

Content Delivery Network

Configuration Guide

Product Documentation



Copyright Notice

©2013-2025 Tencent Cloud. All rights reserved.

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

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parent, subsidiaries and affiliated companies, as the case may be. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Configuration Guide

Domain Management

- Domain Name Operations

- Domain name search

- Copying Configuration

- Batch Changing Configuration

- Configuration Manual

- Shared CNAME

Domain Name Configurations

- Configuration Overview

- Basic Configurations

- Basic Information

- Origin Server Configuration

- Advanced Origin-pull Configuration

- HTTPS Origin-pull algorithm description

Access Control

- Hotlink Protection Configuration

- IP Blocklist/Allowlist Configuration

- IP Access Limit Configuration

- Video Dragging Configuration

- Authentication Configuration

- Instruction

- TypeA

- TypeB

- TypeC

- TypeD

- UA Blocklist/Allowlist Configuration

- Downstream Speed Limit Configuration

- Access Port Configuration

Cache Configuration

- Cache Key Rule Configuration

- Node Cache Validity Configuration

- Status Code Cache Configuration

- HTTP Header Cache Configuration

- Access URL Rewrite Configuration

- Browser Cache Validity Configuration
- Cache Configuration FAQs
- Origin-pull Configuration
 - Range GETs Configuration
 - Follow 301/302 Configuration
 - Origin-pull timeout configuration
 - Request Header Configuration
 - Origin URL Rewrite Configuration
 - Origin-pull SNI
 - Merging Requests
- HTTPS Configuration
 - HTTPS Configuration
 - HTTPS Configuration Guide
 - Forced Redirection Configuration
 - HTTP2.0 configuration
 - OCSP Stapling Configuration
 - HSTS Configuration
 - TLS Version Configuration
 - QUIC
 - FAQs about HTTPS
- Advanced Configuration
 - Usage Limit Configuration
 - HTTP Response Header
 - SEO Configuration
 - Smart Compression Configuration
 - Custom Error Page
 - POST Request Size Configuration
- Image Optimization
- Statistical Analysis
 - Realtime Monitoring
 - Panel Configuration
 - Data Comparison
 - Access Monitoring
 - Origin-Pull Monitoring
 - Status codes description
 - Data Analysis
 - FAQs about Statistical Analysis
- Purge and Prefetch

Purge Cache

Prefetch Cache

History

Purge and Prefetch FAQs

Log Management

Log Service

Real-time Logs

EdgeOne

Service Query

Entire Network Status Monitoring

Verify Tencent IP

Origin-pull Node Query

Content Compliance

Quota Management

Offline Cache

Configuration Guide

Domain Management

Domain Name Operations

Last updated : 2023-06-29 17:45:01

Scenarios

To manage domain names connected to Tencent Cloud CDN, go to the [CDN console](#) and select **Domain Management** from the left sidebar.

You can adjust the list column, batch enable/disable acceleration service for domain names, and batch change domain name projects, tags, and configurations.

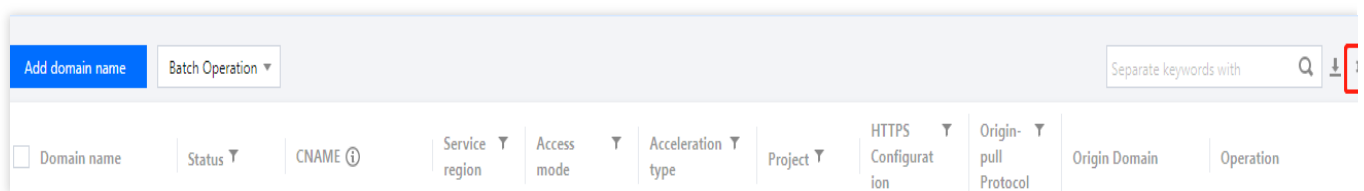
Directions

Adjusting list volumes

Click the



icon on the right of the search bar to open the list field option list. You can choose to display or hide fields and adjust their display order:



Exporting the configuration list

Click the



icon on the right of the search bar to export an Excel file of the domain name list content. You can select up to 1000 domain names to export each time.

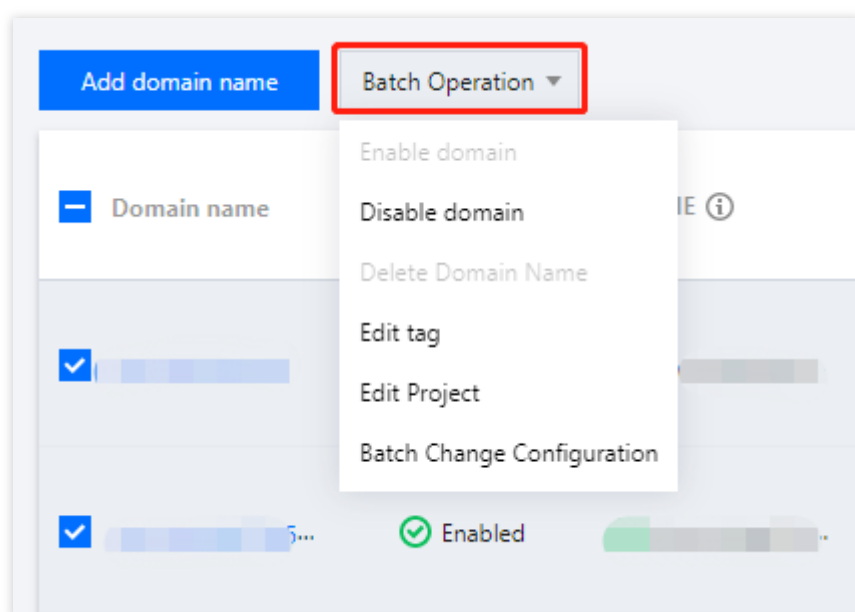
Changing the related project

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

Single domain name: Click **More** > **Modify Project**.

Domain name	Status	CNAME	Service region	Access mode	Acceleration type	Project	HTTPS Configuration	Origin-pull Protocol	Origin Domain	Operation
<input type="checkbox"/>	Enabled		Outside the Chinese mainland	Tencent Cloud COS Origin	Webpage file download	Default Project	Not configured	Follow Protocol		Manage Disable More

Batch change the project: Select target domain names and click **More Actions** -> **Edit Project** on the top. Up to 50 domain names can be selected at a time.



Editing tags

Single domain name: Click the target domain name to enter its configuration page, open the **Basic Configuration** tab, click the pencil icon on the right of **Tag** in the **Basic Information** section.

Batch editing: Select domain names to modify, and click **More Actions** -> **Edit Tag** on the top. Up to 50 domain names are supported. Refresh the page to check the updated tags.

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 name: **More** -> **Disable**.

Batch disable: Select domain names to disable, click **More Actions** -> **Disable Acceleration** on the top.

Enabling the acceleration service

When the acceleration service is enabled for a domain name, the domain name configuration is distributed to cache nodes across the entire network.

Single domain: Click **More** -> **Enable**.

Batch enable: Select domain names to enable, and click **More Actions** -> **Enable Acceleration** on the top.

