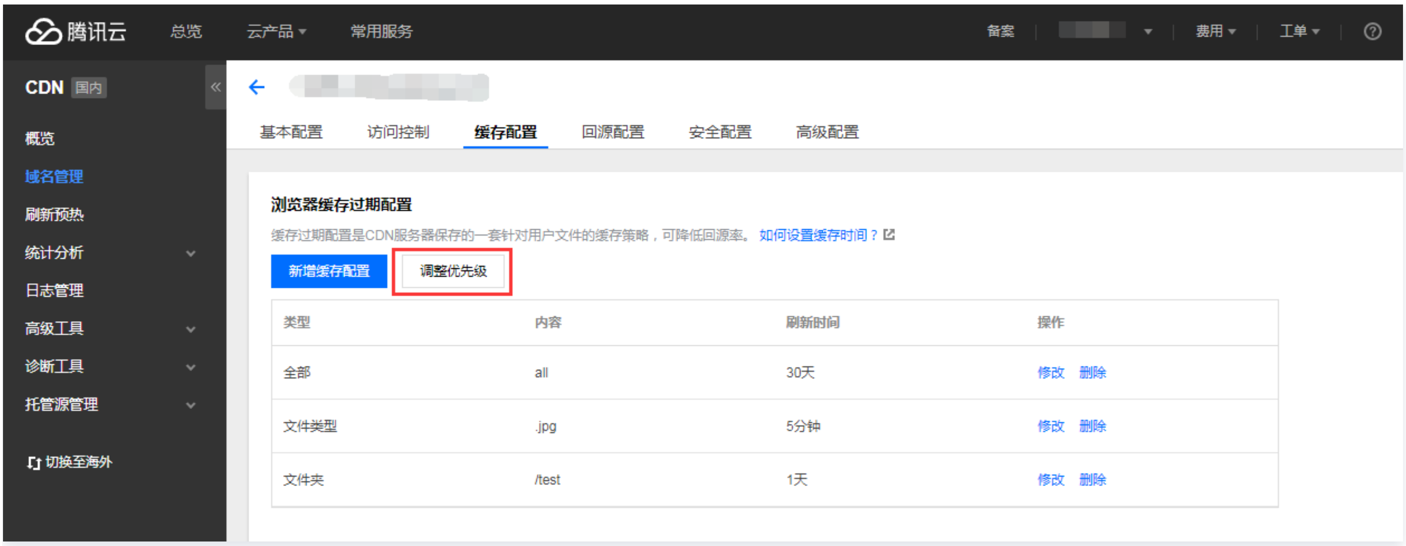
When multiple cache rules are set, there will be overlaps between them, and the ones at the bottom of the list have higher priority than those at the top. For example, if a domain name is configured as follows:

> All files 30 days
> .php .jsp .aspx 0 seconds
> .jpg .png .gif 300 seconds
> /test/*.jpg 400 seconds
> /test/abc.jpg 200 seconds

If the domain name is ` `www.test.com` `, and the resource is ` `www.test.com/test/abc.jpg` `, the matching rule will be as follows:

1. Match with the first rule for all files. It is hit, so the cache validity is 30 days.
2. Match with the second rule. It is not hit.
3. Match with the third rule. It is hit, so the cache validity is 300 seconds.
4. Match with the fourth rule. It is hit, so the cache validity is 400 seconds.
5. Match with the fifth rule. It is hit, so the cache validity is 200 seconds.

Therefore, the final cache validity is 200 seconds, subject to the last matching result.
Click [Adjust Priority] to add cache configurations. You can customize the order of the added cache expiration configurations based on your business scenario.

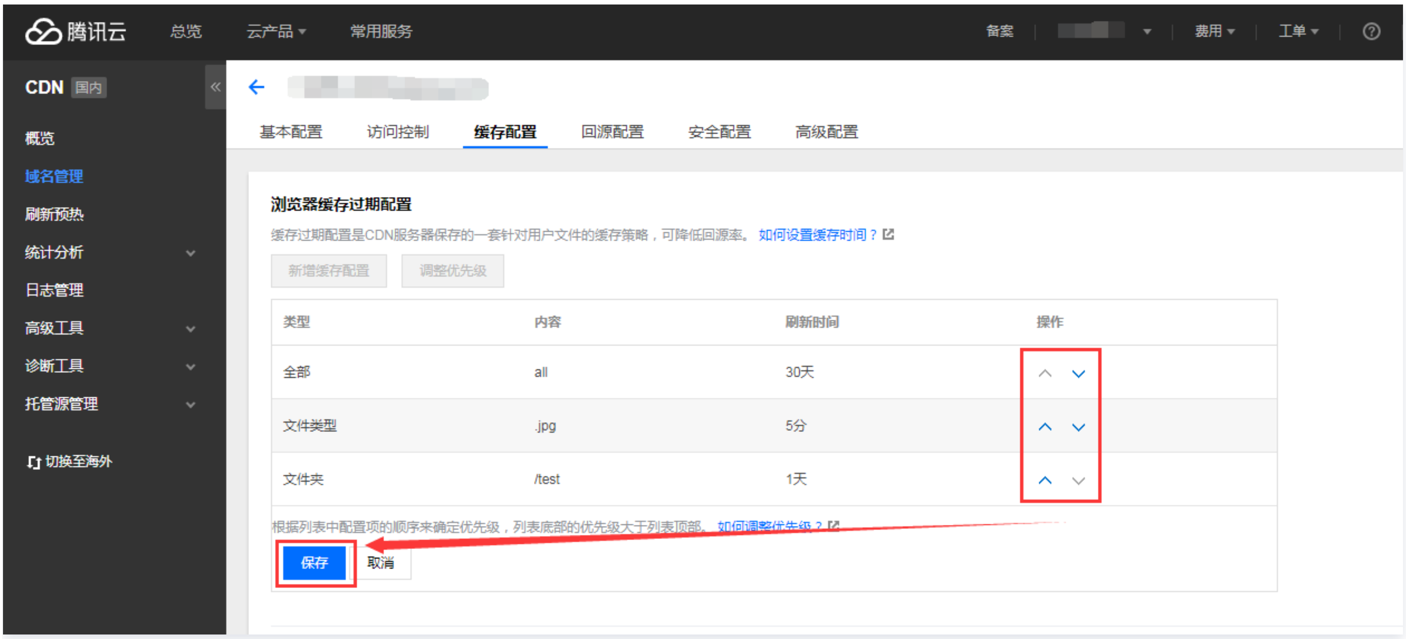


浏览器缓存过期配置

缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 如何设置缓存时间？

类型	内容	刷新时间	操作
全部	all	30天	修改 删除
文件类型	.jpg	5分钟	修改 删除
文件夹	/test	1天	修改 删除

Use the up and down arrows on the right to adjust the order of the cache expiration configurations, and click [Save] to complete the adjustment.



浏览器缓存过期配置

缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 如何设置缓存时间？

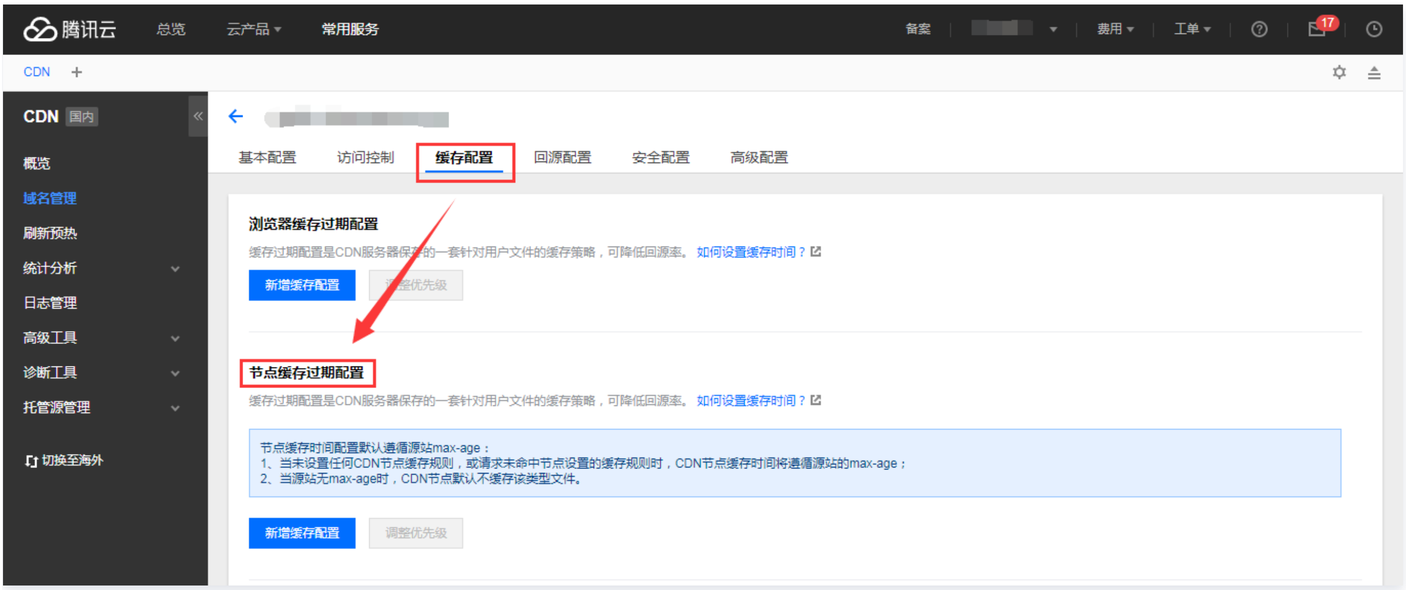
类型	内容	刷新时间	操作
全部	all	30天	^ v
文件类型	.jpg	5分	^ v
文件夹	/test	1天	^ v

根据列表中配置项的顺序来确定优先级，列表底部的优先级大于列表顶部。 如何调整优先级？

Node Cache Expiration Configuration

Configuration Guide

Under the **Browser Cache Validity Configuration** module, you can see the **Node Cache Configuration** module:



浏览器缓存过期配置

缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 如何设置缓存时间？

节点缓存过期配置

缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 如何设置缓存时间？

节点缓存时间配置默认遵循源站max-age：
1、当未设置任何CDN节点缓存规则，或请求未命中节点设置的缓存规则时，CDN节点缓存时间将遵循源站的max-age；
2、当源站无max-age时，CDN节点默认不缓存该类型文件。

During domain access, you can manually add node cache expiration configurations; the system does not add configurations by default.

The default node cache time configuration follows the max-age information in the origin server's response header.

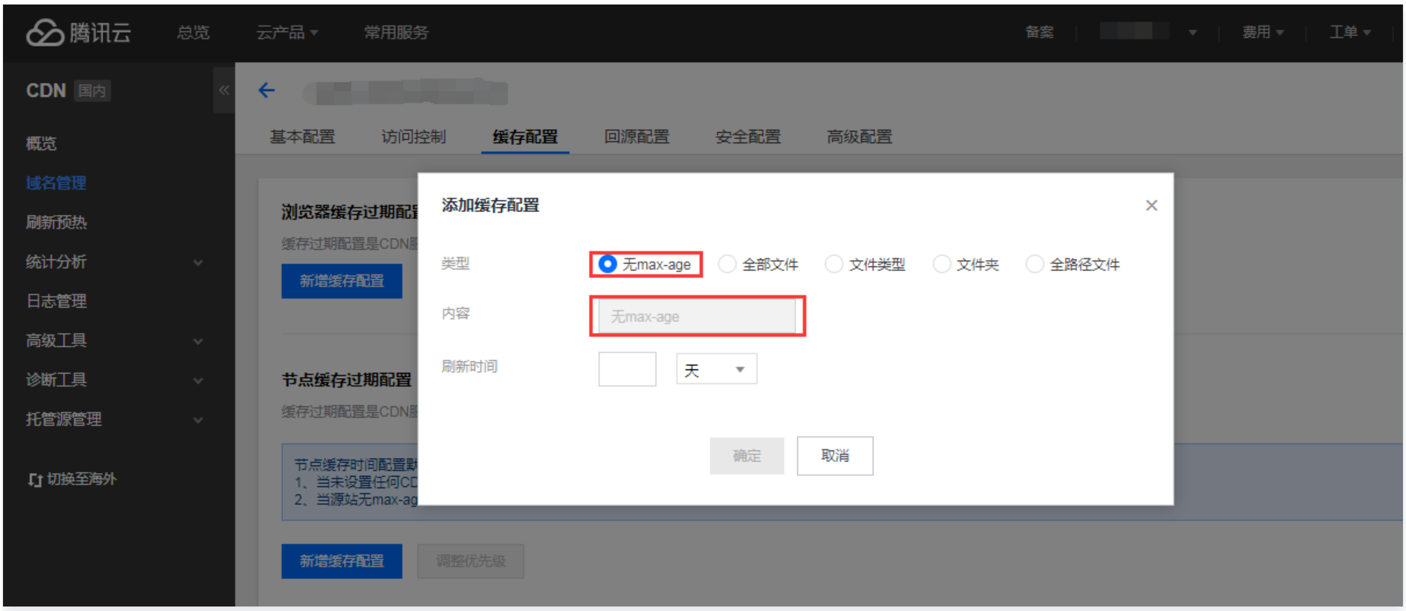
1. If no CDN node cache rules are set, or if the request does not hit the node's cache rules, the CDN node cache time will follow the max-age information from the origin server.
2. If there is no max-age information in the origin server's response header, the CDN node will not cache that type of file by default.

Modify

Click [Add Cache Configuration] to add cache configurations. You can add node cache time configurations based on your own business needs. CDN supports five methods for setting node cache expiration times:

1. Setting cache expiration time for files without max-age

When a user requests a business resource, if the origin server's response header lacks max–age information, you can choose to set a cache expiration time for these files without max–age. The content applies to all files without max–age and cannot be changed, as shown below:



添加缓存配置

类型 ● 无max-age ○ 全部文件 ○ 文件类型 ○ 文件夹 ○ 全路径文件

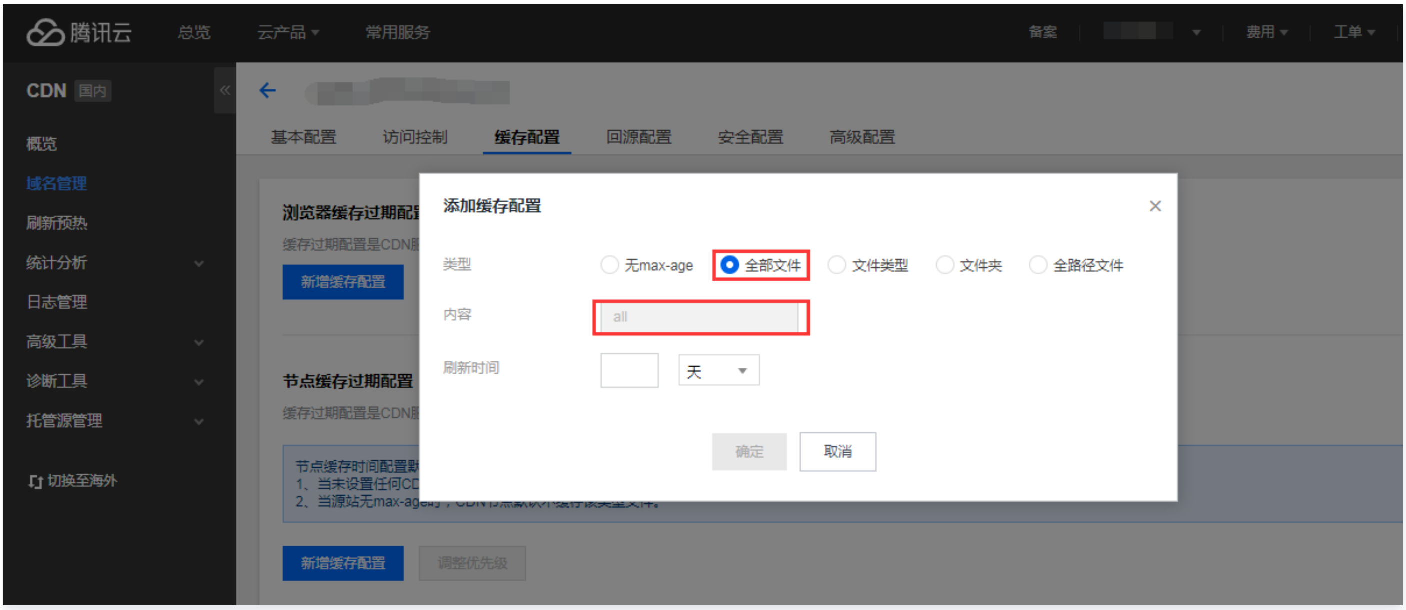
内容 无max-age

刷新时间 天

When the refresh time is set to 0, no caching occurs, and all requests are forwarded to the user's origin server. The maximum cache time cannot exceed 365 days.

2. Setting the cache validity period for all files

You can choose to set the cache validity period for all files. The content is fixed as ` `all` ` and cannot be changed, as shown below:



添加缓存配置

类型 ○ 无max-age ● 全部文件 ○ 文件类型 ○ 文件夹 ○ 全路径文件

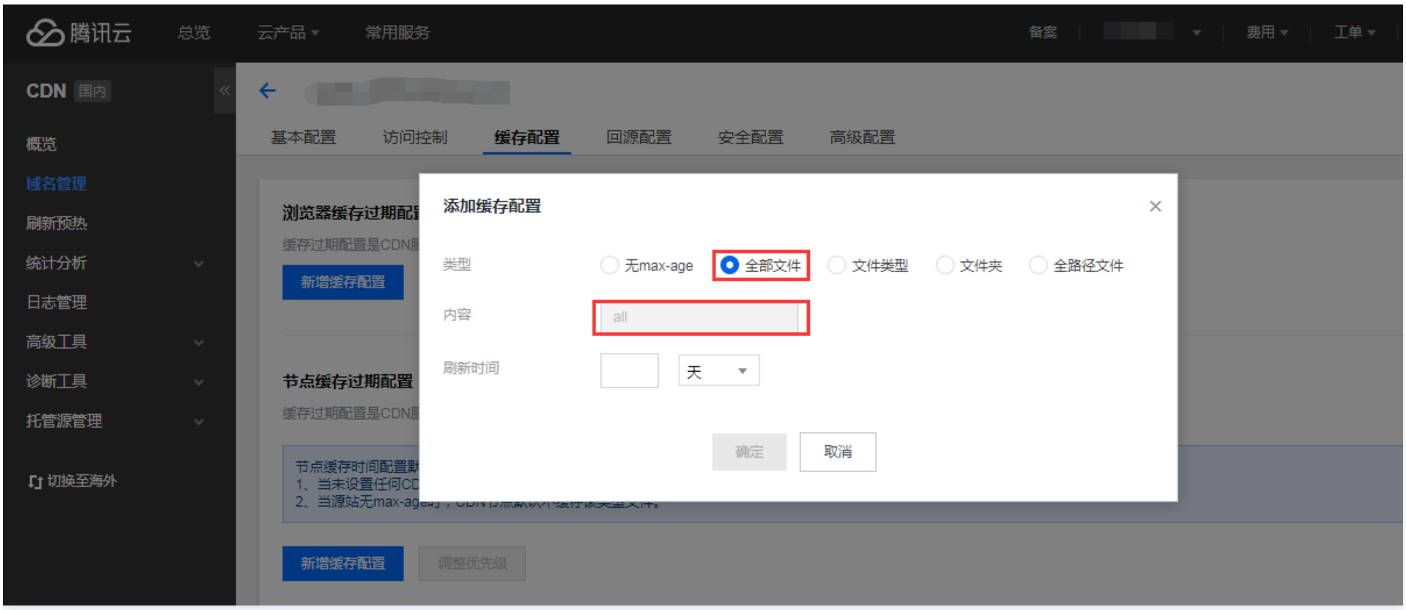
内容 all

刷新时间 天

When the refresh time is set to 0, no caching is done, and all requests are forwarded to the user's origin server; the maximum cache time cannot exceed 365 days.

3. Setting the cache validity period by file type

You can fill in the file type suffix to set the cache time based on the type, as follows:



添加缓存配置

类型 ○ 无max-age ● 全部文件 ○ 文件类型 ○ 文件夹 ○ 全路径文件

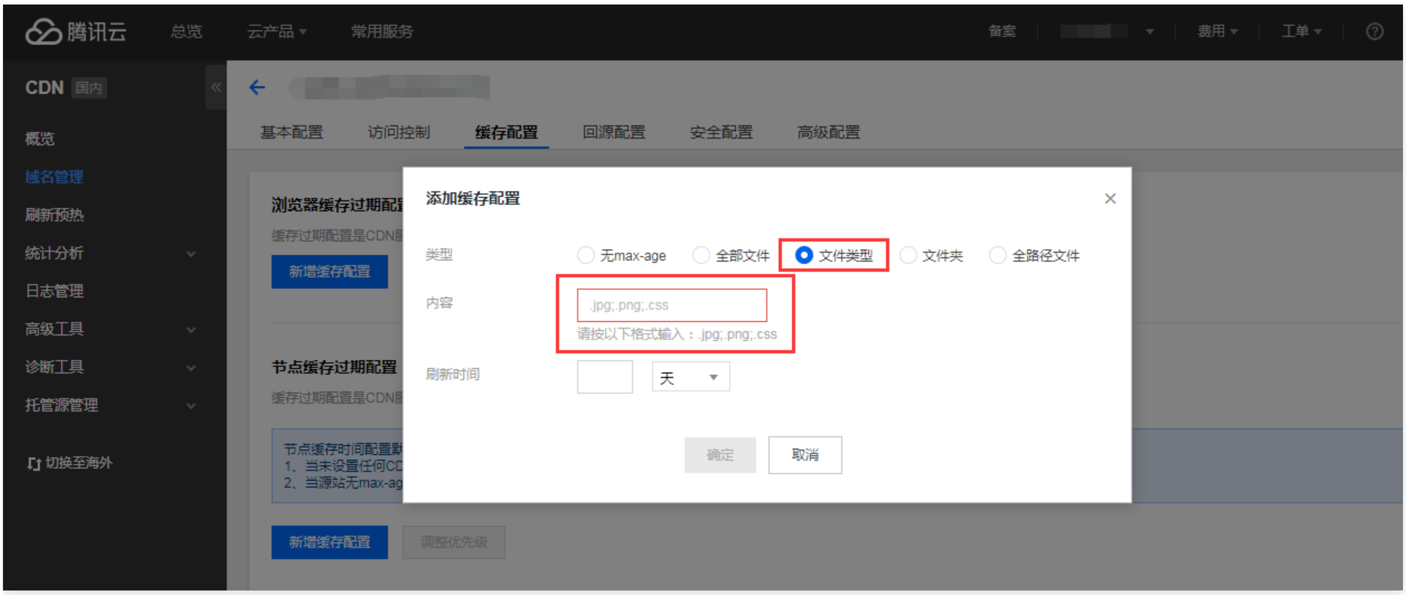
内容 all

刷新时间 天

When configuring the cache time, you can enter multiple items separated by `` `;` ``. The content is case-sensitive and must be a file suffix starting with `` `.` ``, such as `` `.png` ``. When the refresh time is set to 0, no caching is done, and all requests are forwarded to the user's origin server; the maximum cache time cannot exceed 365 days.

4. Setting the cache validity period by folder

You can fill in the folder path to set the cache time based on the folder, as follows:



添加缓存配置

类型 ○ 无max-age ○ 全部文件 ● 文件类型 ○ 文件夹 ○ 全路径文件

内容 .jpg;.png;.css

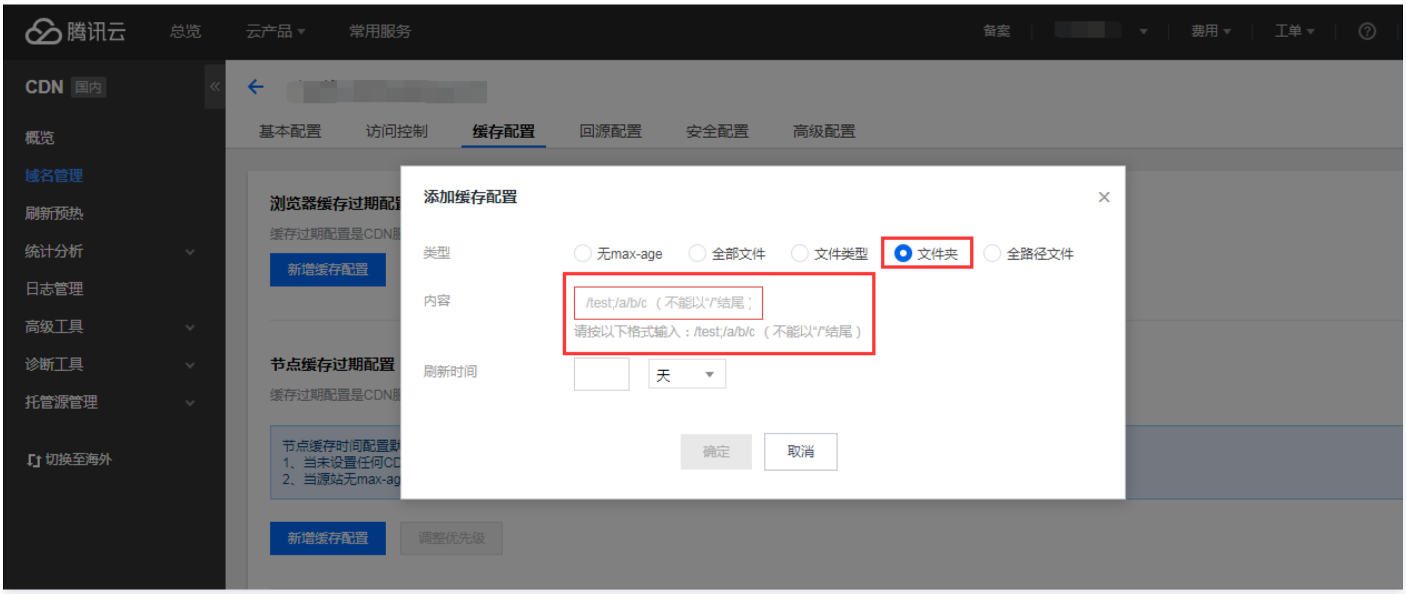
请按以下格式输入：.jpg;.png;.css

刷新时间 天

When configuring the cache time, you can enter multiple items separated by `` `;` ``. The content is case-sensitive and must be a folder starting with `` `/` ``. When the refresh time is set to 0, no caching is done, and all requests are forwarded to the user's origin server; the maximum cache time cannot exceed 365 days.

5. Setting the cache validity period for full-path files

You can set the cache time for a specific file as follows:



添加缓存配置

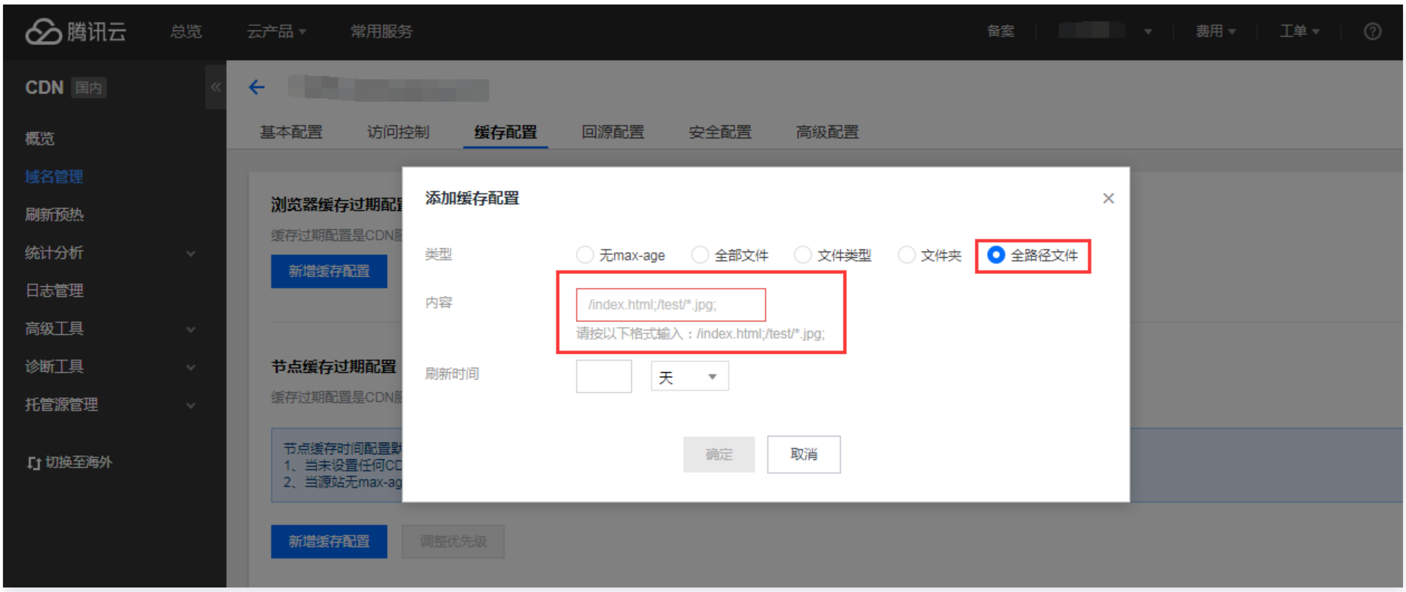
类型: ○ 无max-age ○ 全部文件 ○ 文件类型 ● 文件夹 ○ 全路径文件

内容: /test;/a/b/c （不能以"/"结尾）

请按以下格式输入：/test;/a/b/c （不能以"/"结尾）

刷新时间: 天

When configuring the cache time, you can enter multiple items separated by ` ; ` . The content is case-sensitive and supports ` * ` to match a certain type of file, such as ` /test/abc/*.jpg ` :



添加缓存配置

类型: ○ 无max-age ○ 全部文件 ○ 文件类型 ○ 文件夹 ● 全路径文件

内容: /index.html;/test/*.jpg;

请按以下格式输入：/index.html;/test/*.jpg;

刷新时间: 天

Priority

When multiple cache rules are set, there will be overlaps between them, and the ones at the bottom of the list have higher priority than those at the top. For example, if a domain name is configured as follows:

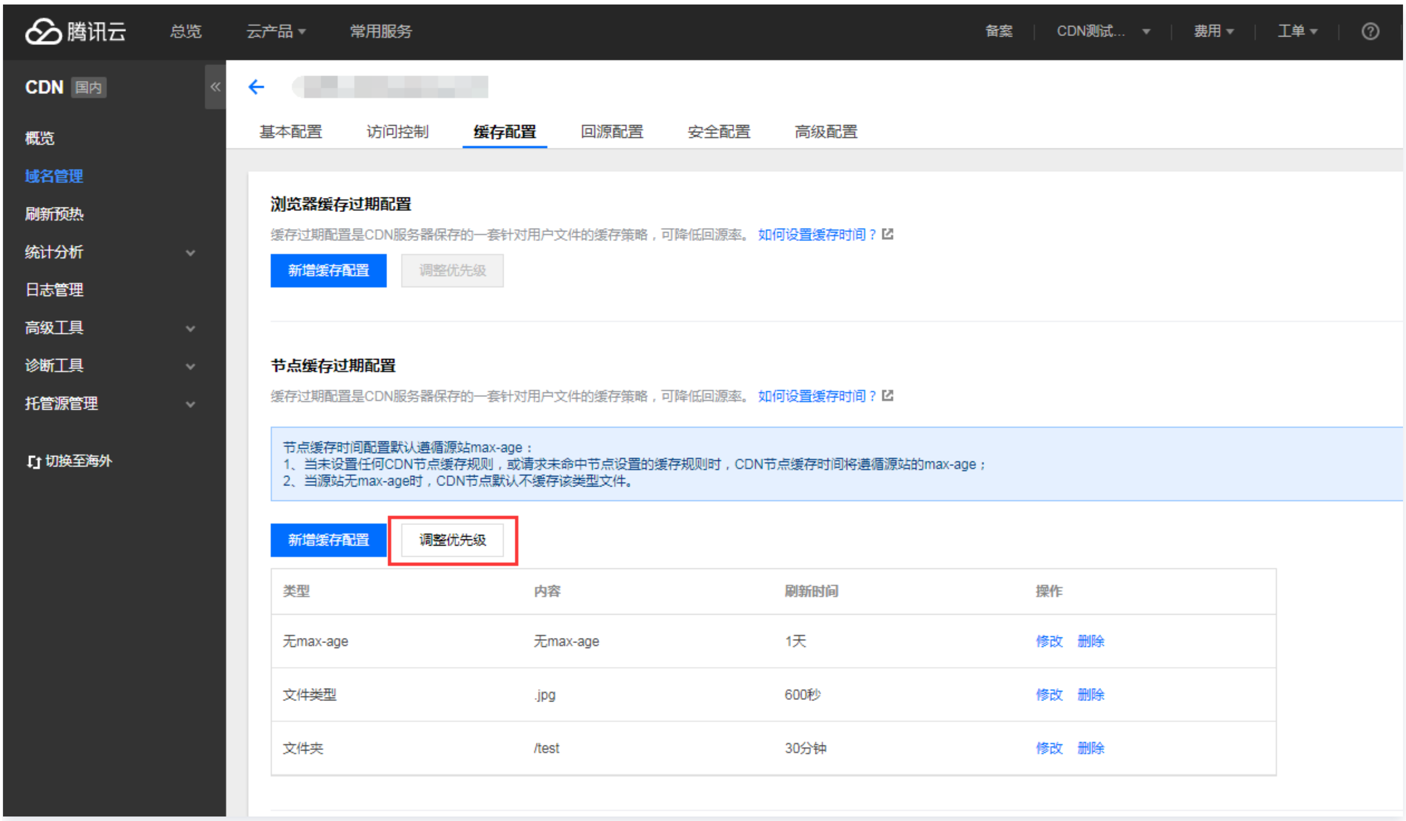
> All files 30 days
> None max-age 60 seconds
> .php .jsp .aspx 0 seconds
> .jpg .png .gif 300 seconds
> /test/*.jpg 400 seconds
> /test/abc.jpg 200 seconds

If the domain name is ` www.test.com ` and the resource is ` www.test.com/test/abc.jpg ` , with the origin server response header ` Cache-Control: max-age=600 ` , the matching method is as follows:

1. Match with the first rule for all files. It is hit, so the cache validity is 30 days.
2. Match with the second rule. It is not hit.
3. Match with the third rule. It is not hit.

4. Match with the fourth rule. It is hit, so the cache validity is 300 seconds.
5. Match with the fifth rule. It is hit, so the cache validity is 400 seconds.
6. Match with the sixth rule. It is hit, so the cache validity is 200 seconds.

Therefore, the final cache validity is 200 seconds, subject to the last matching result.
Click [Adjust Priority] to add cache configurations. You can customize the order of the added cache expiration configurations based on your business scenario.



浏览器缓存过期配置

缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 如何设置缓存时间？

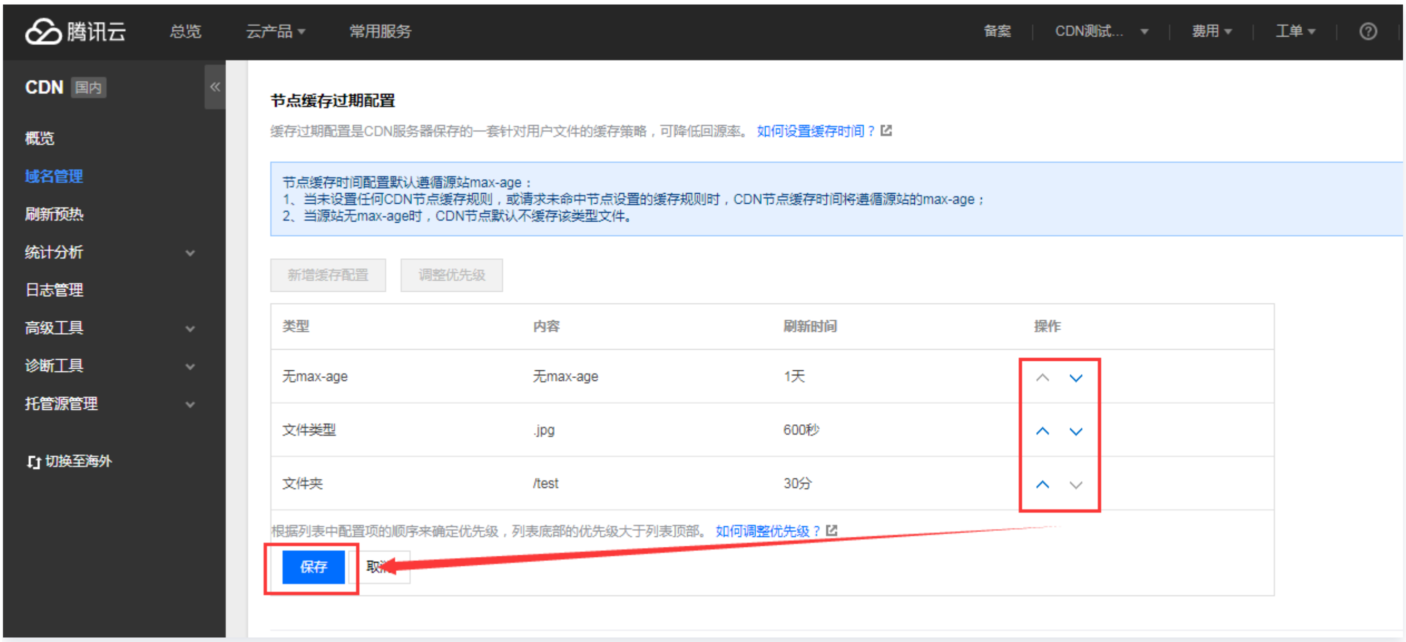
节点缓存过期配置

缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 如何设置缓存时间？

节点缓存时间配置默认遵循源站max-age：
1、当未设置任何CDN节点缓存规则，或请求未命中节点设置的缓存规则时，CDN节点缓存时间将遵循源站的max-age；
2、当源站无max-age时，CDN节点默认不缓存该类型文件。

类型	内容	刷新时间	操作
无max-age	无max-age	1天	修改 删除
文件类型	.jpg	600秒	修改 删除
文件夹	/test	30分钟	修改 删除

Use the right side up and down arrows to adjust the order of cache expiration configurations. Click [Save] to complete the adjustment.



节点缓存过期配置

缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 如何设置缓存时间？

节点缓存时间配置默认遵循源站max-age：
1、当未设置任何CDN节点缓存规则，或请求未命中节点设置的缓存规则时，CDN节点缓存时间将遵循源站的max-age；
2、当源站无max-age时，CDN节点默认不缓存该类型文件。

类型	内容	刷新时间	操作
无max-age	无max-age	1天	∧ ∨
文件类型	.jpg	600秒	∧ ∨
文件夹	/test	30分	∧ ∨

根据列表中配置项的顺序来确定优先级，列表底部的优先级大于列表顶部。 如何调整优先级？

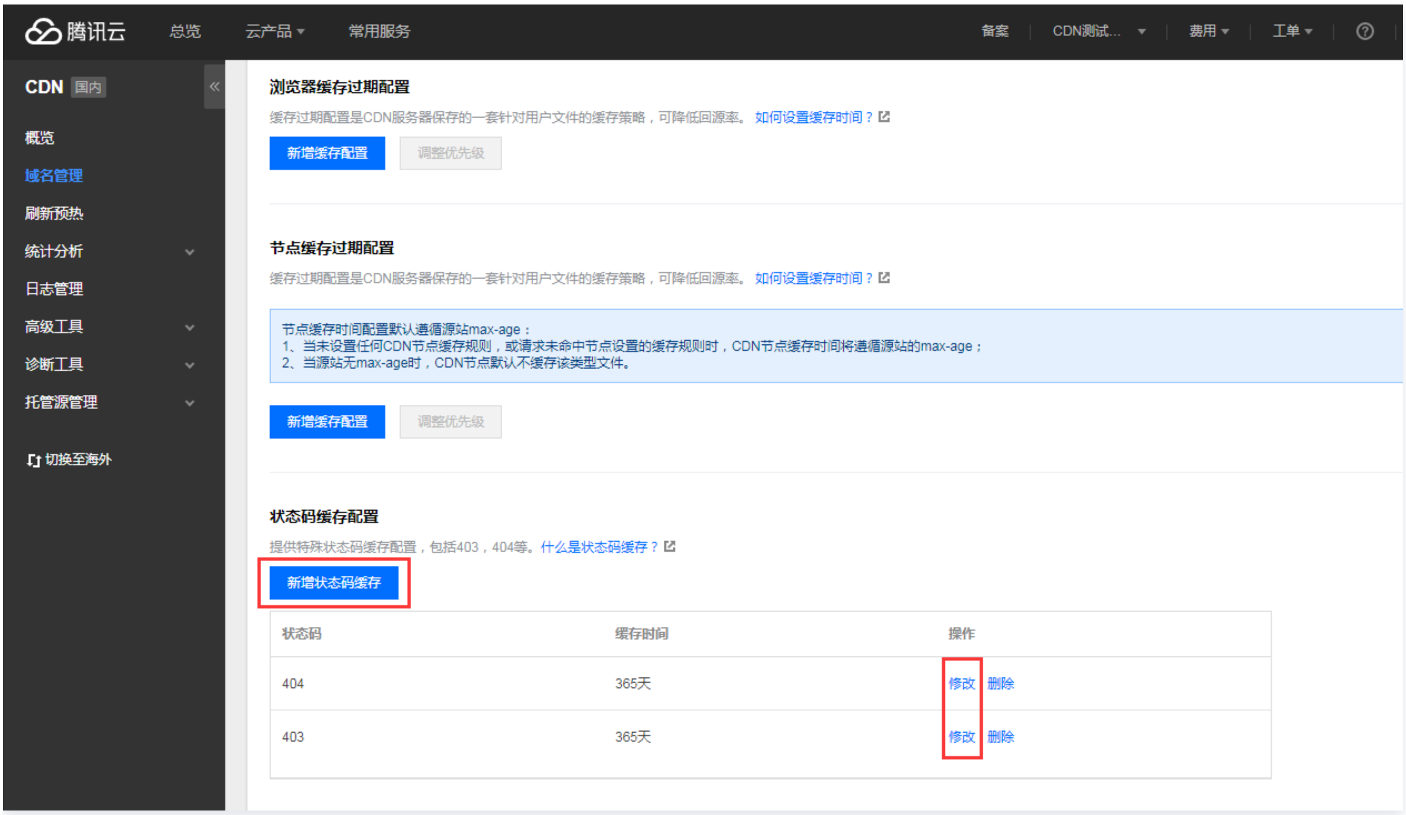
Header Cache

When resources hit the cache at the node, CDN will cache the following headers from the origin server by default and return them to users.

- Access-Control-Allow-Origin
- Timing-Allow-Origin
- Content-Disposition
- Accept-Ranges

Status Code Cache

When the CDN node requests resources from the origin server, in addition to the above caching strategies, it will also cache according to your configured caching strategy when the status code is 403 or 404:
You can adjust the 403 and 404 cache time in the [Cache Configuration] under the [Status Code Cache] module:



浏览器缓存过期配置

缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 如何设置缓存时间？

节点缓存过期配置

缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 如何设置缓存时间？

节点缓存时间配置默认遵循源站max-age：
1、当未设置任何CDN节点缓存规则，或请求未命中节点设置的缓存规则时，CDN节点缓存时间将遵循源站的max-age；
2、当源站无max-age时，CDN节点默认不缓存该类型文件。

状态码缓存配置

提供特殊状态码缓存配置，包括403，404等。什么是状态码缓存？

状态码	缓存时间	操作
404	365天	修改 删除
403	365天	修改 删除

The 403 and 404 status code cache time can be adjusted to 0 to 365 days.
Note: If the cache expiration time for the file is 0, after generating 403/404, it will still follow the no-cache principle and direct pass-through.

Back-to-origin Configurations
Range GETs Configuration

Last updated: 2024-12-31 17:38:52

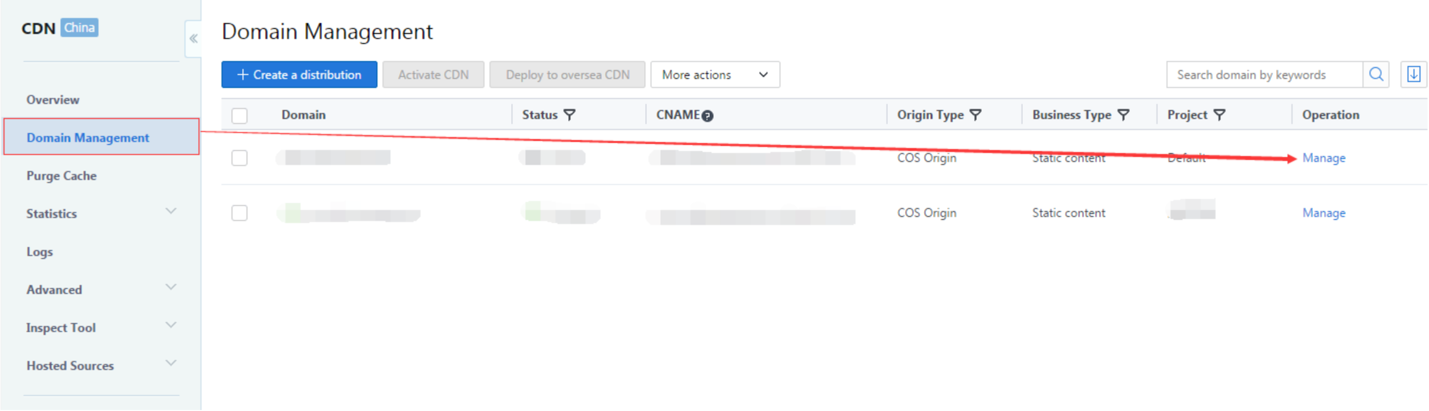
Overview

CDN provides Range GETs Configuration feature which can effectively reduce back-to-origin rate of large files and improve response speed.

The origin server is required to support Range requests

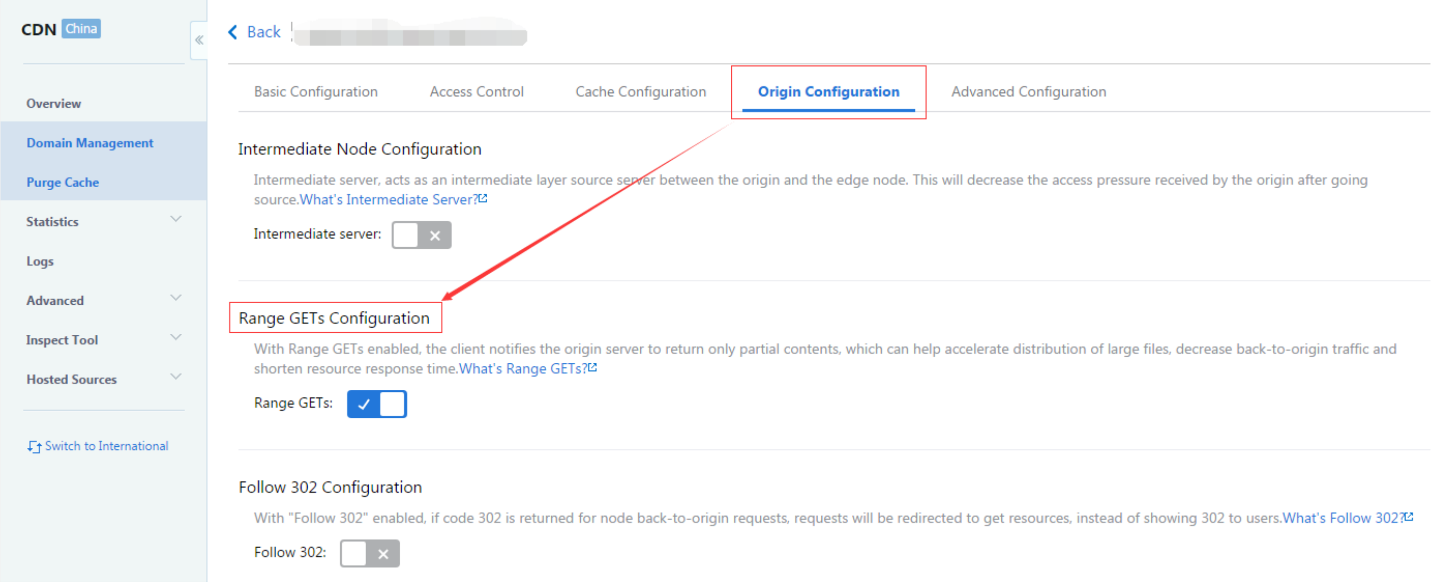
Configuration Instructions

Log in to CDN Console and go to "Domain Management" page. Then click **Manage** button to the right of the domain name to enter the management page:



Domain	Status	CNAME	Origin Type	Business Type	Project	Operation
[illegible]	[illegible]	[illegible]	COS Origin	Static content	Default	Manage
[illegible]	[illegible]	[illegible]	COS Origin	Static content	[illegible]	Manage

You can find **Range GETs Configuration** in "Origin Configuration":



Intermediate Node Configuration

Intermediate server, acts as an intermediate layer source server between the origin and the edge node. This will decrease the access pressure received by the origin after going source.What's Intermediate Server?

Intermediate server: ☒

Range GETs Configuration

With Range GETs enabled, the client notifies the origin server to return only partial contents, which can help accelerate distribution of large files, decrease back-to-origin traffic and shorten resource response time.What's Range GETs?

Range GETs: ✓

Follow 302 Configuration

With "Follow 302" enabled, if code 302 is returned for node back-to-origin requests, requests will be redirected to get resources, instead of showing 302 to users.What's Follow 302?

Follow 302: ☒

Default Configuration

By default, Range GETs Configuration is **Enabled**.

Result of Configuration

If a user makes a request for resource: `http://www.test.com/test.apk` when the node receives the request and finds out that the cached test.apk has expired, it will send a back-to-origin request.

When Range GETs Configuration is enabled:

- The node will use a Range back-to-origin request to acquire the resource in slices.
- If the request sent from the user is also a Range request, when the slices stored on the node meet the condition, they will be directly returned to the user, who needs not to wait for all slices.

When Range GETs Configuration is disabled:

- The node will get the entire resource directly from the origin server

Note:

- The origin server is required to support Range requests, otherwise the back-to-origin request will fail;
- If the resource has never been cached on this node, the resource will not be returned in slices for the initial back-to-origin request;
- When Range GETs Configuration is enabled, resources will be cached in slices on the node, but all slices have the same cache expiration time and follow the cache expiration rule specified by the user.

Follow 302 Configuration

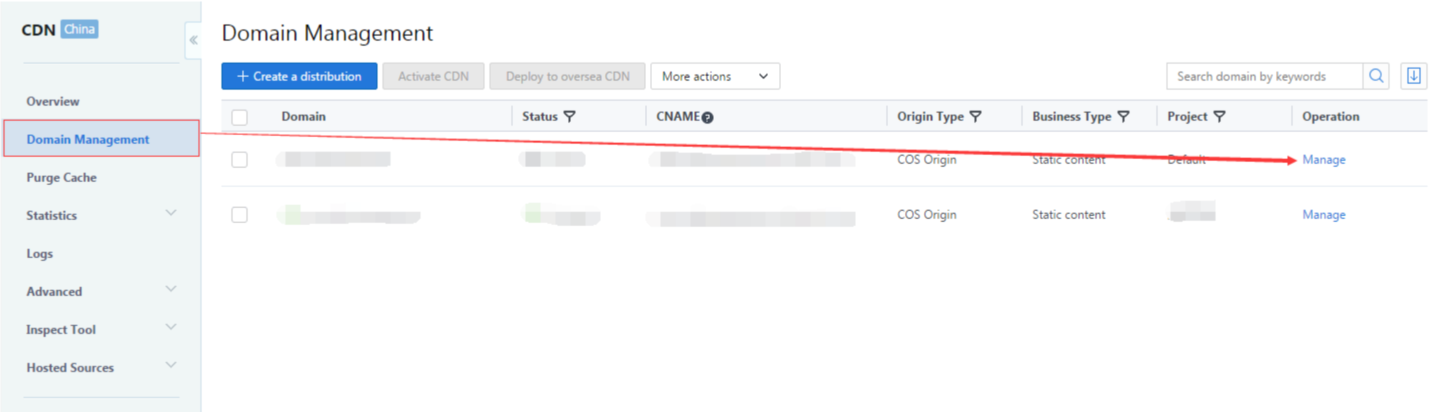
Last updated：2024-12-31 17:39:00

Overview

CDN provides "Follow 302 Configuration" feature.

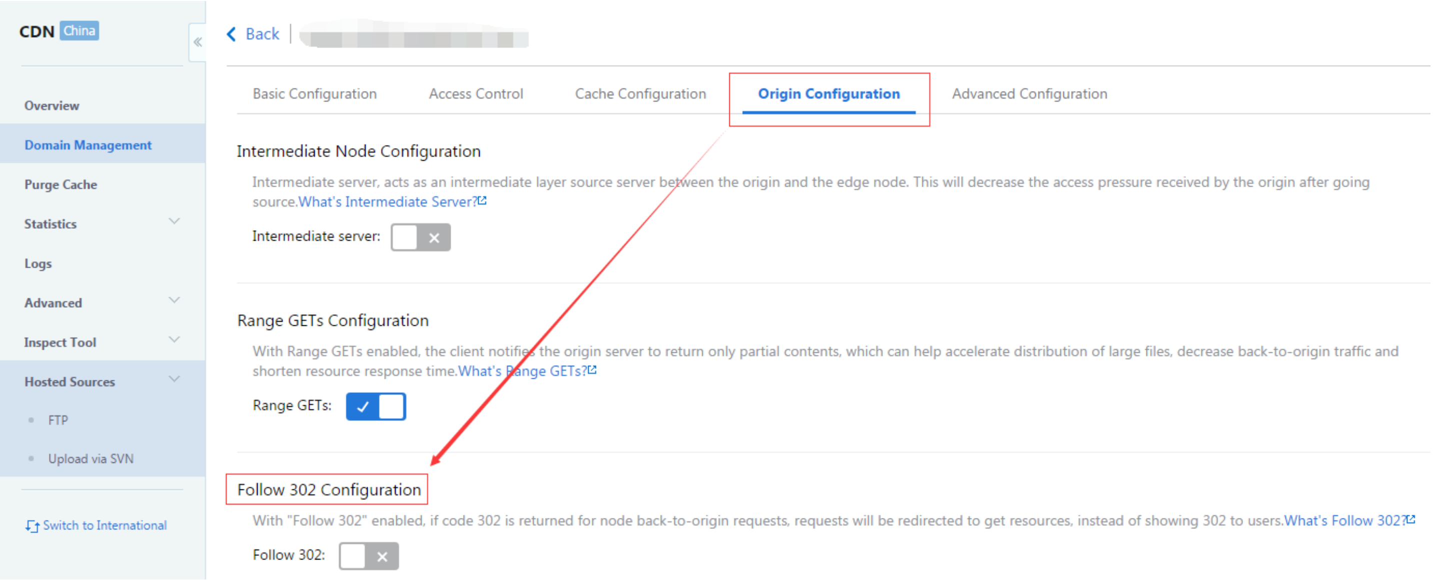
Configuration Instructions

Log in to CDN Console and go to "Domain Management" page. Then click **Manage** button to the right of the domain name to enter the management page:



Domain	Status	CNAME	Origin Type	Business Type	Project	Operation
[redacted]	[redacted]	[redacted]	COS Origin	Static content	Default	Manage
[redacted]	[redacted]	[redacted]	COS Origin	Static content	[redacted]	Manage

You can find **Follow 302 Configuration** in "Origin Configuration":



Intermediate Node Configuration

Intermediate server, acts as an intermediate layer source server between the origin and the edge node. This will decrease the access pressure received by the origin after going source.What's Intermediate Server?

Intermediate server: ✕

Range GETs Configuration

With Range GETs enabled, the client notifies the origin server to return only partial contents, which can help accelerate distribution of large files, decrease back-to-origin traffic and shorten resource response time.What's Range GETs?

Range GETs: ✓

Follow 302 Configuration

With "Follow 302" enabled, if code 302 is returned for node back-to-origin requests, requests will be redirected to get resources, instead of showing 302 to users.What's Follow 302?

Follow 302: ✕

Default Configuration

By default, Follow 302 Configuration is **disabled**.

Result of Configuration

For example, if a user requests for resource `http://www.test1.com/1.jpg` and the resource isn't cached on the node, the node will request to acquire the resource from the origin server. If the HTTP Response status code sent from the origin server is 302, the request will be redirected to `http://www.test2.com/2.jpg`.

When Follow 302 Configuration is disabled:

- Since the resource is not cached in cased of status code 302, the node will directly transmit the HTTP Response to the user.

- When a user sends request to `http://www.test2.com/2.jpg`, there will be no acceleration if this domain is not connected to CDN.
- If another user sends a request to `http://www.test1.com/1.jpg` at this point, the above process will be repeated.

When Follow 302 Configuration is enabled:

- When Follow 302 Configuration is enabled, the node will directly request for the resource if it receives the status code 302 as HTTP Response.
- The resource will be acquired, cached to the node and then returned to the user.
- If another user also sends a request for `http://www.test2.com/1.jpg`, the resource will be hit on this node.

Note:

- When Follow 302 Configuration is enabled, a maximum of **3 redirections** are allowed. If the limit is exceeded, status code 302 will be returned directly to the user.