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 domain names

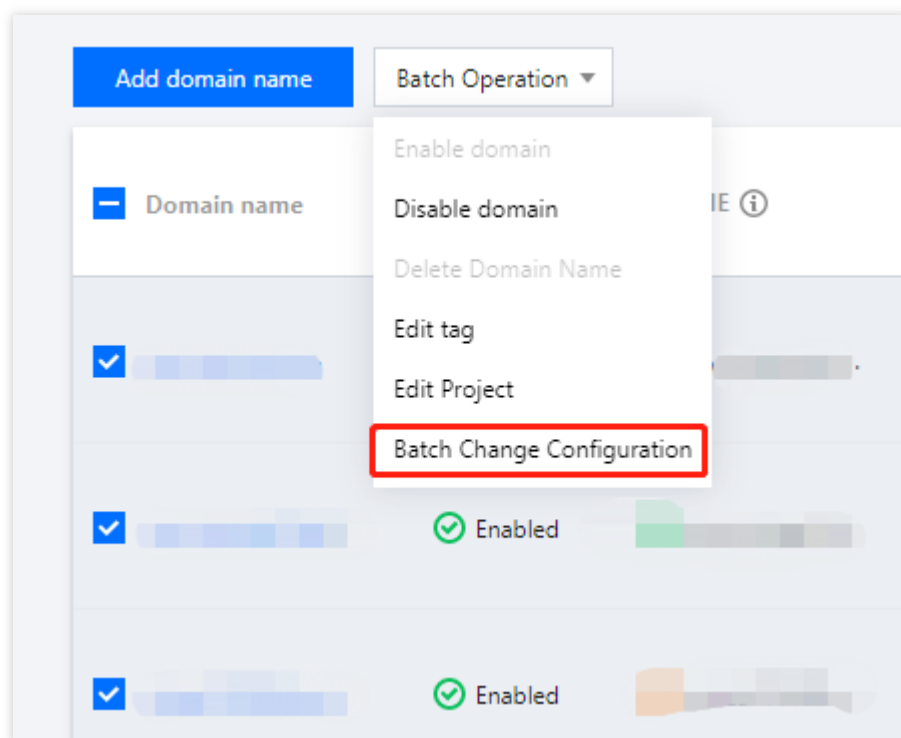
To delete an accelerated domain name, you need to disable it first. After the deletion, all data of the domain names will be cleared and cannot be restored. You can no longer check their statistical data.

Single domain name: Locate the domain name, click **More** -> **Delete**.

Batch delete: Select domain names to delete, and click **More Actions** -> **Delete** on the top.

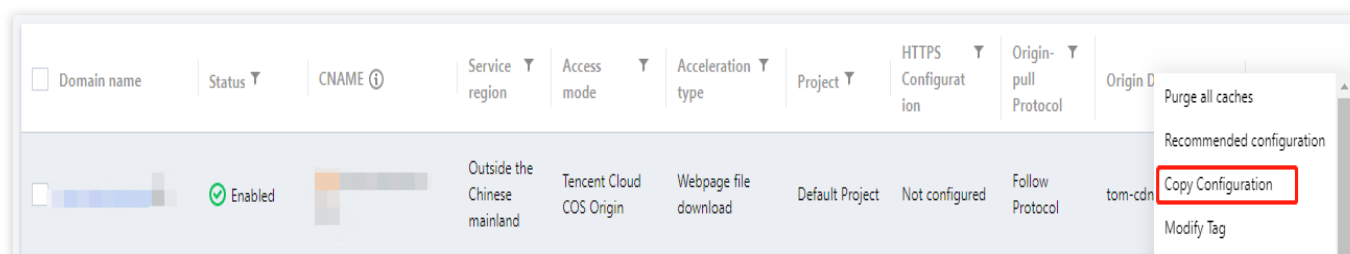
Batch changing configurations

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](#).



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](#).



Purging all caches

To purge all cached resources on the CDN nodes under the current domain name, click **More** on the right of the domain name, and click **Purge all caches** in the pop-up window.

Add domain name

Batch Operation

Separate keywords with

<input type="checkbox"/> Domain name	Status	CNAME	Service region	Access mode	Acceleration type	Project	HTTPS Configuration	Origin-pull Protocol	Origin ID
<input type="checkbox"/>	Enabled		Outside the Chinese mainland	Tencent Cloud COS Origin	Webpage file download	Default Project	Not configured	Follow Protocol	<div>Purge all caches</div> <div>Recommended configuration</div> <div>Copy Configuration</div> <div>Modify Tag</div>

Domain name search

Last updated : 2020-03-03 15:05:53

Operation Scenarios

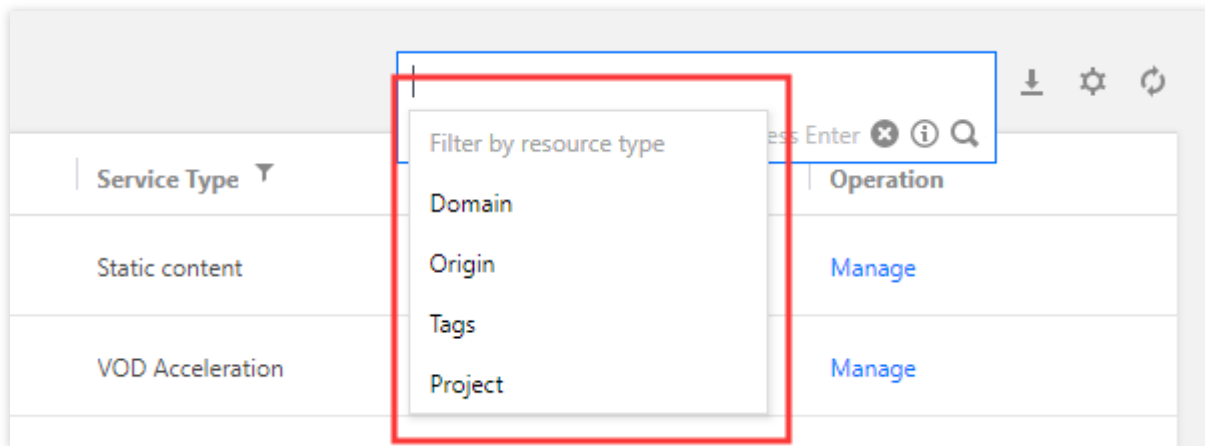
You can use the domain name search feature to find a specific domain name. You can filter domain names by multiple criteria such as domain name, origin server, tag, and project as well as multiple keywords.

Note :

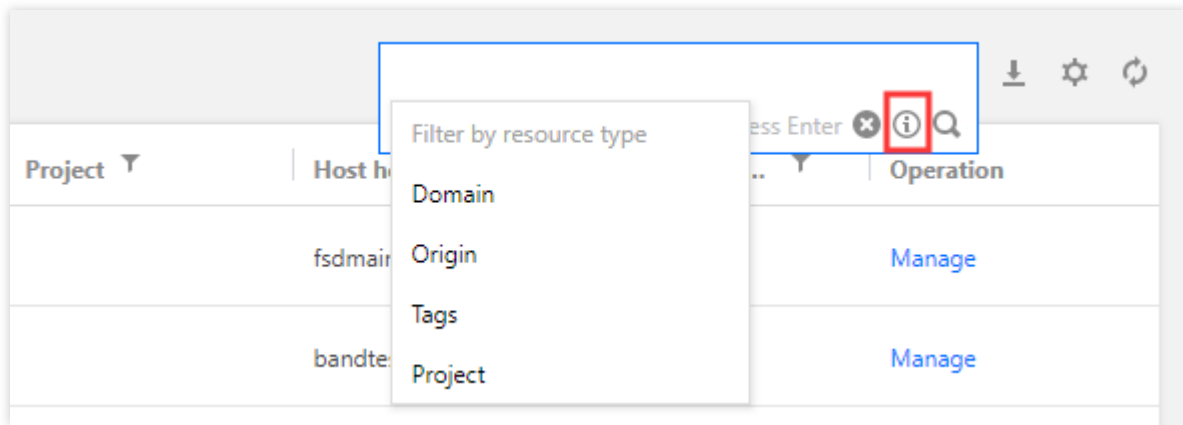
A tag is provided by Tencent Cloud to identify resources on the cloud. For more information on tags and how to manage it, please see [Tag](#).

Directions

1. Log in to the [CDN Console](#) and click **Domain Management** on the left sidebar to enter the management page.
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.



3. If you have questions about the input resource attribute or input format, click the **i** icon for [help with search](#).

**Note :**

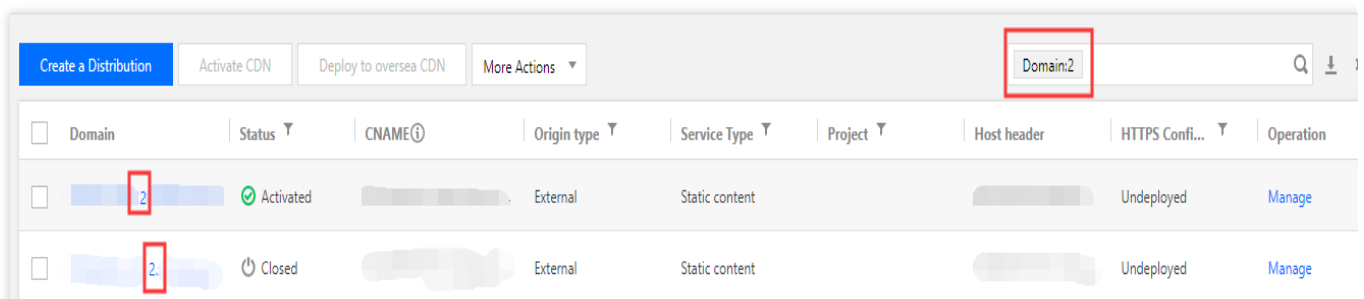
Only master origin servers can be searched for, not slave servers.

Use semicolon (;) to separate origin server IP addresses when searching for multiple origin servers.

Only single-keyword search is supported for domain names and origin servers.

Search Description

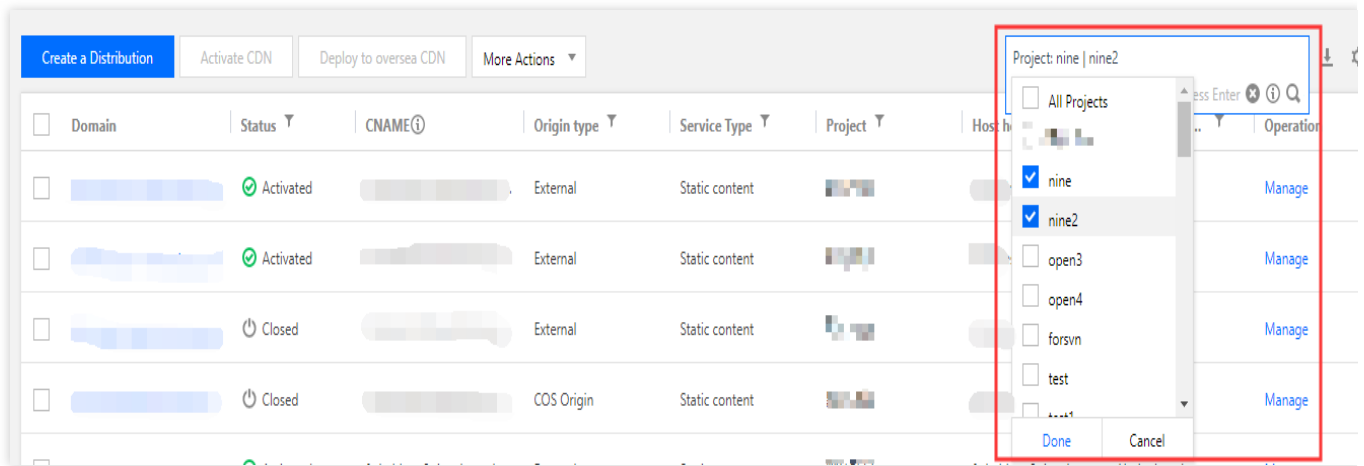
Search by domain name: Enter a complete or partial domain name for search. Fuzzy search is supported.



Search by origin server: Enter a complete or partial origin server for search. Fuzzy search is supported.

Search by tag: Enter a complete tag, and a list of domain names that contain the entered tag will be returned. Fuzzy search is not supported.

Search by project: You can select multiple projects as a filter.



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. Use vertical bar (|) to separate multiple keywords.

Help with search

Type	Input Format	Example	Search Box Example	Description
Single keyword	Keyword	www.test.com		Filters domain names containing www.test.com
Single domain name attribute	Attribute:keyword	Origin server:1.1.1.1		Filters domain names where origin server contains 1.1.1.1
Multiple domain name attributes	Attribute:keyword return Attribute:keyword	Domain name:test Origin server:1.1.1.1		Filters domain names where domain name contains "test" and origin server contains "1.1.1.1"
Single domain	Attribute:keyword keyword	Project:test1 test2		Filters domain names where project contains test1 or test2

name attribute with multiple keywords			<div>Project:test1 test2</div>	domain name contains "test2" from selected project. The domain and origin attributes do not support multi-keyword search.
Copied character	(Pasted character)	test abc	<div>Domain:test abc</div>	Filters domain names containing "test" or "abc".

Note :

CDN cannot make global searches if no attribute is entered. Therefore, the **domain name** attribute is added for search by default. In other words, when you enter a single keyword, the content in the search box will be `domain name:www.test.com` ; when you copy characters, the content in the search box will be `domain name:test|abc` .

Copying Configuration

Last updated : 2020-12-28 11:32:31

Configuration Overview

With the Duplicate Configuration feature, you can duplicate configurations of an existing forwarding domain name to one or multiple new forwarding domain names.