Origin-pull Timeout

Last updated：2024-12-31 17:39:25

Configuration Scenario

The origin timeout includes TCP connection time configuration and origin load time configuration:

- TCP connection time: refers to the TCP connection timeout period, which defaults to 5 seconds and can be set up to 60 seconds;
- Origin load time: refers to the data load timeout period after a successful TCP connection, which defaults to 10 seconds and can be set up to 300 seconds.

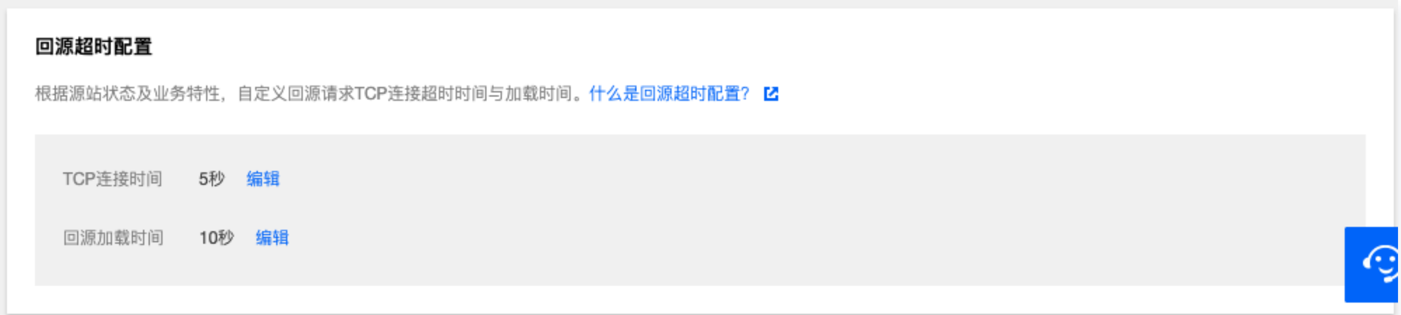
With a short origin timeout, origin failure situations may occur due to network issues. If the origin timeout is set too long, failed requests may occupy connections for a long time due to the website's data processing limitations, causing normal requests to become inaccessible. It is recommended to adjust the origin TCP connection timeout and origin data load timeout according to your origin server data processing conditions and network environment to ensure normal origin.

Configuration Guide

Viewing Configuration

Log in to the CDN console, select **Domain Name Management** from the menu bar, click **Management** on the right side of the domain name to enter the domain configuration page, and you can see the origin timeout configuration in **Origin-pull Configuration**. By default:

- The TCP connection timeout period is 5 seconds.
- The origin-pull loading timeout period is 10 seconds.



回源超时配置

根据源站状态及业务特性，自定义回源请求TCP连接超时时间与加载时间。什么是回源超时配置?

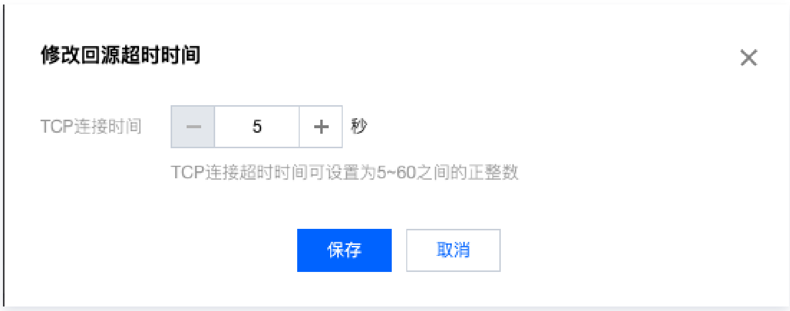
TCP连接时间 5秒 编辑

回源加载时间 10秒 编辑

Modify

By clicking **Edit** on the right, you can modify the corresponding timeout as needed:

- The TCP connection timeout period can be set to 5-60 seconds.

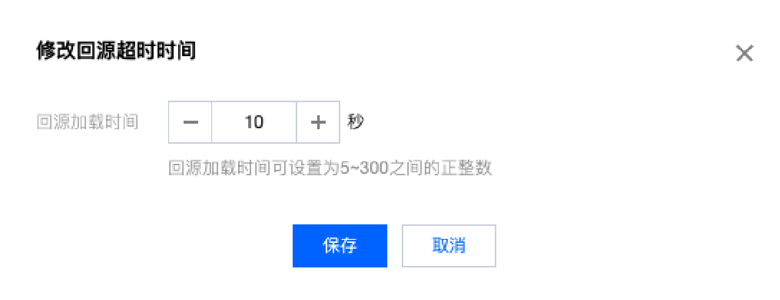


修改回源超时时间

TCP连接时间 5 秒

TCP连接超时时间可设置为5~60之间的正整数

- The origin-pull loading timeout period can be set to 5-300 seconds.



修改回源超时时间

回源加载时间 10 秒

回源加载时间可设置为5~300之间的正整数

Note

If your acceleration domain name is configured for global acceleration, the configured origin-pull timeout period will take effect globally. This configuration does not distinguish between requests from Mainland China and from outside Mainland China.

Origin Request Header Configuration

Last updated：2024-12-31 17:39:36

Feature Introduction

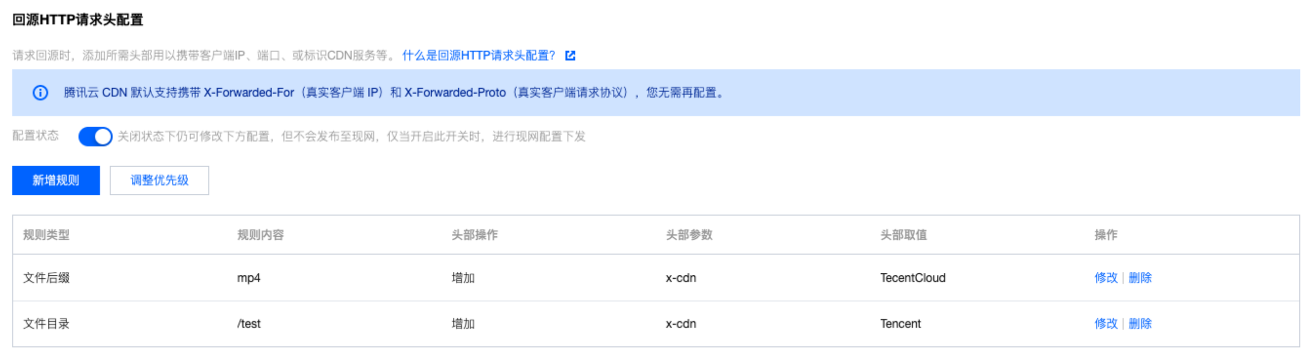
Tencent Cloud CDN supports carrying some headers by default for origin-pull and also allows custom configuration of origin HTTP request headers for statistics and analysis of origin server business conditions.

> **Note**
> - Tencent Cloud CDN supports carrying X-Forwarded-For (real client IP) and X-Forwarded-Proto (real client request protocol) by default, so you do not need to configure them again.
> - If you have configured the X-Forward-For header for all files, it is recommended to delete this rule and use the default standard header X-Forwarded-For **(note the change in the header parameter name)**.
> - Domains created after December 6, 2021, will be configured with the Tencent-Acceleration-Domain-Name (acceleration domain name) header by default, which you can modify or delete in the configuration.
> - If your origin link includes CLB load balancing products or other Nginx proxies, avoid configuring the X-Real-IP request header. For details, refer to: How to configure origin HTTP request headers when the origin link includes CLB load balancing?

Operation Guide

Viewing Configuration

Log in to the cdn console, select **domain name management** from the menu bar, click **management** on the right side of the domain name, and you will see the origin HTTP request header configuration in the **origin-pull configuration**, which is disabled by default with no configuration:



回源HTTP请求头配置

请求回源时，添加所需头部用以携带客户端IP、端口、或标识CDN服务等。 什么是回源HTTP请求头配置？

腾讯云 CDN 默认支持携带 X-Forwarded-For（真实客户端 IP）和 X-Forwarded-Proto（真实客户端请求协议），您无需再配置。

配置状态 ● 关闭状态下仍可修改下方配置，但不会发布至现网，仅当开启此开关时，进行现网配置下发

规则类型	规则内容	头部操作	头部参数	头部取值	操作
文件后缀	mp4	增加	x-cdn	TecentCloud	修改 | 删除
文件目录	/test	增加	x-cdn	Tencent	修改 | 删除

Operation Type

Operation Type	Description
Settings	Change the value of the specified request header parameter to the set value. If the specified header does not exist, it will be added. If an origin header with the same name already exists, the original value will be overwritten.
Increased	Add specified origin request header parameter. If a header with the same name already exists, the new value will be appended.
Delete	Delete specified request header parameter.

> **Note**
> - Bottom priority is higher than top - This relative position priority is limited to the same type header operation, such as among multiple add header rules, multiple delete header rules, or multiple set header rules. (Note: Unordered list content)
> - When different types of header operations act on the same origin request header parameter simultaneously, they are executed according to the priority of the operation types in the order: add > delete > set. For example, if there are rules to

add, delete, and set the X-CDN header at the same time, it will first add, then delete, and finally set. (Note: Unordered list content)

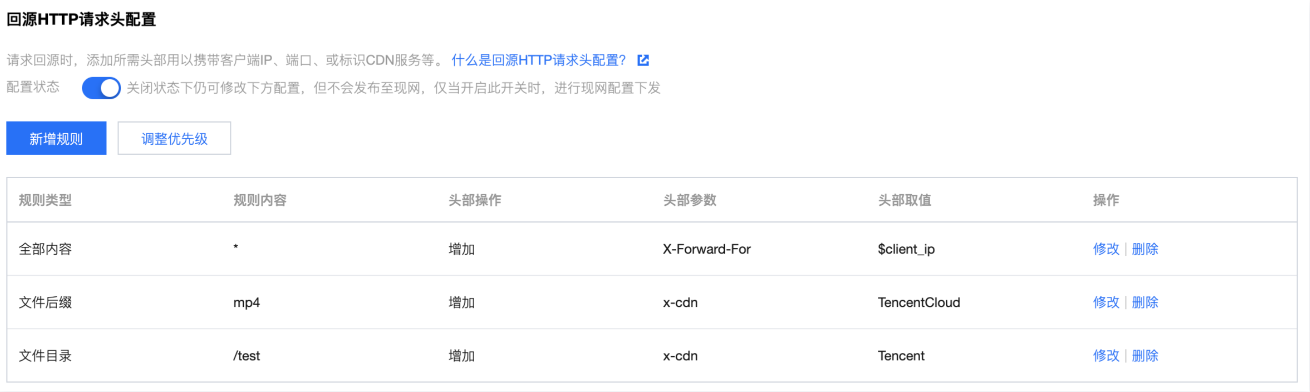
Header Parameter

Header Parameter	Description
X-Forward-Port	Used to carry the real client port header. Its value defaults to the $remote_port variable and cannot be modified.
Tencent-Acceleration-Domain-Name	The header used to carry user acceleration domain name has a value of $host variable.
Custom header	The default length of the custom header key is 1-100 characters, consisting of digits 0-9, letters a-z, A-Z, and the special character `-` . The value length is 1-2000 characters, Chinese is not supported. If the header value is a variable, currently only $remote_port and $client_ip are supported. Some standard headers do not support self-service setting/adding/deleting. For the specific list, please refer to the document Must-Knows.

> **Note**
> - Up to 10 rules can be configured for the origin HTTP request header configuration.
> - Supported effect types: all content, file extension, file directory, and specified file. Regular matching is currently not supported.

Configuration Example

If the request header configuration of the accelerated domain `cloud.tencent.com` is as follows:



回源HTTP请求头配置

请求回源时，添加所需头部用以携带客户端IP、端口、或标识CDN服务等。 什么是回源HTTP请求头配置?

配置状态 ● 关闭状态下仍可修改下方配置，但不会发布至现网，仅当开启此开关时，进行现网配置下发

规则类型	规则内容	头部操作	头部参数	头部取值	操作
全部内容	*	增加	X-Forward-For	$client_ip	修改 | 删除
文件后缀	mp4	增加	x-cdn	TencentCloud	修改 | 删除
文件目录	/test	增加	x-cdn	Tencent	修改 | 删除

If accessing the resource: `http://cloud.tencent.com/test/test.mp4`
Matching `mp4` file suffix and `/test` directory, since it is the same header operation type - add, the bottom priority is greater than the top, thus adding `x-cdn:Tencent` header.

Notes

The following standard headers are temporarily not supported for setting/adding/deleting request headers:

www-authenticate	authorization	proxy-authenticate	proxy-authorization
age	cache-control	clear-site-data	expires
pragma	warning	accept-ch	accept-ch-lifetime
early-data	content-dpr	dpr	device-memory
save-data	viewport-width	width	last-modified

etag	if-match	if-none-match	if-modified-since
if-unmodified-since	vary	connection	keep-alive
accept	accept-charset	expect	max-forwards
access-control-allow-origin	access-control-max-age	access-control-allow-headers	access-control-allow-methods
access-control-expose-headers	access-control-allow-credentials	access-control-request-headers	access-control-request-method
origin	timing-allow-origin	dnt	tk
content-disposition	content-length	content-type	content-encoding
content-language	content-location	forwarded	x-forwarded-host
x-forwarded-proto	via	from	host
referer-policy	allow	server	accept-ranges
range	if-range	content-range	cross-origin-embedder-policy
cross-origin-opener-policy	cross-origin-resource-policy	content-security-policy	content-security-policy-report-only
expect-ct	feature-policy	strict-transport-security	upgrade-insecure-requests
x-content-type-options	x-download-options	x-frame-options(xfo)	x-permitted-cross-domain-policies
x-powered-by	x-xss-protection	public-key-pins	public-key-pins-report-only
sec-fetch-site	sec-fetch-mode	sec-fetch-user	sec-fetch-dest
last-event-id	nel	ping-from	ping-to
report-to	transfer-encoding	te	trailer
sec-websocket-key	sec-websocket-extensions	sec-websocket-accept	sec-websocket-protocol
sec-websocket-version	accept-push-policy	accept-signature	alt-svc
date	large-allocation	link	push-policy
retry-after	signature	signed-headers	server-timing
service-worker-allowed	sourcemap	upgrade	x-dns-prefetch-control
x-firefox-spdy	x-pingback	x-requested-with	x-robots-tag
x-ua-compatible	max-age		

Origin URL Rewriting

Last updated：2024-12-31 17:39:48

If you need to modify the origin-pull request URL to the URL that matches the origin server, you can use the origin URL rewrite configuration in Tencent Cloud CDN.

Applicable scenario

1. The resource path on the origin server has changed, but users still request using the original URL. You can use origin URL rewrite to point the original URL to the new resource path.
2. The same resource is reused across multiple sites within the origin server. You can use origin URL rewrite to point the resource to the specified resource path.

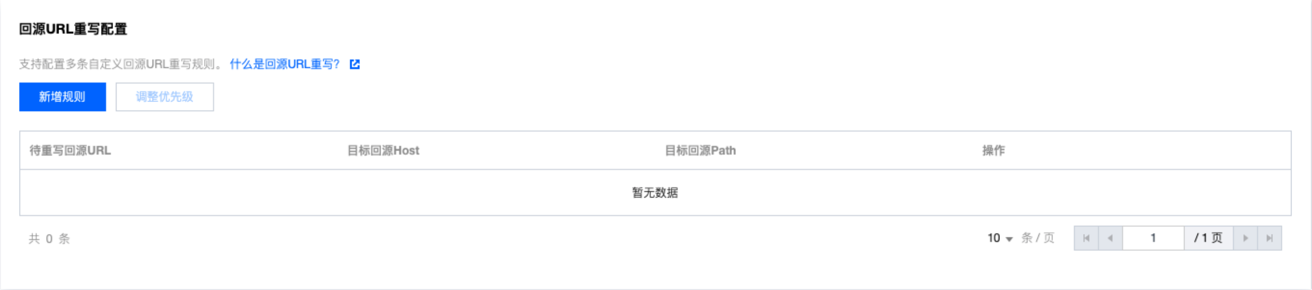
Notes

1. This feature configuration is not available for ECDN domain name.
2. If you need to specify different path files to point to different origin servers, you can use the Advanced Origin-pull Configuration feature. Advanced Origin-pull Configuration supports pointing to the specified origin server based on client IP, file suffix, file directory, full path file, home page, and other rules.
3. If you have multiple origin servers configured with different path origin rules, you can use origin URL rewrite to achieve path-based origin while rewriting the origin URL path. Therefore, when using origin URL rewrite, please ensure whether Advanced Origin-pull Configuration is set to prevent inaccurate origin pointing, causing access failure.

Configuration Instructions

Configuration in domain management

1. Log in to the CDN Console.
2. Click **Domain Management** in the left menu to enter the domain management list;
3. Select the domain to configure and click **Management** to enter the domain configuration page;
4. Click **Origin-pull Configuration** to switch to the Origin-pull Configuration tab. In the tab, you can see the Origin-pull URL Rewrite configuration item;



回源URL重写配置

支持配置多条自定义回源URL重写规则。什么是回源URL重写？

待重写回源URL	目标回源Host	目标回源Path	操作
暂无数据			

5. Click **add new rule** to add a new Origin-pull URL Rewrite configuration rule. Fill in the constraints within the rule as follows:

Configuration Item	Description
Match settings	1. The default is prefix matching. For example, if the origin-pull URL to be rewritten is /test, it will match all files under the /test path. 2. If full path matching is selected, it will precisely match the specified file path. For example, if the origin-pull URL to be rewritten is /test/a.jpg, it will precisely match the /test/a.jpg file.
Origin-pull URL to be rewritten	1. Starting with /, the default is prefix matching, supporting the use of wildcard * for matching (e.g., /test/*/*.jpg). If a specified file directory is used, it should not end with "/" (e.g., /test). 2. Wildcard * can also be used to match URL parameters. For example, if the URL is /test/a.jpg?imageMogr2/thumbnail/!50px, you can use /test/a.jpg*, where the wildcard * represents all parameters after the question mark. 3. In full path matching mode, wildcard * is not supported.

Target origin host	The origin host specifies the specific site accessed on the origin server by the origin pull request, defaulting to the current origin host. 1. If your origin target is Tencent Cloud COS or a third-party object storage, it is recommended to specify the origin host to be consistent with the current origin host; otherwise, it may cause origin fetch failure. 2. If your origin-pull target is another site within your own server origin server, you can change the Host header to the domain name of the corresponding site, excluding `http://` or `https://` prefixes.
Target origin path	Starting with / (e.g., /newtest/b.jpg), wildcard * can be captured by $n (n=1,2,3....), for example: If the origin-pull URL to be rewritten is configured as /test/*/*.jpg and the target origin path is configured as /newtest/$1/$2.jpg, then when the user access request's origin-pull URL is /test/a/b.jpg, $1 will capture the first wildcard content, which is a; $2 will capture the second wildcard content, which is b. The actual origin-pull URL will be rewritten to /newtest/a/b.jpg.

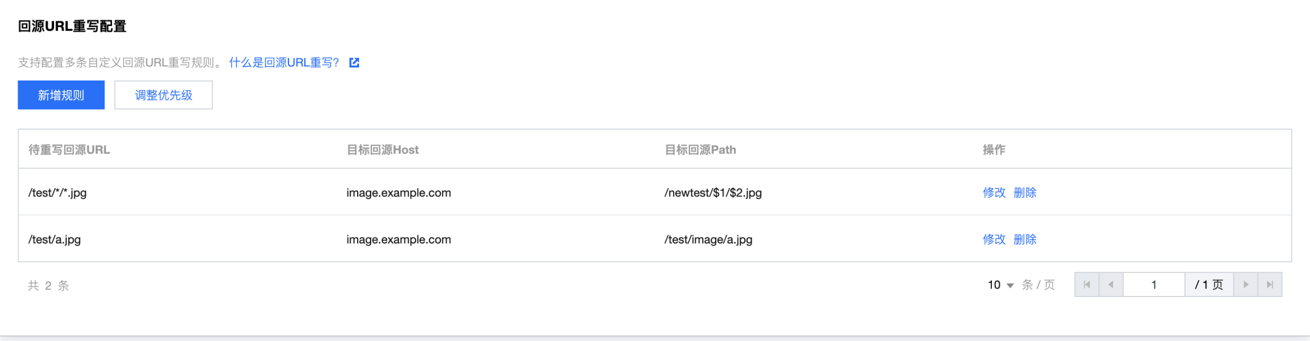
Configuration limitations

- Each domain name can have up to 100 rewrite rules;
- Up to 5 wildcards `*` and 10 capture placeholders `$n` are supported, other regex matching conditions are not supported.
- You can adjust the priority for multiple rules. Rules at the bottom of the list have higher priority.

Configuration Example

Sample 1

User access domain: example.com, origin server address: 1.1.1.1, origin-pull rule configuration as follows:



回源URL重写配置

支持配置多条自定义回源URL重写规则。 什么是回源URL重写？

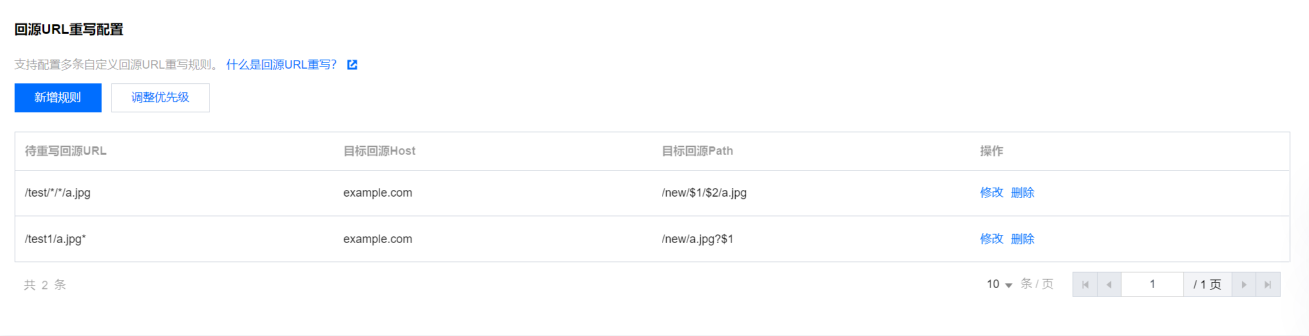
待重写回源URL	目标回源Host	目标回源Path	操作
/test/*/*.jpg	image.example.com	/newtest/$1/$2.jpg	修改 删除
/test/a.jpg	image.example.com	/test/image/a.jpg	修改 删除

共 2 条

- When the user accesses the URL: `http://example.com/test/a.jpg` , it hits the bottom rule. According to the specified HOST configuration, the origin-pull will point to the resource in the `image.example.com` site on the origin server 1.1.1.1. The final origin access path will be `http://image.example.com/test/image/a.jpg` on the 1.1.1.1 server.
- When the user accesses the URL: `http://example.com/test/a/b.jpg` , it hits the top rule. According to the specified HOST configuration, the origin-pull will point to the resource in the `image.example.com` site on the origin server 1.1.1.1. Based on the wildcard capture rule, the final origin access path will be `http://image.example.com/newtest/a/b.jpg` on the 1.1.1.1 server.

Sample 2

User access domain: example.com, origin server address: 1.1.1.1, origin URL rewrite rule configuration as follows:



回源URL重写配置

支持配置多条自定义回源URL重写规则。 什么是回源URL重写？

待重写回源URL	目标回源Host	目标回源Path	操作
/test/*/*/a.jpg	example.com	/new/$1/$2/a.jpg	修改 删除
/test1/a.jpg*	example.com	/new/a.jpg?$1	修改 删除

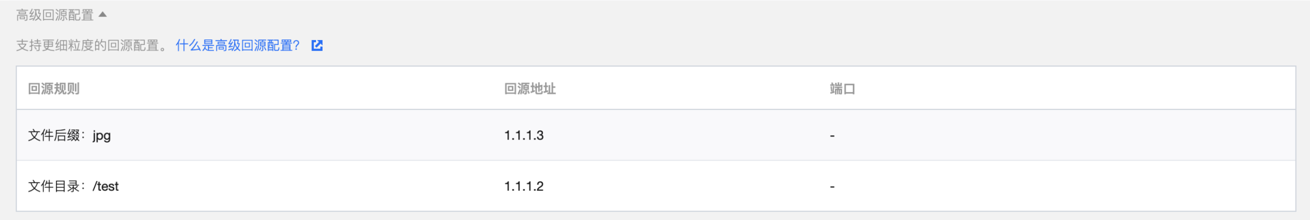
共 2 条

- When the user accesses the URL: `http://example.com/test/a/b/a.jpg` , it hits the top rule. According to the specified HOST configuration, the origin-pull will point to the resource in the example.com site on the origin server 1.1.1.1. By capturing all content of the wildcard * through $1 $2, the final origin access path will be `http://example.com/new/a/b/a.jpg` on the 1.1.1.1 server.

- When the user accesses the URL: `http://example.com/test1/a.jpg?imageMogr2/thumbnail/!50px` , it hits the bottom rule. According to the specified HOST configuration, the origin-pull will point to the resource in the example.com site on the origin server 1.1.1.1. By capturing all content of the wildcard * through $1, including the parameters carried by the original URL, the final origin access path will be `http://example.com/new/a.jpg?imageMogr2/thumbnail/!50px` on the 1.1.1.1 server.

Example 3

User access domain: example.com, and the advanced origin rule is configured as follows:

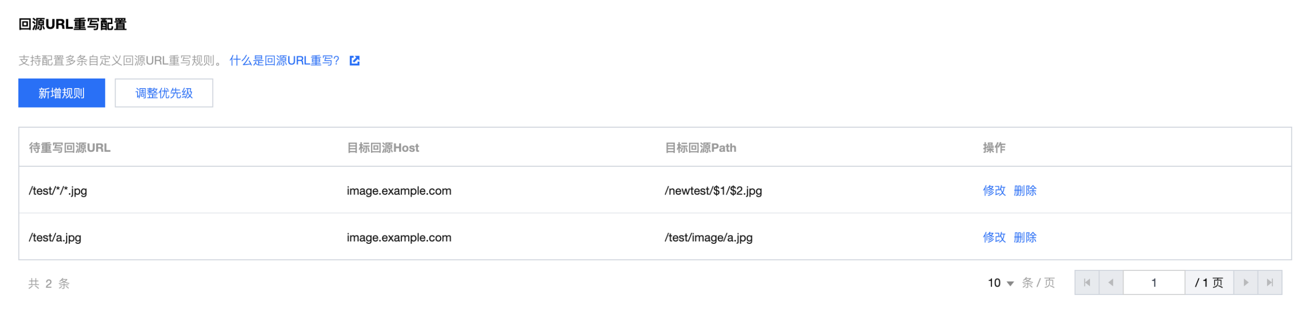


高级回源配置 ▲

支持更细粒度的回源配置。什么是高级回源配置？

回源规则	回源地址	端口
文件后缀：jpg	1.1.1.3	-
文件目录：/test	1.1.1.2	-

At the same time, the origin URL rewrite rule is configured as follows:



回源URL重写配置

支持配置多条自定义回源URL重写规则。什么是回源URL重写？

待重写回源URL	目标回源Host	目标回源Path	操作
/test/*/*.jpg	image.example.com	/newtest/$1/$2.jpg	修改 删除
/test/a.jpg	image.example.com	/test/image/a.jpg	修改 删除

共 2 条

- When the user accesses the URL: `http://example.com/test/a.jpg` , due to the advanced origin rule configuration, the bottom priority is highest, and the priority match directory origin rule is applied. This request will be directed to the origin server 1.1.1.2. Additionally, due to the origin URL rewrite rule, it matches the bottom rule. According to the specified origin HOST configuration, the origin-pull will point to the resource in the `image.example.com` site on the origin server 1.1.1.2. Therefore, the final origin access path will be `http://image.example.com/test/image/a.jpg` on the 1.1.1.2 server.
- When the user accesses the URL: `http://example.com/test/a/b.jpg` , due to the advanced origin rule configuration, it hits the file suffix rule. This request will be directed to the origin server 1.1.1.3. Additionally, due to the origin URL rewrite configuration rule, it matches the first rule. According to the specified HOST configuration, the origin-pull will point to the resource in the `image.example.com` site on the origin server 1.1.1.3. Based on the wildcard capture rule, the final origin access path will be: `http://image.example.com/newtest/a/b.jpg` on the 1.1.1.3 server.

Origin-pull SNI

Last updated：2024-12-31 17:39:59

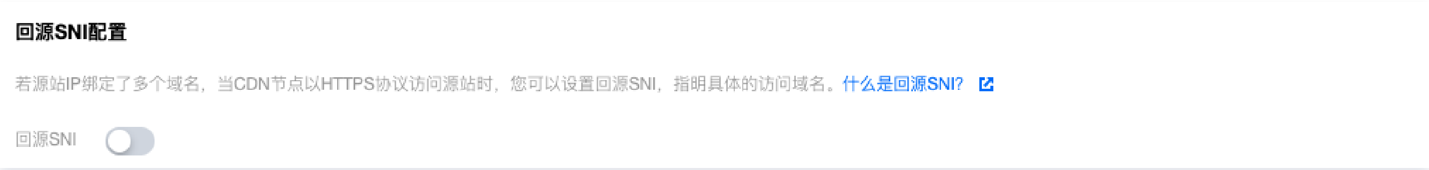
Configuration Scenario

If an origin server IP is bound with multiple domain names, you can set the origin-pull SNI to specify a domain name for CDN nodes to access the origin server via HTTPS.

Configuration Guide

View Configuration

Origin-pull SNI is disabled by default. You can enable it for your needs.



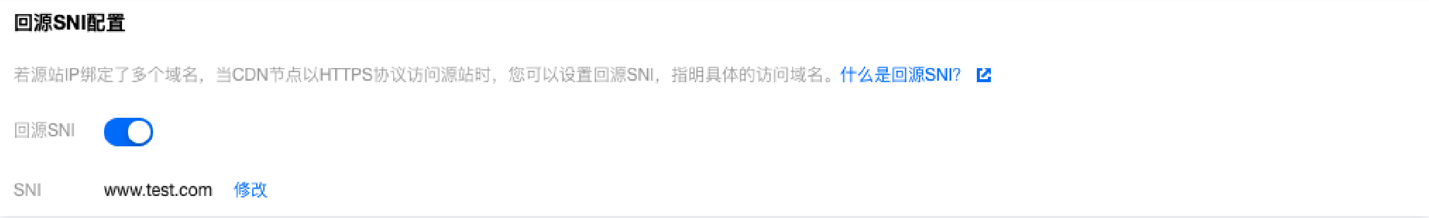
回源SNI配置

若源站IP绑定了多个域名，当CDN节点以HTTPS协议访问源站时，您可以设置回源SNI，指明具体的访问域名。什么是回源SNI?

回源SNI ○

Editing Configuration

After it’s enabled, you need to set the origin SNI and configure the specific access domain name. You can also turn off the configuration switch. When the switch is off, even if there is a specific configuration below, it will not take effect on the live network. Only when the switch is turned on will it be published to the live network.



回源SNI配置

若源站IP绑定了多个域名，当CDN节点以HTTPS协议访问源站时，您可以设置回源SNI，指明具体的访问域名。什么是回源SNI?

回源SNI ●

SNI www.test.com 修改

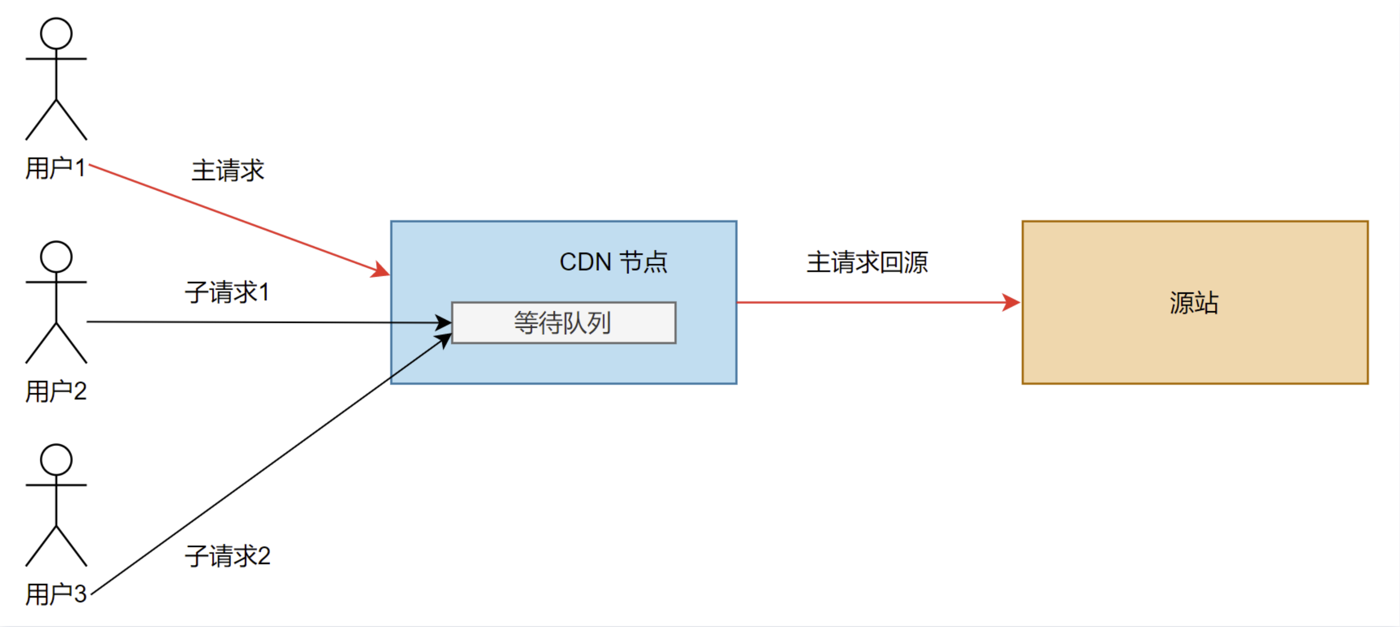
Merge Back to Source Configuration

Last updated：2024-12-31 17:40:12

Origin-pull merging can help increase the cache hit rate and reduce the load pressure for business scenarios with high resource demand and concurrent requests, such as big online promotion events.

Feature Introduction

When multiple users concurrently request the same resource that is not cached on the CDN node, all requests will trigger a pull from the origin, leading to a surge in origin bandwidth and connections. If the origin server has performance bottlenecks, it may result in slow or failed responses from the origin, ultimately affecting the user access experience. Origin-pull merge means that multiple requests for the same resource at the same time will only trigger one pull from the origin if the resource is not cached on the node, while other users wait for the response of the origin-pull request. This feature can effectively alleviate the pressure on the origin server and improve the user hit rate. As shown in the figure below, when three users simultaneously request the same resource from the same node, the main request will pull the resource from the origin, while other sub-requests enter the waiting queue. Once the main request receives the response from the origin, it will deliver the data to the user of the main request and cache it on the CDN node. At the same time, all sub-requests in the waiting queue are notified, and these sub-requests will read the data from the cache and respond to their respective users.



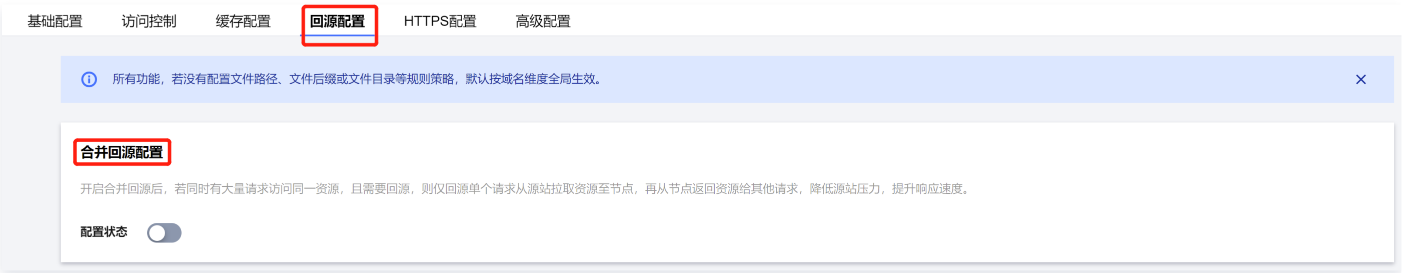
Notes

1. Only merge origin-pull for status code responses 200/206/304.
2. When the origin server returns cache-control: no-cache, no-store, private, or pragma: no-cache, which specifies that the CDN node cannot cache, do not merge origin-pull.
3. Do not merge origin-pull when the origin server returns chunked transfer.
4. Only the GET request method will trigger origin-pull merging.
5. When the http response header from the origin server contains neither content-length nor transfer-encoding, origin-pull merging will not occur.
6. Requests with gzip, br compression will not be merged for origin-pull.

Configuration Instructions

1. Log in to the CDN Console.
2. Click Domain Management in the left menu to enter the domain management list.
3. Select the domain to be configured and click Manage to enter the domain configuration page.

4. Click Origin-pull Configuration to switch to the Origin-pull Configuration tab, where you can see the origin-pull merge configuration item.



所有功能，若没有配置文件路径、文件后缀或文件目录等规则策略，默认按域名维度全局生效。

合并回源配置

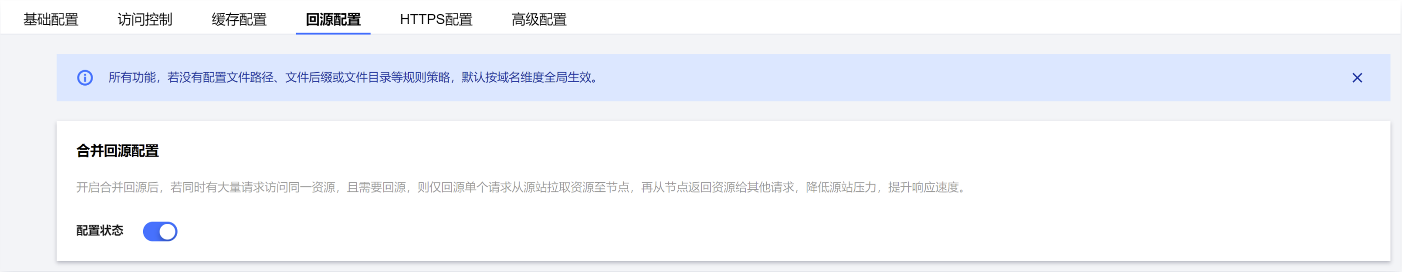
开启合并回源后，若同时有大量请求访问同一资源，且需要回源，则仅回源单个请求从源站拉取资源至节点，再从节点返回资源给其他请求，降低源站压力，提升响应速度。

配置状态

5. Origin-pull merge configuration is disabled by default. You can enable it as needed.

Configuration Example

Enable origin-pull merge.



所有功能，若没有配置文件路径、文件后缀或文件目录等规则策略，默认按域名维度全局生效。

合并回源配置

开启合并回源后，若同时有大量请求访问同一资源，且需要回源，则仅回源单个请求从源站拉取资源至节点，再从节点返回资源给其他请求，降低源站压力，提升响应速度。

配置状态

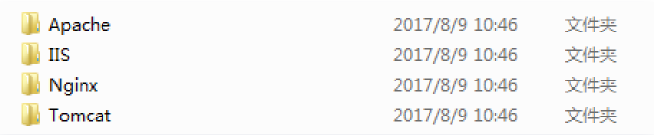
HTTPS Configuration
HTTPS Configuration Notes

Last updated：2024-12-31 17:40:24

If you need to upload and configure a self-owned certificate for your domain, please see below. If the certificate you configure is from Tencent Cloud SSL Certificates Service, you can skip the upload certificate part and directly refer to the content related to managed certificate.

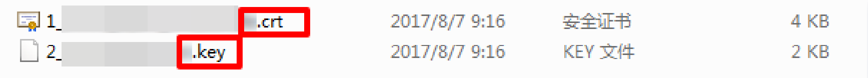
Upload certificate.

The certificates provided by CAs include the following types, of which CDN uses **Nginx**:



Apache	2017/8/9 10:46	文件夹
IIS	2017/8/9 10:46	文件夹
Nginx	2017/8/9 10:46	文件夹
Tomcat	2017/8/9 10:46	文件夹

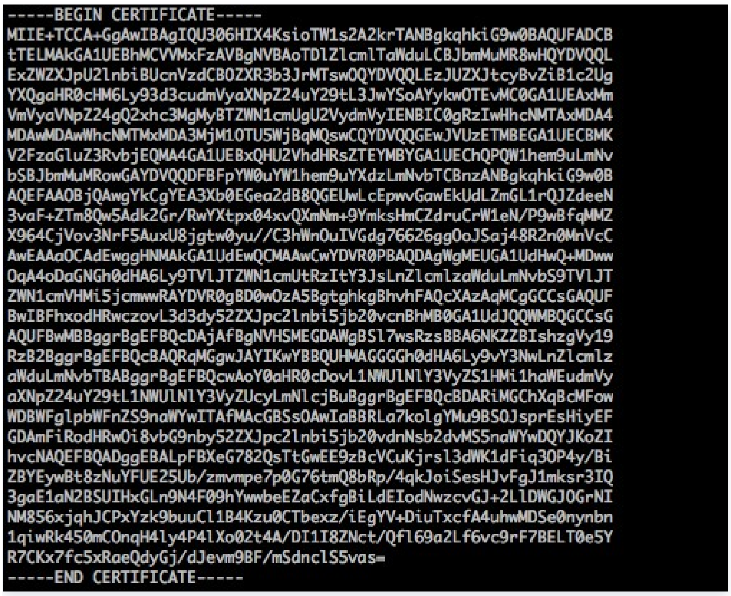
Go to the Nginx folder and open ".crt" (certificate) and ".key" (private key) files with a text editor to view the content of the certificate and private key in PEM format:



1_[redacted].crt	2017/8/7 9:16	安全证书	4 KB
2_[redacted].key	2017/8/7 9:16	KEY 文件	2 KB

Certificate.

Common certificate extensions include ".pem", ".crt", and ".cer". Open a certificate file in a text editor and you can see a certificate similar to the content as shown in the figure below.
A ".pem" certificate begins with "-----BEGIN CERTIFICATE-----" and ends with "-----END CERTIFICATE-----". Every line in between contains 64 characters, while the last line may have less than 64 characters:



```
-----BEGIN CERTIFICATE-----
MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzIwHhcNMTAxMDA4
MDAwMDAwWhcNMTMxMDA3MjM1OTU5WjBqMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
V2FzaGluZ3RvbjEQMA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv
bSBJbmMuMRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWnOuIVGdg76626gg0oJSaj48R2n0MnVcC
AwEAAaOCAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVlJTZWN1cmUtRzItY3JsLnZlcmlzaWduLmNvbS9TVlJT
ZWN1cmVHMi5jcmwwRAYDVR0gBD0wOzA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUF
BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBSl7wsRzsBBA6NKZZBIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWUlNlY3VyZUcyLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFow
WDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEF
GDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq3OP4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2LlDWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

If your certificate is issued by an intermediate CA, your certificate file will consist of multiple certificates. In this case, you need to splice the server certificates and intermediate certificates manually for upload by putting the server certificate content before the intermediate certificate content without any blank lines in between. Please refer to the rules or instructions that came with the certificate.

⚠ **Note**

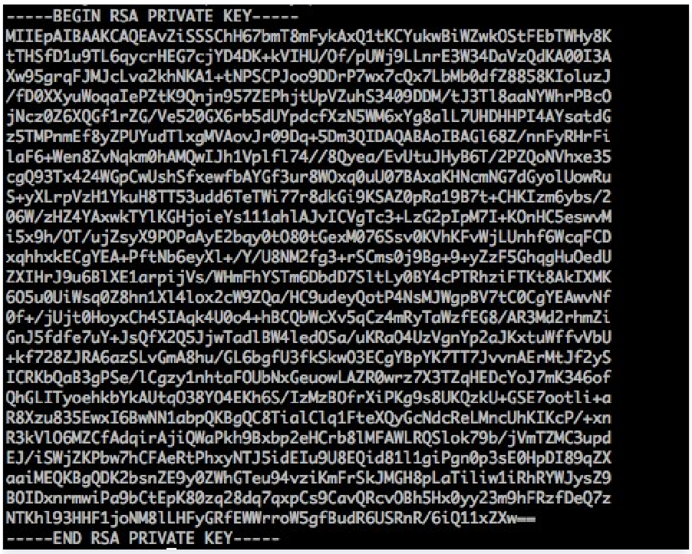
- There should be no blank lines between certificates
- All certificates are in PEM format

The certificate chain issued by an intermediate authority is formatted as follows:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

Private key.

The private key extension is usually ".pem" or ".key". When you open the private key file in a text editor, you will see private key content similar to the format shown below.
Private key PEM format: It starts with "-----BEGIN RSA PRIVATE KEY-----" and ends with "-----END RSA PRIVATE KEY-----". The content in between is 64 characters per line, with the last line possibly being less than 64 characters.



```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAvZiSSSChH67bmT8mFykAxQ1tKCYukwBiWZwkOStFEbTWHy8K
tTHSfD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A
Xw95grqFJMJcLva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ
/fD0XXyuWoqaIePZtK9Qnjn957ZEPhjtUpVZuhS3409DDM/tJ3Tl8aaNYWhrPBcO
jNcz0Z6XQGf1rZG/Ve520GX6rb5dUYpdcfXzN5WM6xYg8alL7UHDHHPI4AYsatdG
z5TMPnmEf8yZPUYudTlxgMVAovJr09Dq+5Dm3QIDAQABAoIBAGl68Z/nnFyRHrFi
laF6+Wen8ZvNqkm0hAMQwIJh1Vplfl74//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35
cgQ93Tx424WGpCwUshSfxewfbAYGf3ur8WOxq0uU07BAxaKHNcmNG7dGyolUowRu
S+yXLrpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2
06W/zHZ4YAxwkTYlKGHjoieYs111ahlAJvICVgTc3+LzG2pIpM7I+KOnHC5eswvM
i5x9h/OT/ujZsyX9POPaAyE2bqy0tO80tGexM076Ssv0KVhKFvWjLUnhf6WcqFCD
xqhhxkECgYEA+PftNb6eyXl+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhqgHuOedU
ZXIHrJ9u6BlXE1arpijVs/WHmFhYSTm6DbdD7SltLy0BY4cPTRhziFTKt8AkIXMK
6O5u0UiWsq0Z8hn1Xl4lox2cW9ZQa/HC9udeyQotP4NsMJWgpBV7tC0CgYEAwvNf
0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzfEG8/AR3Md2rhmZi
GnJ5fdfe7uY+JsQfX2Q5JjwTadlBW4ledOSa/uKRaO4UzVgnYp2aJKxtuWffvVbU
+kf728ZJRA6azSLvGmA8hu/GL6bgfU3fkSkwO3ECgYBpYK7TT7JvvnAErMtJf2yS
ICRKbQaB3gPSe/lCgzy1nhtaFOUbNxGeuowLAZR0wrz7X3TZqHEDcYoJ7mK346of
QhGLITyoehkbYkAUtqO38YO4EKh6S/IzMzBOfrXiPKg9s8UKQzkU+GSE7ootli+a
R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUhKIKcP/+xn
R3kVlO6MZCfAdqirAjiQWaPkh9Bxbp2eHCrb8lMFAWLRQSlok79b/jVmTZMC3upd
EJ/iSWjZKPbw7hCFAeRtPhxyNTJ5idEIu9U8EQid81l1giPgn0p3sE0HpDI89qZX
aaiMEQKBgQDK2bsnZE9y0ZWhGTeu94vziKmFrSkJMGH8pLaTiliw1iRhRYWJysZ9
BOIDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcvOBh5Hx0yy23m9hFRzfDeQ7z
NTKhl93HHF1joNM8lLHFyGRfEWWrroW5gfBudR6USRnR/6iQ11xZXw==
-----END RSA PRIVATE KEY-----
```

If your private key starts with "-----BEGIN PRIVATE KEY-----" and ends with "-----END PRIVATE KEY-----", it is recommended to use the openssl tool for format conversion. The command is as follows:

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

Format conversion

Currently, CDN only supports certificates in PEM format. Certificates in other formats need to be converted to PEM format. It is recommended to use the openssl tool for conversion. Below are methods to convert some popular certificate formats to PEM format.

Converting DER to PEM

DER format is generally used on Java platforms.
Certificate conversion:

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

Private key conversion:

```
openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
```

Converting P7B to PEM

P7B format is generally used on Windows Server and Tomcat.
Certificate conversion:

```
openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer
```

Open outcertificat.cer with a text editor to view the certificate content in PEM format.
Private key conversion: The private key can generally be exported from the IIS server.

Converting PFX to PEM

PFX format is generally used on Windows Server.
Certificate Conversion:

```
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
```

Private key conversion:

```
openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
```

Completing the Certificate Chain

During the process of configuring with your own certificate, the situation where **the certificate chain cannot be completed** may occur. Uploading the certificate via CDN will automatically complete the certificate chain.

Hosted Certificate

Tencent Cloud provides a certificate hosting service: SSL Certificates. You can upload existing certificates to SSL Certificates Service Console for unified hosting and deployment on other Tencent Cloud products. It also allows you to purchase and apply for certificates.
Tencent Cloud SSL Certificates Service provides each user with 20 DV SSL certificates issued by TrustAsia free of charge.

HTTPS Configuration Guide

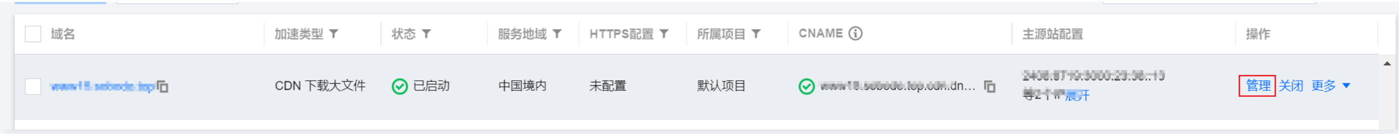
Last updated：2024-12-31 17:40:38

Configuration Scenario

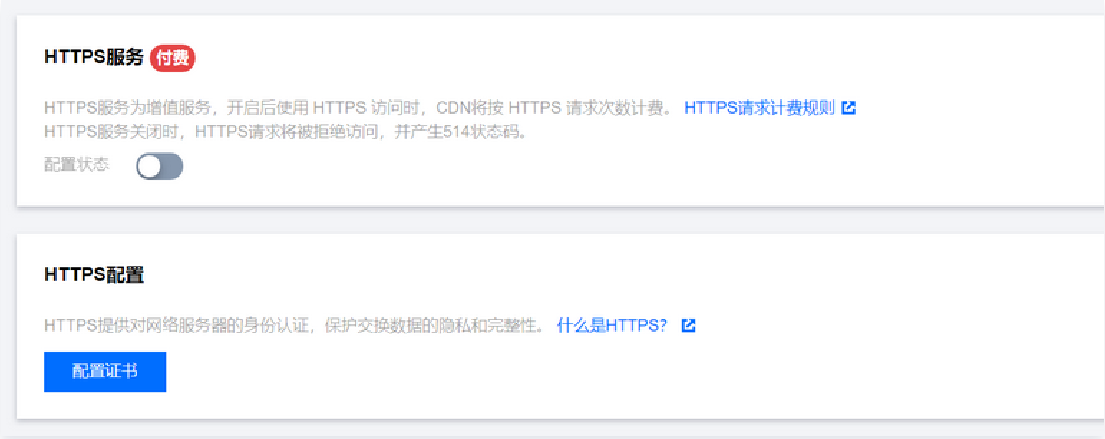
Tencent Cloud CDN supports the HTTPS acceleration service. You can upload certificates to deploy them or directly deploy certificates hosted in Tencent Cloud SSL Certificate Service to the CDN platform. In this way, you can enable the HTTPS acceleration service to implement encrypted data transfer over the entire network.

View Configuration

Log in to the CDN console, select **Domain Management** from the menu bar, click **Management** on the right side of the domain to enter the domain configuration page, and view the HTTPS configuration of the specified domain in **HTTPS Configuration**:



□ 域名	加速类型	状态	服务地域	HTTPS配置	所属项目	CNAME	主源站配置	操作
□ [redacted]	CDN 下载大文件	✓ 已启动	中国境内	未配置	默认项目	✓ [redacted]	[redacted] 展开	管理 关闭 更多 ▾



HTTPS服务 付费

HTTPS服务为增值服务，开启后使用 HTTPS 访问时，CDN将按 HTTPS 请求次数计费。 HTTPS请求计费规则
HTTPS服务关闭时，HTTPS请求将被拒绝访问，并产生514状态码。

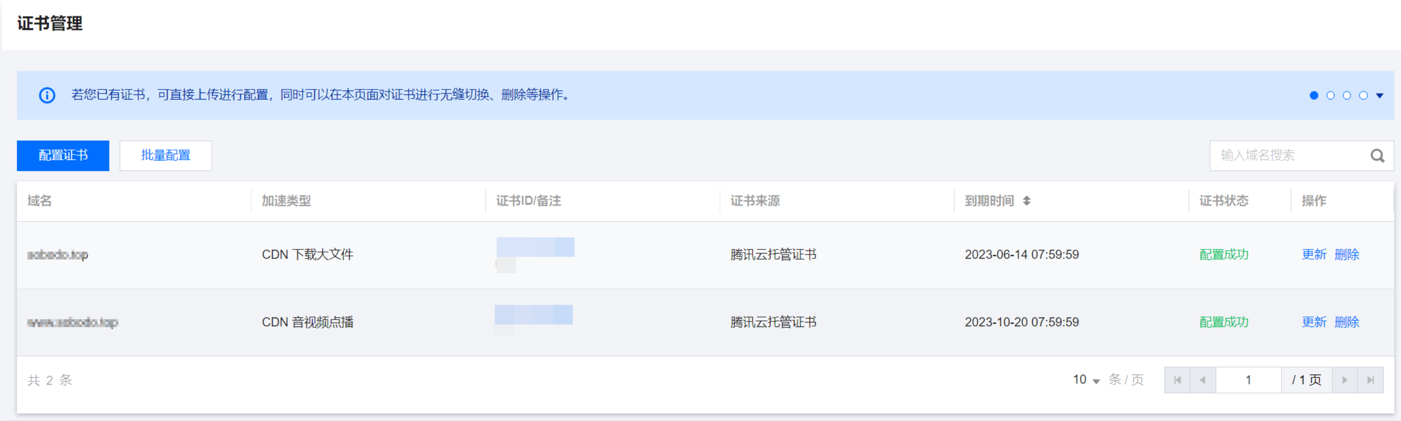
配置状态

HTTPS配置

HTTPS提供对网络服务器的身份认证，保护交换数据的隐私和完整性。 什么是HTTPS?

You can also go to the **Certificate Management** page in the left menu bar to view the list of all domains configured with HTTPS acceleration under the account.

- Certificate list: displays the list of hosted certificates.



证书管理

若您已有证书，可直接上传进行配置，同时可以在本页面对证书进行无缝切换、删除等操作。

域名	加速类型	证书ID/备注	证书来源	到期时间	证书状态	操作
[redacted]	CDN 下载大文件	[redacted]	腾讯云托管证书	2023-06-14 07:59:59	配置成功	更新 删除
[redacted]	CDN 音视频点播	[redacted]	腾讯云托管证书	2023-10-20 07:59:59	配置成功	更新 删除

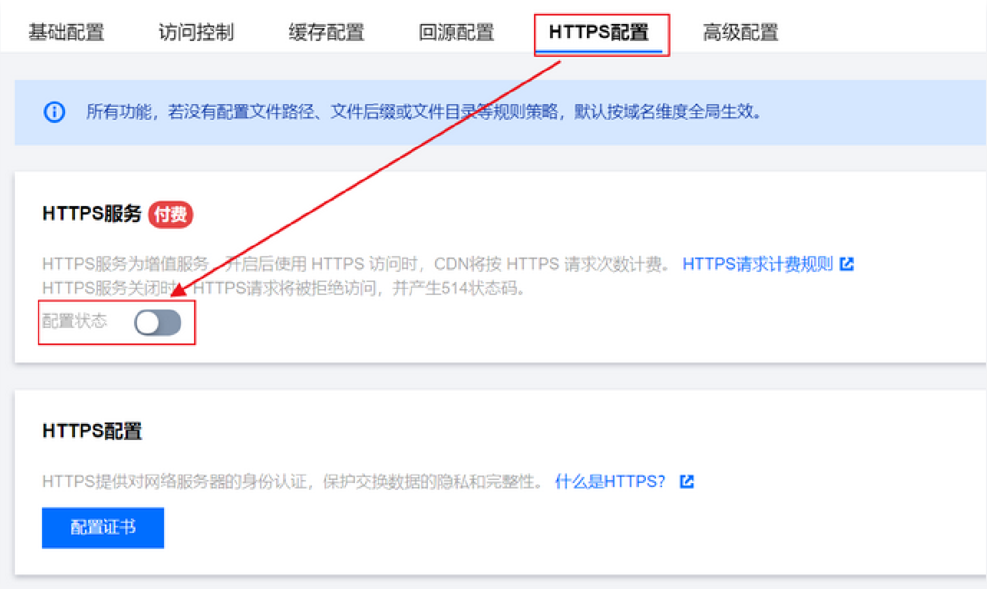
共 2 条 10 条 / 页 1 / 1 页

Certificate configuration

1. Domain name configuration method

1.1 Confirm enabling HTTPS service

Log in to the CDN console, select **Domain Management** from the left menu bar, click **Management** in the domain operation column to enter the domain configuration page, and switch to **HTTPS Configuration**.



所有功能，若没有配置文件路径、文件后缀或文件目录等规则策略，默认按域名维度全局生效。

HTTPS服务 付费

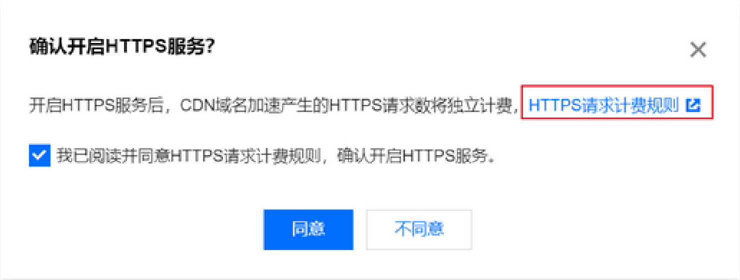
HTTPS服务为增值服务，开启后使用 HTTPS 访问时，CDN将按 HTTPS 请求次数计费。 HTTPS请求计费规则
HTTPS服务关闭时，HTTPS请求将被拒绝访问，并产生514状态码。

配置状态

HTTPS配置

HTTPS提供对网络服务器的身份认证，保护交换数据的隐私和完整性。 什么是HTTPS?

Confirm whether to enable HTTPS service. After enabling, the number of HTTPS requests generated by CDN domain acceleration will be billed separately, HTTPS request billing rules .

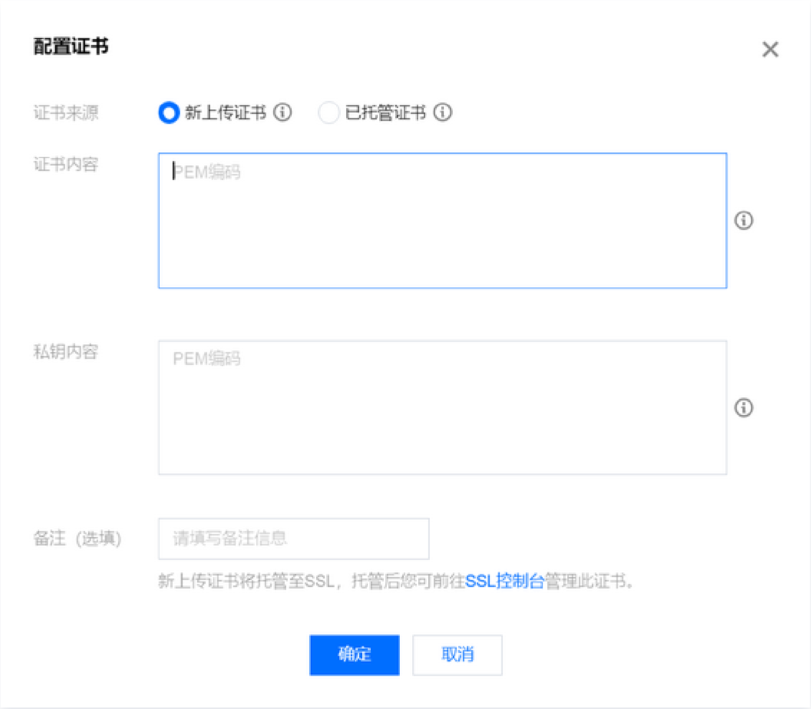

确认开启HTTPS服务?

开启HTTPS服务后，CDN域名加速产生的HTTPS请求数将独立计费，HTTPS请求计费规则

☑ 我已阅读并同意HTTPS请求计费规则，确认开启HTTPS服务。

1.2 Configuring a certificate

Click the **Configuring Certificate** button to add a domain certificate. You can add a certificate in the following two ways:


配置证书

证书来源 ● 新上传证书 ○ 已托管证书

证书内容 PEM编码

私钥内容 PEM编码

备注（选填） 请填写备注信息

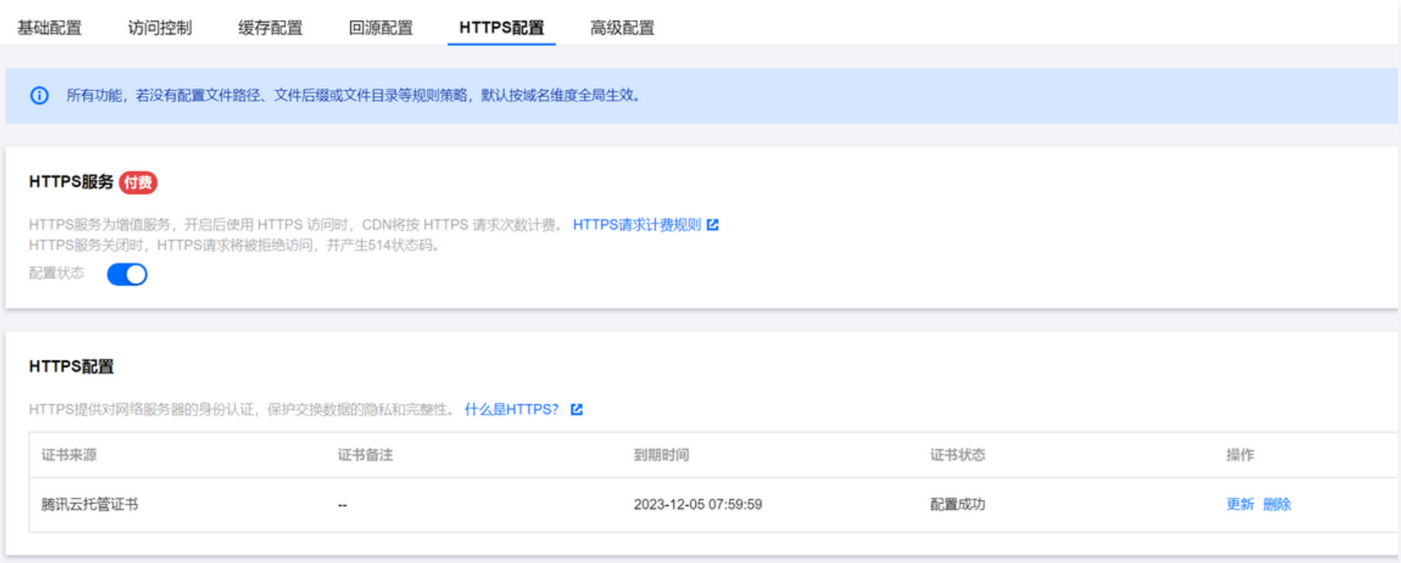
新上传证书将托管至SSL，托管后您可前往SSL控制台管理此证书。

Configuration Method	Description
Uploading a new certificate	Uploading a new certificate requires you to manually upload the certificate content and private key content. Please prepare the relevant certificate content before uploading. For information on how to obtain the certificate content and private key content, refer to HTTPS Configuration.
Hosted certificate	Hosted certificates can be selected from the certificate files you have hosted in the SSL Certificates service. Based on the domain name you are configuring, only certificate files that match the current domain will be displayed. If no matching certificate files exist, you can also apply for a free certificate on the SSL certificate management page.

> ⚠ **Note**
> 1. If the acceleration domain name you are configuring is in a closed status, HTTPS certificate configuration is not allowed.
> 2. `file.myqcloud.com` suffix is the default acceleration domain name for Tencent Cloud Object Storage. No certificate configuration is required to directly perform HTTPS acceleration.
> 3. `image.myqcloud.com` suffix is the default acceleration domain name for Tencent Cloud Cloud Infinite. No certificate configuration is required to directly perform HTTPS acceleration service.

1.3 Editing a certificate

After the certificate is successfully configured, you can view the status and expiration time of the certificate on the HTTPS configuration page of the domain. You can also modify the certificate through the **Update** button or delete the certificate configuration through the **Delete** button.



所有功能，若没有配置文件路径、文件后缀或文件目录等规则策略，默认按域名维度全局生效。

HTTPS服务 付费

HTTPS服务为增值服务，开启后使用 HTTPS 访问时，CDN将按 HTTPS 请求次数计费。 HTTPS请求计费规则
HTTPS服务关闭时，HTTPS请求将被拒绝访问，并产生514状态码。

配置状态 ●

HTTPS配置

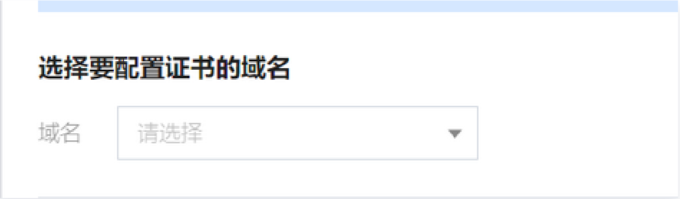
HTTPS提供对网络服务器的身份认证，保护交换数据的隐私和完整性。 什么是HTTPS?

证书来源	证书备注	到期时间	证书状态	操作
腾讯云托管证书	--	2023-12-05 07:59:59	配置成功	更新 删除

2. Configuring Methods Under Certificate Management

2.1 Selecting a domain name

In the left menu bar of the console, enter **Certificate Management**, click **Configuring Certificates** above, and select the acceleration domain for which the certificate needs to be configured;


选择要配置证书的域名

域名 请选择

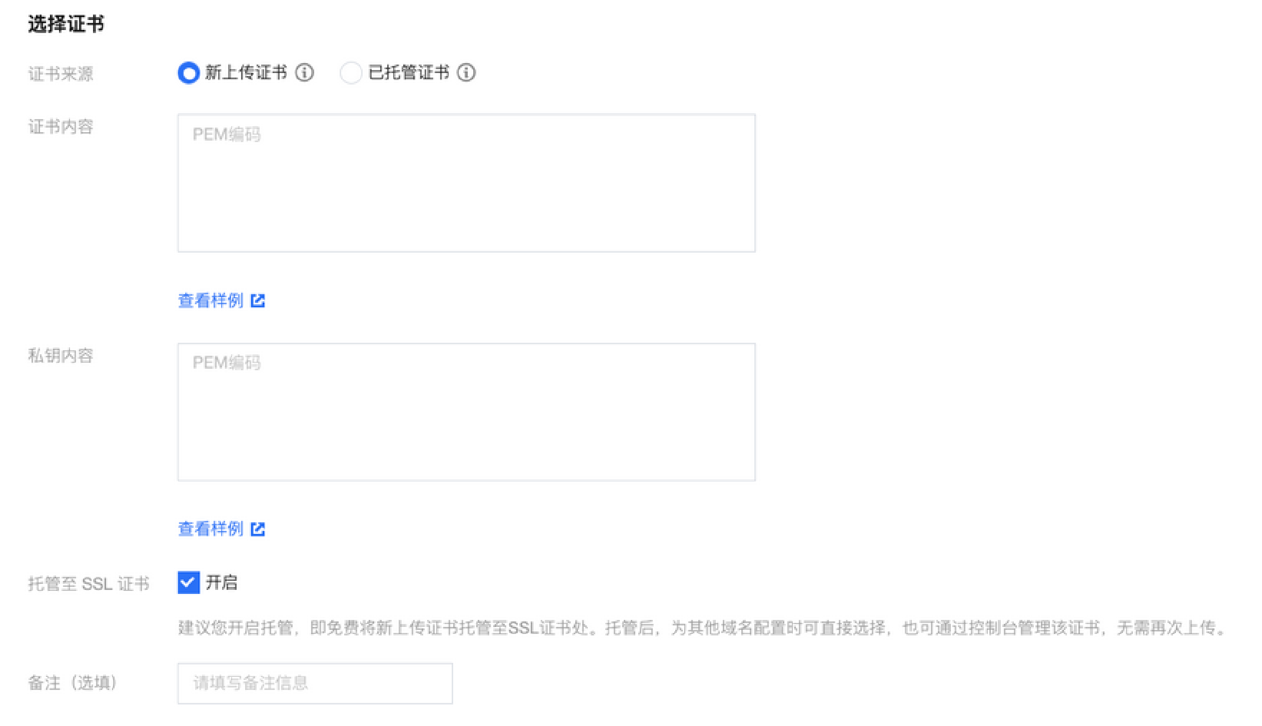
> ⚠ **Note**

> - The status of the acceleration domain name needs to be "Deploying" or "Enabled". Disabled domain names cannot be configured with HTTPS acceleration.
> - `.file.myqcloud.com` suffix is the default acceleration domain name for Tencent Cloud Object Storage. No certificate configuration is required to directly perform HTTPS acceleration.
> - `.image.myqcloud.com` suffix domain name is the default acceleration domain name for Tencent Cloud CI. No certificate configuration is required to directly perform HTTPS acceleration service.

2.2 Selecting a certificate

If there is an existing certificate in PEM format, you can directly paste its content and private key to the corresponding fields:

- Tencent Cloud CDN now supports ECC certificate deployment.
- The certificate content needs to be in PEM format. If not, please refer to PEM Format Conversion.
- You can select a certificate hosted by Tencent Cloud for quick deployment.



选择证书

证书来源 ● 新上传证书 ⓘ ○ 已托管证书 ⓘ

证书内容 PEM编码

查看样例

私钥内容 PEM编码

查看样例

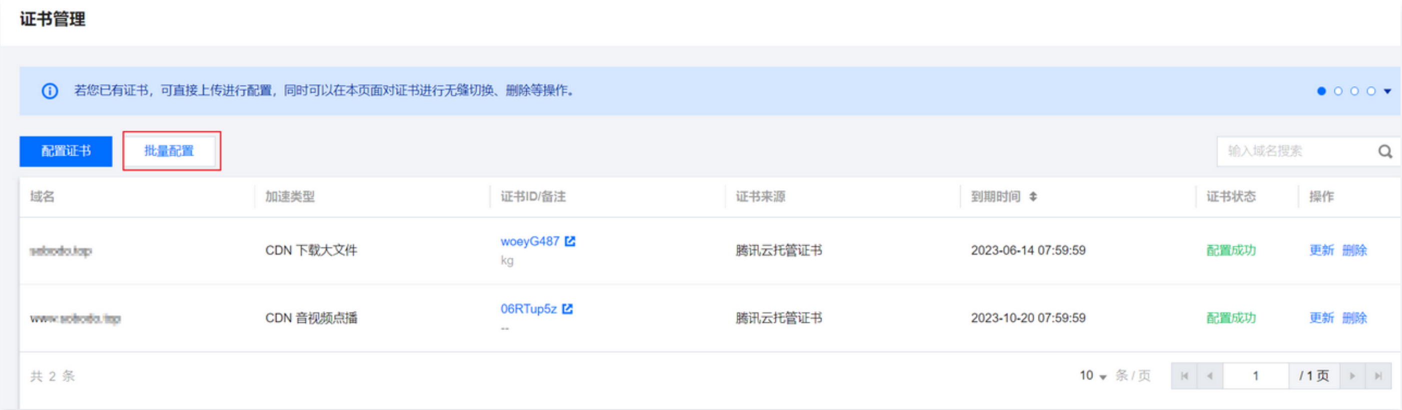
托管至 SSL 证书 ☑ 开启

建议您开启托管，即免费将新上传证书托管至SSL证书处。托管后，为其他域名配置时可直接选择，也可通过控制台管理该证书，无需再次上传。

备注（选填） 请填写备注信息

3. Batch Configuring Methods Under Certificate Management

In the left sidebar menu, go to **Certificate Management** > **Certificate Configuration**, click **Configuring in batches** at the top. You can upload a certificate to automatically match the adapted domain names for batch configuration.



证书管理

ⓘ 若您已有证书，可直接上传进行配置，同时可以在本页面对证书进行无缝切换、删除等操作。

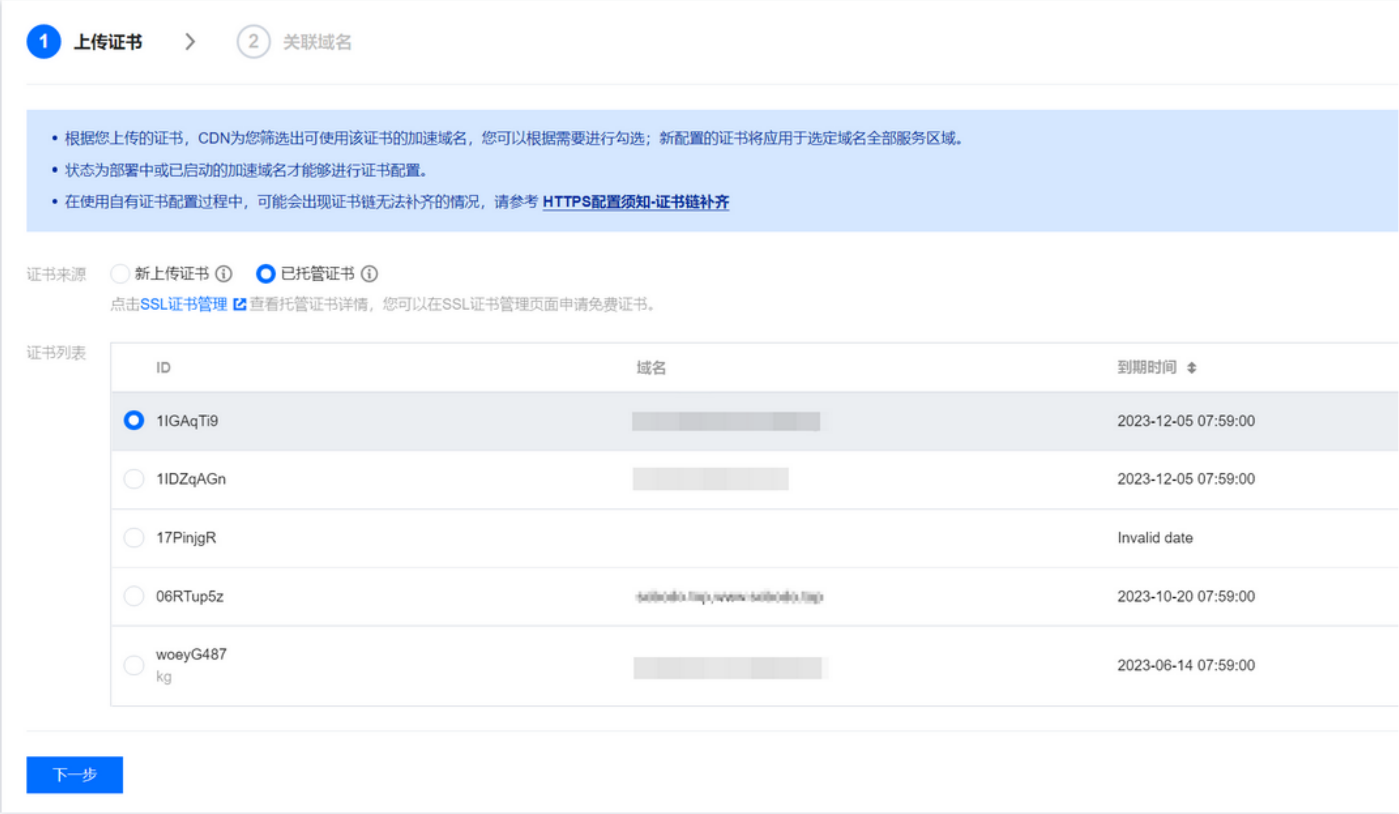
域名	加速类型	证书ID/备注	证书来源	到期时间	证书状态	操作
[redacted]	CDN 下载大文件	woeyG487 kg	腾讯云托管证书	2023-06-14 07:59:59	配置成功	更新 删除
[redacted]	CDN 音视频点播	06RTup5z --	腾讯云托管证书	2023-10-20 07:59:59	配置成功	更新 删除

共 2 条 10 条 / 页 1 / 1 页

3.1 Selecting a certificate

If there is an existing certificate in PEM format, you can directly paste its content and private key to the corresponding fields:

- Tencent Cloud CDN now supports ECC certificate deployment.
- The certificate content needs to be in PEM format. If not, please refer to PEM Format Conversion.
- You can select a hosted certificate for one-click deployment.



1 上传证书 > 2 关联域名

- 根据您上传的证书，CDN为您筛选出可使用该证书的加速域名，您可以根据需要进行勾选；新配置的证书将应用于选定域名全部服务区域。
- 状态为部署中或已启动的加速域名才能够进行证书配置。
- 在使用自有证书配置过程中，可能会出现证书链无法补齐的情况，请参考 HTTPS配置须知-证书链补齐

证书来源 ○ 新上传证书 ⓘ ● 已托管证书 ⓘ

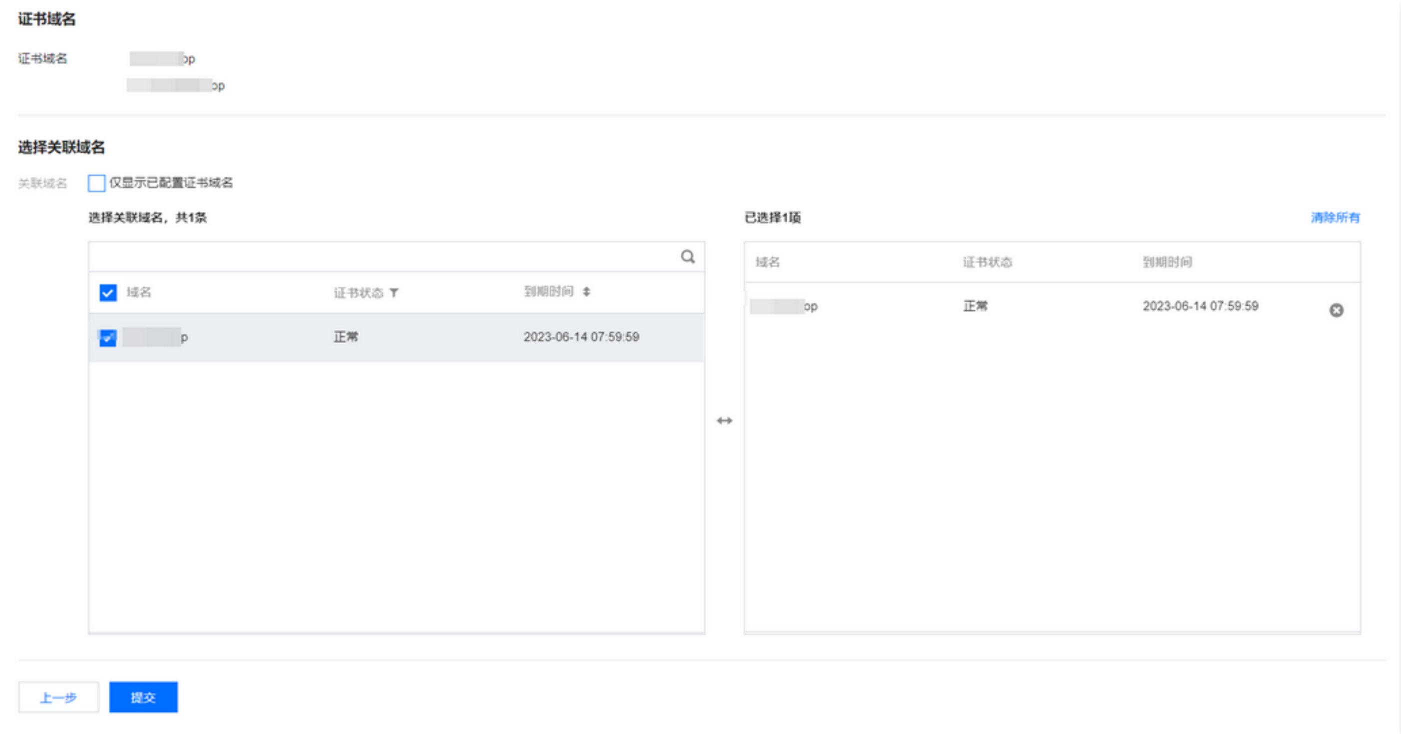
点击SSL证书管理 查看托管证书详情，您可以在SSL证书管理页面申请免费证书。

证书列表

	ID	域名	到期时间
●	1IGAqTi9	[redacted]	2023-12-05 07:59:00
○	1IDZqAGn	[redacted]	2023-12-05 07:59:00
○	17PinjgR		Invalid date
○	06RTup5z	[redacted]	2023-10-20 07:59:00
○	woeyG487 kg	[redacted]	2023-06-14 07:59:00

3.2 Selecting a domain name

Based on the uploaded or selected certificate, CDN will automatically match the domain names that allow the configuration. You can select the domain names for configuration as needed:



证书域名

证书域名 [redacted]op
[redacted]op

选择关联域名

关联域名 □ 仅显示已配置证书域名

选择关联域名，共1条

☑	域名	证书状态	到期时间
☑	[redacted]p	正常	2023-06-14 07:59:59

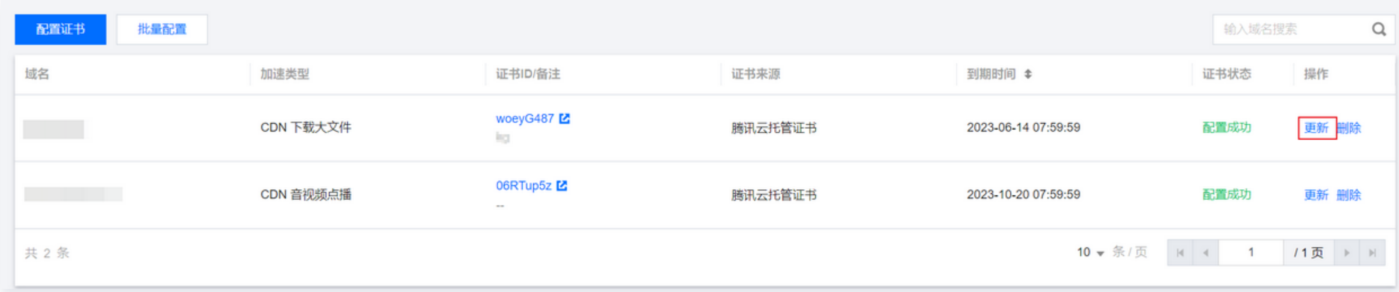
已选择1项 清除所有

域名	证书状态	到期时间
[redacted]op	正常	2023-06-14 07:59:59

Changing a certificate

Modifying a certificate

In the left menu bar of the console, go to **Certificate Management**. Click **Update** on the right side of the certificate you need to modify. You can specify a domain name for certificate update or reconfigure in bulk to overwrite the existing certificate configuration.



域名	加速类型	证书ID/备注	证书来源	到期时间	证书状态	操作
[redacted]	CDN 下载大文件	woeyG487 [redacted]	腾讯云托管证书	2023-06-14 07:59:59	配置成功	更新 删除
[redacted]	CDN 音视频点播	06RTup5z --	腾讯云托管证书	2023-10-20 07:59:59	配置成功	更新 删除

共 2 条 10 条 / 页 1 / 1 页

The updated certificate will take effect across the network nodes seamlessly without affecting the current network HTTPS service. You can also click **Delete** to cancel HTTPS acceleration service.

Certificate expiration

Tencent Cloud will send expiration reminders through SMS, email, and the Message Center 29, 15, and 7 days before the expiration of your certificate and on the day of its expiration. Currently, reminder recipients for SSL certificates can be customized. You can access the Message Subscription page for configuration.

Forced Redirection Configuration

Last updated：2024-12-31 17:40:48

Configuration Scenario

Tencent Cloud CDN supports configuring HTTPS/HTTP forced redirection:

- Domains with HTTPS acceleration can specify 301/302 redirection methods to force redirect all HTTP requests arriving at CDN nodes to HTTPS.
- You can also specify 301/302 redirection methods to force redirect all HTTPS requests arriving at CDN nodes to HTTP requests.
- By default, response headers are not carried during redirection, but this can be changed.

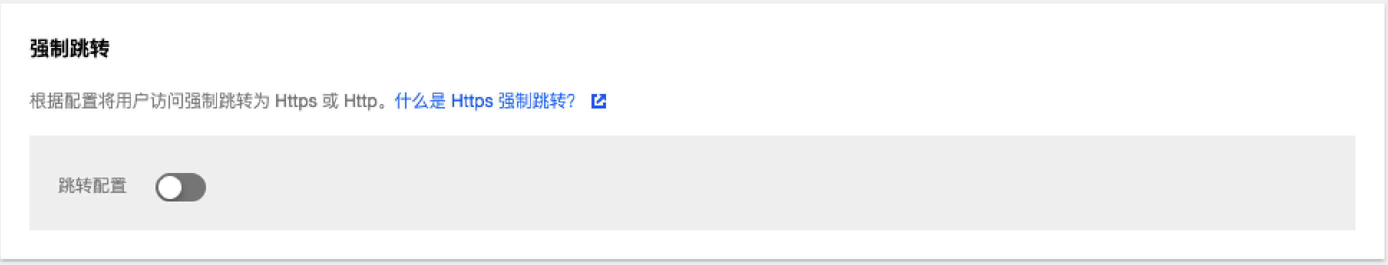
Configuration Guide

Configuration limitations

To configure HTTPS forced redirection, you need to enable HTTPS acceleration in CDN first.

Configuration Instructions

Log in to the CDN console, select **Domain Name Management** from the menu bar, click **Management** on the right side of the domain name, and you will see the **HTTPS Configuration** with the **Forced Redirection** switch. The default is off, and no redirection is performed by default:

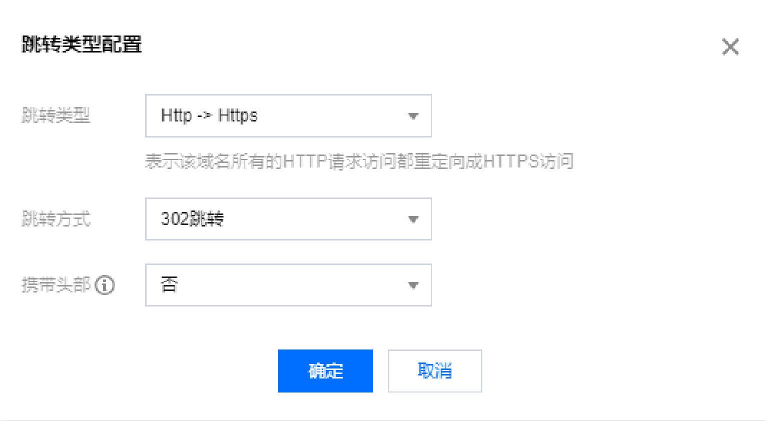


强制跳转

根据配置将用户访问强制跳转为 Https 或 Http。什么是 Https 强制跳转？

跳转配置

Click to enable, you can configure the redirection type, redirection method, and whether to carry headers:



跳转类型配置

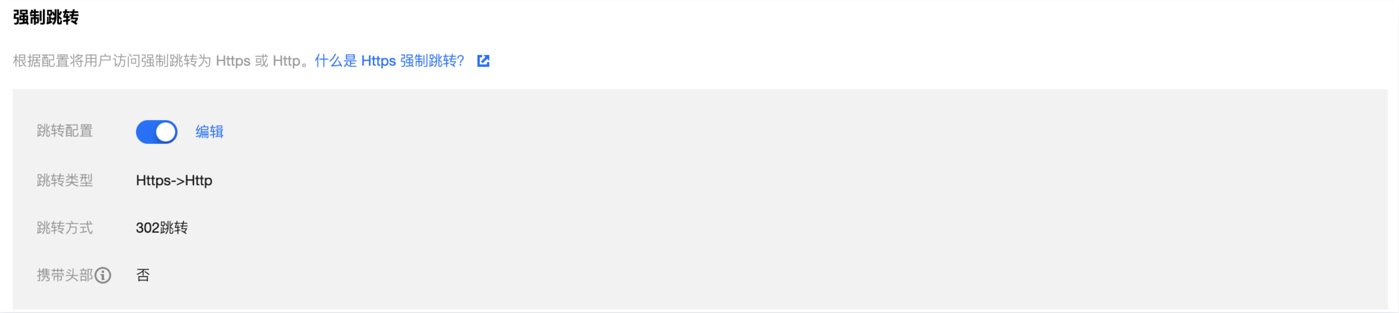
跳转类型：Http -> Https

表示该域名所有的HTTP请求访问都重定向成HTTPS访问

跳转方式：302跳转

携带头部：否

Click confirm to directly publish the configuration to the live network:



强制跳转

根据配置将用户访问强制跳转为 Https 或 Http。什么是 Https 强制跳转？

跳转配置 编辑

跳转类型 Https->Http

跳转方式 302跳转

携带头部 否

HTTP2.0 Configuration

Last updated：2024-12-31 17:40:59

Configuration Scenario

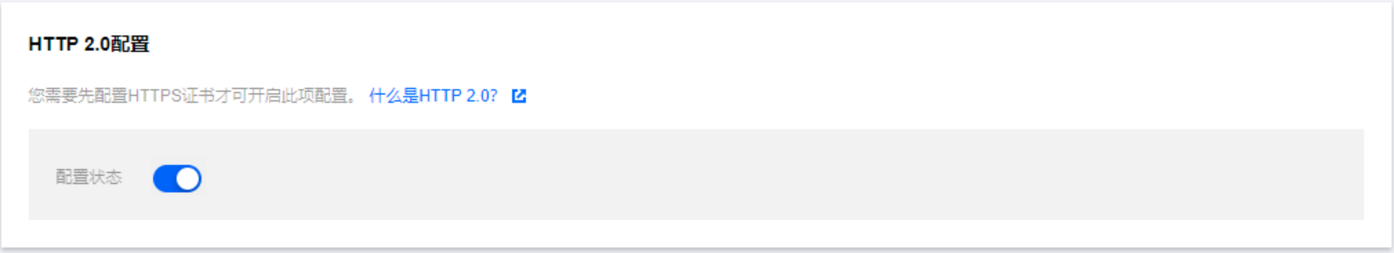
HTTP2.0 is the latest HTTP version which greatly enhances the web performance and further reduces the network delay. HTTP2.0 can be directly enabled for the domain names with certificates configured and HTTPS acceleration enabled.

> **Note**
> Currently, only HTTP2.0 access is supported. HTTP2.0 origin-pull is not supported.

Configuration Guide

Viewing Configuration

Log in to the CDN console, select **Domain Management** from the menu, click **Manage** next to the domain name to enter the domain configuration page, where you can see **HTTPS Configuration**, including **HTTP2.0 Configuration**:



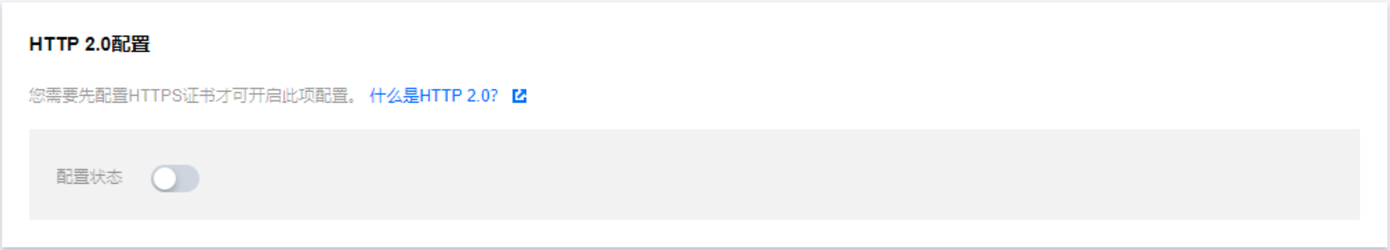
HTTP 2.0配置

您需要先配置HTTPS证书才可开启此项配置。 什么是HTTP 2.0?

配置状态 ●

Modify

By clicking the switch, you can enable or disable HTTP2.0 Configuration. If the certificate configuration is deleted, HTTP2.0 Configuration will be automatically disabled:



HTTP 2.0配置

您需要先配置HTTPS证书才可开启此项配置。 什么是HTTP 2.0?

配置状态 ○

> **Note**
> If a domain name is configured for global acceleration, the HTTP2.0 configuration will be applied to global regions, regardless of whether they’re inside or outside the Chinese mainland.

OCSP Stapling

Last updated：2024-12-31 17:41:10

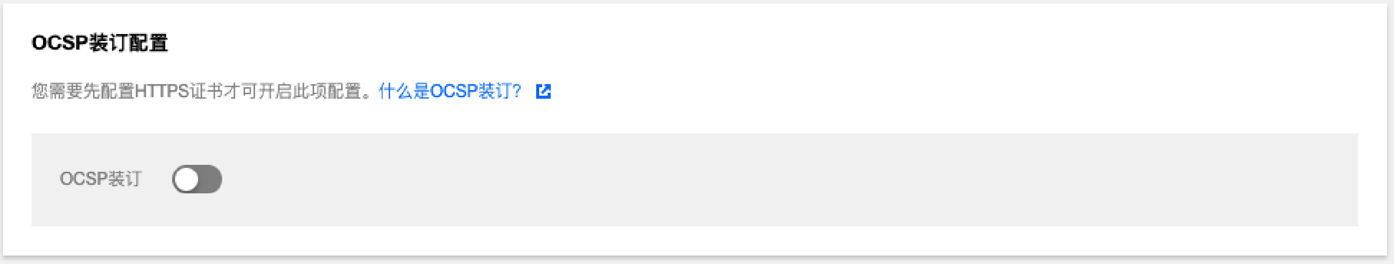
Configuration Scenario

After OCSP stapling (a TLS certificate status query extension) is enabled, the server will send a pre-cached Online Certificate Status Protocol (OCSP) response during the TLS handshake for user verification, so that the user does not need to send a query request to the certificate authority (CA). OCSP stapling greatly improves the efficiency of TLS handshake and reduces user verification time.
Tencent Cloud CDN supports self-service enabling or disabling of OCSP stapling configuration.

Configuration Guide

Viewing Configuration

Log in to the CDN console, select **Domain Management** from the menu, and click on **Management** next to the domain name to enter the domain configuration page. In **HTTPS Configuration**, you can see **OCSP Stapling Configuration**, which is off by default:



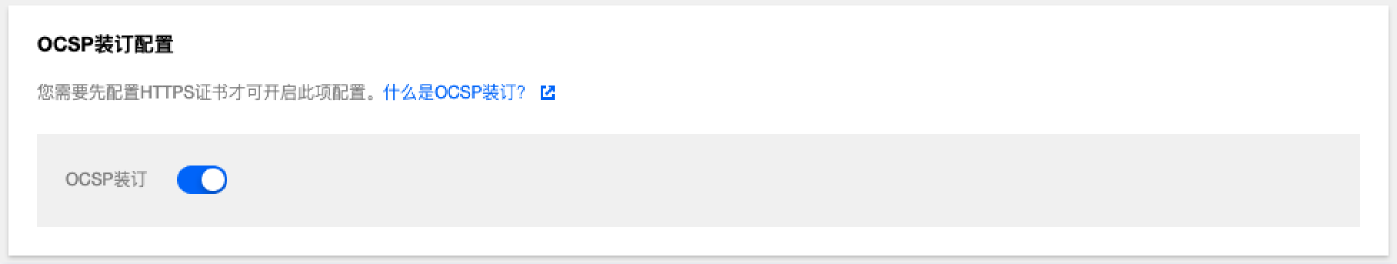
OCSP装订配置

您需要先配置HTTPS证书才可开启此项配置。什么是OCSP装订？

OCSP装订 ○

Modify

If a domain name has been configured with HTTPS acceleration, you can directly click the switch to perform enable or disable operation on OCSP Stapling Configuration. After the certificate configuration is deleted, OCSP Stapling will synchronously become invalid:



OCSP装订配置

您需要先配置HTTPS证书才可开启此项配置。什么是OCSP装订？

OCSP装订 ●

⚠ **Note**

- If your domain name is configured for global acceleration, the OCSP stapling configuration will take effect globally. This configuration does not distinguish between requests from and outside the Chinese mainland.
- `file.myqcloud.com` and `image.myqcloud.com` suffix is the default accelerated domain name for COS, and OCSP stapling is not supported.

HSTS Configuration

Last updated：2024-12-31 17:41:21

Configuration Scenario

HTTP Strict Transport Security (HSTS) is a web security protocol promoted by the Institution of Electronics and Telecommunication Engineers (IETE). It forces the client (such as a browser) to use HTTPS to create a connection with the server so as to help encrypt the website globally.

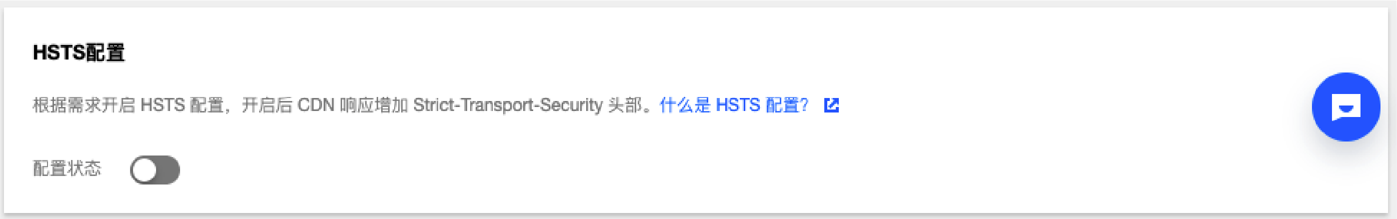
For example, when you have configured an HTTPS certificate, if HSTS configuration is not enabled and HTTPS forced redirection is configured, users can still initiate domain requests through HTTP URLs. When CDN receives such HTTP URL requests, it will modify them to HTTPS through HTTPS forced redirection for encrypted request verification. However, when users send requests to CDN nodes, there is still a risk of hijacking or tampering due to HTTP requests. If HSTS configuration is enabled, users can only make requests through the HTTPS protocol to enhance the security of the request.

Configuration limitations

- The expireTime constraint ranges from 0 to 365 days, and the configuration unit is seconds.
- You can control the includeSubDomain parameter by checking whether to include subdomains.
- To enable HSTS configuration, HTTPS acceleration configuration must be completed first.
- After enabling HSTS, it is recommended to also enable Forced Redirection from HTTP to HTTPS configuration. Otherwise, the browser will not create HSTS cache for HTTP requests.

Configuration Guide

Log in to the CDN console, select **Domain Management** from the menu, click **Management** on the right side of the domain to enter the domain configuration page. In **HTTPS Configuration**, you can see the HSTS configuration module, which is off by default:

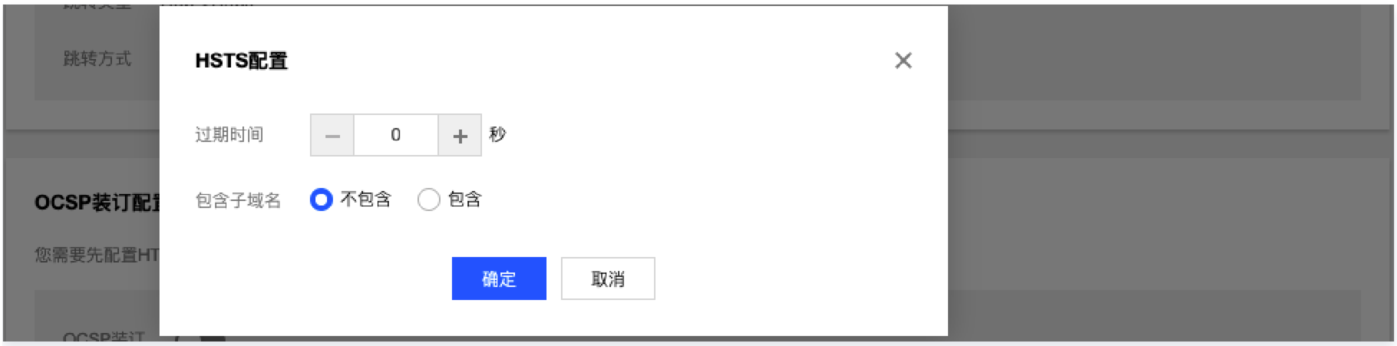


HSTS配置

根据需求开启 HSTS 配置，开启后 CDN 响应增加 Strict-Transport-Security 头部。什么是 HSTS 配置？

配置状态

Click to enable and proceed with the configuration:

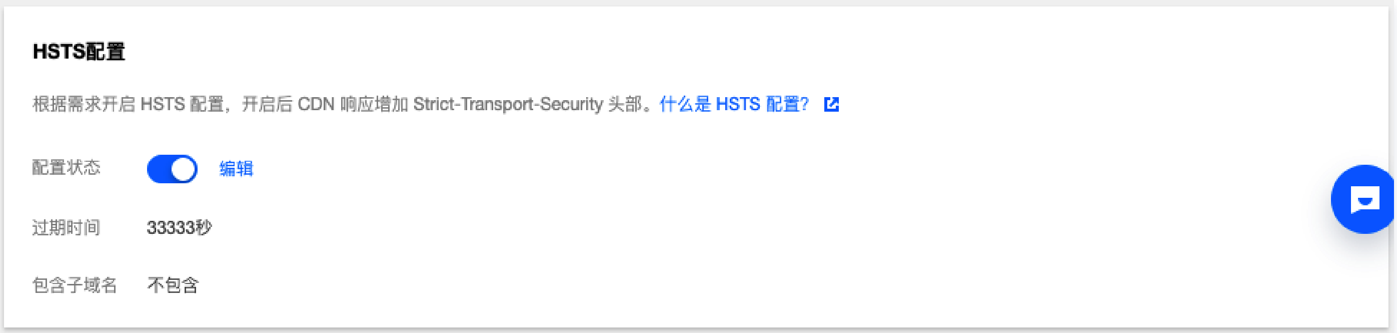


HSTS配置

过期时间 0 秒

包含子域名 ● 不包含 ○ 包含

After clicking **Yes**, the response header value is determined by the configured content. You can click **Edit** to modify:



HSTS配置

根据需求开启 HSTS 配置，开启后 CDN 响应增加 Strict-Transport-Security 头部。什么是 HSTS 配置?

配置状态 编辑

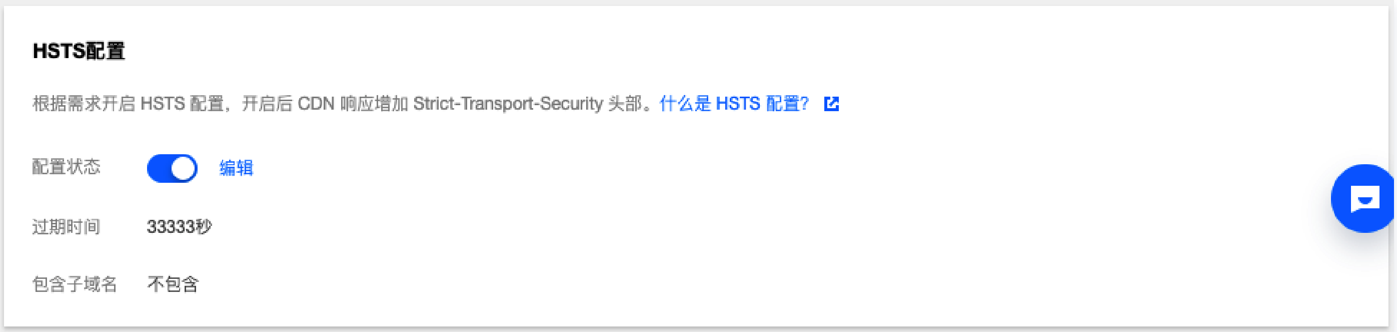
过期时间 33333秒

包含子域名 不包含

The expiration time refers to the cache expiration time of the HSTS response header Strict–Transport–Security in the browser.

Configuration Example

If the HSTS configuration of the domain name `cloud.tencent.com` is as follows:



HSTS配置

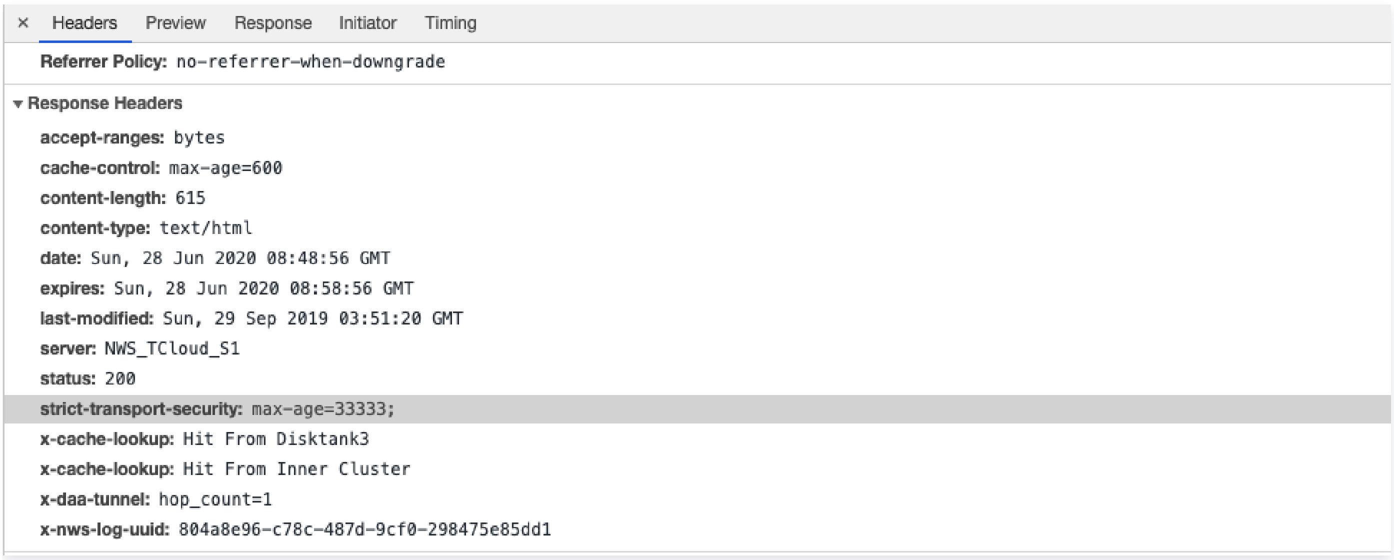
根据需求开启 HSTS 配置，开启后 CDN 响应增加 Strict-Transport-Security 头部。什么是 HSTS 配置?

配置状态 编辑

过期时间 33333秒

包含子域名 不包含

The response header when accessed is:



```
Referrer Policy: no-referrer-when-downgrade

▼ Response Headers
   accept-ranges: bytes
   cache-control: max-age=600
   content-length: 615
   content-type: text/html
   date: Sun, 28 Jun 2020 08:48:56 GMT
   expires: Sun, 28 Jun 2020 08:58:56 GMT
   last-modified: Sun, 29 Sep 2019 03:51:20 GMT
   server: NWS_TCloud_S1
   status: 200
   strict-transport-security: max-age=33333;
   x-cache-lookup: Hit From Disktank3
   x-cache-lookup: Hit From Inner Cluster
   x-daa-tunnel: hop_count=1
   x-nws-log-uuid: 804a8e96-c78c-487d-9cf0-298475e85dd1
```

TLS Version Configuration

Last updated：2024-12-31 17:41:33

Background

Transport Layer Security (TLS) aims to ensure data security and confidentiality during the communication process between two applications. Currently, there are four versions of the TLS protocol: TLS1.0/1.1/1.2/1.3. Lower versions have better compatibility but lower security; higher versions have higher security but weaker compatibility.

TLS Protocol Version	Supported Mainstream Browsers
TLS 1.0	IE6+
	Chrome 1+
	Firefox 2+
TLS 1.1	IE 11+
	Chrome 22+
	Firefox 24+
	ME 12+
	Safari 7+
	Opera 12.1+
TLS 1.2	IE 11+
	Chrome 30+
	ME 12+
	Firefox 27+
	Safari 7+
	Opera 16+
TLS 1.3	Chrome 70+
	Firefox 63+
	ME 79+
	Safari 14+
	Opera 57+

Feature Introduction

Tencent Cloud CDN enables TLS 1.0/1.1/1.2 and disables TLS 1.3 by default. You can enable and disable specified TLS versions as needed.

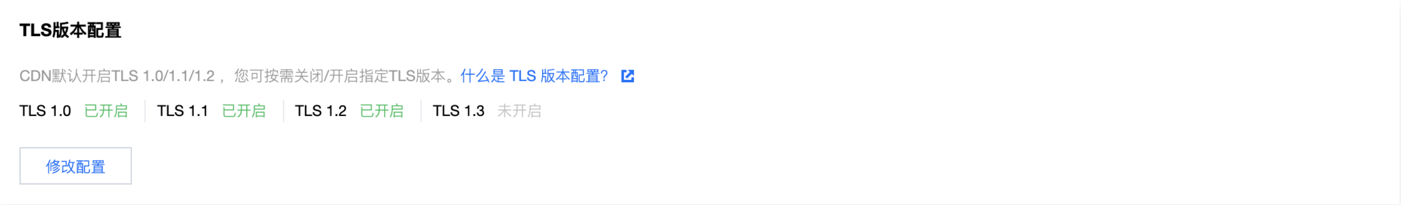
> **Note**
> Note: Make sure the HTTPS certificate is properly configured before configuration.

Configuration Guide

View Configuration

Log in to the CDN console, select **Domain Management** from the left sidebar menu, click **Management** in the domain operation column to enter the domain configuration page, switch the tab to **HTTPS Configuration**, and you will find the **TLS Version Configuration**.

By default, TLS 1.0/1.1/1.2 are in enable status, and TLS 1.3 is in closed status:



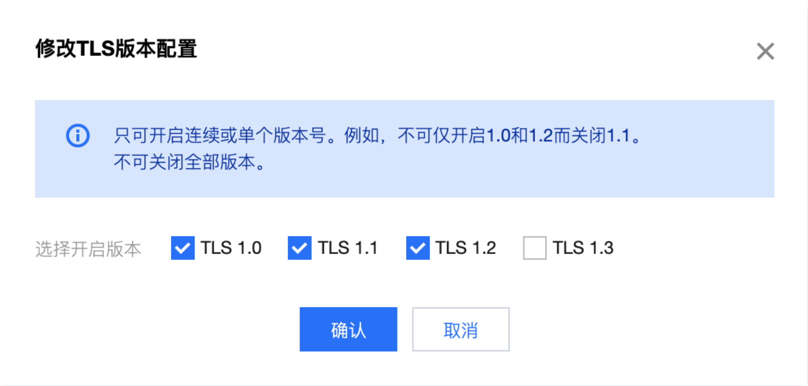
TLS版本配置

CDN默认开启TLS 1.0/1.1/1.2， 您可按需关闭/开启指定TLS版本。什么是 TLS 版本配置？

TLS 1.0 已开启 | TLS 1.1 已开启 | TLS 1.2 已开启 | TLS 1.3 未开启

Modify

You can close/enable specified TLS versions as needed, click **Modify**:



修改TLS版本配置

只可开启连续或单个版本号。例如，不可仅开启1.0和1.2而关闭1.1。
不可关闭全部版本。

选择开启版本 ☑ TLS 1.0 ☑ TLS 1.1 ☑ TLS 1.2 □ TLS 1.3

Configuration limitations

- You can enable a single version or multiple consecutive ones. For example, you can enable version 1.0, 1.1 and 1.2, but not version 1.0 and 1.2.
- You cannot close all versions.

QUIC

Last updated：2024-12-31 17:41:43

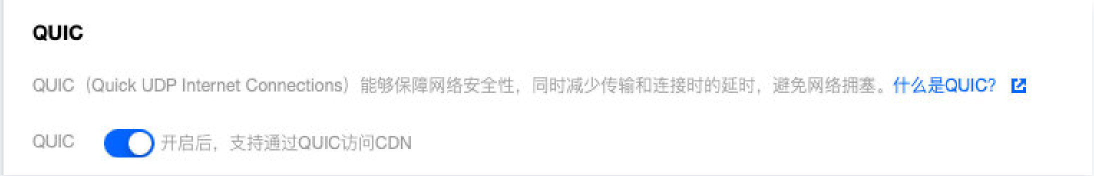
Feature Introduction

Quick UDP Internet Connections (QUIC) is a general network protocol based on UDP. It can provide good service in weak network environments with severe packet loss and network delay, reduce transmission and connection delay, and avoid network congestion. It also offers security equivalent to TLS/SSL to ensure network security. You can enable the QUIC protocol to ensure data transfer security and improve access efficiency when clients access CDN nodes.
Currently default supported versions are h3-29, h3-Q050, h3-Q046, h3-Q043, Q046, and Q043.

Operation Guide

Enabling QUIC

After successfully adding a domain name by logging in to the CDN console, you can enter domain management, switch the tab to **HTTPS Configuration**, and find the **QUIC** configuration: default to off state, you can self-enable it.
Note: Please configure the HTTPS certificate before enabling.



QUIC

QUIC（Quick UDP Internet Connections）能够保障网络安全性，同时减少传输和连接时的延时，避免网络拥塞。什么是QUIC?

QUIC ● 开启后，支持通过QUIC访问CDN

Notes:
- Switching service types concerns resource scheduling on the platform. After enabling QUIC, we recommend not switching the service types for domain names.
- The QUIC protocol is more suitable for weak network environments, with more obvious optimization effects.
- Currently, QUIC back to source is not supported. For QUIC requests, CDN defaults to HTTP protocol back to the origin server. If the origin server only supports HTTPS protocol requests, you can change the CDN back to source protocol to HTTPS. (Note)
- Some platforms outside China do not support QUIC. If the QUIC configuration is not visible in the console, you can adjust the acceleration region to within China or submit a ticket for backend assistance. (Note)

Disabling QUIC

Enter Console Domain Management > HTTPS Configuration > QUIC to disable the QUIC feature.

Billing Rules

QUIC access is a value-added service, which is billed based on the number of QUIC requests and supports pay-as-you-go. For details, see Billing Instructions.

FAQs about HTTPS

Last updated：2024-12-31 17:41:55

What is HTTPS?

HTTPS, which stands for Hypertext Transfer Protocol Secure, is a security protocol that encrypts data transmission based on the HTTP protocol to effectively ensure the security of data transfer. When configuring HTTPS, you need to provide a certificate corresponding to the domain name and deploy it on all CDN nodes to achieve encrypted data transmission across the entire network.

Does CDN support HTTPS configuration?

Tencent Cloud CDN fully supports HTTPS configuration. You can either upload your own certificate for deployment or go to the Certificate Management Console to apply for a third-party certificate that is provided by TrustAsia free of charge.

How do I configure an HTTPS certificate?

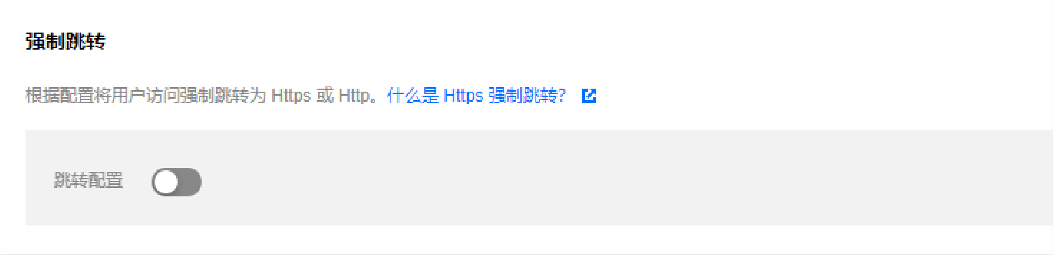
You can configure the HTTPS certificate in the CDN Console. For more information, see HTTPS Configuration.

Do the HTTPS certificates on CDN nodes need to be synchronized with HTTPS certificate updates on the origin server?

No. Updating the HTTPS certificate of your origin server does not affect the one configured on CDN. You only need to update the HTTPS certificate on CDN when it is or about to be expired.

Is there any way for users to allow only HTTPS access and forbid HTTP access?

Use the Forced Redirection feature. After successfully configuring an HTTPS certificate, you can enable the HTTP->HTTPS feature. Once enabled, even if users initiate HTTP requests, they will be forcibly redirected to HTTPS for access.



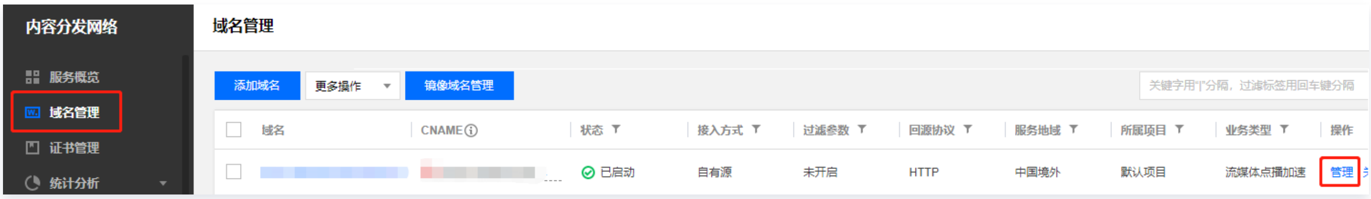
强制跳转

根据配置将用户访问强制跳转为 Https 或 Http。什么是 Https 强制跳转?

Why does HTTPS access not work after CDN is configured?

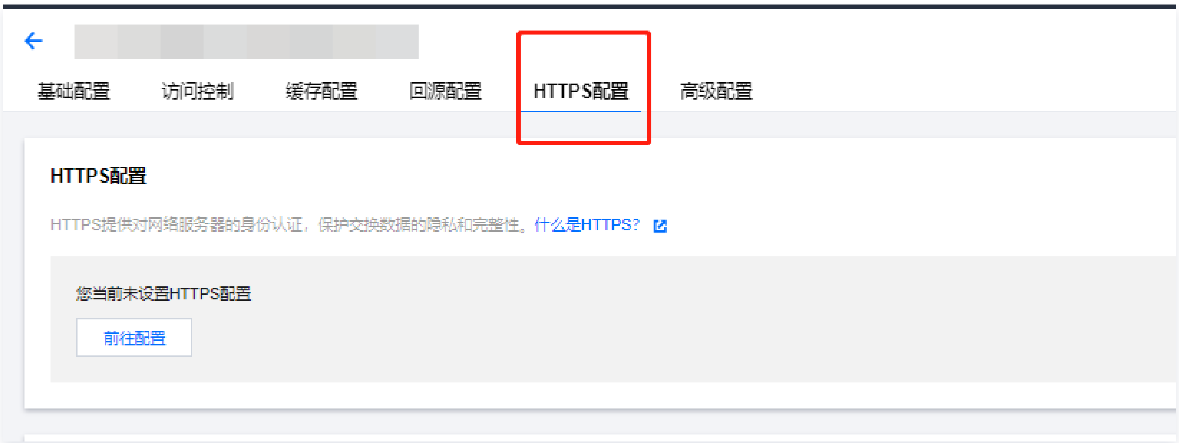
For HTTPS access, please configure it as instructed:

1. Log in to the CDN console, click **Domain Management** on the left sidebar to enter the domain management page. Click the **Management** button on the right side of the domain to enter the management page.



域名	CNAME	状态	接入方式	过滤参数	回源协议	服务地域	所属项目	业务类型	操作
[redacted]	[redacted]	已启动	自有源	未开启	HTTP	中国境外	默认项目	流媒体点播加速	管理

2. Click **HTTPS Configuration**, find the HTTPS configuration module. Click **Go to Configure** to jump to the certificate management page to configure the certificate. For the configuration process, please refer to Certificate Configuration.



HTTPS配置

HTTPS提供对网络服务器的身份认证，保护交换数据的隐私和完整性。什么是HTTPS?

您当前未设置HTTPS配置

After the certificate is successfully configured, you can enable HTTPS access.

Which TLS Versions Does CDN Support

Hello, Tencent Cloud CDN enables TLS 1.0/1.1/1.2 and disables TLS 1.3 by default. You can enable and disable TLS versions as needed.

> **Note**
> - Note: Make sure the HTTPS certificate is properly configured before configuration.
> - You can enable a single version or multiple consecutive ones. For example, you can enable version 1.0, 1.1 and 1.2, but not version 1.0 and 1.2.
> - You cannot disable all versions. For configuration, please refer to the document Configuration Guide.

Enabling QUIC on CDN

CDN supports QUIC. For how to enable it, refer to QUIC.

Does CDN Support Automatic Certificate Renewal

Custom uploaded certificates and free certificates applied for in the SSL console do not support automatically renewing new certificates. If you purchased a multi-year certificate in the SSL console, it can automatically issue the second certificate. For details, see Multi-Year Certificate Plan Description.

Does CDN Support HTTP 2.0

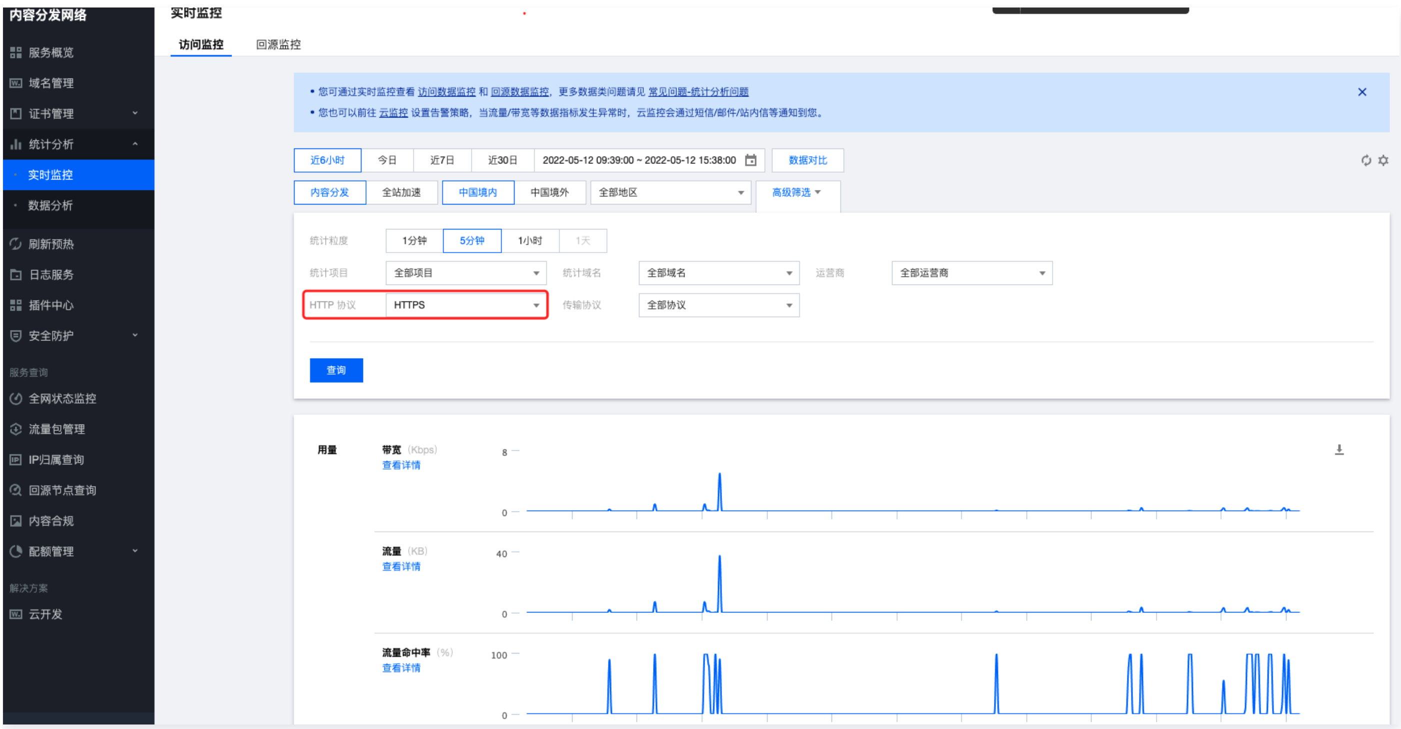
HTTP 2.0 is supported from the client to the CDN node. Please configure an HTTPS certificate before enabling HTTP 2.0. HTTP 2.0 is not supported from the CDN node to the origin server.

How to Batch Configure CDN Certificates

If you have a multi-domain certificate or a wildcard domain certificate, it can be applied to multiple CDN accelerated domains. You can add configurations to multiple domains at once through batch configuration.
Please refer to Batch Configuring Certificates in Certificate Management.

Viewing the Usage of HTTPS Requests

You can obtain the HTTPS usage data by selecting HTTPS under HTTP protocol and clicking **Inquiry** through **Real-Time Monitoring** > **Access Monitoring** in the console.



- 您可通过实时监控查看 访问数据监控 和 回源数据监控，更多数据类问题请见 常见问题-统计分析问题
- 您也可以前往 云监控 设置告警策略，当流量/带宽等数据指标发生异常时，云监控会通过短信/邮件/站内信等通知到您。

近6小时 2022-05-12 09:39:00 ~ 2022-05-12 15:38:00

统计粒度 5分钟

统计项目 全部项目 统计域名 全部域名 运营商 全部运营商

HTTP 协议 HTTPS 传输协议 全部协议

What to Do If HTTPS Certificates on CDN Conflict with Origin Server Certificates

The HTTPS certificate on the CDN and the HTTPS certificate on the origin server exist independently and do not affect each other.

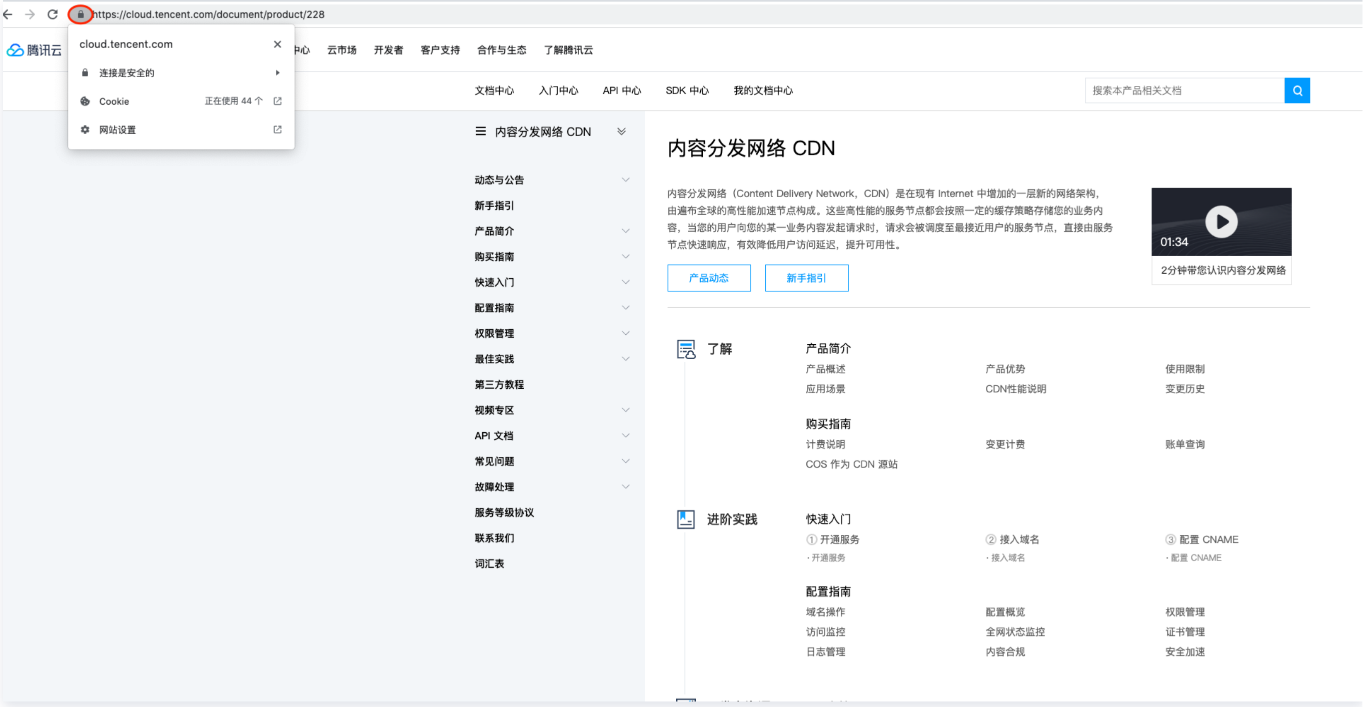
Using HTTP Access After Configuring HTTPS

After configuring HTTPS, both HTTP access and HTTPS access are simultaneously supported.

Verifying If the CDN Certificate Is Successfully Deployed

After the certificate is successfully installed and your domain name is resolved to a server IP address, perform the following steps to check the validity status of the HTTPS certificate:

1. Open a browser (Chrome is used as an example), and enter the domain name address bound to the certificate in the HTTPS format in the address bar.
2. Press Enter to access the domain address. Check for the following conditions:
   - You can successfully access the website using the domain name address.
   - A security lock icon is displayed on the left of the address in the browser address bar, which indicates that your HTTPS certificate has taken effect as shown in the following figure:



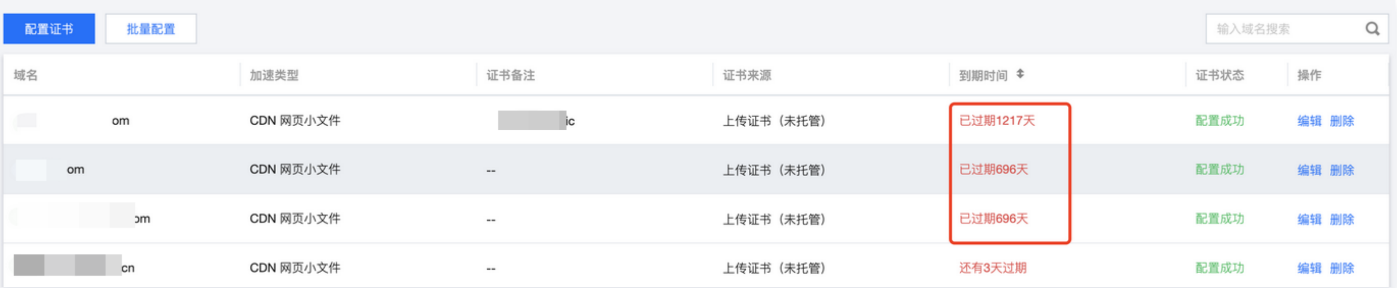
内容分发网络（Content Delivery Network，CDN）是在现有 Internet 中增加的一层新的网络架构，由遍布全球的高性能加速节点构成。这些高性能的服务节点都会按照一定的缓存策略存储您的业务内容，当您的用户向您的某一业务内容发起请求时，请求会被调度至最接近用户的服务节点，直接由服务节点快速响应，有效降低用户访问延迟，提升可用性。

Certificate Risk on Website, How to Handle

If you have configured an HTTPS certificate on the CDN node but the verification is not effective, possible reasons are:

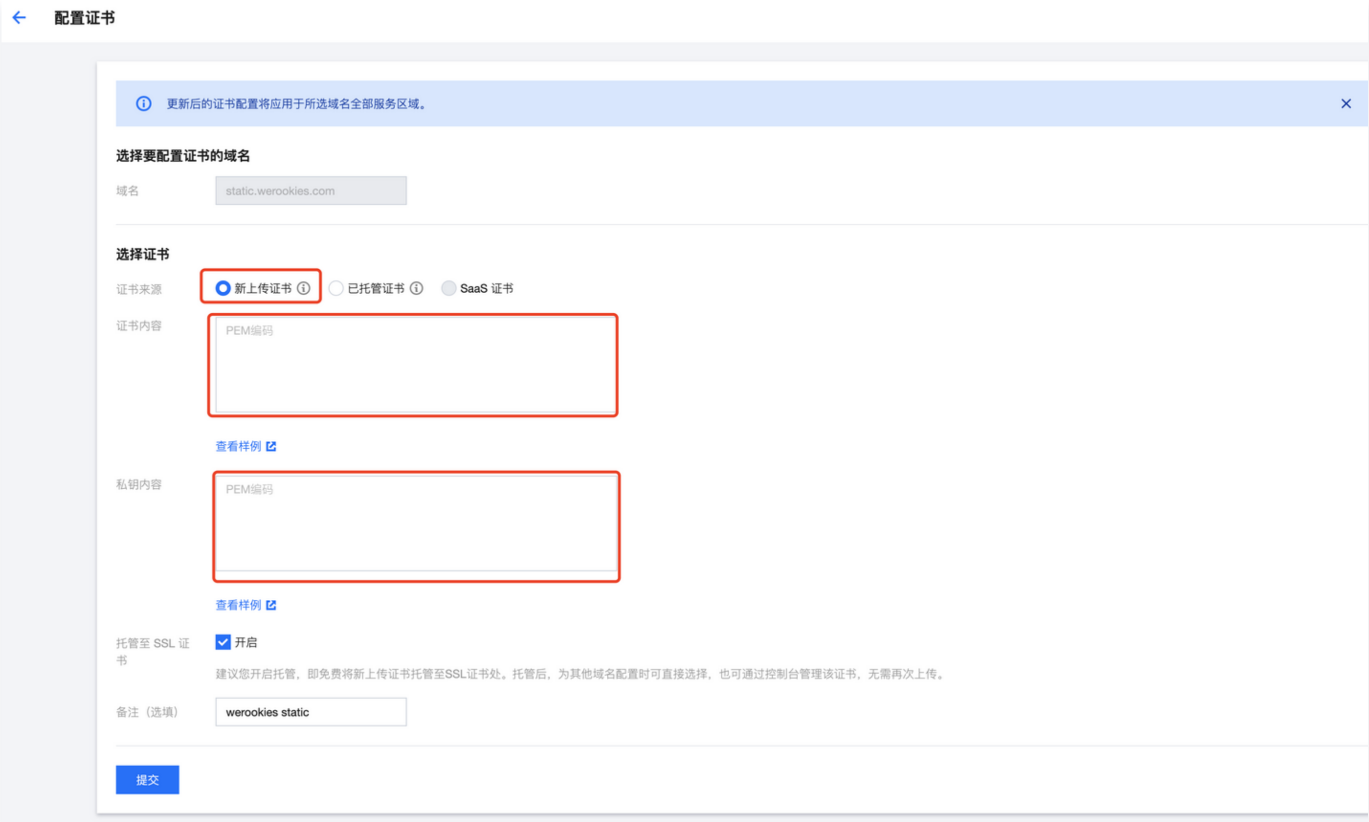
- certificate has expired
- certificate has a validity period. when the certificate expires, it becomes invalid, causing HTTPS access issues.
- Solution: You need to go to the console to replace the certificate. Custom uploaded certificates and free certificates applied for in the SSL console do not support automatic renewal of new certificates. If you purchased a multi-year certificate in the SSL console, it can automatically issue the second certificate. For details, see the multi-year certificate plan description.
- self-signed HTTPS certificate applied. not issued by CA institution, self-generated certificates are called self-signed certificates. these certificates are not trusted by major browsers, are easily forged, and pose security risks. solution: it is recommended to apply for a CA institution issued certificate in the tencent cloud ssl console.
- system time is incorrect. incorrect system time can cause certificate expiration or verification failed. solution: configure the system time correctly.
- There are HTTP link resources on the webpage, i.e., the webpage uses HTTP protocol links.
  For example: the webpage uses HTTP image links
  Solution: change HTTP protocol links to HTTPS protocol links
- Outdated TLS version
  Lower versions of TLS have many security vulnerabilities, posing a security risk of being attacked.
  Solution: Tencent Cloud CDN enables TLS 1.0/1.1/1.2 and disables TLS 1.3 by default. TLSv1.2 and TLSv1.3 are currently recognized as higher security protocols. You can disable TLS 1.0/1.1 and enable TLSv1.2 and TLSv1.3 as needed.
- Weak cipher suite used.
  Weak cipher suites have many security vulnerabilities, posing a security risk of being attacked.
  Solution: For secure encryption and authentication, it is recommended to use 128-bit AEC, GCM configuration; for key exchange mechanism, use ECDHE_RSA.

What to Do After the Certificate Expires



域名	加速类型	证书备注	证书来源	到期时间	证书状态	操作
[redacted] om	CDN 网页小文件	[redacted] ic	上传证书（未托管）	已过期1217天	配置成功	编辑 删除
[redacted] om	CDN 网页小文件	--	上传证书（未托管）	已过期696天	配置成功	编辑 删除
[redacted] om	CDN 网页小文件	--	上传证书（未托管）	已过期696天	配置成功	编辑 删除
[redacted] cn	CDN 网页小文件	--	上传证书（未托管）	还有3天过期	配置成功	编辑 删除

1. If your certificate is a self-owned certificate, you can update the certificate and private key content by clicking **Edit**. After completing the update, click **Submit**.



更新后的证书配置将应用于所选域名全部服务区域。

选择要配置证书的域名

域名: static.werookies.com

选择证书

证书来源: ● 新上传证书 ○ 已托管证书 ○ SaaS 证书

证书内容: PEM编码

查看样例

私钥内容: PEM编码

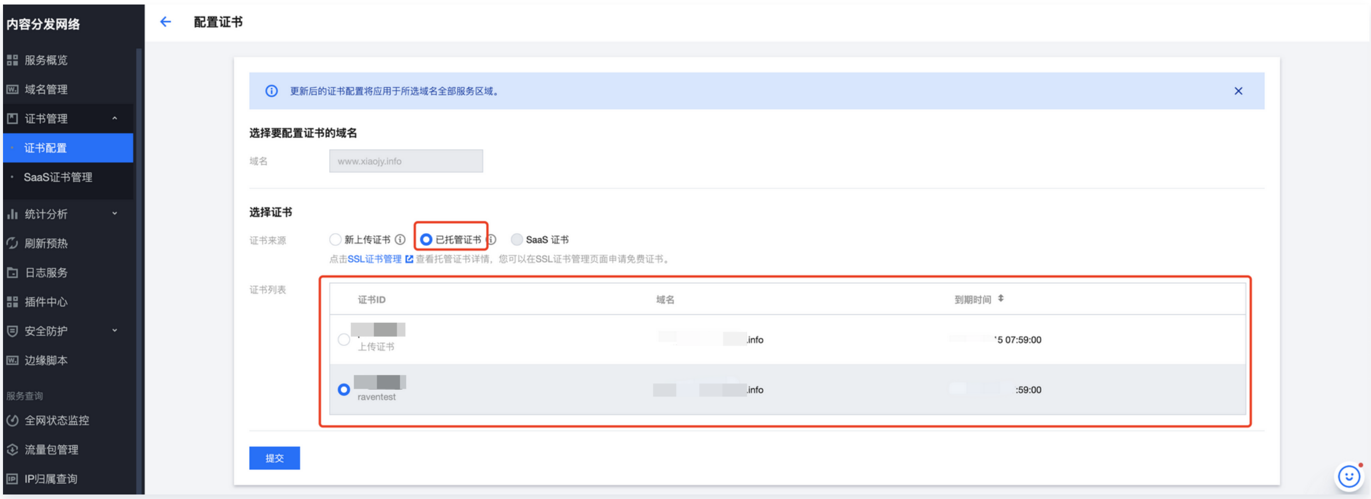
查看样例

托管至 SSL 证书: ☑ 开启

建议您开启托管，即免费将新上传证书托管至SSL证书处。托管后，为其他域名配置时可直接选择，也可通过控制台管理该证书，无需再次上传。

备注（选填）: werookies static

2. If your certificate is a hosted certificate, you can go to the SSL Console to update the certificate and update the association between the domain and the certificate.



更新后的证书配置将应用于所选域名全部服务区域。

选择要配置证书的域名

域名: www.xiaojy.info

选择证书

证书来源: ○ 新上传证书 ● 已托管证书 ○ SaaS 证书

点击SSL证书管理 查看托管证书详情，您可以在SSL证书管理页面申请免费证书。

证书列表

	证书ID	域名	到期时间
○	[redacted] 上传证书	[redacted].info	[redacted]5 07:59:00
●	[redacted] raventest	[redacted].info	[redacted]:59:00

Advanced Configuration
Usage limit configuration

Last updated：2024-12-31 17:42:34

Configuration Scenario

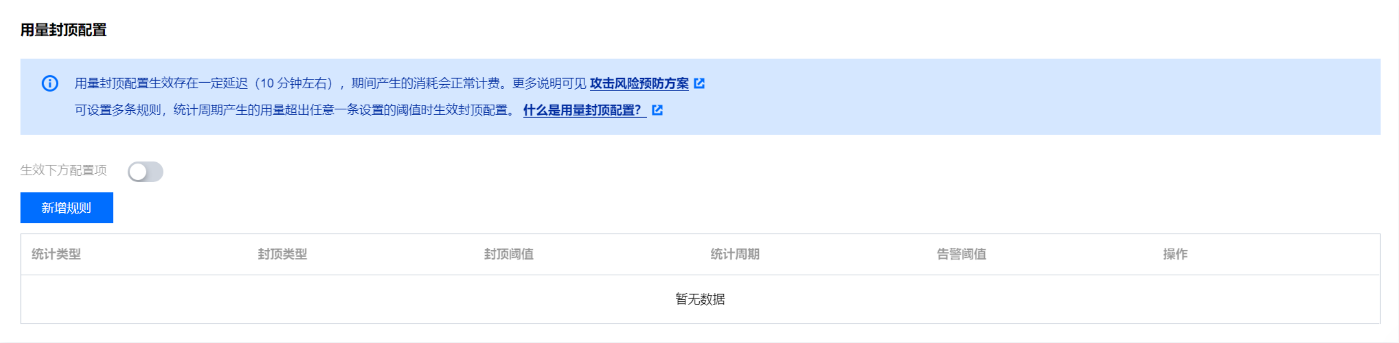
When your prepaid resource package (traffic packages, HTTPS request packages) is exhausted, it will be billed as pay-as-you-go on Tencent Cloud CDN. If you are concerned about large bandwidth or traffic caused by malicious users stealing resources, leading to high bills, you can use the usage limit feature for usage control.
When the bandwidth or traffic usage during a statistical period exceeds the configured alarm threshold, CDN will push a message notification to you; when the access threshold is exceeded, you can disable CDN to avoid incurring more CDN service fees.

> **Note**
> Note: It will take about ten minutes for the usage limit configuration to take effect, during which the usage will be normally billed. For more information, see Attack Risk Prevention Plan .

Configuration Guide

View Configuration

Log in to the CDN console , select **Domain Name Management** from the menu bar, click **Management** on the right side of the domain name to enter the domain name configuration page. In **Advanced Configuration**, you can see the usage limit configuration, which is disabled by default.



用量封顶配置

用量封顶配置生效存在一定延迟（10 分钟左右），期间产生的消耗会正常计费。更多说明可见 攻击风险预防方案
可设置多条规则，统计周期产生的用量超出任意一条设置的阈值时生效封顶配置。 什么是用量封顶配置？

生效下方配置项 ○

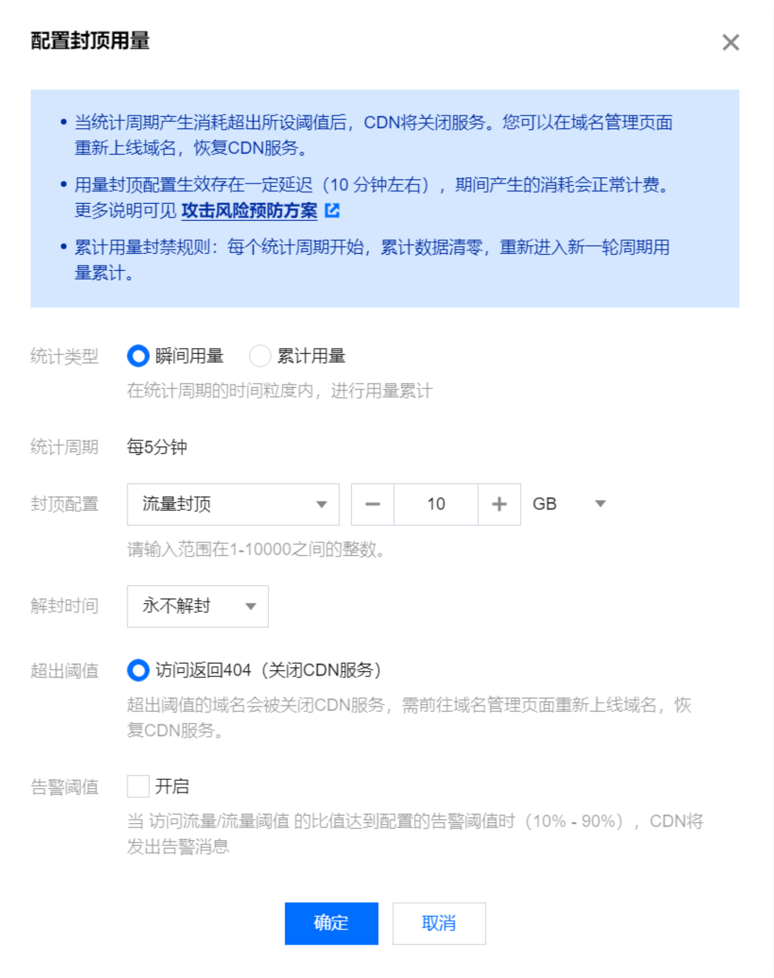
新增规则

统计类型	封顶类型	封顶阈值	统计周期	告警阈值	操作
暂无数据					

Detailed configuration items

1. Adding a new rule

Click Add New Rule to configure:



配置封顶用量

- 当统计周期产生消耗超出所设阈值后，CDN将关闭服务。您可以在域名管理页面重新上线域名，恢复CDN服务。
- 用量封顶配置生效存在一定延迟（10 分钟左右），期间产生的消耗会正常计费。更多说明可见 **攻击风险预防方案**
- 累计用量封禁规则：每个统计周期开始，累计数据清零，重新进入新一轮周期用量累计。

统计类型　● 瞬间用量　○ 累计用量
在统计周期的时间粒度内，进行用量累计

统计周期　每5分钟

封顶配置　流量封顶　10　GB
请输入范围在1-10000之间的整数。

解封时间　永不解封

超出阈值　● 访问返回404（关闭CDN服务）
超出阈值的域名会被关闭CDN服务，需前往域名管理页面重新上线域名，恢复CDN服务。

告警阈值　□ 开启
当 访问流量/流量阈值 的比值达到配置的告警阈值时（10% - 90%），CDN将发出告警消息

- Statistic Type:
  - Instantaneous usage: It collects statistics on the traffic/bandwidth/number of HTTPS requests once every five minutes
  - Cumulative usage: Compared with instantaneous usage, it supports a longer statistical period and provides usage statistics for every hour, calendar day, or calendar month.

> **Note**
> Cumulative usage limit configuration is not supported for domain names with the acceleration type of dynamic content or dynamic & static content.

- Statistical period: Per 5 minutes, per hour, per day (before 24:00 of the day), or per month

> **Note**
> - A statistical period starts from 5 minutes before the configuration time in 5-minute intervals:
> - If the statistical period selection is "per hour," then: (1) For the first data statistical period after setting, the duration will be less than one hour; (2) Entering the next statistical period, usage statistics will be conducted on a natural hour basis. Note: If the rule is configured at 2022-01-13 9:23:10, the first data statistical period is from 9:20:00 to 9:59:59; the next statistical period is from 10:00:00 to 10:59:59.
> - If the statistical period selection is "before 24:00 on the same day," then the cumulative period is from 2022-01-13 9:20:00 to 2022-01-13 23:59:59.
> - If the statistical period selection is "calendar month," then the cumulative period is from 2022-01-13 9:20:00 (effective date) to 2022-01-31 23:59:59, with the next month starting to count from the 1st day at 00:00.

- Capping configuration: Instantaneous usage supports traffic/bandwidth cap; cumulative usage only supports traffic cap.
  - Traffic: It collects statistics on the traffic usage of the domain name. The traffic limit is the maximum traffic for user access to the domain name.

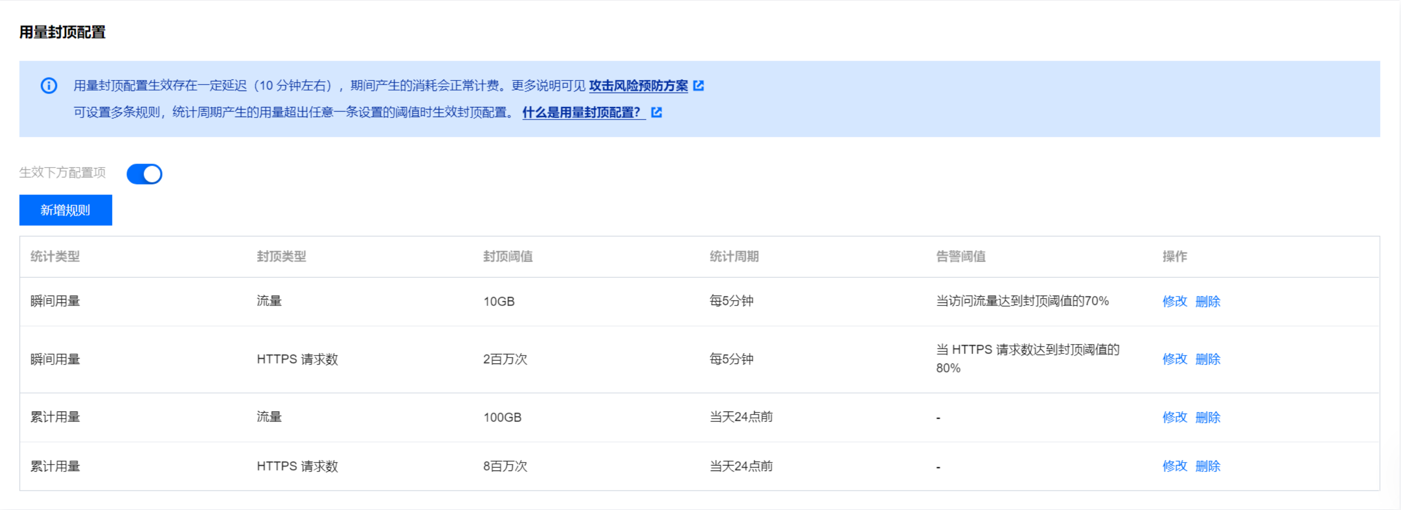
  - Bandwidth: It collects statistics on the bandwidth usage of the domain name. The maximum bandwidth is the maximum bandwidth for user access to the domain name.
  - HTTPS request capping: Refers to the consumption of HTTPS requests for a domain, setting the upper limit for the number of HTTPS requests users can make to that domain.
  - Request capping: Refers to the consumption of requests for a domain, setting the upper limit for the total number of requests users can make to that domain.

> ⚠ **Note**
> Note: HTTPS request capping is only supported for domains with acceleration types of CDN web page small files, CDN large file download, and CDN audio/video on-demand.
> Request cap is only supported for domain names with the acceleration type of ECDN dynamic acceleration and ECDN dynamic & static acceleration. Note: This feature is highlighted.

- Unblocking time: supports scheduled unblocking/never unblock.
  - Scheduled unblocking: Scheduled unblocking supports 60 minutes, 12 hours, 24 hours, 3 days. For example, if the domain ex.com exceeds the threshold, it returns a 404 error (CDN service is disabled), with an automatic unblocking time of 60 minutes. After the domain exceeds the set cumulative usage cap, the CDN service for the domain will be disabled and the acceleration domain will be taken offline. After 60 minutes, the domain will be automatically unblocked and acceleration will be enabled.
  - Never unblock: If you are concerned that your domain may be subject to high traffic/bandwidth attacks, you can set it to never unblock. If set, exceeding the threshold will return a 404 error (CDN service is disabled). Once the domain exceeds the set cumulative usage cap, the domain will be taken offline, and you will need to manually go to the console to enable domain acceleration.
- When cap is exceeded:
  - Access returns 404: Exceeding the threshold will directly disable the CDN service for that domain. You can go to the domain management page to bring the domain back online and restore CDN service.
- Alarm Threshold:
  When the ratio of access bandwidth to traffic limit exceeds the configured percentage (only a multiple of 10 is supported, i.e., 10%-90%), CDN will push an alarm message.

> ⚠ **Note**
> - After detecting that the domain bandwidth (traffic) exceeds the threshold, the configuration to return 404 on access needs to take effect gradually across all network nodes, so there will be a certain effective delay.
> - If the alarm threshold is enabled: As the scanning granularity is 5 minutes, if there is a sudden increase in usage or the configured percentage value is large, it may happen that the percentage threshold is not triggered during the previous scan, and the access threshold is directly reached during the next scan. In this case, CDN will send two notification messages successively: a percentage alarm and an access threshold alarm.
> - Supports configuring multiple rules. Only one rule can be configured for each capping configuration under instant capping and accumulated capping. When any condition threshold is triggered under multiple rules, access returns 404 (i.e., shut down CDN service).

Configuration Example



用量封顶配置

用量封顶配置生效存在一定延迟（10 分钟左右），期间产生的消耗会正常计费。更多说明可见 **攻击风险预防方案**
可设置多条规则，统计周期产生的用量超出任意一条设置的阈值时生效封顶配置。 **什么是用量封顶配置？**

统计类型	封顶类型	封顶阈值	统计周期	告警阈值	操作
瞬间用量	流量	10GB	每5分钟	当访问流量达到封顶阈值的70%	修改 删除
瞬间用量	HTTPS 请求数	2百万次	每5分钟	当 HTTPS 请求数达到封顶阈值的80%	修改 删除
累计用量	流量	100GB	当天24点前	-	修改 删除
累计用量	HTTPS 请求数	8百万次	当天24点前	-	修改 删除

Configuration instructions:

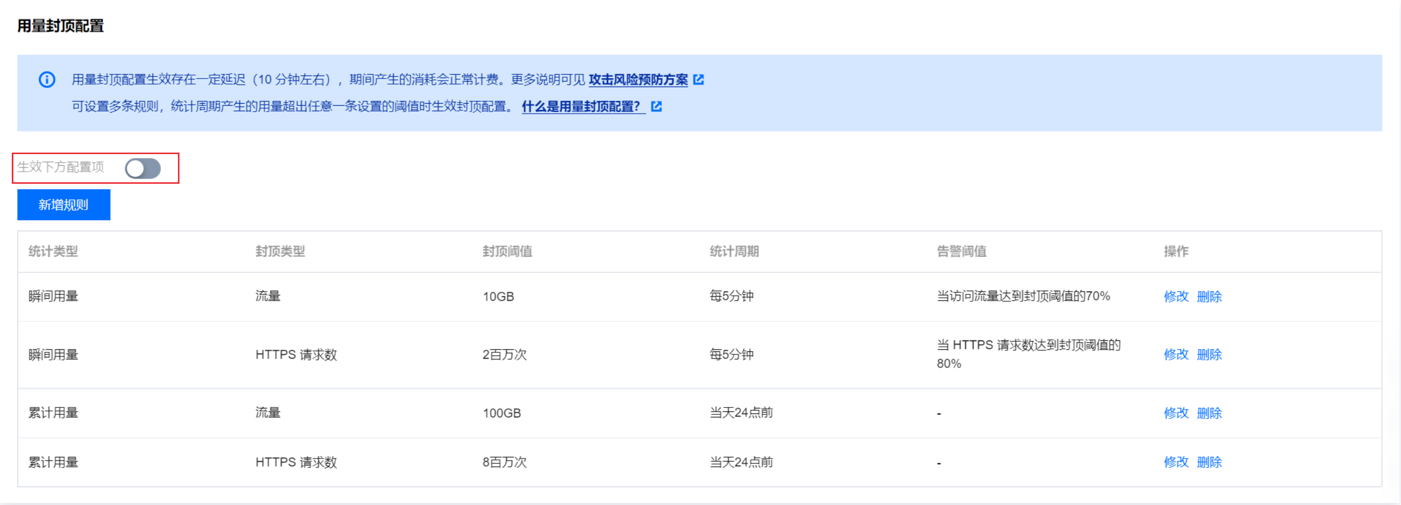
1. 1. If the acceleration domain name consumes 12GB of traffic and 1 million HTTPS requests within 5 minutes, it triggers the 10GB instant traffic capping, and access to the domain name returns 404 in about 10 minutes (shut down CDN service).
2. 2. If the acceleration domain name consumes 3 million HTTPS requests and 5GB of traffic within 5 minutes, it triggers the 2 million instant HTTPS request capping, and access to the domain name returns 404 in about 10 minutes (shut down CDN service).
3. 3. If the acceleration domain name consumes 3 million HTTPS requests and 12GB of traffic within 5 minutes, it triggers the 10GB instant traffic capping and 2 million instant HTTPS request capping, and access to the domain name returns 404 in about 10 minutes (shut down CDN service).
4. 4. If the acceleration domain name accumulates 101GB of traffic and 3 million HTTP requests by 23:00, it triggers the 100GB accumulated traffic capping, and access to the domain name returns 404 in about 10 minutes (shut down CDN service).
5. If the acceleration domain name accumulates 50GB of traffic and 8 million HTTP requests by 23:00, it triggers the 8 million accumulated HTTPS request capping, and access to the domain name returns 404 in about 10 minutes (shut down CDN service).

Note

- Instant usage traffic and bandwidth only support one rule configuration, which is either instant traffic capping or instant bandwidth capping.
- Calendar day and calendar month rules start to be counted from the time the configuration takes effect. For calendar days, the count starts at 00:00, and for calendar months, the count starts at 00:00 on the first day of the next month.

3. Disabling the configuration

You can disable the usage cap by closing the effective configuration item. Even if there is existing configuration below, it will not take effect in the production environment. If needed, re-enable the configuration by turning it on again.



用量封顶配置

用量封顶配置生效存在一定延迟（10 分钟左右），期间产生的消耗会正常计费。更多说明可见 **攻击风险预防方案**
可设置多条规则，统计周期产生的用量超出任意一条设置的阈值时生效封顶配置。 **什么是用量封顶配置？**

统计类型	封顶类型	封顶阈值	统计周期	告警阈值	操作
瞬间用量	流量	10GB	每5分钟	当访问流量达到封顶阈值的70%	修改 删除
瞬间用量	HTTPS 请求数	2百万次	每5分钟	当 HTTPS 请求数达到封顶阈值的80%	修改 删除
累计用量	流量	100GB	当天24点前	-	修改 删除
累计用量	HTTPS 请求数	8百万次	当天24点前	-	修改 删除

HTTP Response Header Configuration

Last updated：2024-12-31 17:42:46

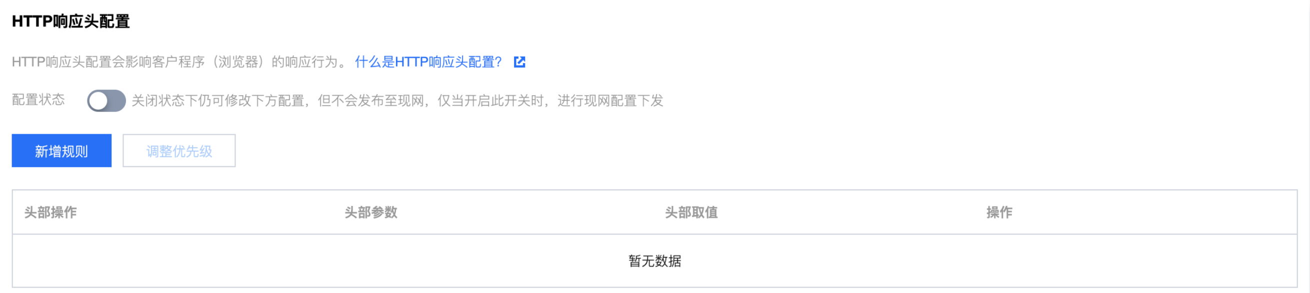
Configuration Scenario

When your business users request business resources, you can configure headers in the returned **response message** to achieve purposes such as cross-domain access. Header configuration works on the domain dimension, so once configured, it will take effect for any resource's response message under the domain. Configuring response headers only affects the client's (e.g., browser) response behavior and does not affect the caching behavior of CDN nodes.

Configuration Guide

Viewing Configuration

Log in to the CDN console, select **Domain Management** from the menu, click **Management** on the right side of the domain to enter the domain configuration page. In **Advanced Configuration**, you can see the response header configuration, which is off by default. Click **Add New Rule** to configure HTTP response header rules:



HTTP响应头配置

HTTP响应头配置会影响客户程序（浏览器）的响应行为。 什么是HTTP响应头配置？

配置状态 关闭状态下仍可修改下方配置，但不会发布至现网，仅当开启此开关时，进行现网配置下发

头部操作	头部参数	头部取值	操作
暂无数据			

Operation Type

Operation Type	Description
Settings	Change the value of the specified response header parameter to the set value. If the specified header does not exist, it will be added. If there are multiple duplicate header parameters, they will all be changed and merged into one header. For example, if the configuration rule is **set x-cdn: value1**, and the request contains multiple x-cdn headers, all headers will be changed and merged into one header x-cdn: value1.
Delete	Delete specified response header parameter.

Note

- Some headers do not support self-service setting/deletion. For the specific list, see the document Note.
- Up to 10 HTTP response header configuration rules can be set.
- Rule priority can be adjusted: rules at the bottom of the list have higher priority. If multiple rules are configured for the same header parameter, the rule at the bottom, i.e., the one with the highest priority, will take effect.

Header Parameter

Header Parameter	Description
Access-Control-Allow-Origin	Used to solve the cross-domain permission issue for resources, the domain value defines the domains allowed to access the resource. If the origin request Host is within the domain configuration list, the corresponding value is directly filled in the return header. A wildcard "*" can also be set to allow requests from all domains. For more information, see Access-Control-Allow-Origin Configuration. Supports inputting "*" or multiple domains/IPs/mixed domain and IP (must include http:// or https://, example: `http://test.com,http://1.1.1.1`, separated by commas) (Note: The input box can accept up to 2000 characters).
Access-Control-Allow-Methods	Indicates which HTTP methods are allowed for cross-origin requests. You can specify multiple methods at a time: Access-Control-Allow-Methods: POST, GET, OPTIONS.

Access-Control-Max-Age	Used to specify the valid time of preflight request, in seconds. For non-simple cross-origin requests, an additional HTTP query request, called a "preflight request," is required before formal communication to determine if the cross-origin request is safe and acceptable. The following requests are considered non-simple cross-origin requests: initiated by methods other than GET, HEAD, or POST, or using POST with data types other than application/x-www-form-urlencoded, multipart/form-data, or text/plain, such as application/xml or text/xml. Use the custom request header: Access-Control-Max-Age:1728000, indicating that within 1728000 seconds (20 days), no additional preflight request will be sent for cross-origin access to the resource.
Access-Control-Expose-Headers	Used to specify which headers can be exposed to the client as part of the response. By default, only 6 headers can be exposed to the client: Cache-Control, Content-Language, Content-Type, Expires, Last-Modified, Pragma. If you want the client to access other header information, you can set it as follows. When entering multiple headers, separate them with "," such as: Access-Control-Expose-Headers: Content-Length,X-My-Header, indicating that the client can access the Content-Length and X-My-Header headers.
Content-Disposition	This header activates download in the browser and sets the default name of the downloaded file. When the server sends a file to the client browser, if it is a file type supported by the browser, such as TXT, JPG, etc., it will be opened directly with the browser by default. If you need to prompt the user to save, you can override the browser's default behavior by configuring the Content-Disposition field. Common configuration is as follows: Content-Disposition:attachment;filename=FileName.txt
Content-Language	Used to define the language code used by the page. Common configuration is as follows: Content-Language: zh-CN Content-Language: en-US
Custom	Support adding custom headers, custom key-value settings. Custom header parameters: composed of uppercase and lowercase letters, numbers, and -, length support 1 - 100 characters. Custom header values: length 1 - 2000 characters, Chinese not supported.

Introduction to Access-Control-Allow-Origin Matching Patterns

Matching Mode	Value	Note:
Full Match	*	When set to *, the header `Access-Control-Allow-Origin:*` is included in the response.

Fixed Match	`http://cloud.tencent.com`
	`https://cloud.tencent.com`
	`http://www.b.com`
		The origin `https://cloud.tencent.com` hits the list, so the header `Access-Control-Allow-Origin: https://cloud.tencent.com` is included in the response.
		The origin `https://www.qq.com` does not hit the list, no change in response.

Second-level wildcard domain matching	`https://*.tencent.com`	The origin `https://cloud.tencent.com` hits the list, so the header `Access-Control-Allow-Origin: https://cloud.tencent.com` is included in the response. The origin `https://cloud.qq.com` does not hit the list, no change in response.
Port Matching	`https://cloud.tencent.com:8080`	When the source is `https://cloud.tencent.com:8080` , which hits the list, the header `Access-Control-Allow-Origin:https://cloud.tencent.com:8080` is added to the response. When the source is `https://cloud.tencent.com` , which does not hit the list, the response is not changed.

⚠ **Note**

> If there are special ports, you need to enter the relevant information in the list. You must specify the port as arbitrary port match is not supported.

Must-Knows

This feature does not support the following headers, meaning the following headers will not take effect:

```
Date
Expires
Content-Type
Content-Encoding
Content-Length
Transfer-Encoding
Cache-Control
If-Modified-Since
Last-Modified
Connection
Content-Range
ETag
Accept-Ranges
Age
Authentication-Info
Proxy-Authenticate
Retry-After
Set-Cookie
Vary
WWW-Authenticate
Content-Location
Content-MD5
Content-Range
Meter
Allow
Error
```

SEO Configuration

Last updated：2024-12-31 17:42:58

Configuration Scenario

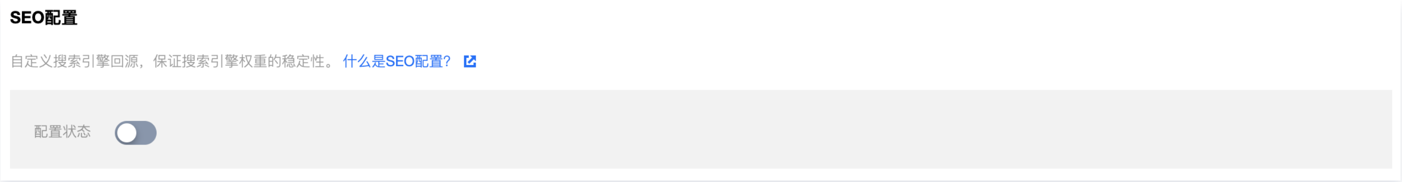
SEO configuration is a feature that solves the problem of incorrect weights for domain name searches due to frequent IP changes by CDN after a domain name is connected to CDN. By identifying whether an access IP belongs to a search engine, you can choose to directly pull the resource from the origin server, ensuring the stability of search engine weights.

> **Note**
> - As search engine IPs are updated very frequently, Tencent Cloud CDN can only guarantee that most but not all search engine IPs can be identified.
> - The SEO configuration feature is only available when the domain's origin type is Self-owned origin server. Note: After enabling the SEO configuration, if there are multiple origin server addresses for the domain, the default origin-pull address will be the first one added.
> - This feature is not supported in regions outside the Chinese mainland currently. If the acceleration region of your domain name is outside the Chinese mainland, this feature cannot be enabled. If your domain name is configured for global acceleration, the SEO configuration will take effect only within Chinese mainland.

Configuration Guide

Viewing Configuration

Log in to the CDN console, select **Domain Management** from the menu, click **Management** on the right side of the domain to enter the domain configuration page. In **Advanced Configuration**, you can see the SEO configuration, which is disabled by default:



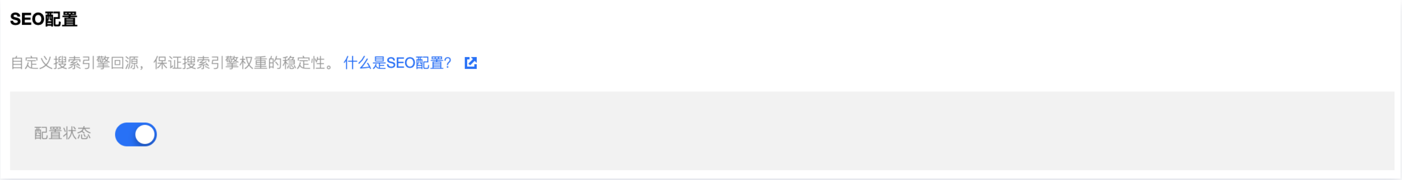
SEO配置

自定义搜索引擎回源，保证搜索引擎权重的稳定性。什么是SEO配置？

配置状态 ○

Modify

You can toggle the switch to enable or disable the SEO configuration service:



SEO配置

自定义搜索引擎回源，保证搜索引擎权重的稳定性。什么是SEO配置？

配置状态 ●

Smart Compression Configuration

Last updated：2024-12-31 17:43:10

Configuration Scenario

With the aid of smart compression, Tencent Cloud CDN can compress the returned resources with Gzip or Brotli according to set rules, which effectively reduces the size of transferred content and costs.

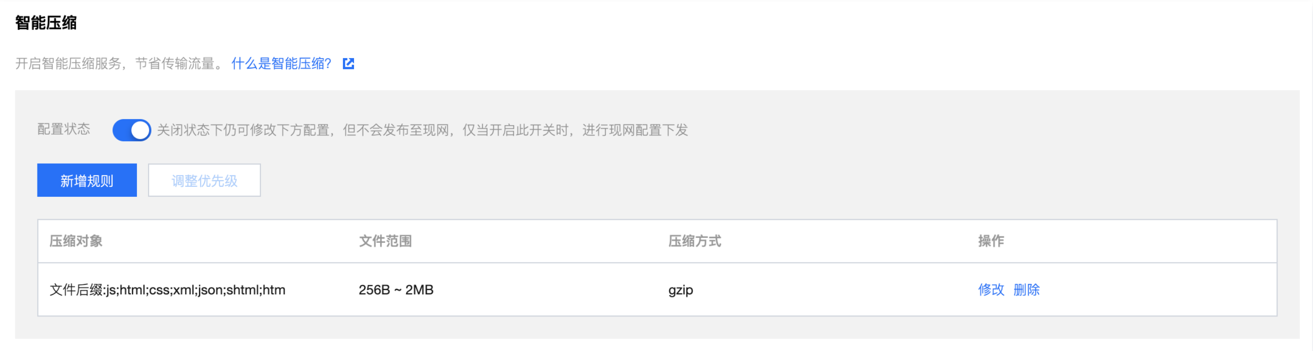
> **Note**
> If your domain name is configured for global acceleration, the smart compression configuration will take effect globally. Regional-specific configurations are not supported.

Configuration Guide

Viewing Configuration

Log in to the CDN Console, select **Domain Name Management** from the menu bar, click **Management** on the right side of the domain name to enter the domain name configuration page, and you can see the smart compression configuration in **Advanced Configuration**, which is enabled by default:

- After an acceleration domain name is connected, resources with sizes ranging from 256 bytes to 2 MB with file extensions .js, .html, .css, .xml, .json, .shtml, and .htm will be compressed with Gzip by default.



智能压缩

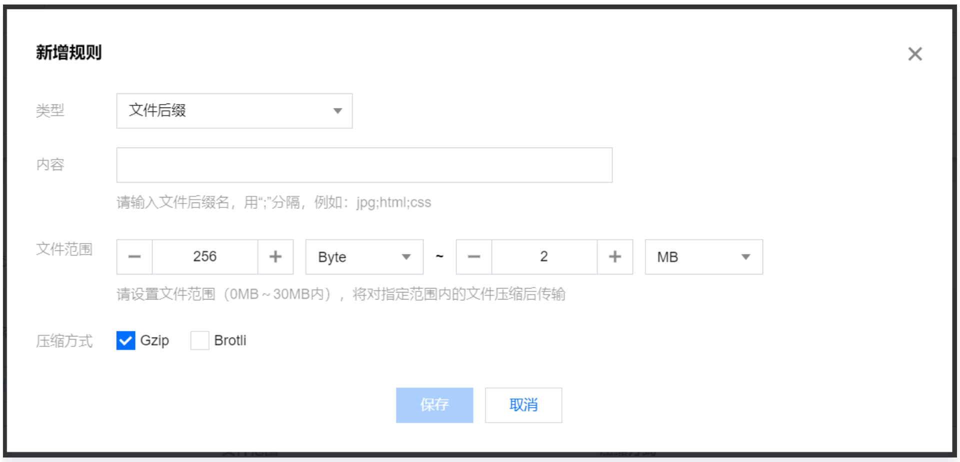
开启智能压缩服务，节省传输流量。什么是智能压缩？

配置状态 ● 关闭状态下仍可修改下方配置，但不会发布至现网，仅当开启此开关时，进行现网配置下发

压缩对象	文件范围	压缩方式	操作
文件后缀:js;html;css;xml;json;shtml;htm	256B ~ 2MB	gzip	修改 删除

Modify

Click **Modify** in the operation column to modify the compression rules:



新增规则

类型: 文件后缀

内容:

请输入文件后缀名，用“;”分隔，例如：jpg;html;css

文件范围: 256 Byte ~ 2 MB

请设置文件范围（0MB ~ 30MB内），将对指定范围内的文件压缩后传输

压缩方式: ☑ Gzip □ Brotli

Configuration limitations

- The default type is file suffix. You can configure all files or specify Content-Type types as needed.
- The total length of the file suffix type content cannot exceed 200 characters.
- The default content types for file Content-Type are text/html;text/xml;text/plain;text/css;text/javascript;application/json;application/javascript;application/x-

javascript;application/rss+xml;application/xml;image/svg+xml;image/tiff. You can configure as needed, up to 100 groups, separated by ";", with each group not exceeding 50 characters.

- Some platforms are being upgraded and do not support the file type (content-type) and Brotli compression.

Precautions

- If Brotli is selected only and the request compression header is gzip, the original resources will be returned without being compressed; if Gzip is selected only and the request compression header is br, the original resources will be returned without being compressed.
- If both Gzip and Brotli compression are enabled and the client request header Accept-Encoding includes both br and gzip:
  - If the CDN node has cached resources compressed in both br and gzip, Brotli compressed resources are returned first.
  - If the CDN node has cached resources compressed only in br, Brotli compressed resources are returned first.
  - If the CDN node has cached resources compressed only in gzip, Gzip compressed resources are returned first.
- Common image file types (PNG, JPG, JPEG, etc.) and video file types (MP4, AVI, WMV, etc.) are already compressed, so enabling Gzip or Brotli compression will have no effect. You do not need to enable compression response for these files.
- If the origin server has enabled the compression feature and the server response header includes Content-Encoding, the CDN compression feature will not take effect.

Custom Error Page

Last updated：2024-12-31 17:43:21

Feature Introduction

You can configure the custom error page, and redirect requests with the specified status code to the specified URL.
Currently supported status codes are as follows:

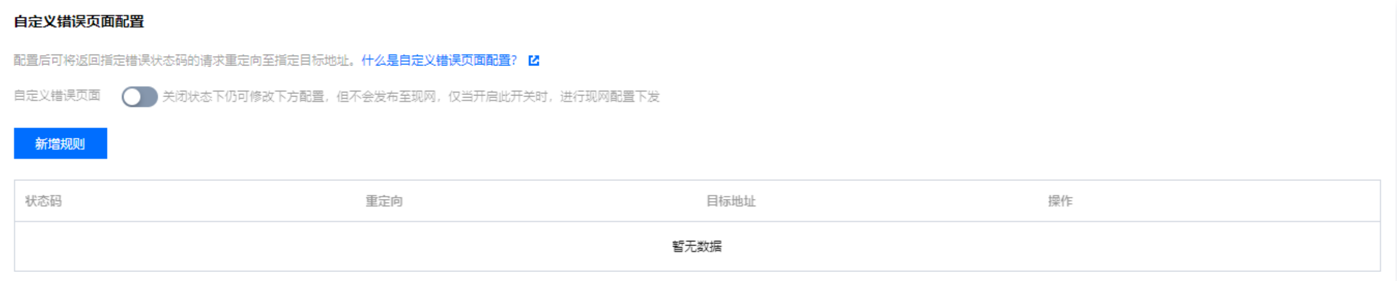
- 4XX: 400, 403, 404, 405, 414, 416, 451
- 5XX: 500, 501, 502, 503, 504

> **Note**
> This feature is only for redirecting requests encountered status codes during origin-pull, but not applicable to requests with status codes returned by any access control features such as the UA blocklist/allowlist configuration.

Configuration Guide

Viewing Configuration

Log in to the CDN Console, select **Domain Management** from the left sidebar menu, click **Management** in the domain operation column to enter the domain configuration page, switch the tab to **Advanced Configuration**, and find the **Custom Error Page Configuration**.
By default, the custom error page configuration is in closed status:



自定义错误页面配置

配置后可将返回指定错误状态码的请求重定向至指定目标地址。什么是自定义错误页面配置？

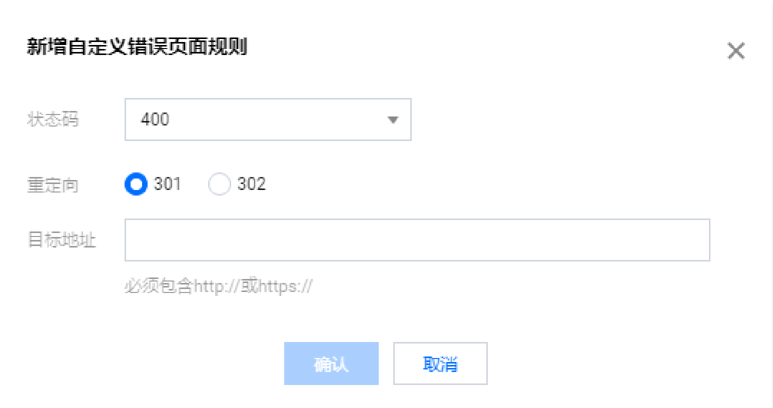
自定义错误页面 ○ 关闭状态下仍可修改下方配置，但不会发布至现网，仅当开启此开关时，进行现网配置下发

新增规则

状态码	重定向	目标地址	操作
暂无数据			

Adding rules

You can add custom error page rules as needed by clicking **Adding Rules**:



新增自定义错误页面规则

状态码 400

重定向 ● 301 ○ 302

目标地址

必须包含http://或https://

确认 取消

Configuration limitations

- Only one rule can be added for each status code, cannot be added repeatedly.
- Redirect: 301 or 302.
- Target address: must include `http://` or `https://` .
- The content can contain up to 1,024 characters and Chinese characters are not supported.

POST Request Size Configuration

Last updated：2024-12-31 17:43:32

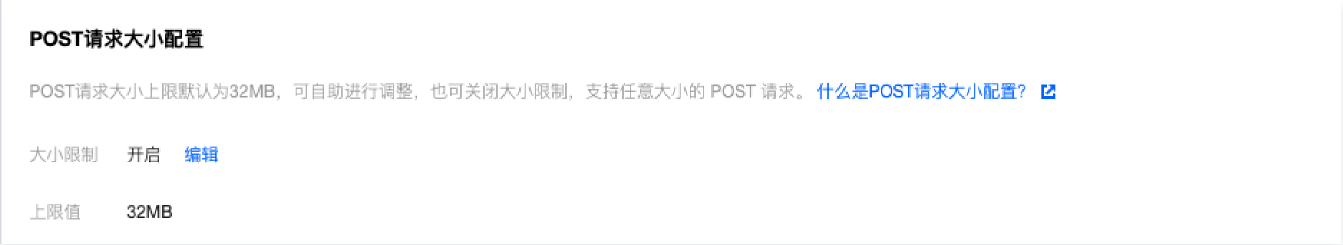
Feature Description

The maximum size of a Tencent Cloud CDN POST request (body) defaults to 32 MB, which can be adjusted as required by your business.

Configuration Guide

View Configuration

Log in to the CDN Console, select **Domain Management** from the left sidebar menu, click **Management** in the domain operation column to enter the domain configuration page, switch the tab to **Advanced Configuration**, and you will find the **POST Request Size Configuration**. The POST request size limit can be customized to enable/disable, and it is disabled by default. When enabled, the maximum adjustable limit is 200 MB.



POST请求大小配置

POST请求大小上限默认为32MB，可自助进行调整，也可关闭大小限制，支持任意大小的 POST 请求。 什么是POST请求大小配置?

大小限制 开启 编辑

上限值 32MB

> **Note**
> On some platforms, there is no size limit on POST requests, and the feature is not supported for some domain names.

WebSocket Configuration

Last updated：2024-12-31 17:43:41

If your business involves scenarios such as barrage chat, interactive live streaming, social subscriptions, collaborative sessions, multiplayer games, market broadcast, sports live update, online education, and IoT, you can configure WebSocket in ECDN for full-site acceleration.

Feature Introduction

WebSocket is a TCP-based persistent protocol that implements full-duplex communication between the client and server and allows the server to proactively send information to the client. Before the emergence of WebSocket, to implement such duplex communication, web applications needed to continuously send HTTP request calls for inquiry, which increased service costs and reduced efficiency. WebSocket has the advantage of full-duplex communication, where the client and server only need to complete a handshake to create a persistent connection and achieve bidirectional data transmission, better saving server resources and bandwidth, and enabling more real-time communication.

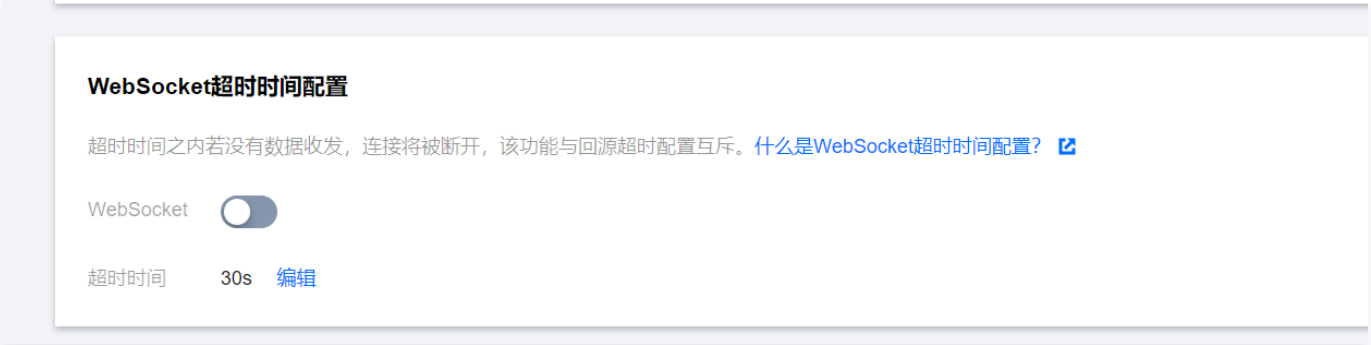
Notes

1. WebSocket is a feature of ECDN full-site acceleration. Before configuring WebSocket, please select an ECDN full-site acceleration domain.
2. WebSocket is a dynamic resource that does not require any caching rules and needs the origin server to support WebSocket.
3. The maximum timeout configuration for WebSocket can be set to 300s. If there is no message passing within the configured time, the default close connection will occur.

Configuration Instructions

Configuration in domain management

1. Log in to the CDN Console.
2. Click **Domain Management** in the left menu to enter the domain management list;
3. Select the ECDN full-site acceleration domain name to be configured, click **manage and enter** the domain configuration page.
4. Click **Advanced Configuration**, find the WebSocket timeout configuration, and you can enable WebSocket;



WebSocket超时时间配置

超时时间之内若没有数据收发，连接将被断开，该功能与回源超时配置互斥。什么是WebSocket超时时间配置？

WebSocket

超时时间 30s 编辑

5. After enabling WebSocket, you can customize the timeout duration within 0-300s.

Recommended Configuration

WebSocket is a session connection established between the client and the origin server. It is recommended to configure the WebSocket timeout according to your heartbeat mechanism. If your WebSocket does not have a heartbeat mechanism, it is recommended to set the WebSocket timeout to 60s.

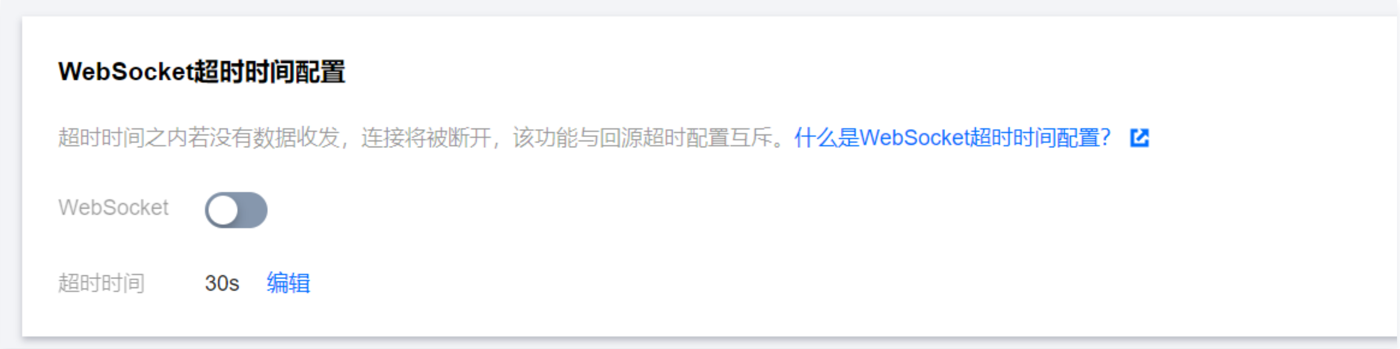
Configuration limitations

WebSocket timeout configuration is only supported for ECDN full-site acceleration domains. If your domain does not belong to an ECDN full-site acceleration domain (acceleration type is ECDN dynamic and static acceleration or ECDN dynamic acceleration), your domain will not be able to configure WebSocket.

Configuration Example

Sample 1

If WebSocket is in closed status, the WebSocket timeout configuration for the domain `cloud.tencent.com` is as follows:



WebSocket超时时间配置

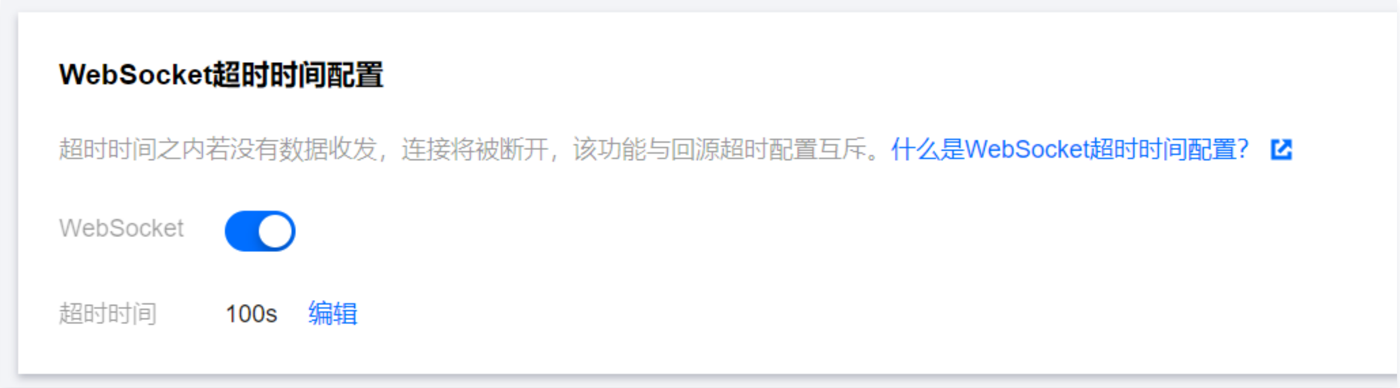
超时时间之内若没有数据收发，连接将被断开，该功能与回源超时配置互斥。什么是WebSocket超时时间配置？

超时时间 30s

`cloud.tencent.com` does not support WebSocket protocol. If there are WebSocket requests, the connection is easily disconnected or failed.

Sample 2

If WebSocket is in enable status and the timeout configuration is 100s, the WebSocket timeout configuration for the domain `cloud.tencent.com` is as follows:



WebSocket超时时间配置

超时时间之内若没有数据收发，连接将被断开，该功能与回源超时配置互斥。什么是WebSocket超时时间配置？

超时时间 100s

`cloud.tencent.com` supports WebSocket protocol. The session persistence time of the protocol follows the WebSocket timeout configuration of 100s. If there is no communication request for more than 100s, the connection will be disconnected.

Associated FAQs

Does CDN support WebSocket?

Image Optimization

Last updated：2024-12-31 17:43:52

Configuration Scenario

When distributing mass images with Tencent Cloud CDN, you can enable image optimization. This feature can automatically compress images that meet specified requirements into WebP, Guetzli, TPG, and AVIF formats, effectively reducing downstream traffic and costs.

> ⚠ Note
>
> If you are currently using the Image Processing feature of Cloud Infinite, adding image processing style parameters to the URL may affect the normal use of this feature and cause the image format to be unable to recognize normally. Therefore, if you need to use both, it is recommended to complete image compression in the image processing style together.

Configuration Guide

Log in to the CDN console, select **Domain Management** from the menu bar, click **Manage** on the right side of the domain to enter the domain configuration page. When the origin server is COS, you can see the **Image Optimization** menu bar:

- The relevant configuration can only be performed when the origin server is COS and the version is COS V5.
- If you have not yet opened the Cloud Infinite service, you can one-click activate it on this page and then proceed with the related configuration for image processing.
- If you have activated the CI service, you can directly configure and enable it.
- If the same image format matches multiple enabled image adaptation features, they will take effect in the order of priority from high to low: AVIF > Guetzli > TPG > WebP. For example, if both AVIF adaptation and WebP adaptation are enabled, and the HTTP request header accept includes image/avif and image/webp when requesting the a.jpg file, image optimization will prioritize AVIF adaptation and convert the image format to AVIF.

> ⓘ Note:
>
> CI is a secure, stable, and efficient cloud data processing service provided by Tencent Cloud. Image processing with WebP, Guetzli, TPG, and other formats will incur CI service charges. Click Billing Instructions for more details.

WebP adaptation

After enabling the WebP adaptive image compression feature, requests that meet the following conditions will directly return the WebP processed image. If the conditions are not met, the original image will be returned:

- The HTTP request header accept includes image/webp.
- The image is in JPG, JPEG, BMP, GIF, or PNG format.

> ⚠ Note
>
> - The cost generated by WebP image compression is attributed to DataV - Basic Image Processing Fees.
> - The image to be processed should not be larger than 20 MB, with the width and height not exceeding 30,000 pixels and the total number of pixels not exceeding 100 million. The width and height of the output image should not exceed 9,999 pixels.
> - For an animated image, the total number of pixels (Width * Height * Number of frames) cannot exceed 100 million pixels, and the number of GIF frames is limited to 300.

Guetzli adaptation

Guetzli image compression is a visually lossless compression service launched by CI, which can compress JPG images at a high ratio, saving download traffic for users, speeding up download times, and improving user experience. It takes advantage of the human eye's insensitivity to certain color gamuts and image details, selectively discarding detail information without affecting visual effects, resulting in approximately 35% to 50% savings in image traffic compared to the original image with the same visual effect. After enabling the Guetzli adaptive image compression feature, requests that meet the following conditions will directly return the image processed by Guetzli:

- The accept header in the HTTP request header contains image/guetzli.
- The image is in JPG or JPEG format.

> ⚠ **Note**
> - Fees incurred by Guetzli image compression are attributed to DataV-Guetzli compression cost.
> - After you enable Guetzli, the original JPG image will be returned when you access the image for the first time, and Guetzli will compress the image asynchronously. If you request the image again after the compression is complete, the compressed image will be returned.
> - Currently, Guetzli can process JPG images whose quality is greater than 70 and number of pixels is smaller than 4 million.

TPG adaptation

TPG compression is an advanced image compression feature provided by Tencent Cloud CI. It converts specified format images into TPG format, greatly reducing the image size, thereby significantly lowering image traffic and improving page load speed.
After enabling the TPG adaptive image compression feature, requests that meet the following conditions will return TPG processed images directly:

- The accept header in the HTTP request header includes image/tpg.
- The image is in JPG, JPEG, BMP, GIF, PNG, or WebP format.

> ⚠ **Note**
> Note: The cost generated by TPG image compression is categorized under DataV's advanced image compression cost.

Adapting to AVIF

AVIF compression is an advanced image compression feature provided by CI. This feature allows the conversion of specified format images into the AVIF format, significantly reducing image size, thus significantly reducing image traffic and improving page loading speed. AVIF is a new image format based on AV1, first introduced by Netflix in February 2020, and is currently supported by browsers such as Chrome and Firefox.
After enabling the AVIF adaptive image compression feature, requests that meet the following conditions will directly return the processed images in AVIF format:

- The HTTP request header includes "image/avif" in the accept part.
- The image is in JPG, JPEG, PNG, BMP, or GIF format.

> ⓘ **Note:**
> - The cost of AVIF compression is attributed to DataV - advanced image compression cost.
> - Size: The input image cannot be larger than 32 MB, with its width and height not exceeding 30,000 pixels, and the total number of pixels not exceeding 250 million. The width and height of the output image cannot exceed 9,999 pixels. For an input animated image, the total number of pixels (Width x Height x Number of frames) cannot exceed 250 million pixels.
> - Number of frames (for animated images): For GIF, the number of frames cannot exceed 300.

Notes

After enabling the adaptive image compression feature:

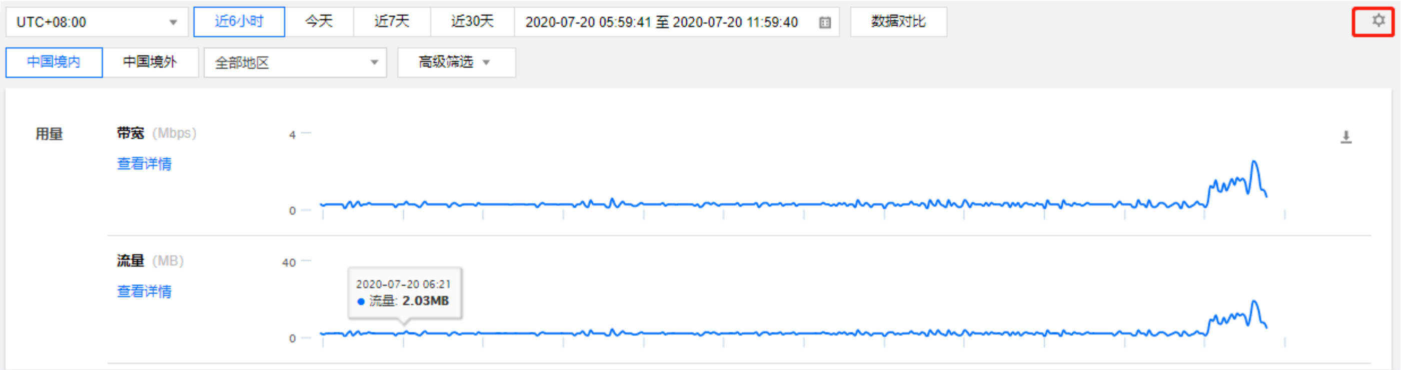
1. The cache key for accessing a URL will change, but the priority of cache key rules at **Cache Configuration - Cache Key Rule Configuration** is higher.
   For example, if image optimization is enabled for jpg files, the request URL `http://www.test.com/a.jpg` will change to `http://www.test.com/a.jpg?xxxxxx`. If **Cache Configuration - Cache Key Rule Configuration** has been set to: all files - ignore all parameters, which has a higher priority, then ignoring all parameters will take effect, and the final request URL will change to `http://www.test.com/a.jpg`.
2. If your origin server has not separately set the Cache-Control header, for compressed images, DataV will default to returning the response header Cache-Control: max-age=2592000. This may cause the browser cache expiration time for compressed and uncompressed images to be inconsistent. You can control the cache expiration time through Browser Cache Validity Configuration.

Statistics and Analysis
Real-Time monitoring
Panel Configuration

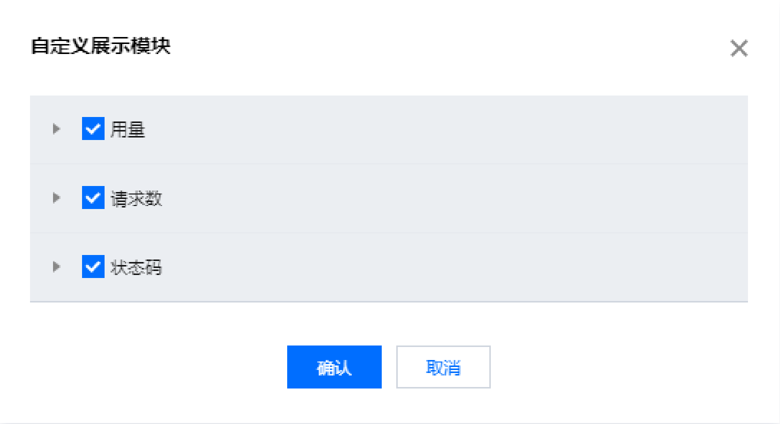
Last updated：2024-12-31 17:44:18

The new real-time monitoring page supports adjusting the indicator panel as needed, making it convenient for you to view the monitoring curves of the indicators you are concerned about.

1. Log in to the CDN console, in the left sidebar, select **Statistical Analysis** > **Real-Time Monitoring**, and enter the management page.
2. Click the configuration icon on the right to enter the configuration page.



3. Select data indicators to display on the overview page as needed: selected indicators will be directly displayed on the overview page, uncheck to default not to display. Real-time monitoring **Access Monitoring** and **Origin-Pull Monitoring** overview pages can both be configured with custom panels.


自定义展示模块

☑ 用量

☑ 请求数

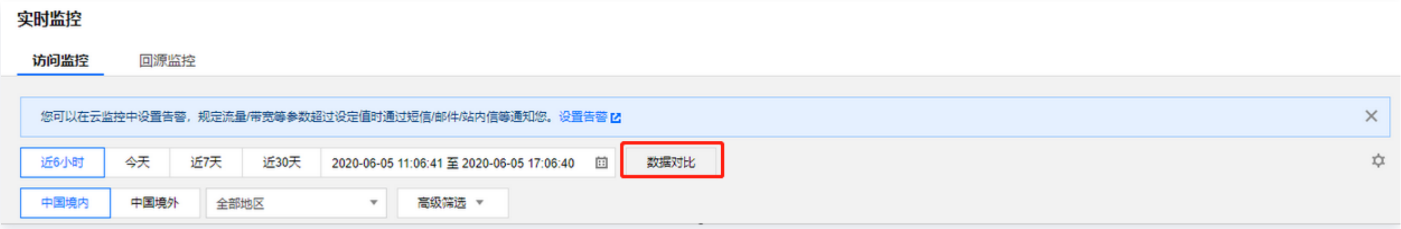
☑ 状态码

Data Comparison

Last updated：2024-12-31 17:44:29

Each subpage of the new real-time monitoring page supports the data curve comparison feature.

1. Log in to the CDN console, in the left sidebar, select **Statistical Analysis** > **Real-Time Monitoring** to enter the management console.
2. After querying the monitoring curve for the specified time interval, click **Data Comparison**, specify the time period, and you can perform data comparison display.

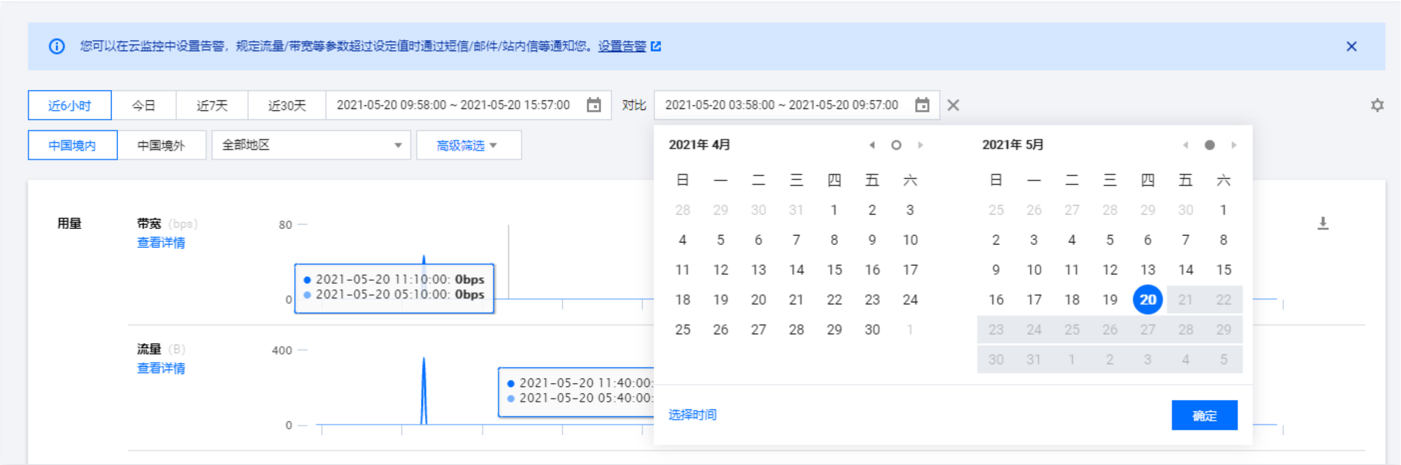


实时监控

您可以在云监控中设置告警，规定流量/带宽等参数超过设定值时通过短信/邮件/站内信等通知您。设置告警

2020-06-05 11:06:41 至 2020-06-05 17:06:40

For your convenience, after specifying the start time, the system will automatically fill in the end time; after specifying the end time, the system will automatically fill in the start time to ensure the consistency of the comparison time period.



您可以在云监控中设置告警，规定流量/带宽等参数超过设定值时通过短信/邮件/站内信等通知您。设置告警

2021-05-20 09:58:00 ~ 2021-05-20 15:57:00 对比 2021-05-20 03:58:00 ~ 2021-05-20 09:57:00

2021-05-20 11:10:00: 0bps
2021-05-20 05:10:00: 0bps

2021-05-20 11:40:00:
2021-05-20 05:40:00:

Access Monitoring

Last updated：2024-12-31 17:44:40

Metric Description

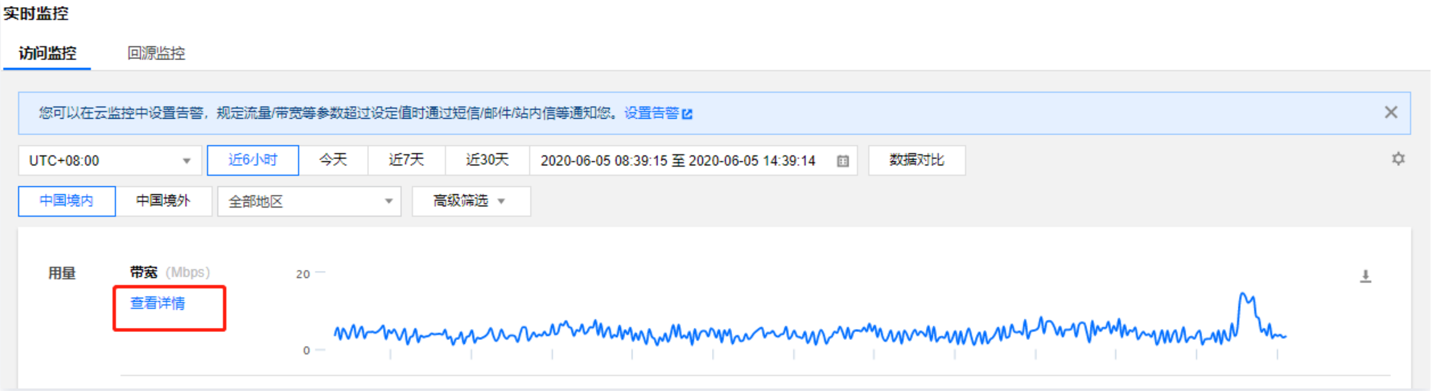
Overview Page Metrics Explanation

Log in to the CDN console, select **Statistical Analysis** > **Real-Time Monitoring** from the left sidebar. After entering the management console, the **Access Monitoring** subpage is displayed by default. It returns the monitoring curve of all domains with a 1-minute granularity for the past 6 hours, including the following metrics:

- Bandwidth: Calculated by dividing the total traffic in one minute by 60 seconds.
- Traffic hit rate: (Total downstream traffic - origin-pull traffic) / total downstream traffic in one minute.
- Percentage of request status codes: Percentage chart of 2XX/3XX/4XX/5XX status codes within the selected time period.
- 2XX request status codes: Status codes generated by 2XX status code monitoring will be counted.
- 3XX request status codes: Status codes generated by 3XX status code monitoring will be counted.
- 4XX request status codes: Status codes generated by 4XX status code monitoring will be counted.
- 5XX request status codes: Status codes generated by 5XX status code monitoring will be counted.

Data on the details page

Click **Viewing Details** under each indicator to enter the metric detail page.

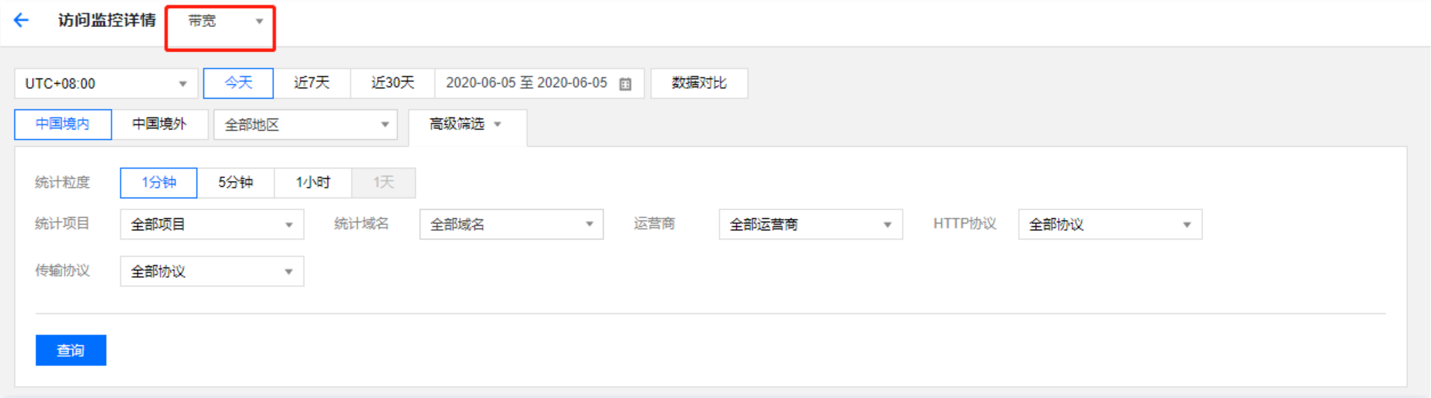


实时监控

您可以在云监控中设置告警，规定流量/带宽等参数超过设定值时通过短信/邮件/站内信等通知您。设置告警

UTC+08:00 近6小时 2020-06-05 08:39:15 至 2020-06-05 14:39:14

You can also quickly switch indicators through the top left on the detail page.



访问监控详情 带宽

UTC+08:00 今天 2020-06-05 至 2020-06-05

统计粒度 1分钟

统计项目 全部项目

统计域名 全部域名

运营商 全部运营商

HTTP协议 全部协议

传输协议 全部协议

The following data can be viewed on the detail page:

- Bandwidth: Total peak bandwidth, real-time bandwidth curve, and bandwidth rankings of domain names (from large to small).
- Traffic: Total traffic, real-time traffic curve, traffic rankings of domain names (from high to low), and traffic rankings of URLs (from high to low).
- Traffic hit rate: Traffic hit rate, real-time traffic hit rate curve, and traffic hit rate rankings of domain names (from high to low).
- Requests: Total requests, real-time request curve, domain request ranking (from high to low), and URL request ranking (from high to low).
- Status code percentage: Pie chart of 2XX, 3XX, 4XX, and 5XX status codes and their counts and percentages.

- 2XX status codes: Real-time monitoring curve of 2XX status codes and their sub-status codes and 2XX status code rankings of domain names (from high to low).
- 3XX status codes: Real-time monitoring curve of 3XX status codes and their sub-status codes and 3XX status code rankings of domain names (from high to low).
- 4XX status codes: Real-time monitoring curve of 4XX status codes and their sub-status codes and 4XX status code rankings of domain names (from high to low).
- 5XX status codes: Real-time monitoring curve of 5XX status codes and their sub-status codes and 5XX status code rankings of domain names (from high to low).

Granularity Description

Granularity description on the overview page

The monitoring page provides curve display options with 1-minute, 5-minute, 1-hour, and 1-day granularity. The minimum displayable time granularity varies based on the selected time interval:

- Time period ⩽ 6 hours: The minimum time granularity is 1 minute. The latency for displaying the 1-minute curve is about 5-10 minutes.
- 6 hours < time period ⩽ 24 hours: The minimum time granularity is 5 minutes. The latency for displaying the 5-minute curve is about 5-10 minutes.
- 24 hours < time period ⩽ 31 days: The minimum time granularity is 1 hour.
- Time period > 31 days: The minimum time granularity is 1 day.

Granularity description on the details page

The time granularity options on the metric details page are as follows:

- Time period ⩽ 1 day: The minimum time granularity is 1 minute. The latency for displaying the 1-minute curve is about 5-10 minutes.
- 1 day < time period ⩽ 31 days: The minimum time granularity can be 5 minutes, 1 hour, or 1 day.
- Time period > 31 days: The minimum time granularity is 1 day.

> **Note**
> - Currently, data query at 1-minute statistics granularity is only supported in mainland China. The minimum granularity for historical data query is 5 minutes.
> - The maximum queryable time interval is the past 90 days.

Aggregation Description

Depending on the data metrics, the aggregation from 1-minute granularity to 5 minutes, 1 hour, or 1 day varies:

- Bandwidth: The smallest granularity provided by CDN for monitoring bandwidth data is 1 minute. Based on industry standard, fees are generally billed by 5-minute granularity, which is calculated by taking the average of 1-minute data values. Therefore, the bandwidth data at a 1-hour or 1-day granularity can be calculated based on the maximum 5-minute bandwidth value.
- Traffic: The traffic data at a 5-minute, 1-hour, or 1-day granularity is obtained by aggregating 1-minute traffic data.
- Traffic hit rate: The traffic hit rate is calculated using the same formula (total downstream traffic - origin traffic) / total downstream traffic based on the selected time granularity, rather than using the arithmetic average of 1-minute result data.
- Number of requests and status codes: Data at a 5-minute, 1-hour, or 1-day granularity is obtained by aggregating 1-minute data.

Data source description

Billable data and log data

- The data counted based on the downstream bytes in the log of an accelerated domain name is application-layer data. The network traffic generated by actual data transfers over the network is around 5-15% more than application-layer traffic.
- TCP/IP headers consumption: For TCP/IP-based HTTP requests, each packet can be up to 1,500 bytes and includes a 40-byte TCP and IP header, which generate traffic during transfer but cannot be counted by the application layer. The overhead of this part is around 3%.

- TCP retransmission: During normal data transfer over the network, around 3–10% of packets are lost on the Internet and retransmitted by the server. This type of traffic cannot be counted by the application layer and accounts for 3–7% of the total traffic.
- As an industry standard, the billable data is the sum of the application-layer data and the above-mentioned overheads. Tencent Cloud CDN takes 10% as the overheads proportion, so the monitored billable traffic/bandwidth is around 110% of the logged data.
- Except for traffic and bandwidth, all other metrics are collected at the application layer. Due to network fluctuation, statistics displayed on the monitoring page are slightly different from those in the log, as data loss may occur during log pulling from nodes or data reporting by servers.

Data source description

- If neither "statistical region" nor "ISP" is selected, the queried data is billing data.
- If "statistical region" or "ISP" is selected, the queried data is log data based on client IP matching calculation in the access logs.

Filtering Instructions

- Currently, dual selection of "statistical region" and "ISP" is not supported. Only specified province query for all ISPs or specified ISP query for all regions is supported.
- Currently, origin monitoring does not support filtering by "statistical region" or "ISP".
- Currently, origin-pull monitoring does not support filtering by HTTPS/HTTP request.

Origin-Pull Monitoring

Last updated：2024-12-31 17:44:50

Metric Description

Overview Page Metrics Description

Log in to the CDN console, select **Statistical Analysis** > **Real-Time Monitoring** from the left directory. After entering the management console, the **Access Monitoring** subpage is displayed by default. Click **Origin-Pull Monitoring** at the top to enter the origin monitoring indicator page, which returns the monitoring curve of all domains with a 1-minute granularity for the past 6 hours, including the following indicators:

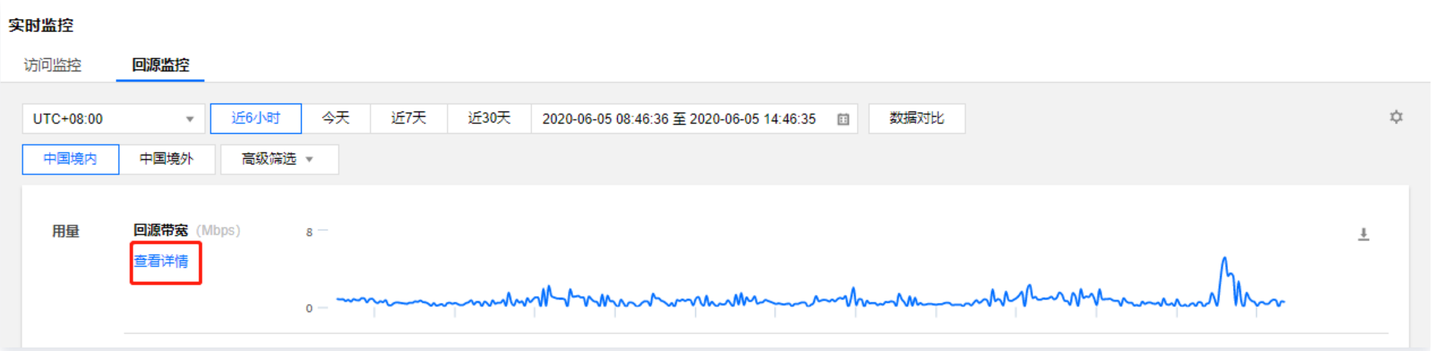
- Origin-pull bandwidth: Calculated by dividing the total origin-pull traffic in one minute by 60 seconds.
- Origin-pull traffic: Total origin-pull traffic in the cache node at the last layer.
- Origin-pull requests: Total number of origin-pull requests in the cache node at the last layer.
- Origin-pull failure rate: Percentage of failing origin-pull requests out of all origin-pull requests.
- Percentage of origin-pull status code: Percentage charts of status codes (2XX/3XX/4XX/5XX) returned for origin-pull requests within the selected time period.
- 2XX origin-pull status codes: Status codes generated by 2XX origin-pull status code monitoring will be counted.
- 3XX origin-pull status codes: Status codes generated by 3XX origin-pull status code monitoring will be counted.
- 4XX origin-pull status codes: Status codes generated by 4XX origin-pull status code monitoring will be counted.
- 5XX origin-pull status codes: Status codes generated by 5XX origin-pull status code monitoring will be counted.

The following situations will be counted as failing origin-pull requests:

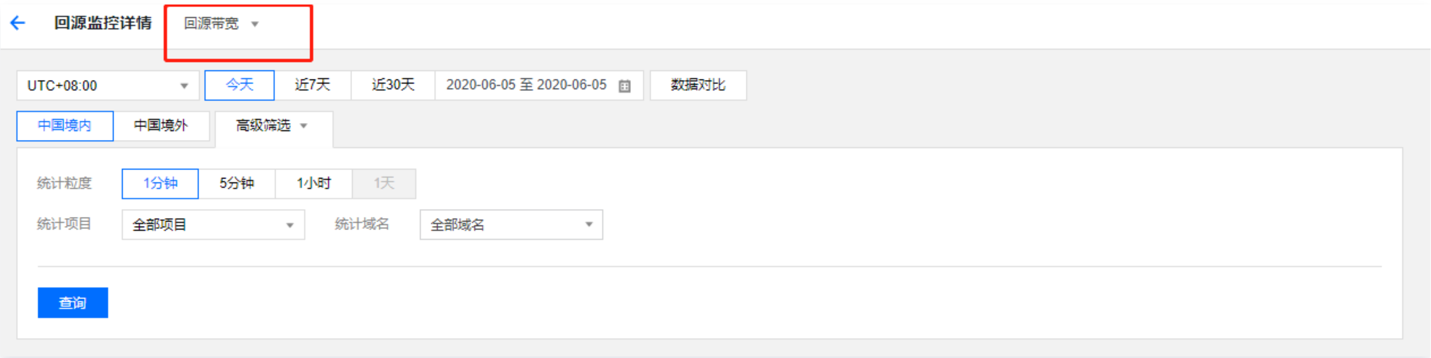
- Timeout in receiving origin-pull data.
- Timeout in sending origin-pull request.
- Timeout in establishing a TCP connection for origin-pull.
- The origin server actively closes the connection.
- HTTP protocol compatibility error of the origin server.

Data on the details page

Click **Viewing Details** under each metric to enter the metric details page.



You can also quickly switch metrics through the top left on the details page.



Granularity Description

Granularity description on the overview page

The monitoring page provides curve display options with 1-minute, 5-minute, 1-hour, and 1-day granularity. The minimum displayable time granularity varies based on the selected time interval:

- Time period ⩽ 6 hours: The minimum time granularity is 1 minute. The latency for displaying the 1-minute curve is about 3 minutes.
- 6 hours < time period ⩽ 24 hours: The minimum time granularity is 5 minutes. The latency for displaying the 5-minute curve is about 5-10 minutes.
- 24 hours < time period ⩽ 31 days: The minimum time granularity is 1 hour.
- Time period > 31 days: The minimum time granularity is 1 day.

Details page granularity description

The time granularity options on the metric details page are as follows:

- Time period ⩽ 24 hours: The minimum time granularity is 1 minute. The latency for displaying the 1-minute curve is about 3 minutes.
- 24 hours < time period ⩽ 31 days: The minimum time granularity can be 5 minutes, 1 hour, or 1 day.
- Time period > 31 days: The minimum time granularity is 1 day.

> ⚠ **Note**
> - The 1-minute granularity data can be queried only after the new version is launched. For historical data, the minimum granularity for query is 5 minutes.
> - The maximum query time period is the last 90 days.

Aggregation Description

Depending on the data metrics, the aggregation from 1-minute granularity to 5 minutes, 1 hour, or 1 day varies:

- Origin-pull bandwidth: The smallest granularity provided by CDN for monitoring bandwidth data is 1 minute. Based on industry standard, fees are generally billed by 5-minute granularity, which is calculated by taking the average of 1-minute data values. Therefore, the bandwidth data at a 1-hour or 1-day granularity can be calculated based on the maximum 5-minute bandwidth value.
- Origin-pull traffic: The traffic data at a 5-minute, 1-hour, or 1-day granularity is obtained by aggregating 1-minute traffic data.
- Origin-pull requests: The request count at a 5-minute, 1-hour, or 1-day granularity is obtained by aggregating 1-minute request counts.
- Origin-pull failure rate: Calculated by dividing the total number of origin-pull failures by the total number of origin-pull requests based on the selected time granularity.
- Origin-pull status codes: The status code data at a 5-minute, 1-hour, or 1-day granularity is obtained by aggregating 1-minute status code data.

Status codes description

Last updated：2024-12-31 17:45:01

The following is an explanation of internal CDN status codes:

Status Code	Meaning	Recommended Solution
0	The request ends before receiving the response status code.	Check if the client prematurely disconnected the request, or check if the origin fetch failed.
400	HTTP request syntax error The server cannot parse the request.	Check whether the request syntax is correct.
403	Access denied	Check the Hotlink protection, authentication configuration, and UA allowlist/denylist in the CDN Console.
404	Server cannot return correct information	Check whether the origin server is normal or if the origin server information and origin domain configuration have changed. For details, see the sudden 404 status of the CDN domain.
413	Content length of the POST request exceeds the limit	Check the content size of the POST request from the client (the maximum size is 32 MB by default).