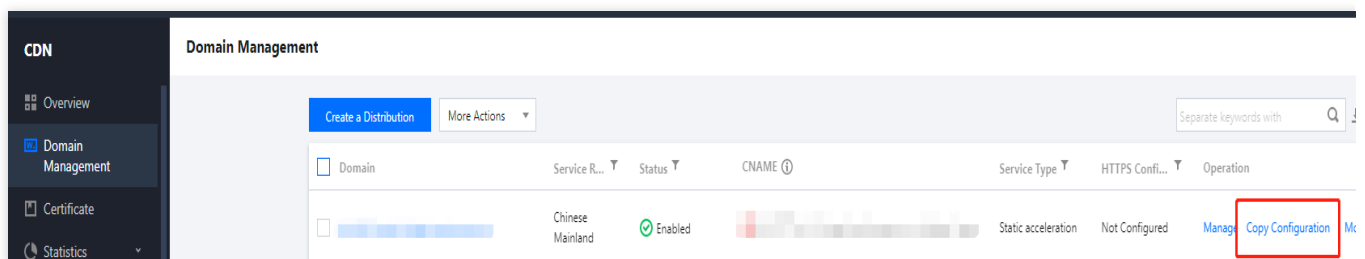
Note:

This feature is not available for domain names that are disabled or blocked, having expired ICP filing (only for Chinese domain names), using external certificates, or with unsupported configurations varying across regions.

Backend configurations (i.e. configurations that not set up in the console) cannot be duplicated.


Configuration Guide

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, click **Duplicate Configuration** on the right of a domain name to enter its configuration page.




Add a new forwarding domain name and submit it. The configurations of the current domain name will be duplicated to the new one.

[←](#) Copy Configuration

Copy the configuration of  to the new domain name below:

ⓘ

Note

The configurations of an existing acceleration domain name can be copied to one or multiple new acceleration domain names [Learn More](#) 

If the original domain name has special configurations on the backend (instead of the console), the special configurations cannot be copied.

Acceleration Domain Name

Add

Copy

Note:

The submitting process cannot be interrupted. You can manage the configuration after the new domain name is successfully added.

The configurations of a new domain name will be deployed to CDN nodes across the entire network, without affecting your running businesses. If you want to enable the acceleration service, you need to configure the CNAME. For configuration directions, please see [CNAME Configuration](#).

Batch Changing Configuration

Last updated : 2021-03-31 16:07:10

Feature Overview

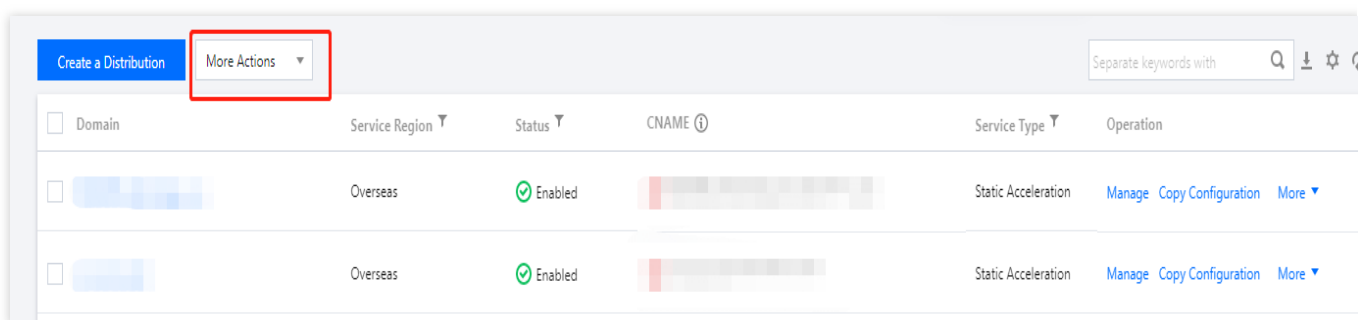
The Batch Change Configuration feature allows you change a configuration item of multiple domain names at the same time.

Note:

Some of the configuration items are not yet available for batch changing.

Directions

Log in to the [CDN console](#) and select **Domain Management** on the left sidebar. Tick two or more enabled domain names, and then click **More Actions** > **Batch Change Configuration** on the top of the domain name list to enter the configuration page.



Note:

Configurations of disabled, blocked, and locked domain names cannot be changed in batches.

For domain name configurations that are not completed on the console, configuration changes do not apply.

Notes

Configuration changes take effect immediately and cannot be reversed.

Choose domain names with the same configurations on acceleration region, service type, or HTTPS certificate

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.

Configuration Manual

Shared CNAME

Last updated : 2023-06-29 17:45:01

Shared CNAME

You can bind multiple domain names to the same custom CNAME for easy management.

Note:

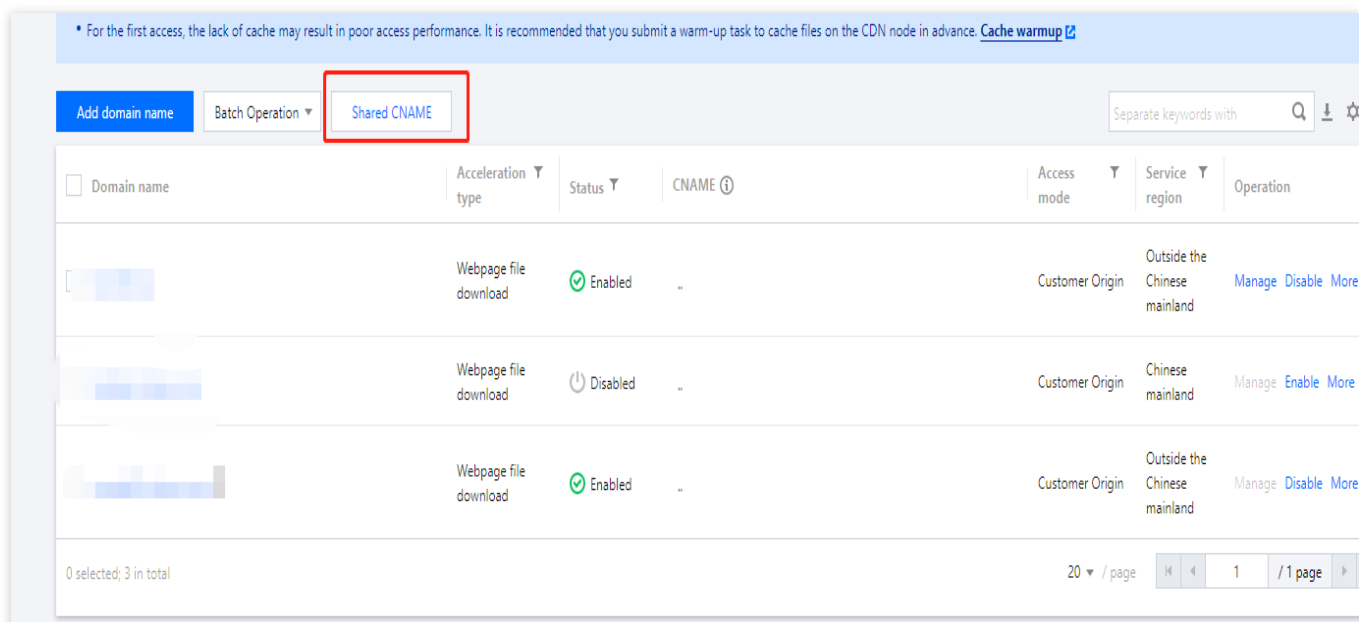
This feature is now only available to beta users.

You need to modify the CNAME resolution of your domain after the operation.

Configuration directions

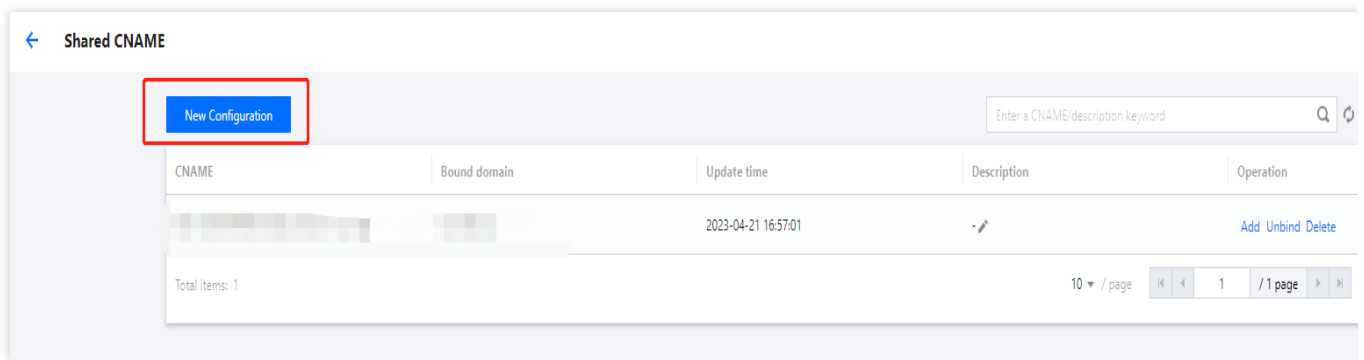
Checking shared CNAMEs

Log in to the [CDN console](#), click **Domain Name Management** from the left sidebar. In the page that appears, click **Shared CNAME**.



Adding a configuration

Click **Add configuration** and complete the configuration.



See below for details:

1. **Select domain name:** Select the target domain name.

Note:

It's recommended to add domain names with the same acceleration region and service type to the same CNAME.

If you have enabled both CDN and ECDN services, you cannot select domain names that use different services.

The domain name to add cannot be closed, blocked, locked or bound with another CNAME.

2. The backend automatically groups the selected domain names by their platforms, and assigns a custom CNAME record to each group. This way, domain names in the same group are bound to the same CNAME record.

Note:

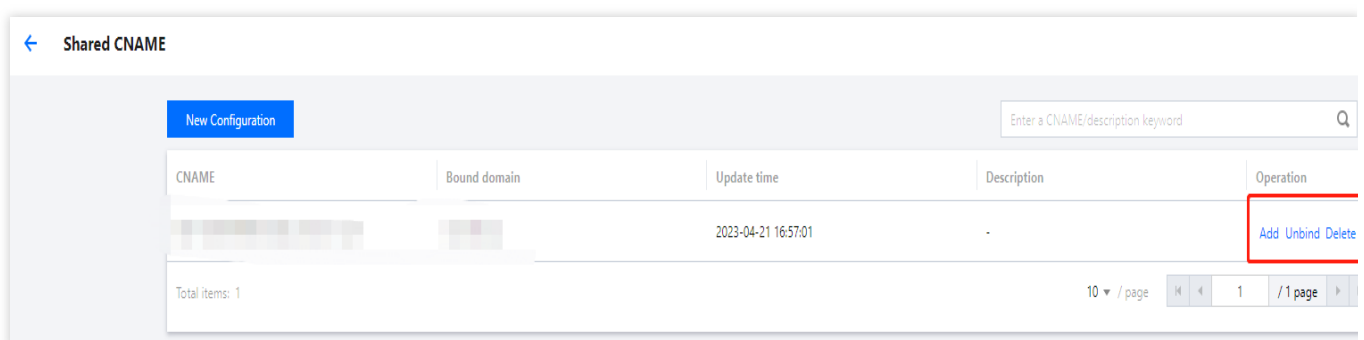
A string in the format of XXX-APPID.shared.cdn.dnsv1.com is appended to a custom CNAME record.

3. Check the assigned CNAME records. The initial CNAME record of a selected domain name will be overwritten by the corresponding shared CNAME record. Therefore, you must manually check the configuration.

Then, click **Confirm** to return to the **Shared CNAME** page and view the configuration.

Editing the configuration

After you configure a shared CNAME record, you can bind more domain names to the record, unbind domain names from the record, and delete the record.



Binding domain names

You can bind more domain names to a shared CNAME record.

Note:

A shared CNAME record is strongly related to the platform of a domain name. You can select only domain names whose platform matches the current shared CNAME record. Unmatched domain names are grayed out and cannot be selected.

Unbinding a domain name

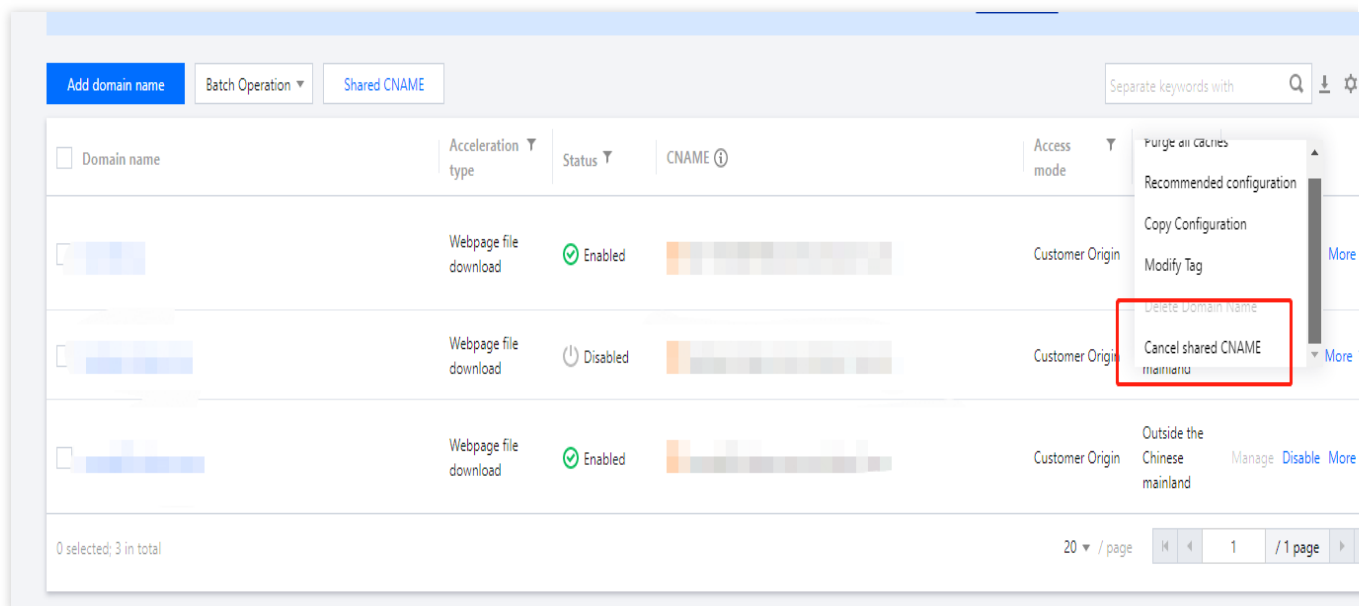
You can unbind a domain name from a shared CNAME record.

Note:

The CNAME configuration of the unbound domain name will be restored to its initial CNAME record. We recommend that you check the CNAME configuration of the domain name after the operation.