414	URL length exceeds the limit	The maximum URL size is 2 KB by default.
423	Looping request	Check the 301/302 configuration, HTTPS origin-pull, and rewriting method of the origin server.
499	The client closes the connection	Check the client status and timeout configuration.
502	Gateway error	Check whether the business origin server is normal.
503	COS frequency control is triggered	Check the cache configuration or whether the COS origin server returns no-cache/no-store.
504	Gateway timeout	Please contact the official website.
509	Blocked due to triggering a CC attack	Please contact us or submit a ticket to unblock.
514	Exceed IP access frequency limit, blocklist access denied, HTTPS access not configured, any one of these three items is hit.	Check the IP access frequency control configuration, IP blocklist and allowlist configuration, and HTTPS configuration in the CDN Console (use HTTPS access when HTTPS service status is off).
524	Trigger platform access overload	Business request burst may trigger platform overload. Please assess the business scale and report to Tencent Cloud. If you have any questions, contact after-sales.
531	Error resolving the origin-pull domain name in the HTTP request	Check the domain name resolution configuration of the origin server.
532	Failed to establish a connection with the origin server in the HTTPS request	Check the port 443 status of the origin server, certificate configuration, or availability of the origin server.
533	Origin-pull connection timeout in the HTTPS request	Check the port 443 status of the origin server, certificate configuration, or availability of the origin server.
537	Origin server data reception timeout in the HTTPS request	Check the stability of the business origin server.

538	SSL handshake of HTTPS request failed	Check the compatibility between the origin server protocol and algorithm.
539	Certificate validation of HTTPS request failed	Check whether the certificate of the origin server is correctly configured (validity period and completeness of the certificate chain).
540	Certificate domain name validation of HTTPS request failed	Check whether the certificate of the origin server is correctly configured.
562	Failed to establish a connection in the HTTPS request	Please contact us and provide the X–NWS–LOG–UUID information or submit a ticket for troubleshooting.
563	Connection timeout in the HTTPS request	Please contact us and provide the X–NWS–LOG–UUID information or submit a ticket for troubleshooting.
564	HTTP origin request failed	If configured for the HTTP origin method, check the origin server load and bandwidth utilization, or access restrictions. If configured for the protocol follow method, check the port 443 status of the origin server and certificate configuration. If the origin server is found to be normal, please contact us and provide the X–NWS–LOG–UUID information or submit a ticket for troubleshooting.
566	WAF interception Anti–fraud automatic interception	Web attack protection recommended action is interception. Traffic anti–fraud automatic interception.
567	Response timeout when the node receives the file	Please contact us and provide the X–NWS–LOG–UUID information or submit a ticket for troubleshooting.

The following are the web server Hypertext Transfer Protocol response status code specification definitions:

Status Code	Meaning
100	The server has received the request header, and the client should continue sending the request body (in cases where a body needs to be sent: for example, a POST request), or if the request has been completed, ignore this response. The server must send a final response to the client after the request has been completed. To have the server check the request header, the client must send Expect: 100–continue as a header in its initial request and receive the 100 Continue status code before sending the body. Response code
101	The server has understood the client's request and will notify the client through the upgrade header to use a different protocol to complete this request. After sending the final blank line of this response, the server will switch to the protocols defined in the upgrade header. Such measures should only be taken when switching to a new protocol is more beneficial. For example, switching to a new HTTP version (such as HTTP/2) is more advantageous than the old version, or switching to a real–time and synchronous protocol (such as WebSocket) to transmit resources that utilize such features.
102	A WebDAV request may contain many sub–requests involving file operations, which take a long time to complete the request. This code indicates that the server has received and is processing the request, but no response is available. This prevents client timeout and assumes the request is lost.
103	Used to return some response headers before the final HTTP message.
200	The request succeeded, and the desired response headers or body will be returned with this response. In a GET request, the response will contain the entity corresponding to the requested resource. In a POST request, the response will contain an entity describing or resulting from the action.
201	The request has been fulfilled, and a new resource has been created according to the needs of the request, with its URI returned in the Location header. If the required resource cannot be established in time, '202 Accepted' should be returned.
202	The server has accepted the request but has not yet processed it. The request may or may not be executed eventually and may be prohibited when processing occurs.
203	The server is a transforming proxy (e.g., network accelerator) that originated a 200 OK status code but responded with a modified version of the original response.

204	The server successfully processed the request and returned no content. In the captive portal feature, when a Wi-Fi device connects to a Wi-Fi access point requiring web authentication, by accessing a site that generates an HTTP 204 response, if the 204 response is received normally, it indicates no web authentication is required. Otherwise, the web browser interface will pop up, displaying the web page authentication interface for user login.
205	The server successfully processed the request but returned no content. Unlike the 204 response, this response requires the requester to reset the document view.
206	The server has successfully processed a partial GET request. HTTP download tools like FlashGet or Thunder use this type of response to implement resuming interrupted downloads or splitting a large document into multiple segments for simultaneous download.
207	Indicates that the message body will be an XML message and may contain a series of independent response codes depending on the number of previous sub-requests.
208	Members bound by DAV have already been listed in the earlier part of the (multi-status) response and are not included again.
226	The server has fulfilled the request for the resource, representing the result of one or more entity actions on the requested entity.
300	The requested resource has a series of alternative feedback information, each with its specific address and browser-driven negotiation information. The user or browser can choose a preferred address for redirection.
301	Moved permanently. The requested resource has been permanently moved to a new URI, the returned information will include the new URI, and the browser will automatically redirect to the new URI. Any future requests for this resource should use the new URI instead.
302	Temporary movement. Similar to 301, but the resource is only temporarily moved. The client should continue to use the original URI.
303	The response to the current request can be found at another URI. When responding to a POST (or PUT/DELETE), the client should assume the server has received the data and should issue a redirect using a separate GET message.
304	Indicates that the resource has not been modified since the version specified by the If-Modified-Since or If-None-Match parameters in the request header. In this case, since the client still has a previously downloaded copy, there is no need to re-transmit the resource.
305	The requested resource must be accessed through the specified proxy. The Location field will provide the URI information of the proxy, and the recipient needs to resend a separate request through this proxy to access the resource.
306	In the latest version of the specification, the 306 status code is no longer used. It originally meant "subsequent requests should use the specified proxy."
307	In this case, the request should be repeated with another URI, but subsequent requests should still use the original URI. Unlike 302, when reissuing the original request, it is not allowed to change the request method. For example, use another POST request to repeat the POST request.
308	Requests and all future requests should repeat using another URI. 307 and 308 repeat the behavior of 302 and 301 but do not allow the HTTP method to change. For example, form submission to a permanently redirected resource may proceed smoothly.
401	Similar to 403 Forbidden, 401 means "unauthorized," indicating the user does not have the necessary credentials.
405	The request method specified in the request line cannot be used for the corresponding resource. The response must return an Allow header to indicate the list of request methods the current resource can accept.
406	The content characteristics of the requested resource cannot meet the conditions in the request header, making the request not acceptable.
407	Similar to a 401 response, except the client must authenticate itself with the proxy server.
408	Request timeout. According to the HTTP specification, the client did not complete sending the request within the server's prepared waiting time. The client can resubmit the request at any time without any changes.

409	Indicates that the request cannot be processed due to a request conflict, such as an edit conflict between multiple simultaneous updates.
410	Indicates that the requested resource is no longer available. This is used when the resource has been intentionally deleted and should be cleared. After receiving a 410 status code, the user should stop requesting the resource again. However, most servers do not use this status code and instead use a 404 status code.
411	The server refuses to accept the request without a defined Content-Length header. After adding a valid Content-Length header indicating the request message body length, the client can resubmit the request.
412	The server could not meet one or more of the preconditions given in the request header fields. This status code allows the client to set preconditions in the request metadata (request header fields) when retrieving a resource to avoid applying the request method to a resource other than the one it intended.
415	The internet media type submitted in the request for the requested method and resource is not a format supported by the server, so the request is rejected. For example, the client uploads an image in SVG format, but the server requires the image to be in JPG format.
416	The client has requested a part of the file, but the server cannot provide that part. For example, if the client requests a part of the file that is beyond the end of the file.
417	The expectation specified in the request header Expect cannot be met by the server, or the server is a proxy server with clear evidence that the expectation cannot be met by the next node on the current route.
500	General error message, the server encountered an unexpected condition that prevented it from fulfilling the request. No specific error message is given.
501	The server does not support a feature required by the current request. The server cannot recognize the requested method and cannot support its request for any resource.
505	The server does not support, or refuses to support, the HTTP version used in the request. This implies that the server cannot or will not use the same version as the client. The response should include an entity that describes why the version is not supported and the protocols supported by the server.
508	The server entered an infinite loop while processing the request.
510	The policy required to access the resource has not been met.

Data analysis

Last updated：2024-12-31 17:45:12

Feature Introduction

Tencent Cloud Content Delivery Network (CDN) mainly analyzes access log data and provides various data metrics on the data analysis page for a multi-dimensional understanding of business data.

> **Note**
> - Note: Due to latency and algorithm impact, top ranking data such as user region distribution and URL ranking are for reference only. Please refer to actual log data analysis.
> - Note: There are differences between monitoring data and log data, which is normal behavior. For detailed description and more data-related issues, see FAQs about Statistical Analysis.

Detailed Description

Log in to the CDN console, click **Statistical Analysis** > **Data Analysis** in the left sidebar to enter the data analysis page.

Query conditions

Please select the correct query conditions based on your actual needs to query data:

- Statistics type: refers to the product type. "Content Delivery" refers to Content Delivery Network (CDN), and "Enterprise Acceleration" refers to Enterprise Content Delivery Network (ECDN).
  Note: Different products support different data metric capabilities. We are continuously completing and updating data analysis capabilities, please follow Product Updates.
- Statistics region: refers to the acceleration region of the domain name.
  Note: Different statistics regions support different data metric capabilities. We are continuously completing and updating data analysis capabilities, please follow Product Updates.
- Statistics project: refers to the project to which the domain name currently belongs.
- Statistics domain: refers to the domain range to query.
- Time selection: refers to the time range to query.
  Note: The time range supported by the metrics is within the last 90 days, among which TOP 1000 URLs, TOP 100 Client IPs, TOP UAs, and TOP 100 Referrers only display data within the last 30 days.
- Display data: supported data metric range

Data Overview

Data overview of the total amount varies by basic billing method:

- For traffic billing: total traffic (monitoring data); average traffic hit rate; number of requests.
- For bandwidth billing: peak bandwidth (monitoring data), origin peak bandwidth; number of requests.

User Access District Distribution

The regional distribution of your business users, i.e., client regional distribution. Identify the region of access users through Client IP to understand the regional distribution of business users.

- Statistics by different provinces within China and by different regions outside China.
- Default rank by traffic, optional rank by request count

> **Note**
> ECDN does not support this metric.

Traffic

Traffic usage trend chart

- Default is billing traffic (i.e., access traffic), optional origin traffic

Bandwidth

Bandwidth usage trend chart

- Default is billing bandwidth (i.e., access bandwidth), optional back-to-origin bandwidth, optional show peak bandwidth curve.

Number of requests

Trend chart of request count.

Error Codes

Total number of error codes and quantity and proportion of different error codes.

TOP 1000 URL

Access URL ranking data.

- Default rank by traffic, optional rank by request count

TOP 10 Projects

Project ranking data varies by basic billing method:

- Bandwidth billing: rank by billing bandwidth
- Traffic billing: rank by billing traffic

> ⚠ **Note**
> Query time must be either 1 day or a full calendar month to select this data metric.

TOP 100 Domain Names

Accelerated domain ranking data varies by basic billing method:

- Bandwidth billing: rank by billing bandwidth
- Traffic billing: rank by billing traffic

> ⚠ **Note**
> Query time must be either 1 day or a full calendar month to select this data metric.

Unique IP Access Requests

Unique IP access requests are calculated by deduplicating the client IPs in the access log data.

- If the query time is less than or equal to one day, a deduplicated IP count curve with a 5-minute granularity will be provided.
- Domain situation is calculated by deduplicating the daily active users for the entire day. For multiple domains/projects/accounts, the daily active users of each domain are accumulated with a 5-minute granularity.

> ⚠ **Note**
> - `Note` : Only data for the last 31 days can be queried.
> - `Note` : ECDN does not support this metric.
> - `Note` : This metric is not supported outside the Chinese mainland.

User ISP Distribution

The distribution of your business users' ISPs is determined by identifying the ISPs of users based on the source Client IP.

- Default statistics by traffic, optional statistics by request count.

TOP 100 Client IPs (Beta)

Client IP Ranking Data

- Default rank by traffic, optional rank by request count

> ⚠ **Note**
> ECDN does not support this metric.

TOP UA (Beta)

UA Information Ranking Data

- Three types available: device, browser, and operating system, with device selected by default
  - Device: most commonly used device type when users visit, such as desktop or mobile device.
  - Browser: most commonly used browser name (or name and version) when users visit, such as Chrome or Firefox.
  - Operating System: most commonly used operating system name (or name and version) when users visit, such as Linux, Mac OS X, or Windows.
- Default rank by traffic, optional rank by request count

> **Note**
> ECDN does not support this metric.

TOP 100 Referer (Beta)

Referer information ranking data

- Default rank by traffic, optional rank by request count

> **Note**
> - `Note` : ECDN does not support this metric.
> - Note: The earliest query time for TOP 100 Client IP (Beta), TOP UA (Beta), and TOP 100 Referer (Beta) is September 20, 2021. There are no data statistics before this date. These three data metrics are in beta and the data is for reference only. For accurate data, please rely on actual log data analysis.

FAQs about Statistical Analysis

Last updated：2024-12-31 17:45:23

How are the bandwidth statistics in access monitoring collected?

Each CDN node collects traffic data in real time and reports it to the computing center, which aggregates the data into total domain traffic data. According to the time period, the traffic is divided by time to convert it into bandwidth data for display. **For example:**

- If the total traffic generated in a minute is 6 MB, then the corresponding bandwidth is (6 * 8) / 60 = 0.8 Mbps.
- As the usage for bill-by-bandwidth is calculated based on the statistics at a 5-minute granularity, the corresponding bandwidth value is total traffic in 5 minutes / 300 seconds.

Why is the traffic usage data shown in the console different from the log data?

The traffic counted based on the downstream bytes in the log of an accelerated domain name is limited to the data at the application layer, while the traffic generated by actual data transfers over the network is around 5-15% more than application-layer traffic.

- TCP/IP headers consumption: For TCP/IP-based HTTP requests, each packet can be up to 1,500 bytes and includes a 40-byte TCP and IP header, which generate traffic during transfer but cannot be counted by the application layer. The overhead of this part is around 3%.
- TCP retransmission: During normal data transfer over the network, around 3-10% of packets are lost on the Internet and retransmitted by the server. This type of traffic cannot be counted by the application layer and accounts for 3-7% of the total traffic.

As an industry standard, billable traffic is application-layer traffic plus the additional traffic described above. Tencent Cloud calculates the additional traffic as 10% of the total, so the traffic usage shown in the console is 110% of that recorded in logs.

How do I calculate the traffic hit rate?

By default, CDN enables L2 cache (edge layer and intermediate layer). As long as a request hits either layer for response, it will be counted as a CDN node hit.
Traffic hit rate = (total downstream traffic - origin-pull traffic) / total downstream traffic.

How do I fix the problem of low traffic hit rate?

For details, please refer to Low Traffic Hit Rate.

Do status code statistics include all status codes?

Yes. In the new version of CDN statistical analysis, monitoring curves are drawn for all status codes generated by origin servers, making it easier for you to troubleshoot.

How are district and ISP statistics calculated?

The district and ISP statistics are calculated based on the client IPs in the access log. As the calculation is completed based on the log, the simply accumulated billable data differs from the billable data when "all districts" or "all ISPs" is selected. For more information, please see the second issue above.

How is CDN origin-pull traffic generated?

CDN origin-pull traffic is generated during the following three situations:

1. The requested resource is not cached on the CDN node and is pulled from the origin server.
2. The manually purged origin server is synced with the node.
3. The origin server is auto-refreshed when the scheduled refresh time is reached

Abnormal CDN Traffic/Undergoing DDoS, CC Attack

Hello, if you think the number of access requests to your business is not large, you can download the access logs and configure the access limits based on your business access situation. CDN does not know your business logic, so no access limits are set for your business by default. Please configure as required by your business. For more information, please see High Bill Risk Warning.
To avoid malicious requests or CC/DDoS attacks to your website, we strongly recommend you complete the following configurations:

1. Hotlink protection configuration: you can control the access to your business resources. By setting an access control policy on the value of the referer field in the HTTP request header, you can restrict the access source to prevent hotlinking by malicious users. For more information, please see Hotlink Protection.
2. IP blocklist/allowlist configuration: You can create filtering policies for source IPs of user requests based on your business needs, helping prevent hotlinking and attacks from malicious IPs. For more information, please see IP Blocklist/Allowlist Configuration.
3. IP access limit configuration: you can defend against CC attacks by limiting the number of access requests per second to a node allowed for a client IP. After the configuration is enabled, a 514 error will be returned for requests that exceed the QPS limit. Setting a lower frequency limit may affect the usage of your business by normal high-frequency users. Therefore, please set the threshold according to your actual business conditions and usage. For more information, please see IP Access Limit Configuration.
4. Bandwidth cap configuration: you can configure a bandwidth cap for a domain name. When the bandwidth consumed by the domain name exceeds this cap within a statistical period (5 minutes), all access requests will be forwarded to the origin server or the CDN service will be disabled depending on your configuration (in both cases, a 404 error will be returned for all access requests). For more information, please see Bandwidth Cap Configuration.

Is there a delay in using APIs to query data? How long is it?

There is a certain delay in using APIs to query data. Queries of real-time data such as access data and billing data have a delay of around 5-10 minutes, while queries of analytical data such as rankings will have delays of approximately half an hour. The data is calibrated on the backend at around 3 am Beijing Time.

Purge and Prefetch
Purge and Prefetch

Last updated：2024-12-31 17:45:48

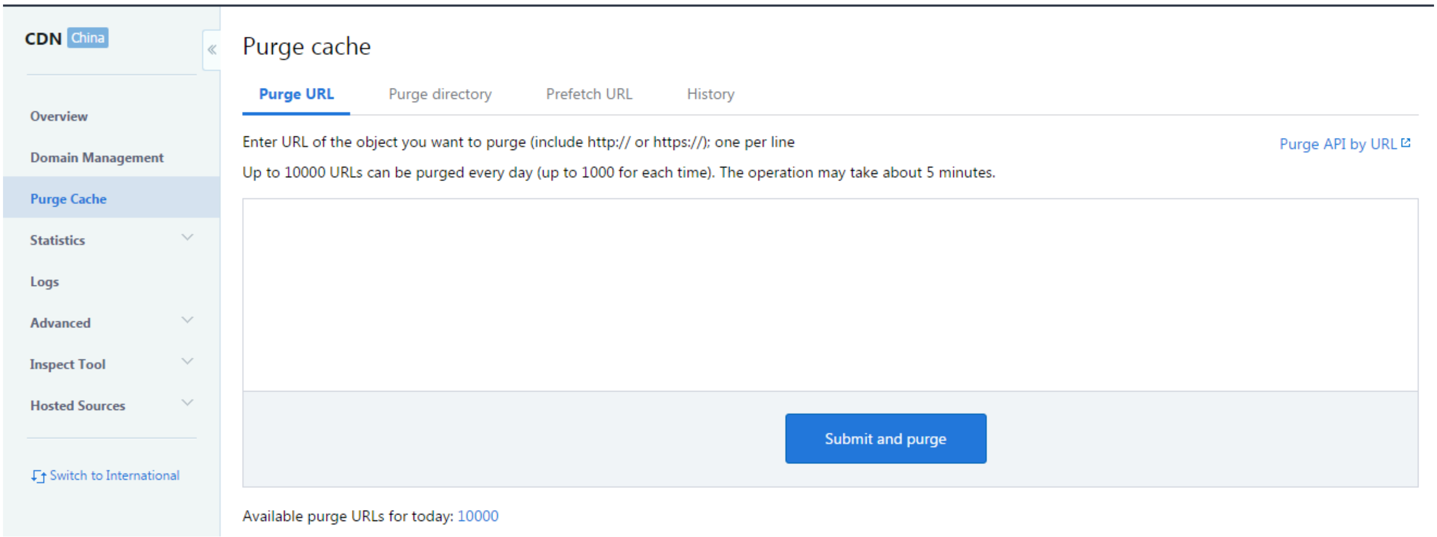
The update mechanism for the resources cached on the nodes in CDN is generally controlled by the cache expiration time. Configuring a reasonable cache expiration time policy can effectively reduce origin-pull rate. For more details, please refer to Cache Expiration in CDN Configuration Manual. When resources have been updated at your origin server, you can use the cache refresh feature if you want users to directly get new resources, instead of old ones, during access.

When resources have been updated at your origin server, you can use CDN's resource prefetch feature to cache the resources at the origin server to all CDN nodes.

URL prefetch feature is under a Gray-box release. It will be fully available in the future.

Purge URL

Log in to CDN Console, select **Purge Cache** menu on the left, and then select **Purge URL**:



Enter URL of the object you want to purge (include http:// or https://); one per line

Up to 10000 URLs can be purged every day (up to 1000 for each time). The operation may take about 5 minutes.

Available purge URLs for today: 10000

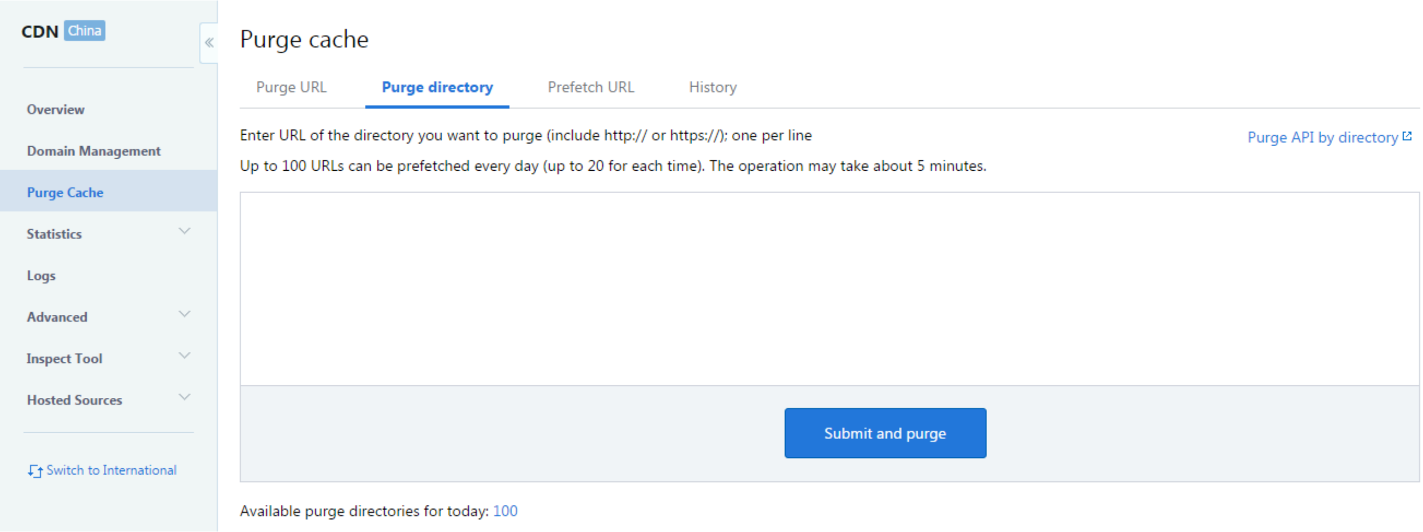
Enter the URLs of objects to be refreshed (must contain http:// or https://), one per line, for example: `http://www.abc.com/test.html`.

Note:

- A maximum of 10,000 URLs are allowed to be refreshed each day and a maximum of 1,000 URLs are allowed to be submitted for each refresh. It takes about 5 to 10 minutes for the refresh to take effect;
- Once a URL is refreshed, the resource from the URL will be set to expired if they have been cached on the CDN nodes across the network. When user's request reaches a node, the node will pull the requested resource from the origin server and then cache it while returning it to the user. In this way, it can be guaranteed that users can get the up-to-date resources;
- It takes 5 minutes for the file refresh to take effect. If the cache validity period set for the file is less than 5 minutes, it is recommended to wait for the timeout and update, instead of using the refresh tool.

Purge Directory

Log in to CDN Console, select the "Purge Cache" menu on the left, and then select the "Purge Directory":



Enter URL of the directory you want to purge (include http:// or https://): one per line

Up to 100 URLs can be prefetched every day (up to 20 for each time). The operation may take about 5 minutes.

Available purge directories for today: 100

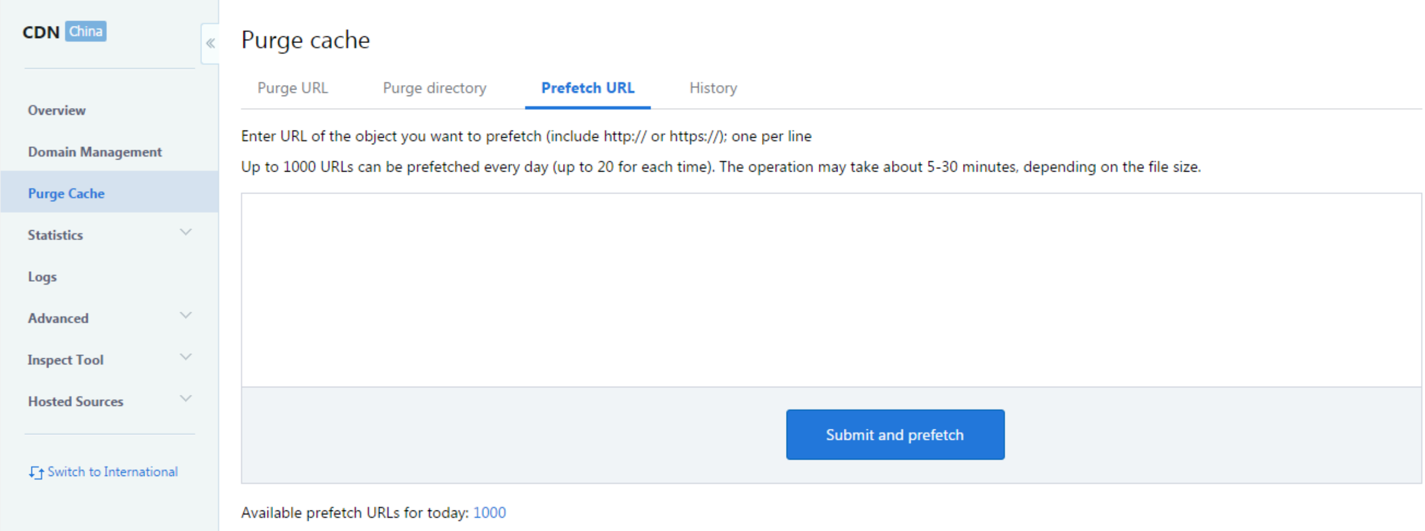
Enter the URLs of directories to be refreshed (must contain http:// or https://), one per line, for example: `http://www.abc.com/test/`.

Note:

- A maximum of 100 directories are allowed to be refreshed each day and a maximum of 20 directories are allowed to be submitted for each refresh. It takes about 5 to 10 minutes for the refresh to take effect;
- It takes 5 minutes for the file refresh to take effect. If the cache validity period set for the file is less than 5 minutes, it is recommended to wait for the timeout and update, instead of using the refresh tool.

URL Prefetch

Log in to CDN Console, select "Purge Cache" menu on the left, and then select "Prefetch URL":



Enter URL of the object you want to prefetch (include http:// or https://): one per line

Up to 1000 URLs can be prefetched every day (up to 20 for each time). The operation may take about 5-30 minutes, depending on the file size.

Available prefetch URLs for today: 1000

Enter the URLs of objects to be prefetched (must contain http:// or https://), one per line, for example: `http://www.abc.com/test.html`.

Note:

- If the resource has been cached on the node and has not expired, it will not be updated to the latest one. If you need to update the resources on all CDN nodes to the latest ones, you can refresh them before prefetch.
- A maximum of 1000 URLs are allowed to be prefetched each day and a maximum of 20 URLs are allowed to be submitted for each prefetch. It takes about 5 to 30 minutes for the prefetch to take effect, depending on the file size;

Task Query

You can query the status of submitted refresh and prefetch tasks in "History" section.

Cache Warming

Last updated：2024-12-31 17:45:57

Feature Introduction

Tencent Cloud CDN provides a prefetch feature that actively loads designated resources from the origin server to CDN cache nodes. When a user makes the first request for a resource, it can be directly retrieved from the CDN cache node without fetching from the origin server again.

> ⚠ **Note**
> - When a node is prefetching, if there is a valid (not expired) resource with the same name already cached, the resource will not be loaded. We recommend performing a full network refresh before submitting a prefetch when updating files with the same name.
> - When a node is prefetching, it will fetch the required content from the origin server. Therefore, submitting a large number of prefetch tasks will increase the bandwidth of the origin server.
> - Warming can be understood as CDN actively simulating a user's first request, requiring the submission of specific resource URL addresses. Therefore, directory warming is not supported.
> - By default, within China, CDN preheats at the middle layer, and outside China, CDN preheats at the edge layer. Preheating to CDN edge nodes within China will be counted as billing traffic. If you need to preheat content to CDN edge nodes within China, you can contact us through Submit a Ticket.

Applicable scenario

Installation package releases

Before releasing any new edition or update of installation packages, you can prefetch the resources to CDN cache nodes. After the official release, massive download requests from users will be directly responded to by global acceleration nodes, increasing download speed and significantly reducing the pressure on the origin server.

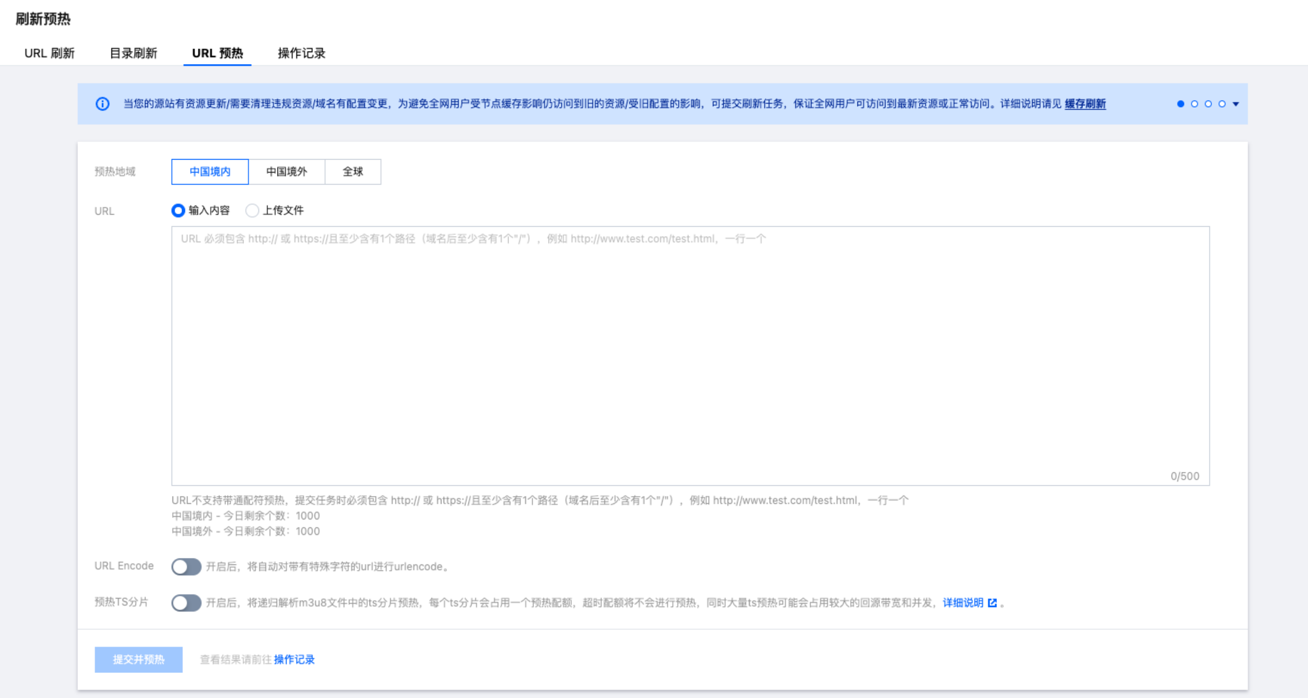
Operational Activities

Before initiating any marketing events, you can prefetch the related web static resources to CDN cache nodes. After events are officially started, all the requested web static resources will be returned from CDN cache nodes, guaranteeing service availability for a better user experience through abundant bandwidth reserve.

Operation Guide

Log in to the CDN console, click **Purge and Prefetch** on the left sidebar, and submit a **Prefetching URL** task as needed:

- The Content Delivery Network (CDN) and full site acceleration (ECDN) domain name URLs support mixed filling submission.
- Task can be submitted by direct input or TXT file upload.
- Supports specifying preheating regions: preheating regions correspond to the acceleration regions of the domain name, please choose as needed.
- Supports preheating TS fragments, default off, you can enable TS fragments as needed, and you should fully assess the impact of enabling TS fragments.



当您的源站有资源更新/需要清理违规资源/域名有配置变更，为避免全网用户受节点缓存影响仍访问到旧的资源/受旧配置的影响，可提交刷新任务，保证全网用户可访问到最新资源或正常访问。详细说明请见 缓存刷新

预热地域: [✓ 中国境内] 中国境外 全球

URL: ● 输入内容 ○ 上传文件

URL 必须包含 http:// 或 https://且至少含有1个路径（域名后至少含有1个"/"），例如 http://www.test.com/test.html，一行一个

0/500

URL不支持带通配符预热，提交任务时必须包含 http:// 或 https://且至少含有1个路径（域名后至少含有1个"/"），例如 http://www.test.com/test.html，一行一个
中国境内 - 今日剩余个数：1000
中国境外 - 今日剩余个数：1000

URL Encode: 开启后，将自动对带有特殊字符的url进行urlencode。

预热TS分片: 开启后，将递归解析m3u8文件中的ts分片预热，每个ts分片会占用一个预热配额，超时配额将不会进行预热，同时大量ts预热可能会占用较大的回源带宽和并发，详细说明 。

提交并预热　查看结果请前往 操作记录

Content Specification

Please first check whether the submitted content meets the specifications.

- URLs must include the http:// or https:// protocol identifier, such as `http://www.test.com/test.html`, one per line.
- Do not submit a domain name that is disabled, locked, or not connected to the current account.
- If you submit tasks by file upload, make sure that the file is in .txt format and doesn't exceed 10 MB in size.
- You cannot submit URLs in the format of `http://*.test.com/` – even if the acceleration domain name is a wildcard domain, you need to submit the corresponding subdomains.
- Submitting URLs containing wildcards is not supported.
- URLs with paths containing Chinese characters are not supported.

Submission limit

The daily URL preheating limit per account is 1,000. For customers who have enabled overseas acceleration, the daily URL refresh limit for overseas in China is 1,000, independent of the domestic quota:

- If you choose to submit content by direct input, the single submission URL preheating limit is 500.
- There is no limit on the number of URLs that are submitted by file upload, but the submissions will be deducted from your daily quota.
- If the domain acceleration region is global and the specified preheating region is global, the quotas for both China and overseas will be consumed simultaneously.
- If you enable preheat TS, it will recursively parse the TS fragment preheating in the m3u8 file. Each TS fragment will occupy one preheating quota, and the timeout quota will not be preheated.

> **Note:**
> - Note: If your remaining daily quota for refresh or prefetch is insufficient, you can apply for a quota increase through **Console** > **Query Service** > **Quota Management**.
> - Note: If you enable ts preheating, it will recursively parse the m3u8 file for ts fragment preheating. A large amount of ts preheating may occupy significant back-to-origin bandwidth and concurrency.

To query operation records, see Operation Record.

Sub-user permissions configuration

URL preheating and query preheating records have been integrated into the permission system, supporting permission configuration at the resource (domain name) level. For a detailed explanation, see Configure permissions.

Operation Records

Last updated：2024-12-31 17:46:06

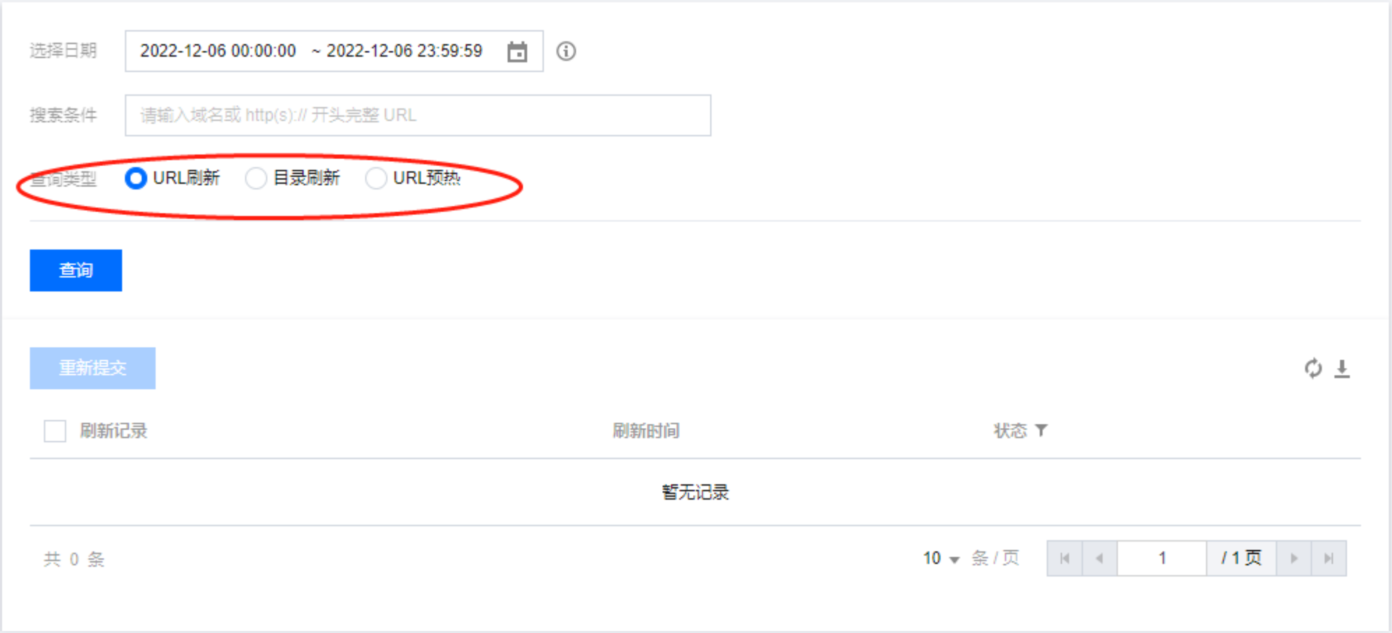
Feature Introduction

After submitting purge and prefetch tasks, you can view detailed records and status of resource purge and prefetch in the **Operation Records** page.