A shared CNAME record must be bound to at least one domain name. If all previously bound domain names are unbound from a shared CNAME record, the shared CNAME record is deleted.

You can also go to the **Domain Management** page, find the target domain name, and choose **More > Cancel shared CNAME** in the **Operation** column to unbind the domain name from its shared CNAME record.



Deleting a shared CNAME record

After you delete a shared CNAME record, all domain names previously bound to it are unbound, and the CNAME configurations of the domain names are restored to the respective initial CNAME records. We recommend that you check the CNAME configurations of the domain names after the operation.

Domain Name Configurations

Configuration Overview

Last updated : 2024-12-30 21:28:47

Configuration Overview

CDN supports various custom configurations and you can adjust them based on your business needs.

Basic configurations

Basic configurations are the contents required for CDN acceleration, including origin server configurations and the basic acceleration service information such as acceleration region and service type, etc.

Configuration	Description
Basic Information	Modifies basic information such as the project, acceleration region, and service type, etc.
Origin Server Configuration	Configures multi-IP round-robin origin-pull, domain name-based origin-pull, weighted round-robin origin-pull, origin domains, and origin-pull protocols. Supports configuring hot backup origin servers. For global acceleration domain names, the acceleration in and outside the Chinese mainland can be configured separately.

Access control

You can configure various rules based on user requests to allow or block access requests.

Configuration	Description
Hotlink Protection	Supports setting referer allowlists and blocklists to determine whether to allow or deny HTTP access requests based on the request referer headers. For global acceleration domain names, the acceleration in and outside the Chinese mainland can be configured separately.
IP Blocklist/Allowlist	Supports setting IP allowlists and blocklists to determine whether to allow or deny HTTP access requests based on the request client IPs. For global acceleration domain names, the acceleration in and outside the Chinese mainland can be configured separately.
IP Access Limit	Limits the frequency that an IP can access a single node to deny the access requests from client IPs exceeding the limit.

Authentication	Supports various timestamp signature algorithms and rules for anti-hotlinking configuration. For global acceleration domain names, the acceleration in and outside the Chinese mainland can be configured separately.
Video Dragging	It is designed for streaming VOD acceleration. With the video dragging feature enabled, you can specify the start point of a video through the parameter <code>start</code> .
UA Blocklist/Allowlist	Determines whether to deny or allow requests according to HTTP request header <code>User-Agent</code> .
Downstream Speed Limit	Controls the CDN access bandwidth by setting the downstream speed limit on a URL.

Cache configuration

Cache configuration controls cache on CDN nodes.

Configuration	Description
Ignore Query String	For resource cache, it supports configuring whether to ignore parameters after "?" in an access URL. We recommend disabling this feature if the parameters after "?" indicate differen contents of your business.
Node Cache Validity	Supports configuring the cache validity of files on nodes based on file path and type.
Status Code Cache	Supports configuring status code cache validity for CDN nodes to respond to 2XX status codes directly, thus reducing pressure on the origin server.
HTTP Header Cache	It can be disabled as needed. CDN nodes cache all origin server response headers by default.
Cache Ignore URL Case	CDN node cache does not ignore letter case by default. Letter case can be ignored as needed.
Access URL Rewrite	Supports customizing URL rewrite configuration to redirect requests from URLs with 302 status code to target URLs.

Origin-pull configuration

Origin-pull configuration controls the process of forwarding requests from CDN nodes to origin servers.

Configuration	Description
Range GETs	Range GETs is used for origin-pull by default. If it is not supported by your origin

	server, you can disable it.
Request Header	Adds specified headers during origin-pull such as the real client IP.
Follow 301/302	It can be enabled for origin-pull as needed.
Origin-pull Timeout	Configures the TCP connection timeout period (which defaults to 5 seconds) and loading period (which defaults to 10 seconds) of origin-pull.

HTTPS acceleration configuration

HTTPS acceleration supports various HTTPS-related configurations.

Configuration	Description
HTTPS Configuration	Supports uploading a self-owned certificate or a hosted certificate to enable HTTPS acceleration.
HTTP2.0 Configuration	With it is 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 access can be achieved with or without a certificate. Forced redirection from HTTP to HTTPS access requires a certificate.
OCSP Stapling	With it is enabled, OCSP stapling is support. Please first configure a certificate to enable OCSP stapling.
HSTS Configuration	If it is enabled, the header <code>strict-transport-security</code> will be added. Please first configure a certificate to enable HSTS configuration.

Advanced configuration

Configuration	Description
Bandwidth Cap Configuration	Supports configuring bandwidth cap for the acceleration in and outside the Chinese mainland. Acceleration service can be stopped as needed if the cap is exceeded. For global acceleration domain names, the acceleration in and outside the Chinese mainland can be configured separately.
SEO Configuration	Supports automatically recognizing that whether an access IP belongs to a search engine. If yes, requests from the IP will be forwarded to the origin server to guarantee the stability of the search engine's weight.
Response Header	Sets HTTP response headers as needed and adds them to the response

Configuration	requests to clients.
Smart Compression Configuration	Performs Gzip or Brotli compression on specified files based on the file type and range.

Basic Configurations

Basic Information

Last updated : 2024-12-30 21:29:05

Configuration Overview


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, service type, and supported protocols on the basic information module of the domain name. You can also modify information such as acceleration region, service type, and project as needed.








Configuration Guide

Viewing basic information

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, click **Manage** on the right of a domain name to enter its configuration page. The domain name basic information is in the **Basic Configuration** tab.

Basic Information

You can modify the domain name basic configuration as needed.[Description](#) 

Region 	Global Modify
Acceleration Domain Name	
CNAME	
Time Created	2021-03-19 18:13:48
Project 	 Modify
Service Type	Static Acceleration 
IPv6 Access 	<input type="checkbox"/> Enable it to allow access through IPv6

Modifying domain name acceleration region

Click **Modify** on the right of the acceleration region to change it.

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 in and outside the Chinese mainland are billed separately at different prices. For more information, please [click here](#).

Modifying project

Click **Modify** on the right of the domain name project to change it.

Note:

Please note that project modification will change the project-based statistics and sub-user permissions. Please modify with caution.

To create a project or manage existing projects, go to the [Project Management](#) page.

Modifying service type

Tencent Cloud CDN optimizes acceleration performance based on the service type. For the best acceleration result, we recommend selecting the service type similar to that of your actual businesses. If you want to adjust it, click

Modify on the right:

Note:

Modifying service type will change the underlying CDN acceleration platform, which may cause a small number of failed requests and increase origin-pull bandwidth. We recommend modifying service type during off-peak hours.

If you cannot find the **Modify** button next to your domain name, please [contact us](#) for assistance.

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.

For global acceleration domain names with IPv6 access enabled, if the acceleration region is switched to the regions outside the Chinese mainland, IPv6 access will be disabled automatically and cannot be enabled.

Origin Server Configuration

Last updated : 2024-12-30 21:29:15

Overview

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

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-board access is required during origin-pull. In this case, the origin-pull effect may not be ensured.

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.

Directions

Primary origin server configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. Open the **Basic Configuration** tab to see the **Origin Server Information** section.

Origin server

You can modify the existing origin server configuration or add hot backup origin servers (only customer origins are supported). If an origin-pull request fails, the hot backup origin server will be requested for resources.[How to set origin servers](#)
If access to the origin server is restricted, you can go to ["Verify Origin-pull Node"](#) to query the allowed origin-pull node IPs by domain name.

Primary origin

Origin type

Customer origin

Origin-pull Protocol

HTTP

Origin address

Origin-pull Rule	Origin-pull address	Port	Weight
All Files		-	-

Advanced origin-pull configuration ▶

Origin Domain

+ Add hot backup origin

Origin server type

Customer origin	You can use a stable business server that is running as the origin server. Enter the corresponding IP list or a domain name as the origin server address.
Tencent Cloud COS Origin	You can select a COS bucket as the origin server. Private bucket access can be enabled.
Third-Party Object Storage Origin	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, and Qiniu Cloud KODO.Note: Currently, ECDN does not support origin servers that are based on third-party object storage services.

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	CDN pulls HTTP or HTTPS content from the origin server over HTTPS.

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 is used for an origin-pull of HTTP content. HTTPS is used for an origin-pull of HTTPS content. HTTPS is also used when you transfer key sensitive content. We recommend that you select this option. Make sure that the origin server is accessible over HTTPS.

Note

If you select HTTPS origin-pull, make sure that the origin server is accessible over HTTPS. Otherwise, origin-pull may fail.

Origin server address

External origin	<p>You can enter multiple origin IPs or origin domain names with one entry per line. Origin-pull from multiple origin IPs in round robin mode: You can enter multiple origin IPs with one entry per line 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.</p> <p>When you enter an origin IP or domain name, you can add a port that ranges from 0 to 65535 and a weight that ranges from 1 to 100 in the format of Origin server address:Port:Weight or Origin server address::Weight. By default, the port is omitted. Note: 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.</p> <p>The origin server address can contain up to 511 characters.</p>
Tencent Cloud COS Origin	<p>Select a COS bucket as the origin server.</p> <p>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.</p> <p>If the access permission of the bucket is set to private read, authorize CDN to access the bucket, and enable origin-pull authentication to allow private bucket access.</p>
Third-Party Object Storage Origin	<p>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, and Qiniu Cloud KODO. Example: my-bucket.s3.ap-east-1.amazonaws.com or my-bucket.oss-cn-beijing.aliyuncs.com. The bucket address cannot contain the http:// or https:// protocol header.</p>

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.

Origin domain

It refers to the domain name that is accessed on the origin server by a CDN node during origin-pull. For more information about how to configure an origin domain, see [Origin domain configuration](#).

Note

The differences between an origin server address and an origin domain are as follows:

Origin server address specifies the IP address to which an origin-pull request is sent.

Origin domain specifies the website corresponding to the IP address to which an origin-pull request is sent.

External 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.
Tencent Cloud 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.
Third-Party Object Storage 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.

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.

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

Origin server

You can modify the existing origin server configuration or add hot backup origin servers (only customer origins are supported). If an origin-pull request fails, the hot backup origin server will be requested for resources. [How to set origin server](#)
If access to the origin server is restricted, you can go to "Verify Origin-pull Node" to query the allowed origin-pull node IPs by domain name.

Primary origin

Origin type

Customer origin

Origin-pull Protocol

HTTP

Origin address

Origin-pull Rule	Origin-pull address	Port	Weight
All Files		-	-

Advanced origin-pull configuration ▶

Origin Domain

+ Add hot backup origin

Note

Primary origin and hot backup origin only allow the same origin-pull protocol. If you need to modify the origin-pull protocol, please do it at the primary origin protocol location. After the modification is successful, the origin-pull protocol of the hot standby origin will be synced and updated.

The origin type of the hot backup origin does not support COS origin and third-party Object storage. If you need a COS origin or third-party Object storage as a hot standby origin, you can fill in the public network access address in the owned origin.

If the primary origin has enabled IPv6, adding a hot standby origin is not supported.

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** to configure different origin servers for different service regions of the acceleration domain name.

Origin server

You can modify the existing origin server configuration or add hot backup origin servers (only customer origins are supported). If an origin-pull request fails, the hot backup origin server will be requested for resources. [How to set origin servers](#)
If access to the origin server is restricted, you can go to "Verify Origin-pull Node" to query the allowed origin-pull node IPs by domain name.

Primary origin

Origin type Customer origin

Origin-pull Protocol HTTP

Origin address

Origin-pull Rule	Origin-pull address	Port	Weight
All Files		80	-

Advanced origin-pull configuration ▶

Origin Domain

[+ Add hot backup origin](#)[+ Region-specific configuration](#) Set up configurations for a specific region

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 Samples

Origin domain configuration

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

Origin server info

You can edit existing origin server or add hot backup origins (only external origin supported). When the back-to-origin request failed, the hot backup origin server will be requested. [How do I set my origin server?](#)

Default Configuration**Primary origin configuration**[Edit](#)

Origin Type	Existing Origin
Origin address	www.abc.com
Origin-pull Protocol	HTTP
Host header	www.def.com

Hot backup origin configuration

If a request fails during origin-pull, it will be forwarded to the hot backup slave origin server for resources.

[Add a backup](#)

The access route for the user will be:

When a user accesses the resource `http://www.test.com/test.txt` that has not been cached on the CDN node, the node will resolve the domain name `www.abc.com` to get the origin server address `1.1.1.1`. Then, the CDN node will access the server `1.1.1.1`, find the `test.txt` file in the website path `www.def.com`, and return the file to the user.

Region-specific configuration

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

Origin server info

You can edit existing origin server or add hot backup origins (only external origin supported). When the back-to-origin request failed, the hot backup origin server will be requested. [How do I set my origin server?](#)

Default Configuration

Primary origin configuration

[Edit](#) [Switch Master/Slave Origin Server](#)

Origin Type	Existing Origin
Origin address	1.1.1.1
Origin-pull Protocol	HTTP
Host header	1.test.com

Hot backup origin configuration

[Edit](#) [Delete](#)

Origin Type	Existing Origin
Origin address	2.2.2.2
Origin-pull Protocol	HTTP
Host header	1.test.com

Overseas Region Configuration

Primary origin configuration

[Edit](#) [Switch Master/Slave Origin Server](#)

Origin Type	Existing Origin
Origin address	3.3.3.3
Origin-pull Protocol	HTTP
Host header	1.test.com

Hot backup origin configuration

[Edit](#) [Delete](#)

Origin Type	Existing Origin
Origin address	4.4.4.4
Origin-pull Protocol	HTTP
Host header	1.test.com

The actual origin-pull will then be:

1. When a user in the Chinese mainland accesses the file `http://www.test.com/test.txt` and the node in the Chinese mainland has not cached this resource, it will forward the request to the server `1.1.1.1` and try to find the `test.txt` file in the website path `1.test.com`. If the resource exists, the node will directly return the file to the user. If not, it will go to step 2.
2. As the CDN node in Mainland China fails to forward the request to the primary origin server and cannot find the resource, it will forward the request to the server `2.2.2.2`, find the `test.txt` file in the website path `2.test.com`, cache and return it to the user.
3. At this time, a user outside the Chinese mainland accesses the file `http://www.test.com/test.txt`. As the node outside the Chinese mainland has not cached this resource, it will forward the request to the server `3.3.3.3` and try to find the `test.txt` file in the website path `3.test.com`. If the resource exists, the node will directly return the file to the user. If not, it will go to step 4.
4. As the CDN node outside the Chinese mainland fails to forward the request to the primary origin server outside the Chinese mainland and cannot find the resource, it will forward the request to the server `4.4.4.4`, find the

`test.txt` file in the website path `4.test.com` , and then cache and return it to the user outside the Chinese mainland.