Operation Guide

Product Use

1. Log in to the CDN console, click **Purge and Prefetch** on the left sidebar, and then click **Operation Record**.
2. Query purge and prefetch tasks by specifying a time period, domain name/URL, or task type. You can specify a complete purge URL/directory or a complete prefetch URL.



选择日期 2022-12-06 00:00:00 ~ 2022-12-06 23:59:59

搜索条件 请输入域名或 http(s):// 开头完整 URL

查询类型 ● URL刷新 ○ 目录刷新 ○ URL预热

Usage Instructions

The console can return up to 10,000 logs at a time, which can be exported to an Excel file. If you have more than 10,000 purge tasks, please query and export them in batches.

Refresh and Prefetch FAQs

Last updated：2024-12-31 17:46:15

When to Use Refresh and Prefetch

- Purge: To ensure that users access to the latest resources when there are resources to update, restricted resources to remove, or domain name configurations to change on your origin server, you can submit a purge task, which can prevent user access to old resources or old configurations from the node cache. For more details, see Purge Cache.
- Prefetch: For operating activities, installation packages or upgrade packages to release, you can submit a prefetch task to prefetch static resources to CDN acceleration nodes, which will reduce strain on the origin server and improve the service availability and user experience. For more details, see Prefetch Cache.

What Is the Difference Between Refresh and Prefetch

- Once a resource is purged, its cache on all CDN nodes across the entire network will be deleted. When a user request arrives at a node, the node will pull the corresponding resource from the origin server, return it to the user, and cache it to the node to ensure that the user can obtain the latest resource.
- When a resource is prefetched, it will be cached in advance to all CDN nodes across the entire network. When a user request arrives at a node, the resource can be directly obtained on the node.

Requirements for Refresh Preheating and How Long It Takes to Take Effect

- Cache Purge
- URL purge: a maximum of 10,000 URLs can be purged each day and a maximum of 1,000 URLs can be submitted for each purge. It takes about 5 minutes for the purge to take effect. If the cache validity period configured for the file is less than 5 minutes, we recommend you wait for the timeout and update instead of using the purge tool.
- Directory purge: a maximum of 100 directories can be purged each day and a maximum of 500 URL directories can be submitted for each purge. It takes about 5 minutes for the purge to take effect. If the cache validity period configured for the folder is less than 5 minutes, we recommend you wait for the timeout and update instead of using the purge tool.
- Resource Prefetching
- URL prefetch: A maximum of 1,000 URLs can be prefetched each day, and a maximum of 500 URLs can be submitted for each prefetch task. It takes about 5 to 30 minutes for the prefetch to take effect, depending on the file size.

If the resource changes on the origin server, will the cache on CDN cache nodes be updated in real time?

No. The cache on CDN cache nodes will not be updated in real time.

- If the resource changes on the origin server and the cache is still valid, CDN cache nodes will not perform origin-pull to update the cache, and thus the resource on the origin server is different from the cache. You can specify a proper cache validity period in the console's Node Cache Validity.
- If the cache validity period is too short, CDN will frequently pull the content from the origin server and more traffic will be consumed on the origin server. If it is too long, the cache will be updated slowly.
- If you need to proactively update the cache of a resource, you can use Purge Cache to actively clear the CDN cache. After clearing the cache, you can use Prefetch Cache to make the CDN actively fetch the latest resources from the origin server, or let a new user request naturally trigger the CDN to fetch the latest resources.
- If you need to regularly update the cache of a resource, you can use scheduled refresh preheating to trigger refresh tasks on time.

How to View the Purge and Prefetch History?

You can check the purge and prefetch history in the CDN console. For more information, see Operation Records.

Can I prefetch with custom request headers?

Not supported.

How do I increase the daily quota limit for purge and prefetch?

In the CDN console, Quota Management allows you to view the CDN-related quota limits and usage. You can request a temporary or permanent quota increase based on your business needs. The currently supported quotas are: URL purge quota, directory purge quota, and URL prefetch quota.

- Temporary quota: When business activities or operational scenarios require a temporary increase in quota, you can apply for a temporary quota for the required time range through quota management. After the temporary quota expires, the current quota will revert to the permanent quota.
- Permanent quota: When the existing quota cannot meet your daily business needs, you can apply for a permanent quota for the corresponding function through quota management. As the permanent quota application takes a long time to process, we recommend requesting a temporary quota to meet your temporary business needs.

What should I pay attention to when prefetching?

When you prefetch the file whose cache is still valid, CDN will not perform origin-pull to update the file. We recommend you purge the cache before submitting a prefetch task.

- During prefetching, CDN will pull the required content from the origin server. If you submit a large batch of prefetch tasks, the bandwidth usage of the origin server will greatly increase. Therefore, a proper number of prefetch tasks is suggested.

Is Traffic Generated by Preheating Charged

- The preheating operation will proactively pull content from the origin server to the intermediate layer nodes of the CDN. Preheating to the intermediate layer nodes will not generate billing traffic. If you need to preheat content to the edge nodes of the CDN, please contact us through Submit a Ticket.
- Because preheating pulls the target file from the origin server, it increases the network traffic of the origin server. Generally, the server or Cloud Object Storage where your origin server is located will charge network traffic fees.

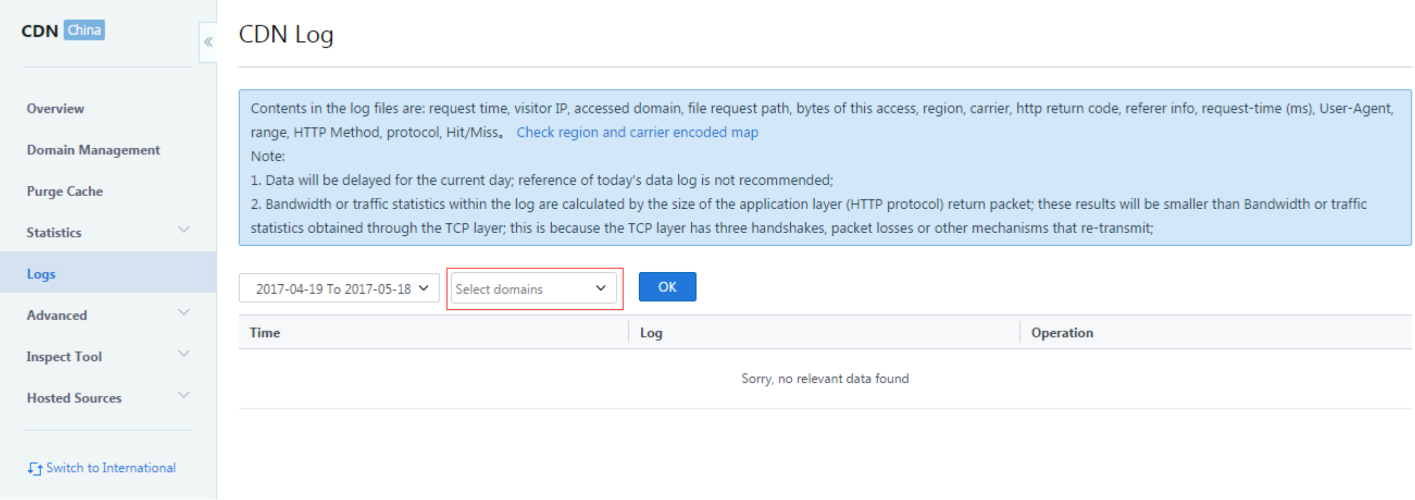
Cloud Log Service
Log Management

Last updated：2024-12-31 17:46:34

You can download the detailed log containing the information about users' access to a connected domain for analysis; CDN provides logs about domains on an hourly basis, and you can download CDN logs for the last 30 days.

Log Download

Log in to CDN Console and select **Logs** page. You'll see the **Log Management** feature provided by CDN.



CDN Log

Contents in the log files are: request time, visitor IP, accessed domain, file request path, bytes of this access, region, carrier, http return code, referer info, request-time (ms), User-Agent, range, HTTP Method, protocol, Hit/Miss。 Check region and carrier encoded map

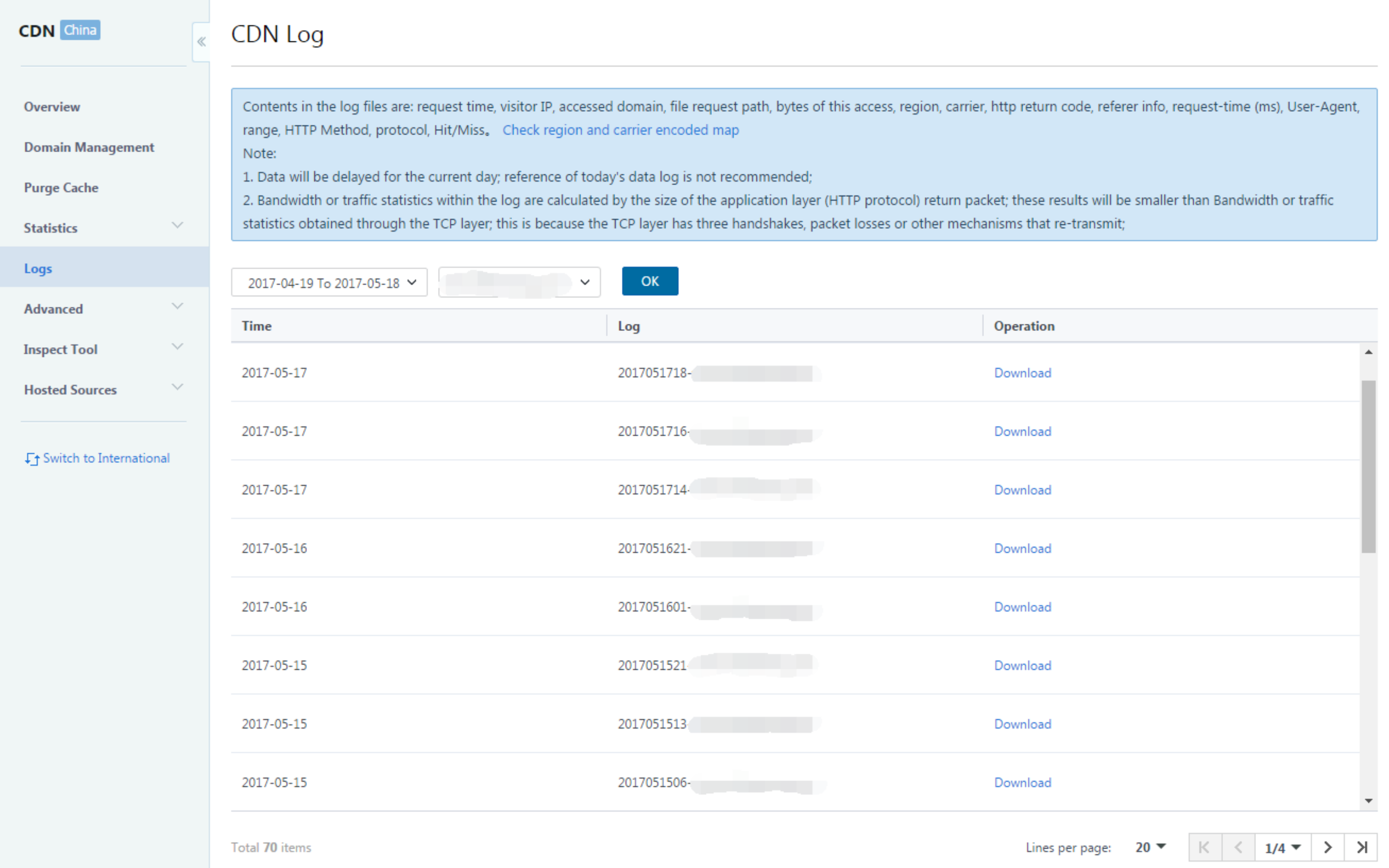
Note:

1. Data will be delayed for the current day; reference of today's data log is not recommended;

2. Bandwidth or traffic statistics within the log are calculated by the size of the application layer (HTTP protocol) return packet; these results will be smaller than Bandwidth or traffic statistics obtained through the TCP layer; this is because the TCP layer has three handshakes, packet losses or other mechanisms that re-transmit;

Time	Log	Operation
Sorry, no relevant data found		

Select the domain for which you want to check logs and the date range, then click **Query** to get the log download link, and click the link to download:



CDN Log

Contents in the log files are: request time, visitor IP, accessed domain, file request path, bytes of this access, region, carrier, http return code, referer info, request-time (ms), User-Agent, range, HTTP Method, protocol, Hit/Miss。 Check region and carrier encoded map

Note:

1. Data will be delayed for the current day; reference of today's data log is not recommended;

2. Bandwidth or traffic statistics within the log are calculated by the size of the application layer (HTTP protocol) return packet; these results will be smaller than Bandwidth or traffic statistics obtained through the TCP layer; this is because the TCP layer has three handshakes, packet losses or other mechanisms that re-transmit;

Time	Log	Operation
2017-05-17	2017051718-[redacted]	Download
2017-05-17	2017051716-[redacted]	Download
2017-05-17	2017051714-[redacted]	Download
2017-05-16	2017051621-[redacted]	Download
2017-05-16	2017051601-[redacted]	Download
2017-05-15	2017051521[redacted]	Download
2017-05-15	2017051513[redacted]	Download
2017-05-15	2017051506-[redacted]	Download

Total 70 items Lines per page: 20 1/4

If there was no request for the domain on that day, no log would be generated. In this case, "No Data" will appear.

Note:

- CDN logs are provided on an hourly basis by default, with 24 log files generated each day;
- CDN logs have a latency of about half an hour in terms of real-timeness and will not be updated after 2 hours.

Log Field Description

The order and meaning of fields in the downloaded log are shown in the following table:

Order	Log Content
1	Request time
2	Client IP of access domain
3	Domain accessed
4	Request path of file
5	Bytes of current access
6	Province
7	ISP
8	HTTP status code
9	Referer info
10	Response time (ms)
11	User-Agent
12	range parameter
13	HTTP Method
14	HTTP protocol ID
15	Cache HIT/MISS

Region Code

1: North China; 2: Northwest China; 3: Northeast China; 4: East China; 5: Central China; 6: Southwest China; 7: South China; 8: Other Regions;

Province Code

22: Beijing; 86: Inner Mongolia; 146: Shanxi; 1069: Hebei; 1177: Tianjin; 119: Ningxia; 152: Shaanxi; 1208: Gansu; 1467: Qinghai; 1468: Xinjiang; 145: Heilongjiang; 1445: Jilin; 1464: Liaoning; 2: Fujian; 120: Jiangsu; 121: Anhui; 122: Shandong; 1050: Shanghai; 1442: Zhejiang; 182: Henan; 1135: Hubei; 1465: Jiangxi; 1466: Hunan; 118: Guizhou; 153: Yunnan; 1051: Chongqing; 1068: Sichuan; 1155: Tibet; 4: Guangdong; 173: Guangxi; 1441: Hainan; 0: Other; 1: Hong Kong, Macao and Taiwan; 1: Overseas;

ISP Mapping

2: China Telecom; 26: China Unicom; 38: CERNET; 43: Great Wall Broadband; 1046: China Mobile; 3947: China Tietong Telecom; -1: Overseas ISPs; 0: Other ISPs;

Note

The bandwidth or traffic data recorded in logs is returned data packet at the application layer (HTTP protocol), and due to such mechanisms as TCP protocol packet loss, three-way handshake and re-transmission, is smaller than that counted through TCP layer.

Overseas CDN Log Download

Overseas CDN is under beta test. If you have activated overseas CDN, you can download overseas CDN logs from log management page of overseas CDN console. Overseas CDN provides domain logs at an hourly basis with a latency of one to two days. You can download the CDN logs for the last 30 days. The fields in overseas CDN log are the same as the ones in domestic CDN log, except that Province field will be replaced by overseas region. The overseas region and ISP mappings are shown below.

Overseas Region Code

73: India; 1195: Indonesia; 1176: Singapore; 57: Thailand; 144: Vietnam; 3701: Malaysia; 2588: Philippines; 2026: Taiwan; 1044: Japan; 3379: Korea; 1200: Hong Kong; 3839: Canada; 669: United States; −2: Other Overseas Regions; −3: Unknown;

Overseas ISP Code

−1: Overseas ISP;

Real-time Logs

Last updated：2024-12-31 17:46:44

Feature Introduction

Tencent Cloud Content Delivery Network (CDN) Real-time Log Service: By real-time collection and delivery of CDN access logs, it enables rapid retrieval and analysis of log data. You can quickly access it through the CDN console, enjoying comprehensive, stable, and reliable log services from log collection, log storage to log retrieval.

Applicable scenario

You can access log data to view or analyze business conditions in multiple dimensions in real time.

Operation Guide

Log in to the CDN console, click **Log Service** in the left directory, and switch to the **Real-time Logs** tab at the top to enter the real-time log page.

Enabling Real-time Log Service

To enable real-time log service, first activate Cloud Log Service (CLS) and authorize CDN to create a logset.

> ⓘ **Note**
> - It is recommended to use the root account to enable the service. If you are a sub-account or collaborator, please refer to Activate Real-time Logging as Sub-account/Collaborator.
> - When you enable the CDN real-time log service, CDN will create a default logset to store CDN logs (one logset per region).
> - CLS logset is a paid service, and the fee is charged by the log service. The CDN log delivery feature is free. For detailed billing information, see Logset Billing Overview.
> - CDN currently supports delivery to Shanghai, Beijing, Chengdu, Chongqing, Nanjing, Guangzhou, and Singapore regions. We are planning to support more regions, so please stay tuned for product updates.

Log Topic Creation

You can create a log topic under the logset to deliver access logs of the target acceleration domain name to Cloud Log Service (CLS) and enable real-time log service.

> ⚠ **Note**
> - Note: Up to 500 log topics can be created under a logset.
> - Note: The name of a new log topic cannot be the same as an existing log topic.
> - Note: You cannot mix CDN and ECDN domain names under the same log topic.
> - The logs of CDN acceleration domain names within China can only be delivered to Shanghai, Beijing, Chengdu, Chongqing, Nanjing, and Guangzhou. The logs outside China can only be delivered to Singapore.
> - Note: ECDN does not support log delivery outside China.

Log Search

Log search supports multiple types of search analysis methods and chart analysis formats. For detailed instructions, see Log Search.

Log search is performed based on log topics. Select the log topic you want to search, click **Search** to enter the log search page.

Managing Log Topics and Log Sets

You can manage the created log topics in the CDN console by clicking the action bar:

- Manage: Update the list of domain names bound to the log topic
- Stop: Stop log delivery to the log topic. Once stopped, all logs of the domain names bound to the log topic will no longer be delivered to the topic, but shipped logs will be retained.

- Start: Start log delivery to the log topic. Once started, all logs of the domain names bound to the log topic will continue to be delivered to the log topic.
- Delete: Delete the log topic. Once deleted, all logs of the domains bound to this log topic will stop being shipped to it, and all shipped logs will be cleared.

For more logset managing operations, such as renaming a logset, you can go to the CLS console.

Real-time Log Field Descriptions

Log Field	Raw Log Type	Log Service Type	Description
app_id	Integer	long	APPID of your Tencent Cloud account
client_ip	String	text	Client IP
file_size	Integer	long	File Size
hit	String	text	Cache hit/miss. Both hits on CDN edge servers and parent nodes are marked as hit
host	String	text	Domain name
http_code	Integer	long	HTTP Status Code
isp	String	text	Carrier
method	String	text	HTTP Method
param	String	text	Parameter carried in URL
proto	String	text	HTTP protocol identifier
prov	String	text	ISP Province
referer	String	text	Referer information, i.e., HTTP source address
request_range	String	text	Range parameter, i.e., request range
request_time	Integer	long	Response time (in milliseconds), which refers to the time it takes for a node to return the response packet after receiving a request.
remote_port	String	long	The port for establishing a connection between the client and the CDN node, if none, it is -
rsp_size	Integer	long	Number of bytes of this access request (including response header and response body size)
time	Integer	long	Request time (end time after completing client request), a UNIX timestamp in seconds.
ua	String	text	User-Agent information
url	String	text	Request path
uuid	String	text	Unique request ID
version	Integer	long	CDN real-time log version

Terms

Logset

The logset is a project management unit in CLS and is used to distinguish logs from different projects. Each logset corresponds to a project or application. The CDN logset has the following basic attribute information:

- Region: The log set belongs to the Region.

> Note
> Currently, Shanghai, Beijing, Chengdu, Chongqing, Nanjing, Guangzhou, and Singapore regions are supported. We are planning to support more regions, please stay tuned for product updates.

- Logset Name: the name of a logset
- Retention period: The retention period of data in the current logset
- Creation time: Logset creation time

Log Topic

The topic is the basic management unit in CLS. A logset can contain multiple topics. Each topic corresponds to a category of application or service. It's recommended to collect similar logs from different machines to the same topic. For example, a business project may have three types of logs: operation logs, application logs, and access logs. You can create a topic for each type.
The log service system manages different log data based on different log topics. Each log topic can be configured with different data sources, index rules, and shipping rules. Therefore, a log topic is the basic unit for configuring and managing log data in the log service. After creating a log topic, you need to configure the corresponding rules to effectively perform log collection, search, analysis, and shipping.
Log topic features include:

- Collect logs to log topics.
- Store and manage logs based on log topics.
- Search and analyze logs by log topics.
- Deliver logs to other platforms based on log topics.
- Download and consume logs from log topics.

> Note
> Note: The above information is extracted from the Cloud Log Service (CLS) product documentation. Please refer to the CLS documentation for accurate details.

FAQs

Why can't I see some logsets and topics in the CDN console that are in the CLS console

In the CDN console, you can only see log topics created by using the CDN role, which is exclusive to the CDN real-time log service. Other logsets and topics will not be synchronized.

Why is my real-time log not retrieving data, resulting in data loss

It may be because your log data volume is large, but the log topic has only a single partition, or auto split is disabled. When you create a log topic, the default number of partitions is 1, and auto split is enabled by default.
It is recommended to estimate the required partitions based on your log volume and configure it in the advanced options of the CLS log topic. For details, refer to Topic Partition.

Can I delete a CDN logset

Yes, you need to delete the logset in the CLS console. Before deletion, you must delete all log topics under the logset. The CDN side will synchronize this deletion status. If needed later, you can recreate the logset and log topics in the CDN console.

Is there a delay in real-time log delivery

Real-time log delivery generally has a 2-5 minute delay due to log packaging and network delivery speed.

Plugins Center

Overview

Last updated：2024-12-31 17:47:16

The Plugin Center is a repository of value-added CDN plugins. It provides extended features for content processing and security protection and works together with other Tencent Cloud services to jointly offer value-added services. Some plugins are paid features. Before activating a plugin, carefully read the billing description in its help documentation.

APK Dynamic Packaging

Last updated：2024-12-31 17:47:23

Feature Introduction

The APK dynamic packaging plugin recognizes certain parameters in request URLs of end users and dynamically writes the information carried in such parameters to the APK on a CDN node for dynamic packaging.

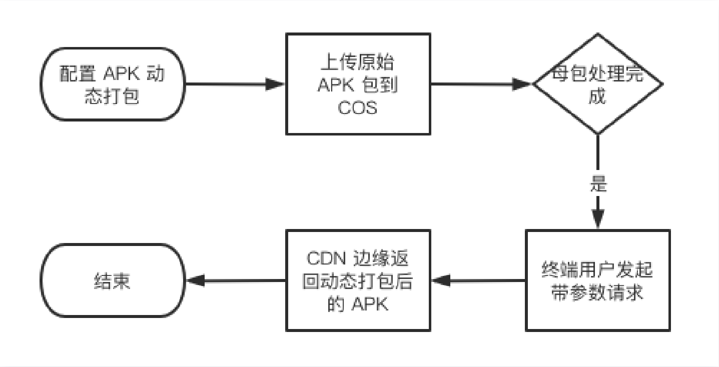
> **Note:**
> - Currently, only nodes in the Chinese mainland support the APK dynamic packaging feature.
> - Currently, only Tencent Cloud COS is supported as the origin for APK dynamic packaging.

Applicable Scenario

- You need to release and promote an app through various channels, such as app market, ad alliance, search engine, and performance-based ad, but don't want to manually maintain an overwhelming number of channel packages.
- You want to implement hot app startup; that is, you can dynamically insert a link into the APK, so that end users will be automatically redirected to the specified page when they open the app for the first time.

Process Flow

1. Log in to the CDN console and complete the relevant configuration of the APK dynamic packaging plugin feature in the plugin center.
2. Upload the original APK to the specified upload directory on the COS origin.
3. Wait for the CDN node to process the parent package.
4. An end user initiates a request with certain parameters.
5. The CDN edge returns the APK file after dynamic packaging.

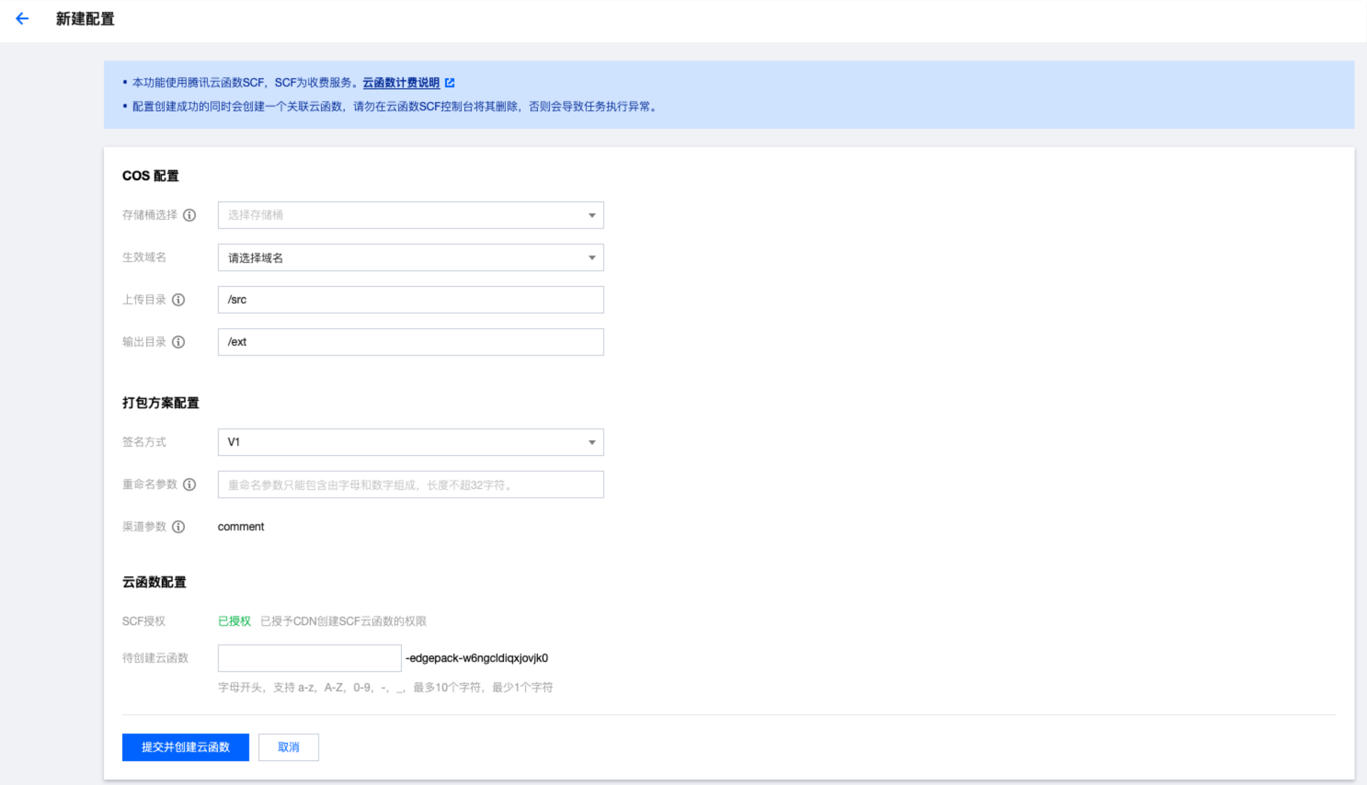


Configuration Guide

Step 1. Add a dynamic packaging configuration

1. Log in to the CDN console, select Plugin Center in the menu bar, and click the switch button on the **APK dynamic packaging** plugin feature card to enable APK dynamic packaging and enter the configuration page.
2. After the feature is activated, you can enter the configuration list and usage view pages through Basic configurations and Usage Statistics at the bottom of the card.

3. On the Basic Configuration page, click Adding a configuration to complete the configuration of the APK packaging task.



新建配置

- 本功能使用腾讯云函数SCF，SCF为收费服务。云函数计费说明
- 配置创建成功的同时会创建一个关联云函数，请勿在云函数SCF控制台将其删除，否则会导致任务执行异常。

COS 配置

存储桶选择: 选择存储桶

生效域名: 请选择域名

上传目录: /src

输出目录: /ext

打包方案配置

签名方式: V1

重命名参数: 重命名参数只能包含由字母和数字组成，长度不超32字符。

渠道参数: comment

云函数配置

SCF授权: 已授权 已授予CDN创建SCF云函数的权限

待创建云函数: -edgepack-w6ngcldiqxjovjk0

字母开头，支持 a-z，A-Z，0-9，-，_，最多10个字符，最少1个字符

- Bucket selection: Choose COS as the origin server. This feature requires using COS in Beijing, Shanghai, Guangzhou, or Chengdu as the origin server.
- Domain Name: The system will automatically select all domain names using the specified COS bucket as the origin. The domain names are used to release the APK, and you can add or remove domain names as needed.
- Upload Directory: Set the upload directory for the original APK in COS. Manually upload the original APK to this directory after completing the configuration.
- Output directory: Set the output directory after the CDN node processes the master package. After uploading the original APK, the system will automatically process, generate a master package with the same name, and upload it to this directory. When constructing the request URL, please point the user request to this directory, not the upload directory.
- Signature Method: Currently, you can dynamically package an APK with Android APK Signature Scheme v1 or v2. A v2 signature supports open-source multi-channel packaging solutions such as Walle and VasDolly. In addition, you can also write a comment to the specified custom block ID.
- Rename Parameter: The rename parameter allows users to generate a new file name based on parameters when downloading files. If not configured, the downloaded file name will be the same as the master package file name.
- Channel Parameter: Fixed at `comment` and cannot be modified.
- SCF configuration: After authorization, the system will automatically generate the SCF based on the configuration.

> **Note**
> Do not delete this SCF in the SCF console!

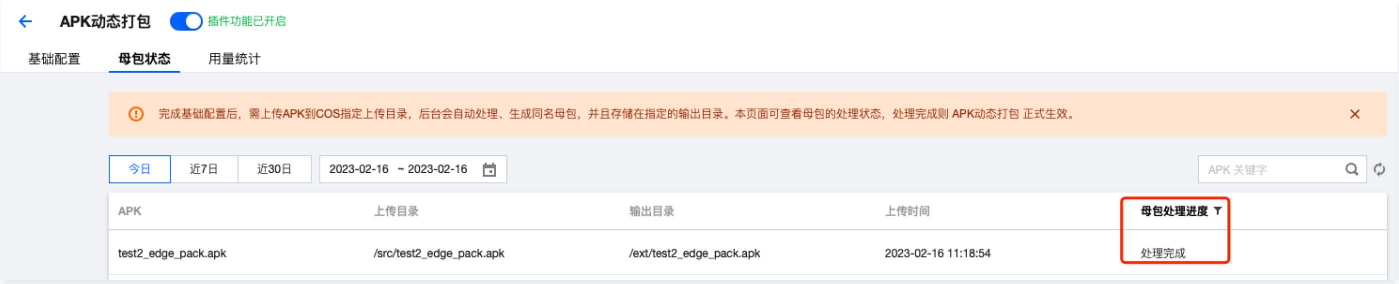
Step 2. Upload the original APK

Log in to the COS console and upload the original APK to the specified upload directory.

> **Note:**
> The original APK can be up to 10 GB in size.

Step 3. Wait for the parent package to be processed

Return to the dynamic packaging feature page in the CDN console, click mother package status to check if the processing progress of the mother package on the CDN node is "processing completed".

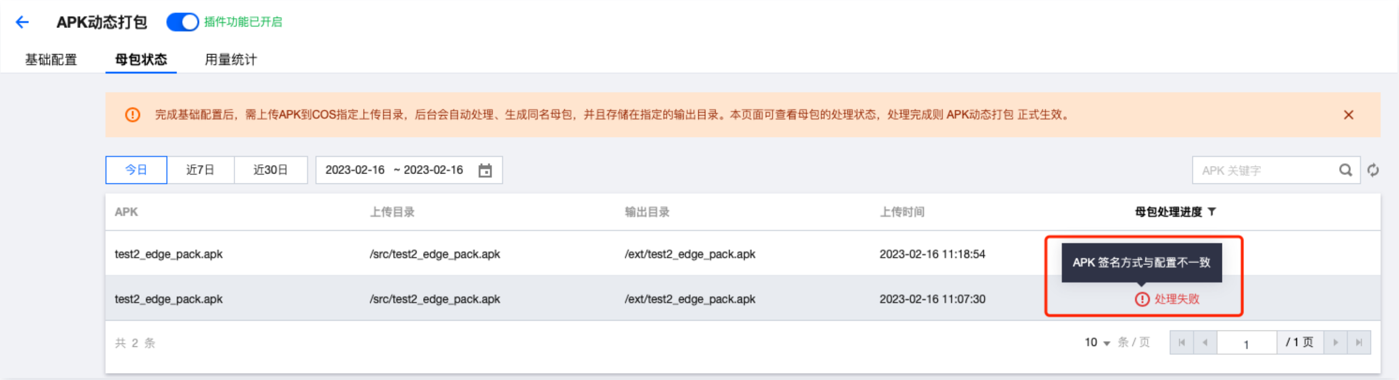


完成基础配置后，需上传APK到COS指定上传目录，后台会自动处理、生成同名母包，并且存储在指定的输出目录。本页面可查看母包的处理状态，处理完成则 APK动态打包 正式生效。

2023-02-16 ~ 2023-02-16

APK	上传目录	输出目录	上传时间	母包处理进度
test2_edge_pack.apk	/src/test2_edge_pack.apk	/ext/test2_edge_pack.apk	2023-02-16 11:18:54	处理完成

If failed processing, you can check the specific reason for the failure.



完成基础配置后，需上传APK到COS指定上传目录，后台会自动处理、生成同名母包，并且存储在指定的输出目录。本页面可查看母包的处理状态，处理完成则 APK动态打包 正式生效。

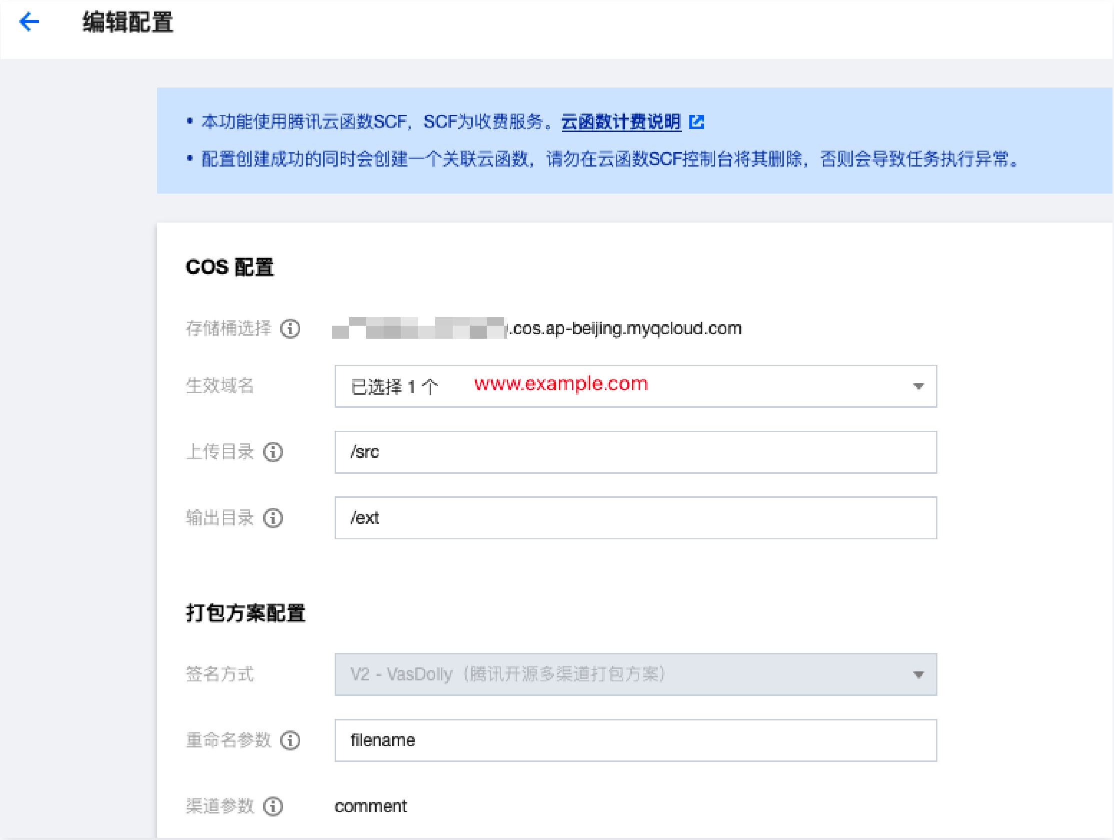
2023-02-16 ~ 2023-02-16

APK	上传目录	输出目录	上传时间	母包处理进度
test2_edge_pack.apk	/src/test2_edge_pack.apk	/ext/test2_edge_pack.apk	2023-02-16 11:18:54	APK 签名方式与配置不一致
test2_edge_pack.apk	/src/test2_edge_pack.apk	/ext/test2_edge_pack.apk	2023-02-16 11:07:30	处理失败

共 2 条　10 条 / 页　1 / 1 页

Step 4. Release the dynamic packaging URL

After the parent package is processed, you can release the dynamic packaging URL as follows:
If the task information is as follows:



- 本功能使用腾讯云函数SCF，SCF为收费服务。云函数计费说明
- 配置创建成功的同时会创建一个关联云函数，请勿在云函数SCF控制台将其删除，否则会导致任务执行异常。

COS 配置

存储桶选择	[redacted].cos.ap-beijing.myqcloud.com
生效域名	已选择 1 个　www.example.com
上传目录	/src
输出目录	/ext

打包方案配置

签名方式	V2 - VasDolly（腾讯开源多渠道打包方案）
重命名参数	filename
渠道参数	comment

The corresponding published URL is: `https://www.example.com/ext/test2_edge_pack.apk?comment=pipeline` .
An end user can request this URL to get the APK package containing the pipeline channel information from the CDN edge.

If the rename parameter is configured, the URL can be: `https://www.example.com/ext/test2_edge_pack.apk?comment=pipeline&filename=newfilename`, which means the file name will be displayed as "newfilename" after the user requests the download.

Fee Description

For cost details, please refer to APK Dynamic Packaging Billing Rules.

FAQs

1. After uploading the mother package, you find that the channel information is not packaged through the src directory download?
   src is the upload directory. The mother package is processed through scf and finally output to the ext directory. You need to access the ext directory for automatic packaging.
2. walle format, comment=123456, walle-cli query error, indicating incorrect json format?
   walle's channel information format requires json format and urlencode. The backend will urldecode the comment information and directly write it into the corresponding blockid-value, so the comment content should be urlencode(json). For example: if the channel information is 123456, the walle value is `{"channel":"123456"}, comment=%7B%22channel%22%3A%22123456%22%7D`.
3. The Android client extracts the channel name with %00, %00, etc.?
   %00, %00, etc. are placeholders reserved for edge packaging. There are two resolutions.
   - Resolution one: You can handle it yourself by deleting the whitespace characters after the channel information.
   - Resolution two: If using the V2-vasdolly signing method, you can upgrade the vasdolly sdk version to 3.0.6 to automatically remove the reserved placeholders.

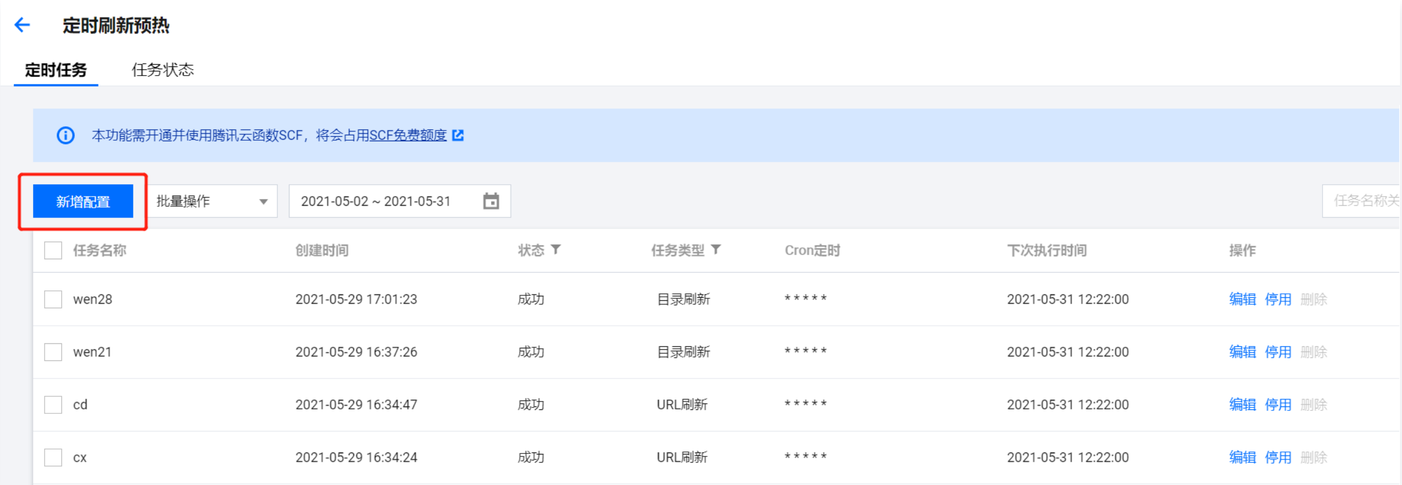
Scheduled Purge and Prefetch

Last updated：2024-12-31 17:47:29

Scheduled purge/prefetch tasks can be triggered through SCF. Such tasks are included in the daily purge/prefetch quota and may fail to be executed if the quota is exceeded.

Configuration Instructions

Log in to the CDN console, select **plugin center** from the menu bar, click the scheduled purge and prefetch plugin feature card, and enable scheduled purge and prefetch to enter the task configuration page. After the first activation, you can also click the bottom of the card's **basic configuration** to enter the task list page for scheduled purge and prefetch configuration.



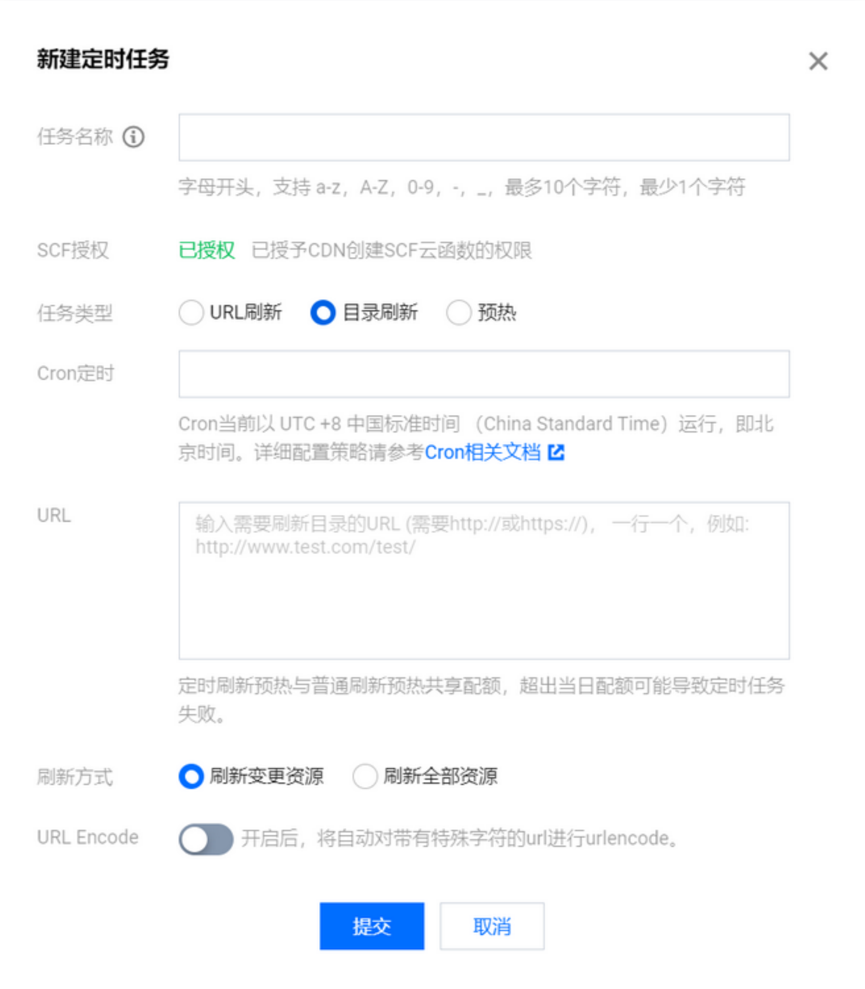
定时刷新预热

定时任务 任务状态

本功能需开通并使用腾讯云函数SCF，将会占用SCF免费额度

□ 任务名称	创建时间	状态	任务类型	Cron定时	下次执行时间	操作
□ wen28	2021-05-29 17:01:23	成功	目录刷新	*****	2021-05-31 12:22:00	编辑 停用 删除
□ wen21	2021-05-29 16:37:26	成功	目录刷新	*****	2021-05-31 12:22:00	编辑 停用 删除
□ cd	2021-05-29 16:34:47	成功	URL刷新	*****	2021-05-31 12:22:00	编辑 停用 删除
□ cx	2021-05-29 16:34:24	成功	URL刷新	*****	2021-05-31 12:22:00	编辑 停用 删除

On the new scheduled task interface, select the corresponding task type, set the cron scheduled expression (see below), enter the corresponding purge/prefetch URL, and authorize SCF. The system will automatically generate the corresponding SCF cloud function and trigger the corresponding task on time.



新建定时任务

任务名称

字母开头，支持 a-z，A-Z，0-9，-，_，最多10个字符，最少1个字符

SCF授权 已授权 已授予CDN创建SCF云函数的权限

任务类型 ○ URL刷新 ● 目录刷新 ○ 预热

Cron定时

Cron当前以 UTC +8 中国标准时间 （China Standard Time）运行，即北京时间。详细配置策略请参考Cron相关文档

URL

输入需要刷新目录的URL (需要http://或https://)，一行一个，例如: http://www.test.com/test/

定时刷新预热与普通刷新预热共享配额，超出当日配额可能导致定时任务失败。

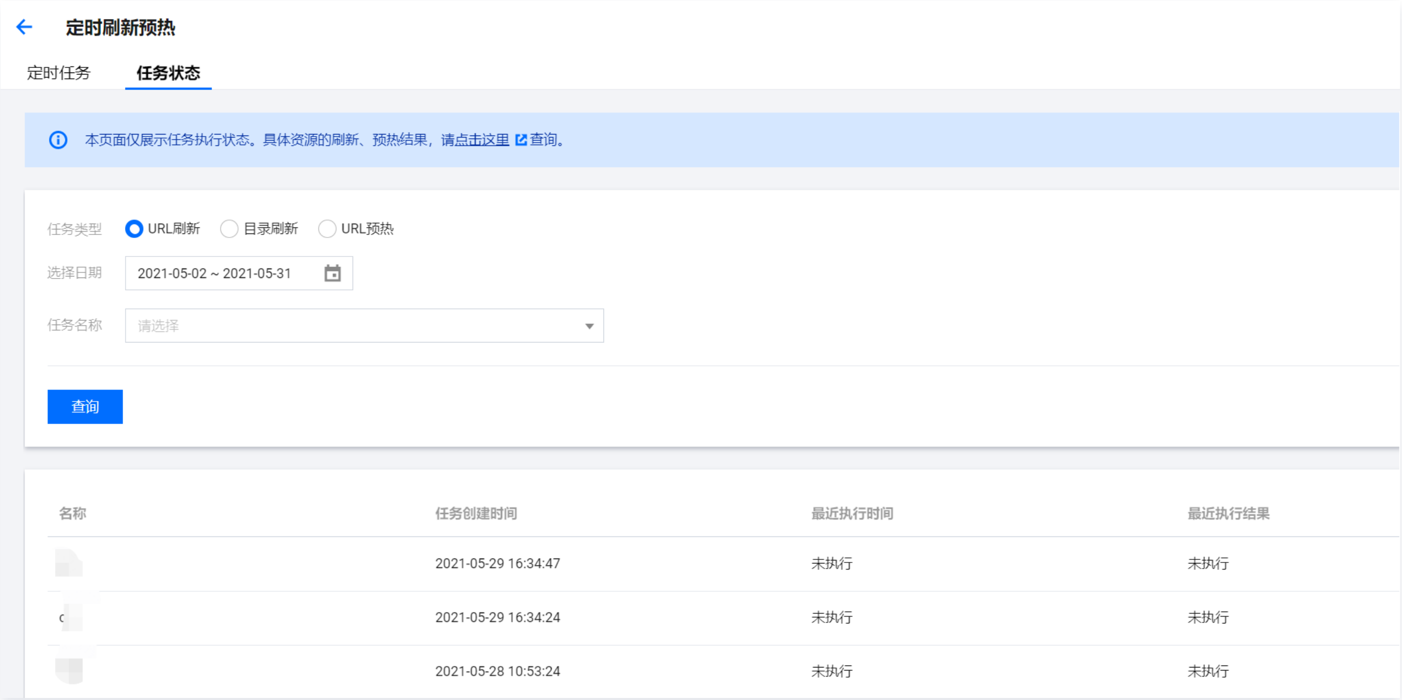
刷新方式 ● 刷新变更资源 ○ 刷新全部资源

URL Encode 开启后，将自动对带有特殊字符的url进行urlencode。

Note

Do not delete this SCF in the SCF console!

On the task status page, you can view the last execution of the scheduled task.



定时刷新预热

定时任务 任务状态

本页面仅展示任务执行状态。具体资源的刷新、预热结果，请点击这里 查询。

任务类型 ● URL刷新 ○ 目录刷新 ○ URL预热

选择日期 2021-05-02 ~ 2021-05-31

任务名称 请选择

查询

名称	任务创建时间	最近执行时间	最近执行结果
[redacted]	2021-05-29 16:34:47	未执行	未执行
[redacted]	2021-05-29 16:34:24	未执行	未执行
[redacted]	2021-05-28 10:53:24	未执行	未执行

Cron Expression

A cron expression contains seven values, each separated by a space.

Bit count	Field	Value range	Wildcard
First	Second	An integer between 0 and 59	, − * /
Second	Minute	An integer between 0 and 59	, − * /
Third	Hour	An integer between 0 and 23	, − * /
Fourth	Day	An integer between 1 and 31 (the number of days in the month needs to be considered)	, − * /
Fifth	Month	An integer between 1 and 12 or JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, or DEC	, − * /
Sixth	Day of week	An integer between 0 and 6 or MON, TUE, WED, THU, FRI, SAT, or SUN, where 0 means Monday, 1 means Tuesday, and so on	, − * /
Seventh	Year	An integer between 1970-2099	, − * /

Wildcards have the following meanings:

Wildcard	Meaning
, (comma)	It represents the union of characters separated by commas; for example, in the "Hour" field, 1, 2, 3 means 1:00, 2:00, and 3:00.
(dash)	It contains all values in the specified range; for example, in the "Day" field, 1–15 contains the 1st to the 15th day of the specified month
(asterisk)	It means all values; for example, in the "Hour" field, * means every o'clock
/ (forward	It specifies the increment; for example, in the "Minute" field, you can enter 1/10 to specify repeating every ten minutes from the first minute on (e.g., at the 11th minute, the 21st minute, the 31st minute, and so on)

slash)	

> **Note**
> When both the "Day" and "Week" fields in a cron expression are specified, they are in an "or" relationship, i.e., the conditions of both are effective separately.

Example

One-time task

- `33 22 11 6 7 * 2021` means triggering the task at 11:22:33 on 2021-7-6.
- `00 00 20 25 10 * 2021` means triggering the task at 20:00:00 on 2021-10-25.

Periodic task

- `*/5 * * * * * *` means triggering the task once every 5 seconds.
- `0 0 2 1 * * *` means triggering the task once at 2 AM on the 1st day of every month.
- `0 15 10 * * MON-FRI *` means triggering the task once every day at 10:15 AM Monday through Friday.
- `0 0 10,14,16 * * * *` means triggering the task every day at 10 AM, 2 PM, and 4 PM.
- `0 */30 9-17 * * * *` means triggering the task once every half hour from 9 AM to 5 PM every day.
- `0 0 12 * * WED *` means triggering the task once at 12:00 noon every Wednesday.

Fee Description

The scheduled purge/prefetch feature is free of charge. However, it will call SCF to create scheduled tasks, which will incur SCF fees. For more information, see Billing Overview.

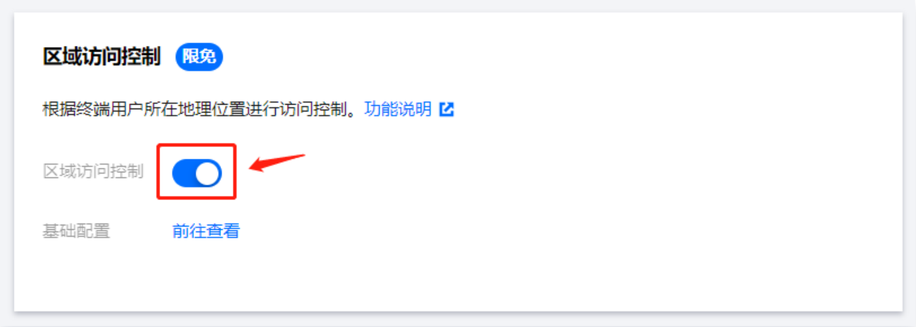
Regional Access Control

Last updated：2024-12-31 17:47:42

Regional access control identifies the location of end users through Client IP, allowing customers to set access privileges for all content or specified directories for users in different regions. Tencent Cloud regularly updates the IPv4 database for global regions, and a small number of IP terminals not in the database cannot be identified.

Configuration Instructions

Log in to the CDN Console, select **Plugin Center** from the menu bar, find the regional access control feature card, and click to activate. After first-time activation, click **Go to View** at the bottom of the card to enter the regional access control configuration list page.



区域访问控制 限免

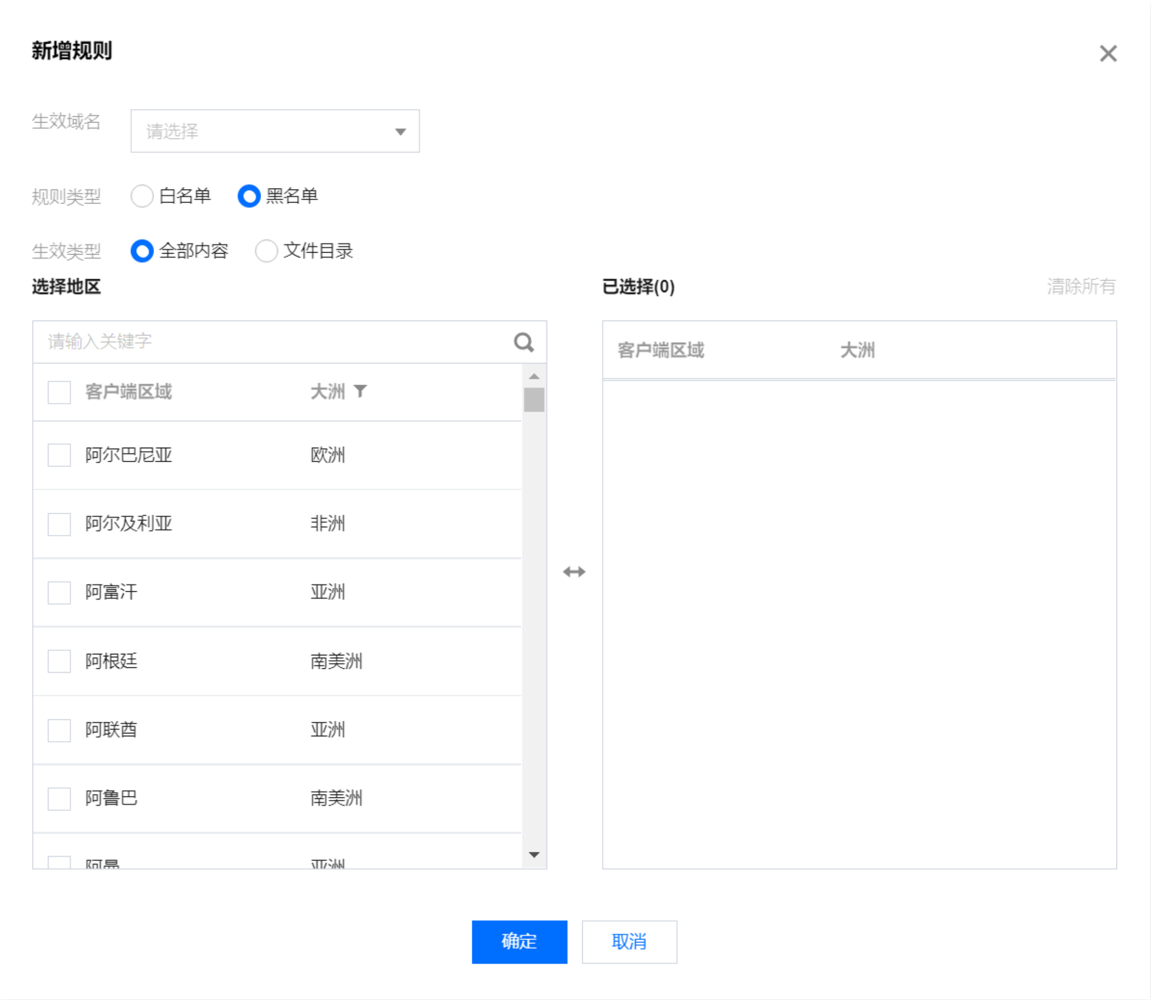
根据终端用户所在地理位置进行访问控制。功能说明

区域访问控制 ●

基础配置 前往查看

Click **Add New Rule** to set regional access control allowlist/denylist for all content/specified directories. Multiple selections for end user regions are supported.

Rule Type	Description
Allowlist	Access permission for selected regions, access denied for other regions.
Blocklist	Access denied for selected regions, access permission for other regions.



新增规则

生效域名 请选择

规则类型 ○ 白名单 ● 黑名单

生效类型 ● 全部内容 ○ 文件目录

选择地区

请输入关键字

□	客户端区域	大洲
□	阿尔巴尼亚	欧洲
□	阿尔及利亚	非洲
□	阿富汗	亚洲
□	阿根廷	南美洲
□	阿联酋	亚洲
□	阿鲁巴	南美洲
□	阿曼	亚洲

已选择(0) 清除所有

客户端区域	大洲

Note:

- Each domain name can be configured with up to 20 region access control rules.
- Note: The priority at the bottom of the list is higher than that at the top.
- Domains with IPv6 access enabled do not support enabling the regional access control plugin.
- The same directory of the same domain (or all content) can only set an allowlist once.
- It is recommended to configure one type of rule (allowlist/denylist) for a single domain name to avoid overly complex effective conditions.

Supported Regions

Region	Specific Area
Asia	Hong Kong (China), Taiwan (China), within China, Macao (China), Vietnam, Jordan, British Indian Ocean Territory, Indonesia, India, Israel, Iran, Iraq, Yemen, Armenia, Syria, New Caledonia, Singapore, Uzbekistan, Brunei, Turkmenistan, Thailand, Tajikistan, Sri Lanka, Christmas Island, Saudi Arabia, Japan, Nepal, Myanmar, Bangladesh, Mongolia, Malaysia, Maldives, Lebanon, Laos, Kuwait, Cocos (Keeling) Islands, Qatar, Cambodia, Kyrgyzstan, South Korea, Kazakhstan, Georgia, Philippines, Timor-Leste, North Korea, Bhutan, Bahrain, Palestine, Pakistan, Oman, United Arab Emirates, Afghanistan
Europe	Albania, Azerbaijan, Ireland, Estonia, Andorra, Austria, Aland Islands, Bulgaria, North Macedonia, Belgium, Iceland, Bosnia and Herzegovina, Poland, Denmark, Germany, France, Faroe Islands, Vatican, Finland, Guernsey, Netherlands, Montenegro, Czech Republic, Croatia, Latvia, Lithuania, Liechtenstein, Luxembourg, Romania, Isle of Man, Malta, Moldova, Monaco, Norway, Portugal, Sweden, Switzerland, Serbia, Cyprus, San Marino, Slovakia,

	Slovenia, Svalbard and Jan Mayen, Türkiye, Ukraine, Spain, Greece, Hungary, Italy, United Kingdom, Jersey, Gibraltar
South America	Argentina, Aruba, Paraguay, Brazil, Bolivia, Ecuador, French Guiana, Falkland Islands, Guyana, Netherlands Caribbean Region, Curacao, Peru, Suriname, Trinidad and Tobago, Venezuela, Uruguay, Chile
Africa	Algeria, Egypt, Ethiopia, Angola, Benin, Botswana, Burkina Faso, Burundi, Equatorial Guinea, Togo, Eritrea, Cape Verde, Gambia, Republic of the Congo, Democratic Republic of the Congo, Djibouti, Guinea, Guinea-Bissau, Ghana, Gabon, Zimbabwe, Cameroon, Comoros, Côte d'Ivoire, Kenya, Lesotho, Liberia, Libya, Réunion, Rwanda, Madagascar, Malawi, Mali, Mayotte, Mauritius, Mauritania, Mozambique, Namibia, South Africa, South Sudan, Niger, Nigeria, Sierra Leone, Senegal, Seychelles, São Tomé and Príncipe, Eswatini, Sudan, Somalia, Tanzania, Tunisia, Uganda, Western Sahara, Jamaica, Zambia, Chad, Central African Republic
Oceania	Australia, Papua New Guinea, Northern Mariana Islands, French Polynesia, Fiji, Guam, Kiribati, Cook Islands, Marshall Islands, American Samoa, Federated States of Micronesia, Nauru, Niue, Norfolk Island, Palau, Pitcairn Islands, Samoa, Solomon Islands, Tonga, Tuvalu, Tokelau, Wallis and Futuna, Vanuatu, New Zealand
North America	Anguilla, Antigua and Barbuda, Barbados, Bahamas, Panama, Bermuda, Puerto Rico, Belize, Dominican Republic, Dominica, Saint Martin (French part), Colombia, Costa Rica, Grenada, Greenland, Cuba, Guadeloupe, Haiti, Saint Martin (Dutch part), Honduras, Canada, Cayman Islands, Martinique, United States, United States Minor Outlying Islands, United States Virgin Islands, Montserrat, Morocco, Mexico, Nicaragua, El Salvador, Saint Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Pierre and Miquelon, Saint Vincent and the Grenadines, Turks and Caicos Islands, Guatemala, British Virgin Islands

Fee Description

1. In areas not covered by service or during peak business hours, client requests from accessible regions may be routed to other serviceable regions, which may incur billing traffic from other regions during the period. For details, see Billing Instructions.
2. For terminal requests that are denied access, a 514 response will include minimal request data, generating a small amount of traffic.
3. For terminal HTTPS protocol requests that are denied access, the number of HTTPS requests with a 514 response will not be included in HTTPS billing data.
4. For ECDN accelerated domain names, terminal requests that are denied access and return a 514 status code will incur request count fees.

Performance Monitoring

Last updated：2024-12-31 17:48:00

Feature Introduction

The performance monitoring feature is a one-stop frontend monitoring solution designed for web and mini program monitoring. You only need to install its SDK to your project and complete simple configuration, and then it will take care of the user page quality in an all-around manner, truly enabling cost-effective usage and non-intrusive monitoring. This helps you stay up to date with the page performance and frontend quality.

> **Note:**
> Performance monitoring is provided by Tencent Cloud Real User Monitoring (RUM). After activation, you can also manage your applications in the RUM console. For detailed operation documentation, refer to: RUM Operation Guide.

Fee Description

Performance monitoring provides 500,000 free reporting times per application per day. The excess will be charged by Tencent Cloud RUM. For billing details, please refer to RUM - Billing Overview.

Applicable scenario

- **Page performance analysis:** This feature offers metrics such as first screen load time, time to establish TCP connection, time to first byte (TTFB), and SSL time. In addition, it supports the latest Web Vitals standards, Google's webpage loading speed and experience metrics, for you to optimize the user experience in an all-around manner.
- **Page exception analysis**: This feature helps you quickly locate page exceptions, including page stutter, page crash, no response after operation, and inability to operate the page.
- **Page log query:** This feature allows you to search for user logs. Then, you can restore the scene of the anomaly and get enough information to locate problems.
- **User access analysis:** This feature displays the business PV/UV and top access metrics of each page. It analyzes the user access data in various dimensions, including network, browser, and region.
- **API monitoring:** The embedded SDK actively reports the APIs requested by the frontend, and the performance monitoring module will collect key API metrics such as API request duration and HTTP code success rates, helping you quickly locate API anomalies.
- **Static resource optimization**: This feature monitors the loading time of static resources like JavaScript scripts, CSS style sheets, and images for you to locate the root causes of problems and optimize the loading of such resources to enhance user experience.
- **Custom information reporting**: If the data actively reported by the SDK cannot meet your needs, you can customize the logs, events, and resource speed test metrics to be reported.

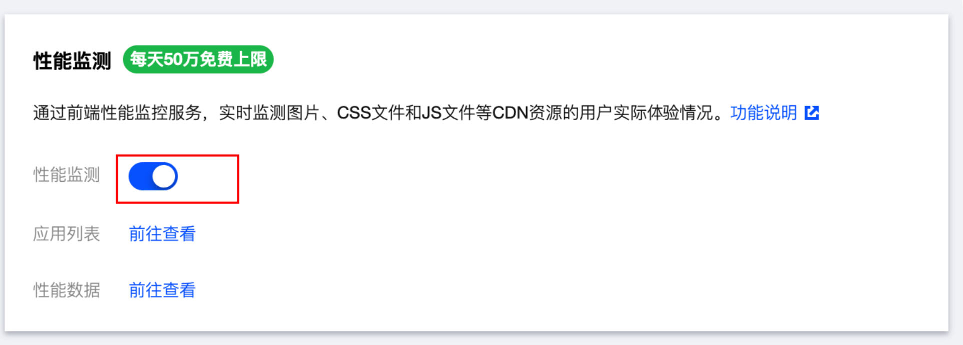
Configuration Process

1. Log in to the CDN console in the plugin center to enable the performance monitoring service.
2. Select the access method and integrate it into the application.
3. Analyze the page performance and frontend quality through aggregated analysis and page analysis.
4. You can also configure alarms for key metrics, so that when a metric becomes abnormal, you will receive prompt notifications and can take measures accordingly.

Configuration Guide

Step 1. Enable the performance monitoring feature

1. Log in to the CDN Console in the Plugin Center.
2. Find the performance monitoring feature card, click the enable button on the right side of performance monitoring, and confirm activation of the performance monitoring service.



性能监测 每天50万免费上限

通过前端性能监控服务，实时监测图片、CSS文件和JS文件等CDN资源的用户实际体验情况。功能说明

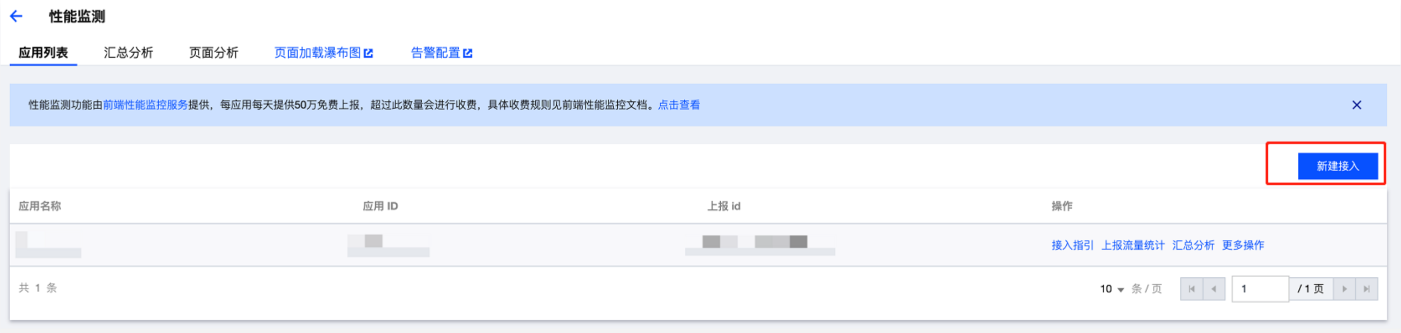
性能监测 ●

应用列表 前往查看

性能数据 前往查看

Step 2. Connect your application

After successfully enabling the performance monitoring service, you will be redirected to the application list. Click to create a new application integration. Follow the prompts on the page to select the domain to be integrated and integrate the performance monitoring SDK as instructed.



性能监测功能由前端性能监控服务提供，每应用每天提供50万免费上报，超过此数量会进行收费，具体收费规则见前端性能监控文档。点击查看

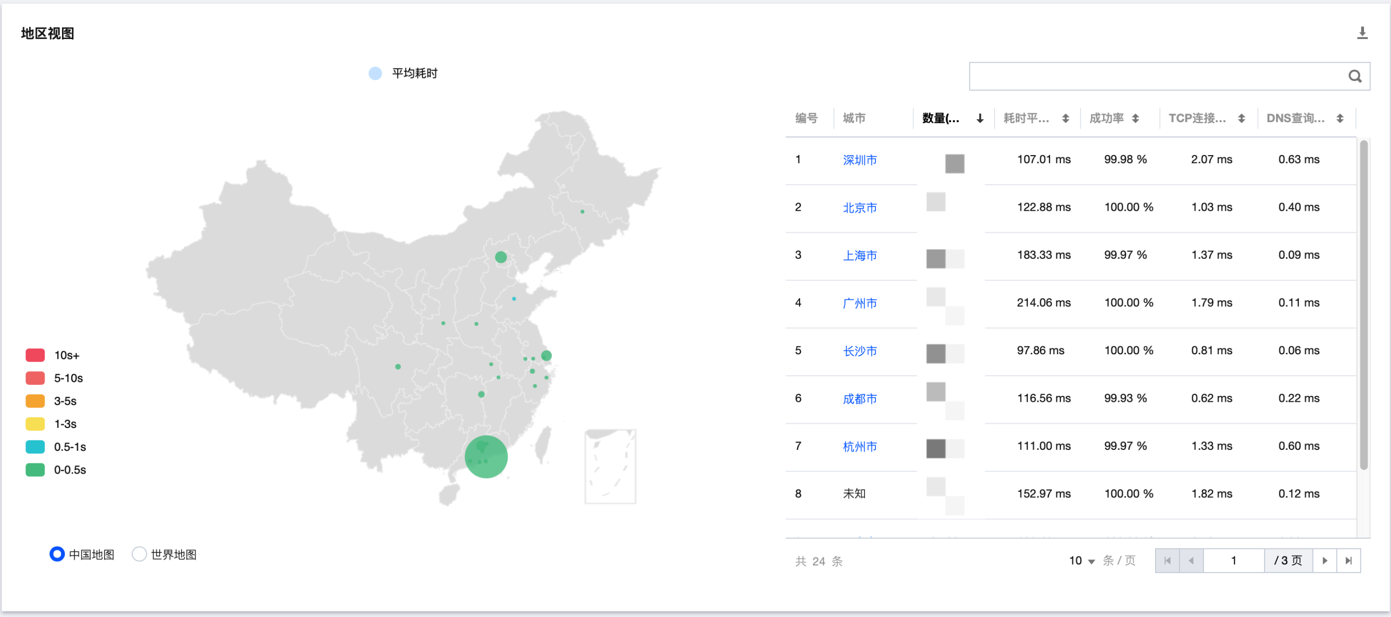
新建接入

应用名称	应用 ID	上报 id	操作
[redacted]	[redacted]	[redacted]	接入指引 上报流量统计 汇总分析 更多操作

共 1 条　10 条 / 页　1 / 1 页

Step 3. Analyze the performance

After successfully integrating the application performance SDK, wait for a few minutes. You can then click to summarize analysis in the performance monitoring feature card to view the summary of static resources. Switch the top menu to "Page Analysis" to view the static resource loading status of individual pages.



编号	城市	数量(...	耗时平...	成功率	TCP连接...	DNS查询...
1	深圳市	[redacted]	107.01 ms	99.98 %	2.07 ms	0.63 ms
2	北京市	[redacted]	122.88 ms	100.00 %	1.03 ms	0.40 ms
3	上海市	[redacted]	183.33 ms	99.97 %	1.37 ms	0.09 ms
4	广州市	[redacted]	214.06 ms	100.00 %	1.79 ms	0.11 ms
5	长沙市	[redacted]	97.86 ms	100.00 %	0.81 ms	0.06 ms
6	成都市	[redacted]	116.56 ms	99.93 %	0.62 ms	0.22 ms
7	杭州市	[redacted]	111.00 ms	99.97 %	1.33 ms	0.60 ms
8	未知	[redacted]	152.97 ms	100.00 %	1.82 ms	0.12 ms

共 24 条　10 条 / 页　1 / 3 页

Step 4. Configure an alarm policy

On the performance observation management page, switch the top menu bar to "Alarm Configuration" and refer to the Creating Alarm Policy document.

CDN Speed Test

Last updated：2024-12-31 17:48:24

Feature Introduction

CDN speed test uses a scheduled task configured in Cloud Automated Testing (CAT) to access the target resource from globally distributed real terminal nodes. This simulates the access experience of real users to test and monitor the CDN performance. It works in a zero-code non-intrusive manner to help you continuously monitor the accuracy, quality, and stability of CDN resource download in all regions.

Applicable scenario

CDN performance pre-validation

Before CDN service selection or migration, you can quickly predict the performance in all or specified regions after connection to CDN without modifying the production network environment. Then, you can design CDN optimization or migration plans and policies accordingly.

CDN performance monitoring

Based on regular testing and alarming, CDN speed test monitors availability problems caused by the unavailability of the origin or CDN service. In addition, it also collects detailed end-to-end phase-specific time statistics to help you continuously monitor the CDN service performance, such as time taken for DNS, TCP connection establishment, CDN server response, first packet arrival, and entire file loading.

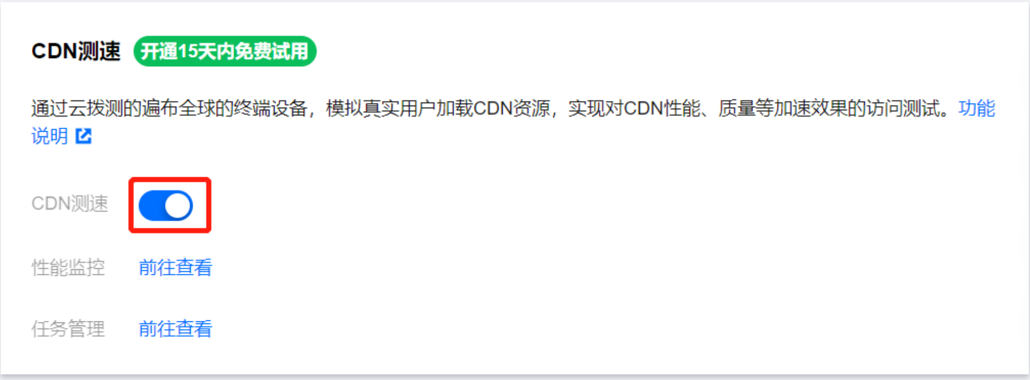
Resource update verification

After a CDN resource is updated, CDN speed test can actively test and compare the resource MD5 value to check whether the resource cached at each access point is updated promptly. This prevents resource update failures and avoids a poor user experience and business losses. For more scenarios and best practices such as network failures, on-demand and live experience monitoring, and page performance analysis, refer to CAT - User Guide.

Configuration Instructions

Step 1. Enable the CDN speed test feature

Log in to the CDN Console. Find the CDN speed test feature card. For the first-time setup, you need to create a service preset role and grant Content Delivery Network-related permissions. After successful authorization, click the enable button on the right side of the CDN speed test.



CDN测速 开通15天内免费试用

通过云拨测的遍布全球的终端设备，模拟真实用户加载CDN资源，实现对CDN性能、质量等加速效果的访问测试。功能说明

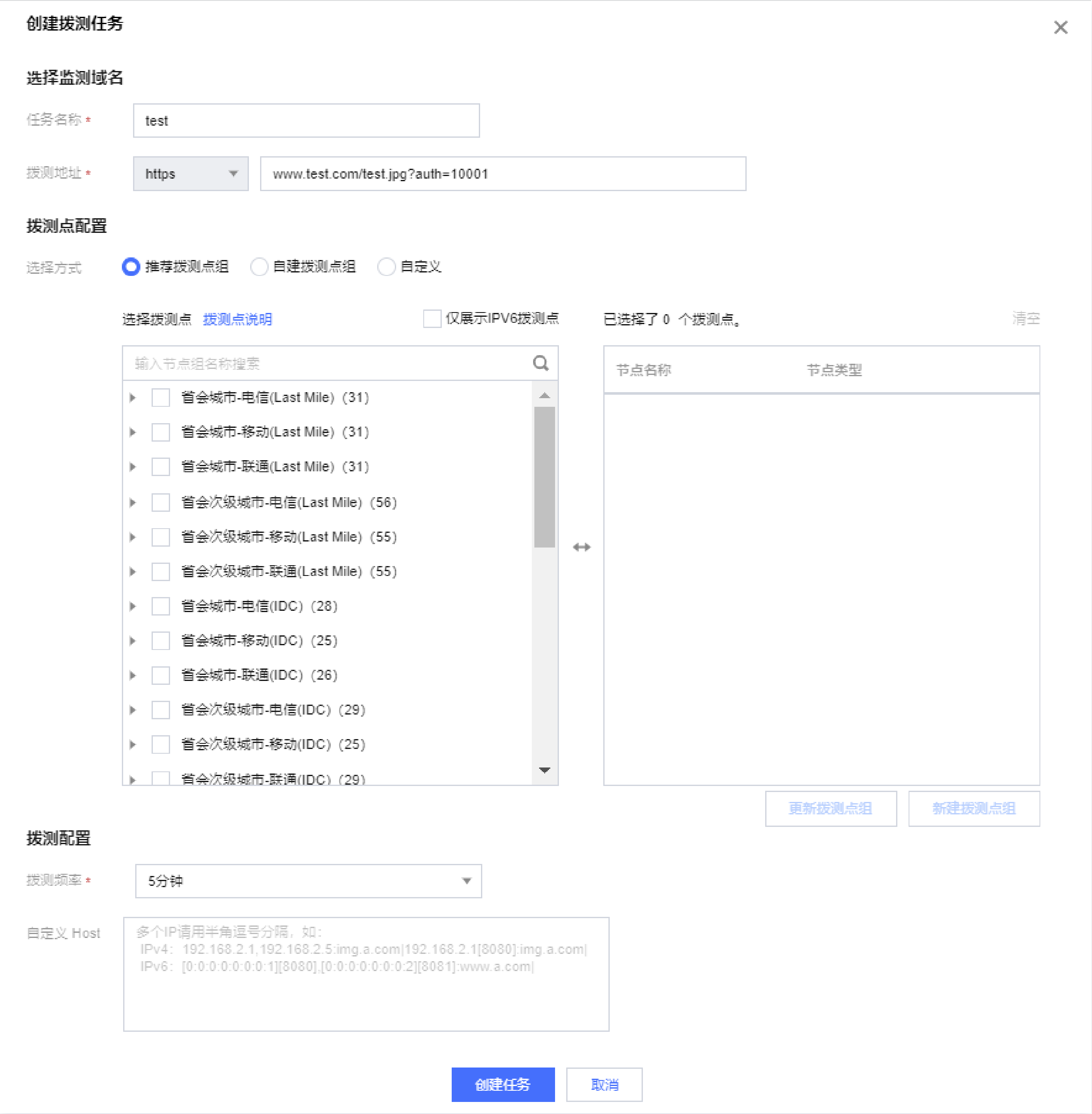
CDN测速

性能监控 前往查看

任务管理 前往查看

Step 2. Create a monitoring task

1. Enter the task list page and click the Create Task button.
2. From all available URLs, select the URLs for which to simulate user access requests (up to five URLs can be monitored at the same time), select the test points of ISPs in the regions where you want to simulate access requests, and enable the test task.



创建拨测任务

选择监测域名

任务名称 *: test

拨测地址 *: https www.test.com/test.jpg?auth=10001

拨测点配置

选择方式: ● 推荐拨测点组 ○ 自建拨测点组 ○ 自定义

选择拨测点 拨测点说明 □ 仅展示IPV6拨测点

- □ 省会城市-电信(Last Mile)（31）
- □ 省会城市-移动(Last Mile)（31）
- □ 省会城市-联通(Last Mile)（31）
- □ 省会次级城市-电信(Last Mile)（56）
- □ 省会次级城市-移动(Last Mile)（55）
- □ 省会次级城市-联通(Last Mile)（55）
- □ 省会城市-电信(IDC)（28）
- □ 省会城市-移动(IDC)（25）
- □ 省会城市-联通(IDC)（26）
- □ 省会次级城市-电信(IDC)（29）
- □ 省会次级城市-移动(IDC)（25）
- □ 省会次级城市-联通(IDC)（29）

已选择了 0 个拨测点。

节点名称	节点类型

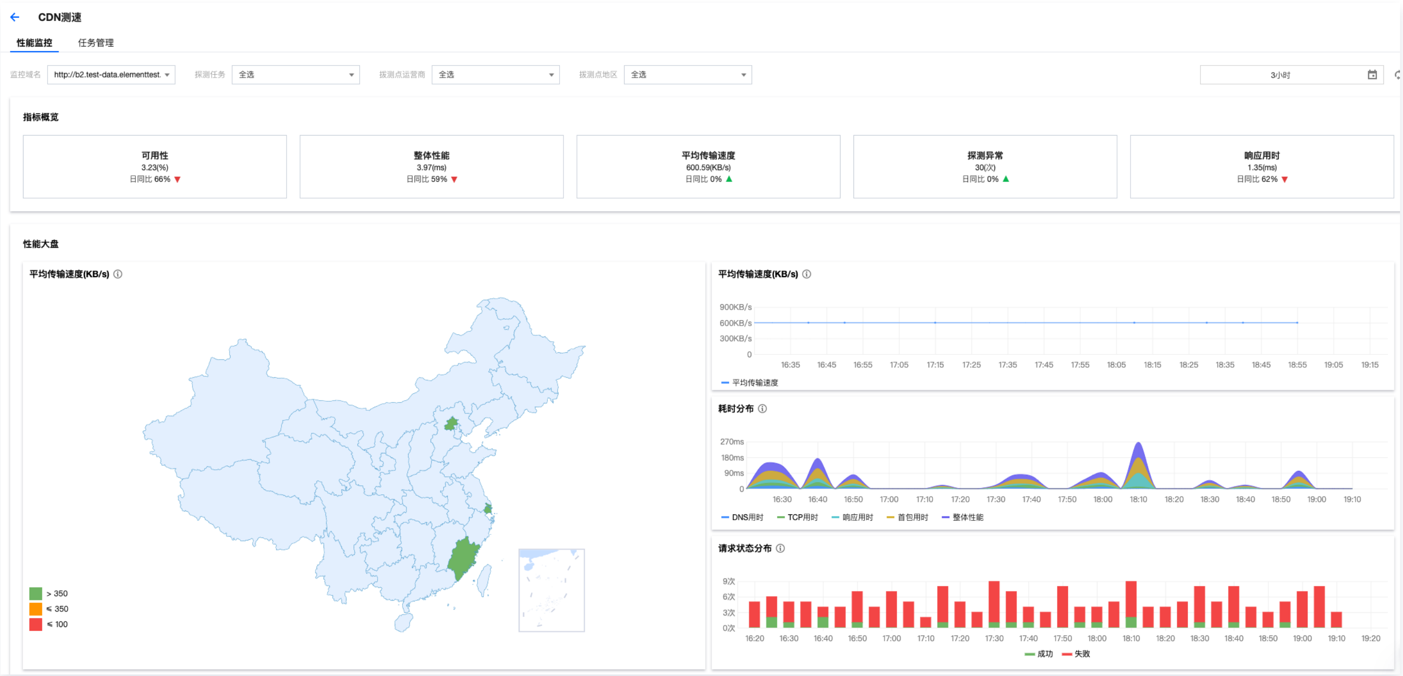
拨测配置

拨测频率 *: 5分钟

自定义 Host: 多个IP请用半角逗号分隔，如：
IPv4：192.168.2.1,192.168.2.5:img.a.com|192.168.2.1[8080]:img.a.com|
IPv6：[0:0:0:0:0:0:0:1][8080],[0:0:0:0:0:0:0:2][8081]:www.a.com|

Step 3. Analyze the performance in various dimensions

After 10-20 minutes of creating a task, the test data will be returned from test points around the world. You can view various core metrics of each resource on the performance dashboard. In the middle of the page, you can analyze specified metrics and lines and view the performance differences between regions, ISPs, and specific lines.



CDN测速

性能监控 任务管理

监控域名 http://b2.test-data.elementtest.
探测任务 全选
拨测点运营商 全选
拨测点地区 全选
3小时

指标概览

可用性	整体性能	平均传输速度	探测异常	响应用时
3.23(%)	3.97(ms)	600.59(KB/s)	30(次)	1.35(ms)
日同比 66% ▼	日同比 59% ▼	日同比 0% ▲	日同比 0% ▲	日同比 62% ▼

性能大盘

Step 4. Analyze details and troubleshoot failures

Click a single task to view more detailed data metrics, including time taken in each phase, network layer hop path, file MD5 values, and complete task logs. For element download or network issues, you can create dedicated page performance or network quality tasks to get more specific metric data.

Fee Description

Cloud CAT offers a 15-day free trial for all users. After the trial period expires, tasks will automatically pause. You can enable pay-as-you-go as needed or purchase prepaid resource packages to continue using the service. For trial period usage restrictions and price details, refer to Cloud CAT - Billing Overview.

Secure Acceleration

Last updated：2024-12-31 17:48:58

Tencent Cloud has fully upgraded the edge security acceleration platform (Tencent Cloud EdgeOne, EdgeOne). Based on Tencent Cloud's globally distributed edge nodes, EdgeOne provides users with both CDN acceleration and edge security protection capabilities. Compared to traditional independent security protection and acceleration products, EdgeOne offers out-of-the-box security protection capabilities at edge nodes, building more comprehensive DDoS protection, web protection, and bot management capabilities. It supports a variety of custom rule controls, providing users with more flexible and powerful security protection capabilities.
To protect your domain names connected to CDN, migrate your service to EdgeOne as follows.

Directions

Step One: Determining the Domain Names That Need Security Protection

EdgeOne will provide package purchase and security protection capabilities based on sites. If you need to migrate to EdgeOne, you should first determine the number of sites required for the domain names that need security protection to understand how many sites you will need after migrating to EdgeOne. See examples below:

CDN Domain Requiring Security Protection	EdgeOne Site	Description

`www.example.com`
`test.example.com`
`image.example.com`
	`example.com`	The primary domain is consistent, only one site needs to be accessed, and enable security protection for all site domains.

`www.example.com`
`test.example.com`
`www.site.com`
	`example.com`
	`site.com`
		The main domain is inconsistent. You need to separately access the two sites `example.com` and `site.com`, and then enable security protection for each site's domain name.

Step Two: Accessing the EdgeOne Console to Add Site and Accelerated Domain Name

Go to the EdgeOne Console to complete the corresponding EdgeOne site access and add the acceleration domain name according to the CDN domain name that needs to enable security protection in step one. For detailed steps, see Quick Start from Scratch to Access EdgeOne.
To add a site, you need to subscribe to an EdgeOne plan. The Standard plan is recommended as it offers DDoS mitigation, web protection, CC protection and bot management along with limited security traffic and requests. For more details, see EdgeOne Plans.

> **Note:**
> Security features (including DDoS mitigation and web protection) are enabled automatically once your acceleration domain name is added to EdgeOne. To customize the security configuration as needed, refer to Step 3.

(Optional) Step 3: Customize security policies

If you need to customize security policies based on your current business, such as adding IP allowlist and blocklist, configuring region blocking, or customizing web protection rules, refer to the following documentation for configuration details.

- DDoS Mitigation
- Web Protection
- Bot Management

CDN Refund

If you have already purchased an EdgeOne package and confirmed the migration of services to the EdgeOne platform, and there are unused resource packages in CDN, you can contact Online Customer Service. After providing relevant purchase records, a resource package refund will be provided according to the percentage of remaining resource package usage.

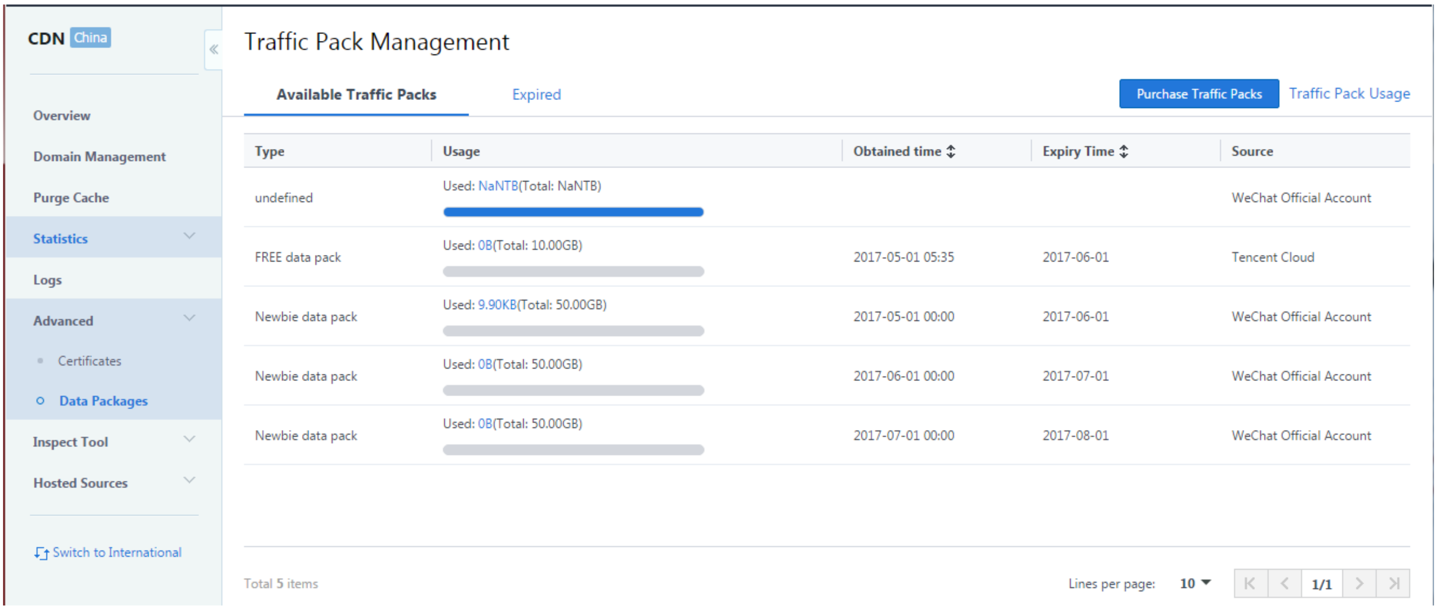
Query service

Manage Traffic Packages

Last updated：2024-12-31 17:49:29

If your billing method is Pay by Traffic, you can purchase a traffic package for cost saving. You can check the usage of traffic package in CDN Console to keep track of the balance of traffic package in real time and top it up in time so that your use of CDN services will not be affected.

Log in to CDN Console, select **Advanced**->**Data Packages**:



Type	Usage	Obtained time	Expiry Time	Source
undefined	Used: NaNTB(Total: NaNTB)			WeChat Official Account
FREE data pack	Used: 0B(Total: 10.00GB)	2017-05-01 05:35	2017-06-01	Tencent Cloud
Newbie data pack	Used: 9.90KB(Total: 50.00GB)	2017-05-01 00:00	2017-06-01	WeChat Official Account
Newbie data pack	Used: 0B(Total: 50.00GB)	2017-06-01 00:00	2017-07-01	WeChat Official Account
Newbie data pack	Used: 0B(Total: 50.00GB)	2017-07-01 00:00	2017-08-01	WeChat Official Account

This page provides the history of purchase and usage of traffic packages.

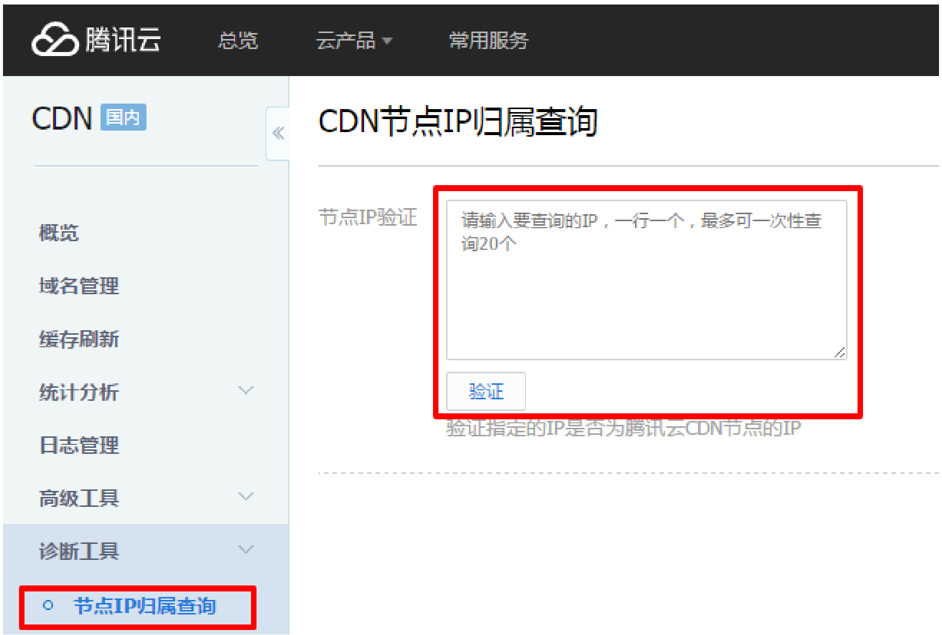
Verify Tencent IP Tool

Last updated：2024-12-31 17:49:36

Tencent Cloud CDN allows you to check whether an IP is a Tencent Cloud CDN server IP.

How to Use

Log in to CDN console. Select **Inspect Tool** - **Verify Tencent IP Tool** from the left panel.

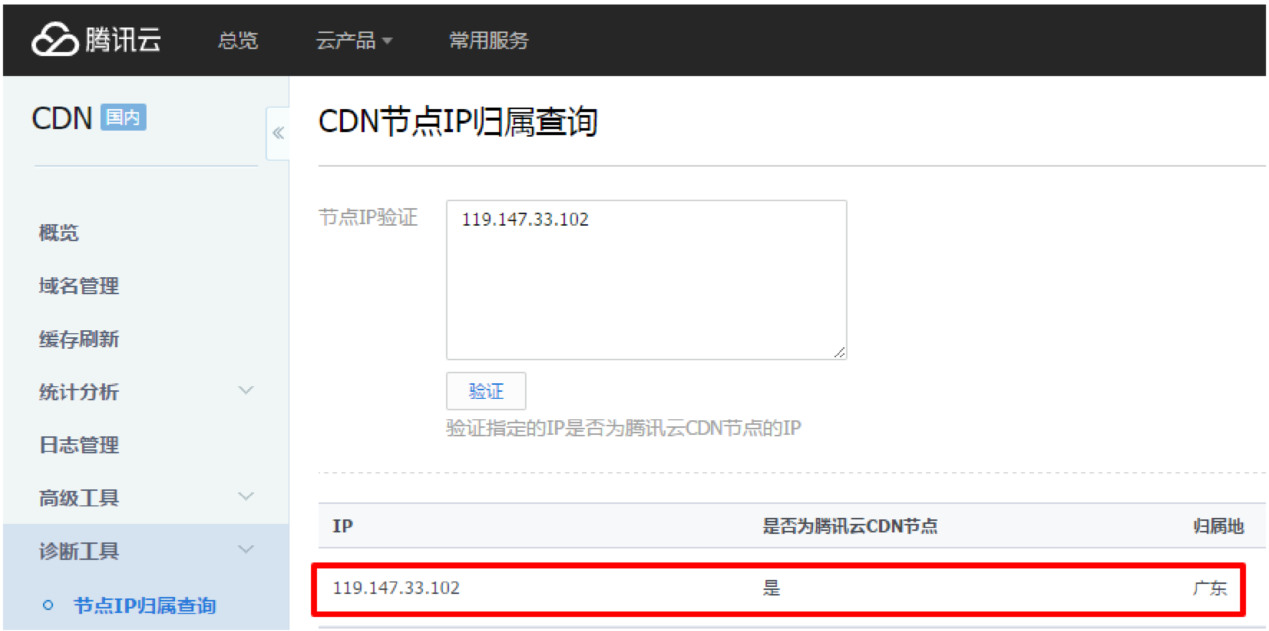


CDN节点IP归属查询

节点IP验证: 请输入要查询的IP，一行一个，最多可一次性查询20个

验证指定的IP是否为腾讯云CDN节点的IP

Enter IPs that you want to check in the text box (one per line, up to 20 per time). Click **Verify** to get the result. For Tencent Cloud CDN IPs, the region of the IP is displayed.



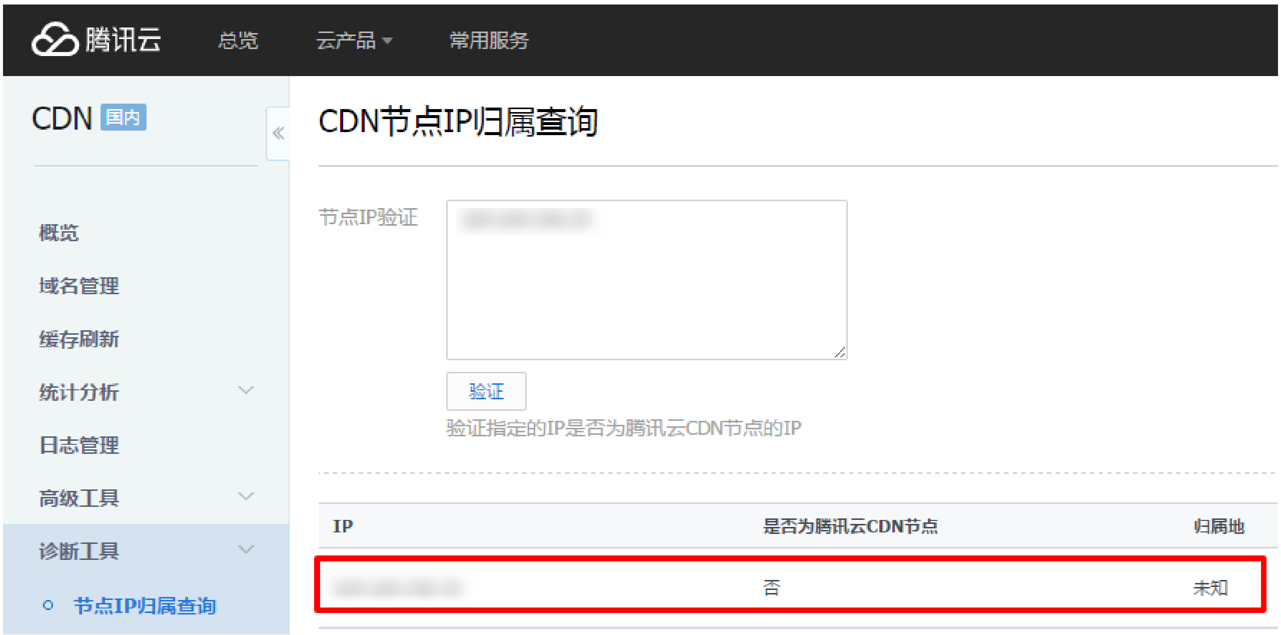
CDN节点IP归属查询

节点IP验证: 119.147.33.102

验证指定的IP是否为腾讯云CDN节点的IP

IP	是否为腾讯云CDN节点	归属地
119.147.33.102	是	广东

For non-Tencent Cloud CDN IPs, the region is **Unknown**.



CDN节点IP归属查询

节点IP验证 [redacted]

验证指定的IP是否为腾讯云CDN节点的IP

IP	是否为腾讯云CDN节点	归属地
[redacted]	否	未知

Origin-pull Node Query

Last updated：2024-12-31 17:49:45

Feature Introduction

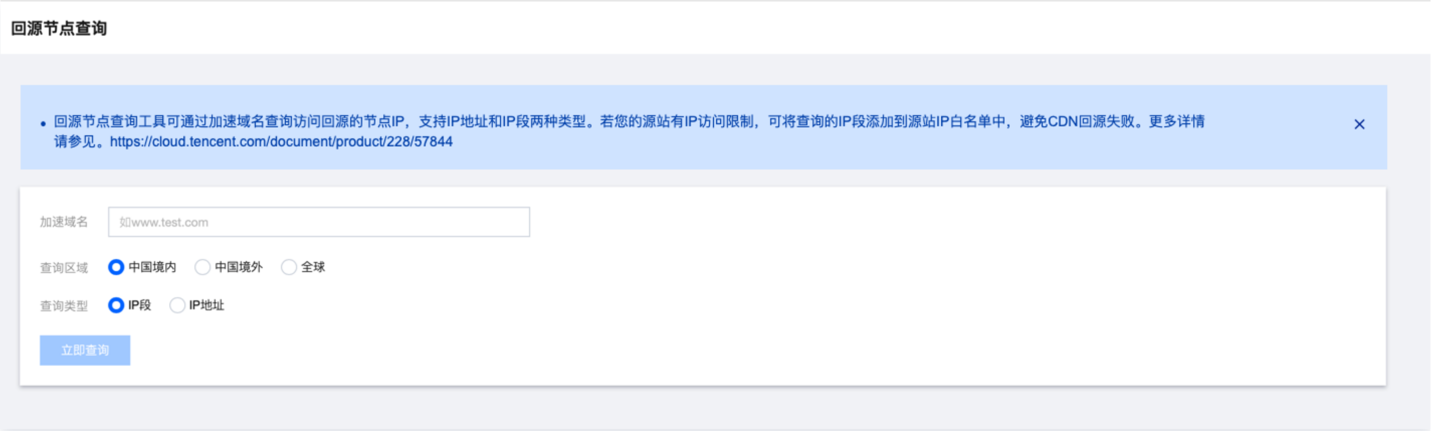
Tencent Cloud CDN supports querying the origin-pull node IPs for acceleration domain names, including both IP ranges and IP addresses.

Applicable scenario

Business access control requirements.

Operation Guide

Log in to the CDN console and choose **Service Query** > **Origin-pull Node Query** on the left sidebar.



回源节点查询

- 回源节点查询工具可通过加速域名查询访问回源的节点IP，支持IP地址和IP段两种类型。若您的源站有IP访问限制，可将查询的IP段添加到源站IP白名单中，避免CDN回源失败。更多详情请参见。https://cloud.tencent.com/document/product/228/57844

加速域名 如www.test.com

查询区域 ● 中国境内 ○ 中国境外 ○ 全球

查询类型 ● IP段 ○ IP地址

Use instructions:

- Specify a valid acceleration domain name that is connected to CDN and enabled.
- For the query region, select the acceleration region of the acceleration domain name.
- Select the query type based on your business needs.
- ISP information is not supported outside China.
- You can download the query results to your local device.

Diagnostic Tools

Last updated：2024-12-31 17:49:59

Feature Introduction

CDN provides a self-diagnosis tool. If a URL cannot be accessed, you can use the tool to identify the cause of the failure by checking the DNS resolution configuration, cache nodes, and origin server network. The tool also offers solutions to help you troubleshoot the failure or optimize the configuration.

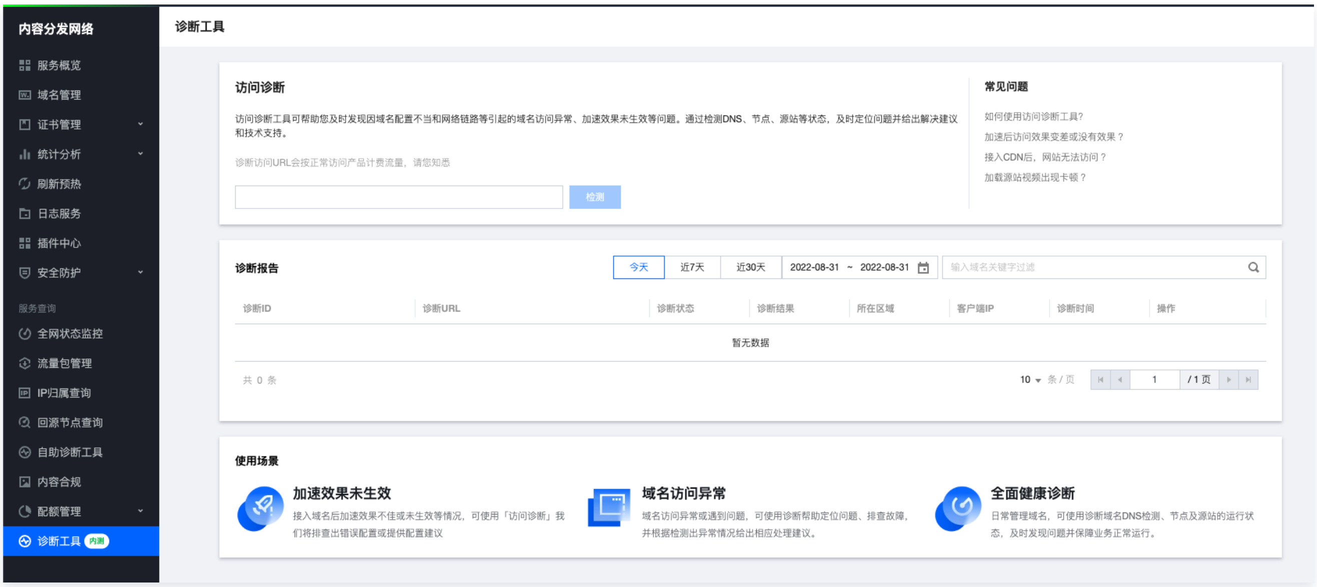
> **Note**
> - Only supports HTTP protocol URL diagnosis.
> - The resource URL to be diagnosed must be a domain name in active status under your account access.
> - The traffic generated during diagnosis is included in billing traffic as normal access behavior.

Applicable Scenario

The diagnosis tool is applicable when you encounter issues such as CDN access failure, URL access exception, or slow access rate.

Operation Guide

1. Log in to the CDN console, select **Query service** > **Diagnostic Tools (Beta)** from the left menu to enter the diagnostic page, as shown below:



诊断工具

访问诊断

访问诊断工具可帮助您及时发现因域名配置不当和网络链路等引起的域名访问异常、加速效果未生效等问题。通过检测DNS、节点、源站等状态，及时定位问题并给出解决建议和技术支持。

诊断访问URL会按正常访问产品计费流量，请您知悉

常见问题

如何使用访问诊断工具?

加速后访问效果变差或没有效果？

接入CDN后，网站无法访问？

加载源站视频出现卡顿？

诊断报告

诊断ID	诊断URL	诊断状态	诊断结果	所在区域	客户端IP	诊断时间	操作
暂无数据							

共 0 条　10 条 / 页　1 / 1 页

使用场景

加速效果未生效

接入域名后加速效果不佳或未生效等情况，可使用「访问诊断」我们将排查出错误配置或提供配置建议

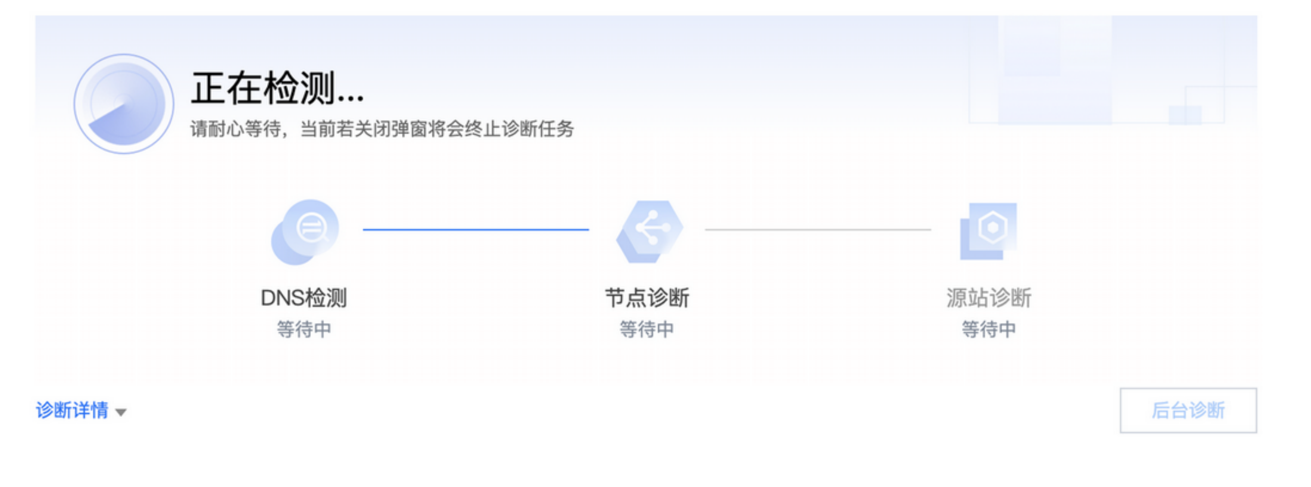
域名访问异常

域名访问异常或遇到问题，可使用诊断帮助定位问题、排查故障，并根据检测出异常情况给出相应处理建议。

全面健康诊断

日常管理域名，可使用诊断域名DNS检测、节点及源站的运行状态，及时发现问题并保障业务正常运行。

2. Start diagnosis: Enter the link to be diagnosed, click **Detect**, and the real-time diagnosis page will pop up.

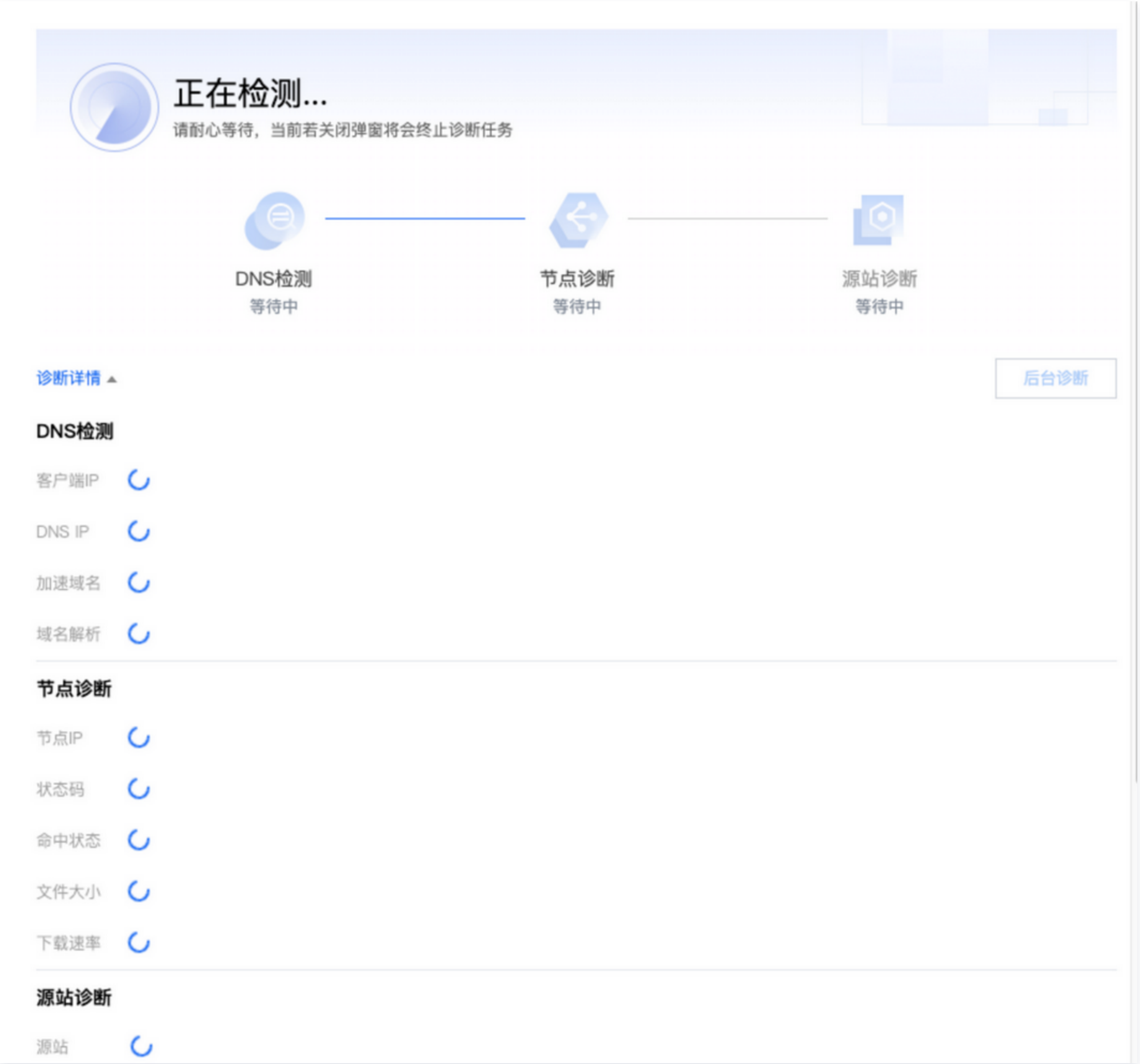


正在检测...

请耐心等待，当前若关闭弹窗将会终止诊断任务

- ○ Since the diagnosis process takes some time, it is recommended not to close the diagnosis page, as it may cause the diagnosis to be interrupted.
- ○ You can also click **Backend Diagnosis** to enter the backend diagnosis.

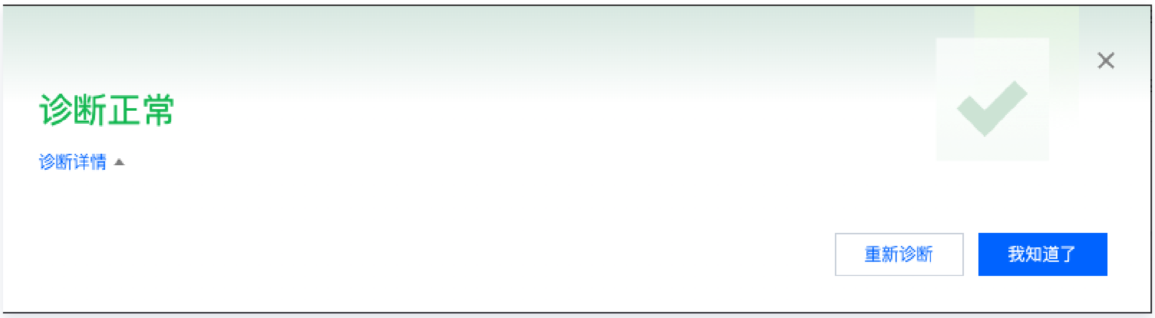
- Click **Diagnosis Details** to expand more detection items.



正在检测...

请耐心等待，当前若关闭弹窗将会终止诊断任务

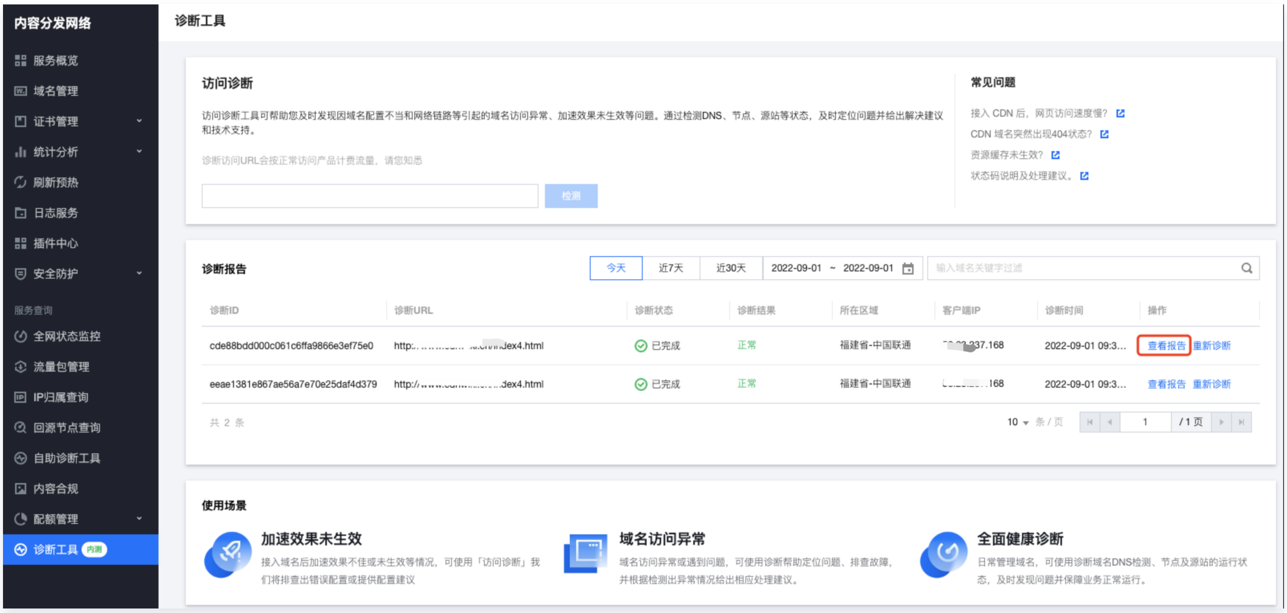
3. Diagnosis complete: When the diagnosis is finished, the final diagnosis result will be displayed in real-time:



诊断正常

4. Viewing the report:
    - When the diagnosis is complete on the diagnosis page, you can click **Diagnosis Details** to view the diagnosis report.

- In the diagnosis report list at the diagnosis menu entry, you can also click **View Report** to view it, as shown below:



诊断工具

访问诊断

访问诊断工具可帮助您及时发现因域名配置不当和网络链路等引起的域名访问异常、加速效果未生效等问题。通过检测DNS、节点、源站等状态，及时定位问题并给出解决建议和技术支持。

诊断访问URL会按正常访问产品计费流量，请您知悉

检测

常见问题

接入 CDN 后，网页访问速度慢？

CDN 域名突然出现404状态？

资源缓存未生效？

状态码说明及处理建议。

诊断报告

今天 近7天 近30天 2022-09-01 ~ 2022-09-01 输入域名关键字过滤

诊断ID	诊断URL	诊断状态	诊断结果	所在区域	客户端IP	诊断时间	操作
cde88bdd000c061c6ffa9866e3ef75e0	http:[redacted]dex4.html	✓ 已完成	正常	福建省-中国联通	[redacted]237.168	2022-09-01 09:3...	查看报告 重新诊断
eeae1381e867ae56a7e70e25daf4d379	http:/[redacted]dex4.html	✓ 已完成	正常	福建省-中国联通	[redacted]168	2022-09-01 09:3...	查看报告 重新诊断

共 2 条 10 条 / 页 1 / 1 页

使用场景

加速效果未生效

接入域名后加速效果不佳或未生效等情况，可使用「访问诊断」我们将排查出错误配置或提供配置建议

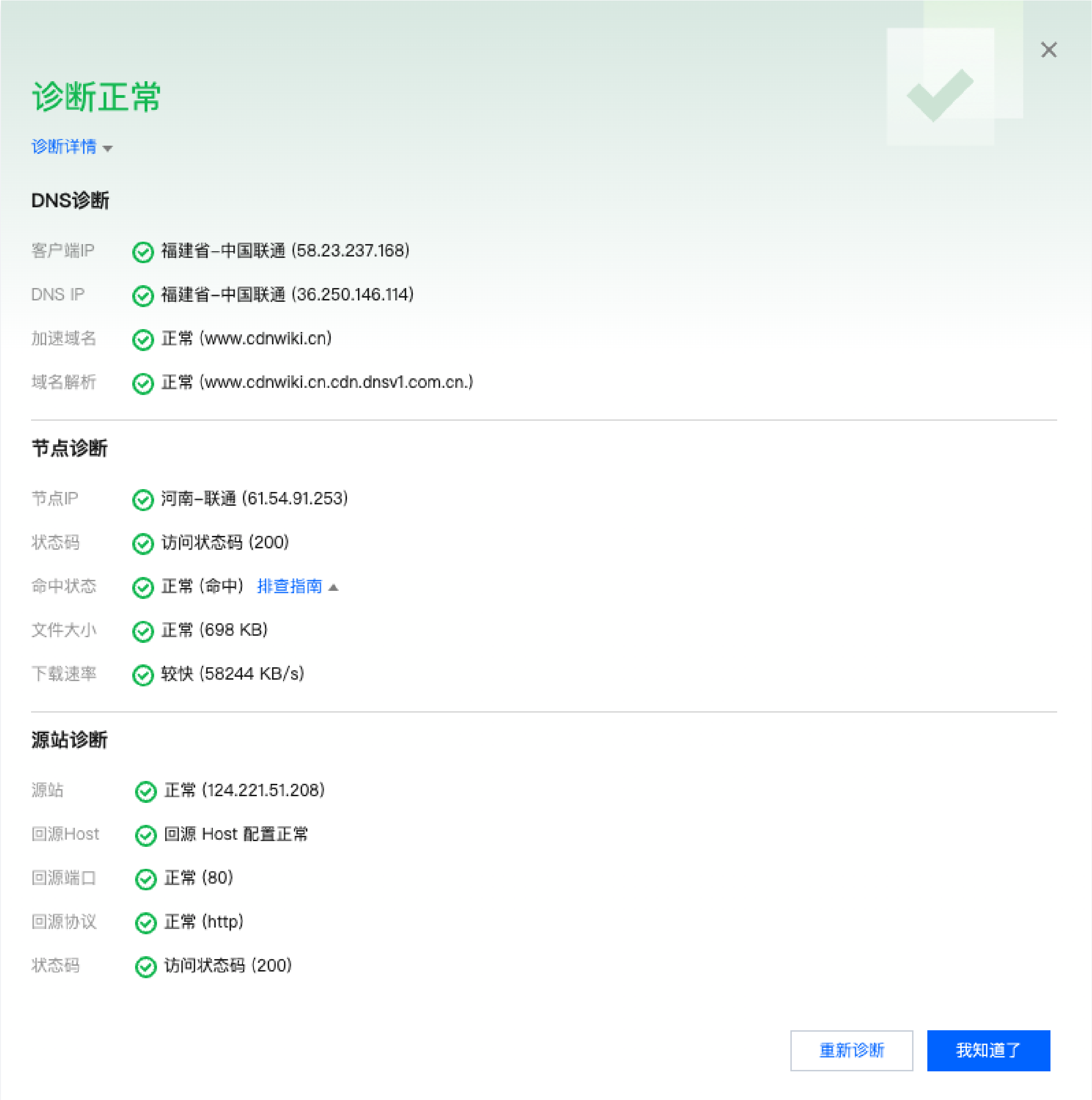
域名访问异常

域名访问异常或遇到问题，可使用诊断帮助定位问题、排查故障，并根据检测出异常情况给出相应处理建议。

全面健康诊断

日常管理域名，可使用诊断域名DNS检测、节点及源站的运行状态，及时发现问题并保障业务正常运行。

5. Diagnosis Report Description:



诊断正常

诊断详情

DNS诊断

客户端IP	✓ 福建省–中国联通 (58.23.237.168)
DNS IP	✓ 福建省–中国联通 (36.250.146.114)
加速域名	✓ 正常 (www.cdnwiki.cn)
域名解析	✓ 正常 (www.cdnwiki.cn.cdn.dnsv1.com.cn.)

节点诊断

节点IP	✓ 河南–联通 (61.54.91.253)
状态码	✓ 访问状态码 (200)
命中状态	✓ 正常 (命中) 排查指南
文件大小	✓ 正常 (698 KB)
下载速率	✓ 较快 (58244 KB/s)

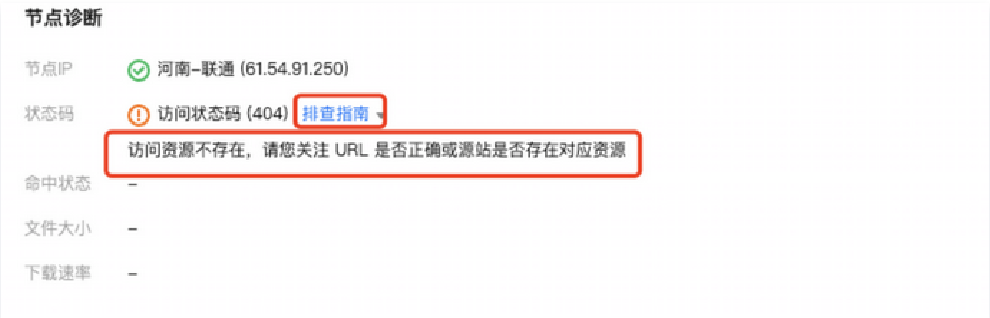
源站诊断

源站	✓ 正常 (124.221.51.208)
回源Host	✓ 回源 Host 配置正常
回源端口	✓ 正常 (80)
回源协议	✓ 正常 (http)
状态码	✓ 访问状态码 (200)

重新诊断 我知道了

Detection Module	Detection Items	Description
DNS diagnosis	Client IP	Display the client exit IP you diagnosed.
	DNS IP	Display the IP of your Local DNS in your region.
	Acceleration Domain Name	Detect the domain name corresponding to the URL.
	Domain Name Resolution	CNAME domain name corresponding to the accelerated domain name in the CDN console. If the display here is not as expected, it may be that your domain name resolution record is not added or incorrectly added.
Node diagnostics	Node IP	The Tencent Cloud acceleration node IP obtained when accessing your acceleration domain name.
	Status code.	The HTTP response status code of this diagnostic request URL, except for 2XX, indicates that the request file did not receive a response.
	Hit status	Shows whether this diagnostic request hit the acceleration node. If multiple diagnostics do not hit, check the cache configuration.
	File Size	Shows the file size of this diagnostic URL as a reference for response duration or download speed.
	Download speed	Shows the download speed of this diagnostic. The download speed is calculated as: file size / response duration from the edge node to the end of the download. If the file is small, the download speed may be distorted.
Origin server diagnosis	Origin Server	Display the address of your origin server.
	Origin-pull host	Display the current host configuration.
	Origin-pull Port	Display the current origin port, default is 80 if not configured.
	Origin-pull Protocol	Display the current origin-pull protocol configuration.
	Status code.	Display the HTTP status code of the origin server request file.

6. Diagnostic troubleshooting guide description:
 If there are exceptions or optimized detection items, the troubleshooting guide will be displayed. You can click **troubleshooting guide** to self-check exception reasons, as shown below:



节点诊断

节点IP	✓ 河南-联通 (61.54.91.250)
状态码	! 访问状态码 (404) 排查指南
	访问资源不存在，请您关注 URL 是否正确或源站是否存在对应资源
命中状态	-
文件大小	-
下载速率	-

Restricted Contents

Last updated：2024-12-31 17:50:21

Notes about Forbidden Resources

According to Article 4 of Tencent Cloud Service Agreement (Click to view), during the use of the Service, you shall abide by any applicable laws or regulations, and maintain the order and security of the Internet, and shall not engage in or facilitate any activity in violation of such laws or regulations, including but not limited to the following activities:

- Any activities that endanger national security, honor and interests, incite to subvert state power and overthrow the socialist system, split the state, undermine national unity, and propagate terrorism, extremism, ethnic hatred or ethnic discrimination;
- Fraud, false or misleading behaviors or any behavior (such as using private server or hack tools) that infringes on any legitimate rights and interests of others such as intellectual property right;
- Release and dissemination of SPAM, information that endanger national order and security, or reactionary, superstitious, obscene, pornographic, vulgar contents or illegal information;
- Any activities in violation of the operational rules of network, device or service linked with Tencent Cloud network; Any illegal or unauthorized interception, theft, interference or surveillance;
- Any activities that undermine or attempt to undermine the network security, including but not limited to malicious scanning over website and server, intrusion into a system and illegal acquisition of data by means of viruses, Trojan-horse programs, malicious codes, phishing and other methods;
- Any activities that change or attempt to change the system configuration provided by Tencent Cloud service or that compromise the system security; Any activities that prevent or disrupt the operation of Tencent Cloud service or the use of such service by others by technical or other means; Any activities that disturb or attempt to disturb the normal operation of any Tencent Cloud products, services and features in any way, or creation, release, dissemination of any tools and methods for such purposes;
- Any activities (including but not limited to "DNS resolution, "security service", "domain reselling" reverse proxy") that lead to frequent exposure of your business to such attacks as DDoS attack and affect Tencent Cloud service platform or others due to your failure to correct such activities in a timely manner or eliminate the effect of such activities as required by Tencent Cloud.
- Other activities in violation of laws or regulations, including but not limited to gambling.

If you are detected by Tencent Cloud CDN or reported by other users to have conducted any of the above activities, you may be blocked at the resource (URL) and domain level depending on the severity of your activity. A 403 error is returned when you access the forbidden resources.

You are notified of being blocked by email, SMS, or internal message. For any questions, contact us by submitting tickets.

If you have disputes about the forbidden resources, click the link in the email to go to the forbidden resource console for snapshots and appeal.

Quota Management

Last updated：2024-12-31 17:50:33

Feature Introduction

Quota management is a feature that enables you to view and manage quotas in the Content Delivery Network (CDN) console. You can check the CDN-related quota limits and usage, and apply for temporary or permanent quota increases based on business needs. The following quota types can be requested on a temporary or permanent basis: URL purge quota, directory purge quota, URL prefetch quota, and CDN domain limit.

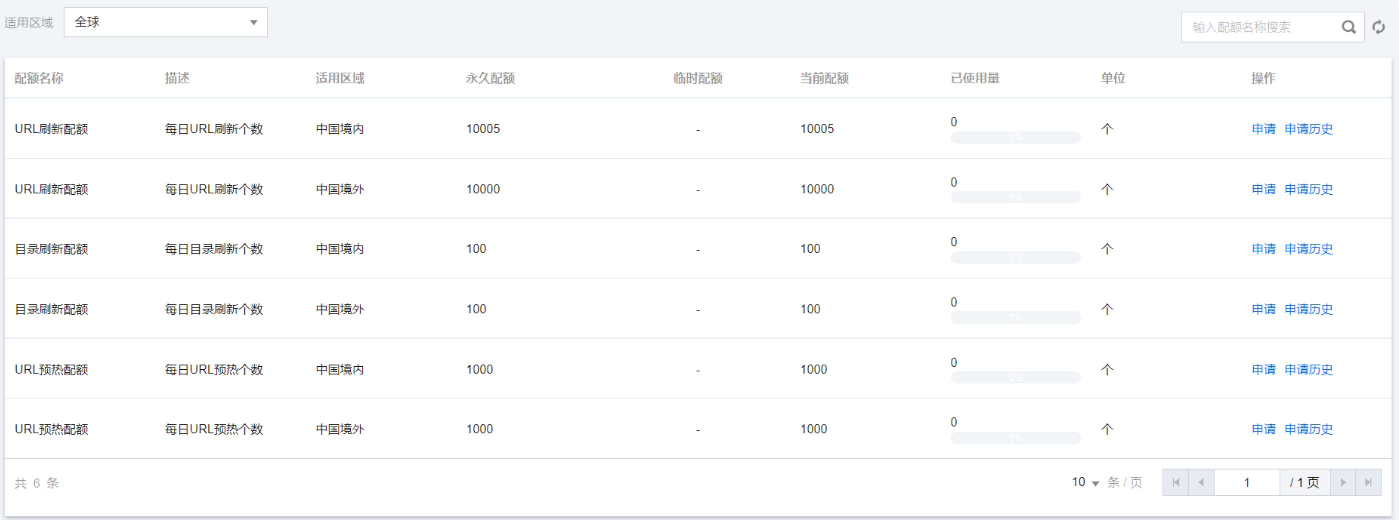
Applicable scenario

- **Temporary quota**: When business activities or operational scenarios require a temporary increase in quota, you can apply for a temporary quota for the required time range through quota management. When the temporary quota expires, the current quota will revert to the permanent quota.
- **Permanent Quota**: When the existing quota cannot meet your daily business needs, you can apply for a permanent quota for the corresponding feature through Quota Management. The approval process for a permanent quota takes longer, so for temporary business needs, it is recommended to apply for a temporary quota.

Operation Guide

Viewing quotas

Log in to the CDN console, click on **Quota Management** > **Quota Details** in the left sidebar to enter the quota details page, where you can view the current quota status or apply for a quota.



适用区域 全球

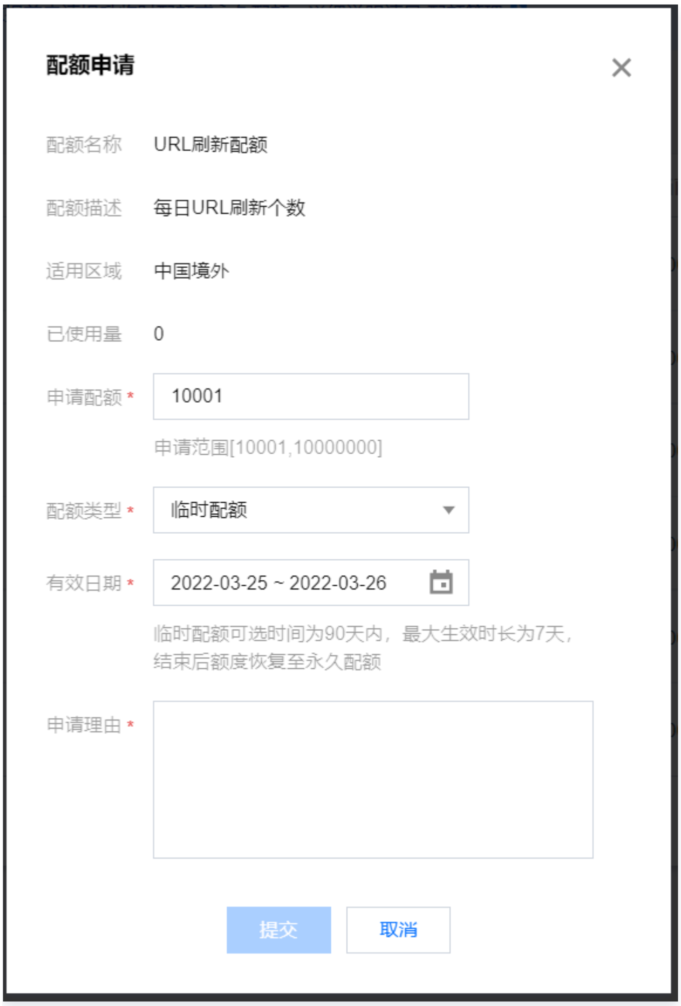
配额名称	描述	适用区域	永久配额	临时配额	当前配额	已使用量	单位	操作
URL刷新配额	每日URL刷新个数	中国境内	10005	-	10005	0	个	申请 申请历史
URL刷新配额	每日URL刷新个数	中国境外	10000	-	10000	0	个	申请 申请历史
目录刷新配额	每日目录刷新个数	中国境内	100	-	100	0	个	申请 申请历史
目录刷新配额	每日目录刷新个数	中国境外	100	-	100	0	个	申请 申请历史
URL预热配额	每日URL预热个数	中国境内	1000	-	1000	0	个	申请 申请历史
URL预热配额	每日URL预热个数	中国境外	1000	-	1000	0	个	申请 申请历史

Note:

- The current quota represents the maximum limit of this quota. If there are multiple temporary quotas effective at the current time, the current quota is the maximum value among all temporary and permanently effective quotas. Note: This is highlighted content.
- The temporary quota will take effect at 00:00 on the start date and end at 24:00 on the end date. After it expires, the quota will revert to the permanent quota.
- URL purge quota, directory purge quota, and URL prefetch quota all take effect on a daily basis, and the used amount will be reset every day at 00:00.
- Quotas for regions within and outside the Chinese mainland are independent of each other and need to be applied for separately.
- The cdn domain limit is a permanently effective quota, not differentiated by region. Note: This is highlighted content.

Applying for quotas

Click **Apply** to enter the selected quota application page, complete and submit the application form.



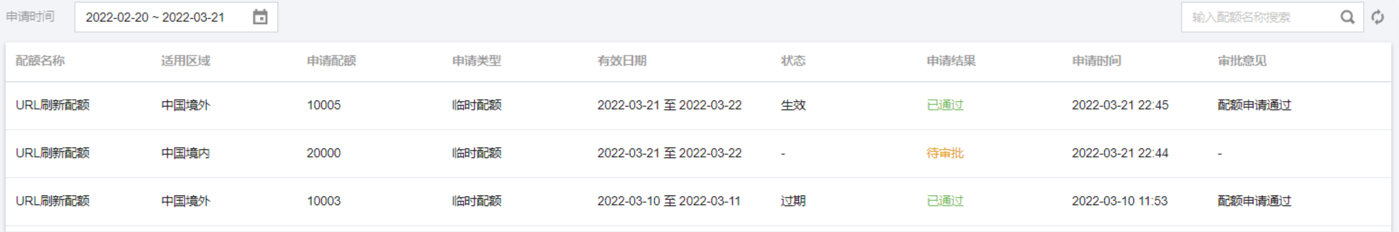
配额申请

配额名称	URL刷新配额
配额描述	每日URL刷新个数
适用区域	中国境外
已使用量	0
申请配额 *	10001 申请范围[10001,10000000]
配额类型 *	临时配额
有效日期 *	2022-03-25 ~ 2022-03-26 临时配额可选时间为90天内，最大生效时长为7天，结束后额度恢复至永久配额
申请理由 *	

> **Note:**
> - A temporary quota must be between the permanent quota +1 and 10000000.
> - For temporary quotas, the optional validity date can be selected within a range of 90 days, and the maximum effective duration is 7 days.
> - To increase the chances of your quota application being approved, please provide a reasonable quota value and a detailed reason for your application.
> - If you are currently applying for a quota as the CDN domain name upper limit quota, it is recommended that the current domain usage exceeds 70% and the number of domain name quotas applied for does not exceed twice the current quota; otherwise, it may be rejected.

Application History

Click **Application History**, or select **Quota Management** > **Application History** on the left sidebar to enter the application history page, where you can view the approval status of your quota application.



申请时间 2022-02-20 ~ 2022-03-21

配额名称	适用区域	申请配额	申请类型	有效日期	状态	申请结果	申请时间	审批意见
URL刷新配额	中国境外	10005	临时配额	2022-03-21 至 2022-03-22	生效	已通过	2022-03-21 22:45	配额申请通过
URL刷新配额	中国境内	20000	临时配额	2022-03-21 至 2022-03-22	-	待审批	2022-03-21 22:44	-
URL刷新配额	中国境外	10003	临时配额	2022-03-10 至 2022-03-11	过期	已通过	2022-03-10 11:53	配额申请通过

> **Note:**

> - When the application result is **approved**, it means the quota application has been approved; if the approval has not passed, it is recommended to apply for **temporary quota**, or adjust the quota application and resubmit the application reasons.
> - When a temporary quota expires, it is no longer valid, and the quota type will turn permanent, or stay temporary if you still have other valid temporary quotas.

Browser Cache TTL

Last updated：2024-12-31 17:51:09

Configuration Scenario

When your origin site fails and resources cannot be pulled from it normally, if offline cache is enabled, the content cached in CDN can be used.

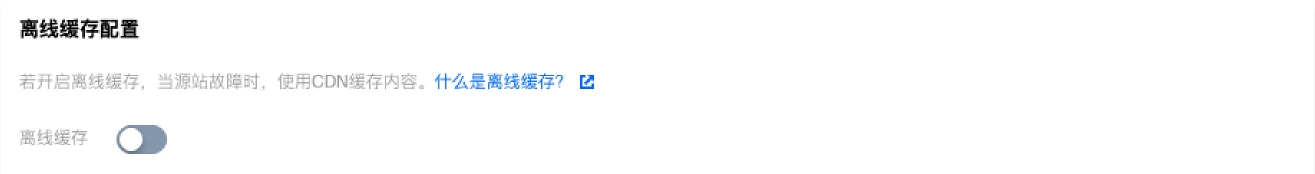
- If there is cached content on nodes, it will be returned. Even if the hit content has expired, it will still be returned until the origin server recovers to resume normal origin-pull.
- If there is no cached content on nodes, an error message indicating that the origin server fails will be returned.

> Note
> - The origin server is considered faulty if it does not return a status code and header definition when CDN retrieves content.
> - Offline cache is supported only for acceleration domain names in the Chinese mainland.
> - This feature is currently unavailable on some platforms due to ongoing upgrades.
> - When you enable the offline cache feature, this domain does not support the configuration copy feature.

Configuration Guide

Viewing Configuration

Offline cache is disabled by default. You can enable or disable it as needed.



离线缓存配置

若开启离线缓存，当源站故障时，使用CDN缓存内容。什么是离线缓存？

离线缓存 ○