Advanced Origin-pull Configuration

Last updated : 2024-12-30 21:29:33

Advanced origin-Pull configurations

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.

Restrictions

By default, the origin-pull protocol and origin domain of the primary origin server are adopted for the advanced origin-pull configuration and cannot be modified.

Configuration Guide

Configuration in domain management

1. Log in to the [CDN console](#).
2. Click **Domain Management** on the left sidebar to enter the domain name management list.
3. Select the target domain name and click **Manage** to enter the domain name configuration page.
4. On the **Basic information** tab, find the **Origin server** section and click **Edit** in the top-right corner of the **Primary origin** section.

Origin server

You can modify the existing origin server configuration or add hot backup origin servers (only customer origins are supported). If an origin-pull request fails, the hot backup origin server will be requested for resources.[How to set origin servers](#)
If access to the origin server is restricted, you can go to "[Verify Origin-pull Node](#)" to query the allowed origin-pull node IPs by domain name.

Primary origin

Origin type Customer origin

Origin-pull Protocol HTTPS

Origin address

Origin-pull Rule	Origin-pull address	Port	Weight
All Files		-	-

Advanced origin-pull configuration ▶

Origin Domain

+ Add hot backup origin

5. Click **Advanced origin-pull configuration**.

Origin server

You can modify the existing origin server configuration or add hot backup origin servers (only customer origins are supported). If an origin-pull request fails, the hot backup origin server will be requested for resources. [How to set origin server](#)
If access to the origin server is restricted, you can go to ["Verify Origin-pull Node"](#) to query the allowed origin-pull node IPs by domain name.

Primary origin

Origin type ☒ Customer Origin ☐ Tencent Cloud COS Origin ☐ Third-Party Object Storage Origin ⓘ

Origin-pull Protocol ☒ HTTP ☐ HTTPS ☐ Follow Protocol
If your origin server supports HTTPS, you can use the protocol to prevent origin-pull data theft and tampering.

Origin address

Origin-pull ...	Origin-pull Address (Origin:Port:Weight)	Oper
All Files	<input type="text" value=""/>	: 1-65535 : 1-100
Add origin		

Advanced origin-pull configuration ▲

It supports more refined origin-pull settings. [What's advanced origin-pull configuration](#)

Origin-pull Rule	Origin-pull Address (Origin:Port)	Oper
File extension ▼ <input type="text" value="jpg;png;css"/>	<input type="text" value="Please enter the origin server (IP/domain name) address"/> : 1-65535	Delete
Add origin		

Origin Domain

An origin domain refers to the website domain name accessed at the origin server by a CDN node during origin-pull. [What's the origin domain](#)
Please ensure your origin domain can be accessed. Otherwise, origin-pull may fail, which will affect your business.
Note: if you enter the address of the Tencent Cloud COS origin or third-party object storage origin for origin address, the origin domain needs to be the same as the origin address

[Save](#) [Cancel](#)

6. Set the configuration items in the **Advanced origin-pull configuration** section as described in the following table.

Item	Description
Origin-pull Rule	<p>Client requests can be forwarded by the following rules:</p> <p>Client IP: This rule directs origin-pull requests of clients inside or outside the specified region to the specified origin address.</p> <p>File extension: This rule directs origin-pull requests for the specified file extensions to the specified origin address. If you specify multiple file extensions, separate them with semicolons (;).</p> <p>File directory: This rule directs origin-pull requests for files in the specified directory to the specified origin address. If you specify multiple directories, separate them with semicolons (;).</p>

	<p>Full path: This rule directs origin-pull requests for a specific file with its full path, such as <code>/a/1.jpg</code>, to the specified origin address. If you specify multiple files with their full paths, separate the files with semicolons (;).</p> <p>Homepage: This rule directs origin-pull requests for files on the homepage to the specified origin address.</p>
Origin-pull Address	You can specify domain names or IP addresses. One origin-pull address is required for an origin-pull rule. In addition, the value of the origin domain specified for the primary domain name in the Origin server section is used.
Port	You can specify a custom origin-pull port number. If you do not specify custom port numbers, port 80 is used for origin-pull over HTTP and port 443 is used for origin-pull over HTTPS. The origin-pull protocol depends on settings of the origin server. If you select HTTPS for Origin-pull Protocol in the Origin server section, the requests hit by an advanced origin-pull rule are forwarded over HTTPS.

Configuration limitations

Each domain name can be configured with up to 50 rules.

The origin-pull address of a single rule can be an IP, domain name, and port (range: 0 - 65535; port can be omitted). If "HTTPS" or "Follow Protocol" is selected as the origin-pull protocol, the port should be 443 or left empty.

More actions: you can adjust rule priority and edit or delete multiple rules in batches.

Rule priorities

First, the priority of a client IP rule is lower than that of a path-based rule. Second, if multiple path-based rules are specified, rules at lower positions in the rule list have higher priorities.

For example, you have specified that origin-pull requests of clients from the Jiangsu region are forwarded to

`1.1.1.1` and origin-pull requests for files whose path contains `/test` are forwarded to `2.2.2.2`. When a client from the Jiangsu region accesses `/test`, the origin-pull request is forwarded to `2.2.2.2`.

Sample configuration

Example:

This example describes three origin-pull scenarios, assuming that you have configured `www.example.com` as the CDN acceleration domain name, with the advanced origin-pull rules configured as shown in the following figure:

Origin-pull Rule	Origin-pull address	Port
File extensionjpg	1.1.1.1	-
File directory/vod	1.1.1.3	-
Full File Path/image/1.jpg	1.1.1.4	-
Homepage/	1.1.1.5	-
Client IP LocationGuangdong	1.1.1.2	-

Scenario 1: A client from the Shanghai region accesses `http://www.example.com/vod/`. In this case, the origin-pull request hits the **File directory** rule and is forwarded to `1.1.1.3`.

Scenario 2: A client from the Guangdong region accesses `http://www.example.com/`. In this case, the origin-pull request hits both the **Homepage** rule and the **Client IP** rule. As the **Homepage** rule has a higher priority, the origin-pull request is forwarded to `1.1.1.5`.

Scenario 3: A client from the Guangdong region accesses `http://www.example.com/image/1.jpg`. In this case, the origin-pull request hits the **File extension**, **Full path**, and **Client IP** rules at the same time. As a path-based rule has a higher priority over an IP-based rule, and the **Full path** rule is listed lower than the **File extension** rule, the origin-pull request is forwarded to `1.1.1.4`.

HTTPS Origin-pull algorithm description

Last updated : 2024-12-30 21:29:48

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

Hotlink Protection Configuration

Last updated : 2024-12-30 21:34:43

Configuration Overview

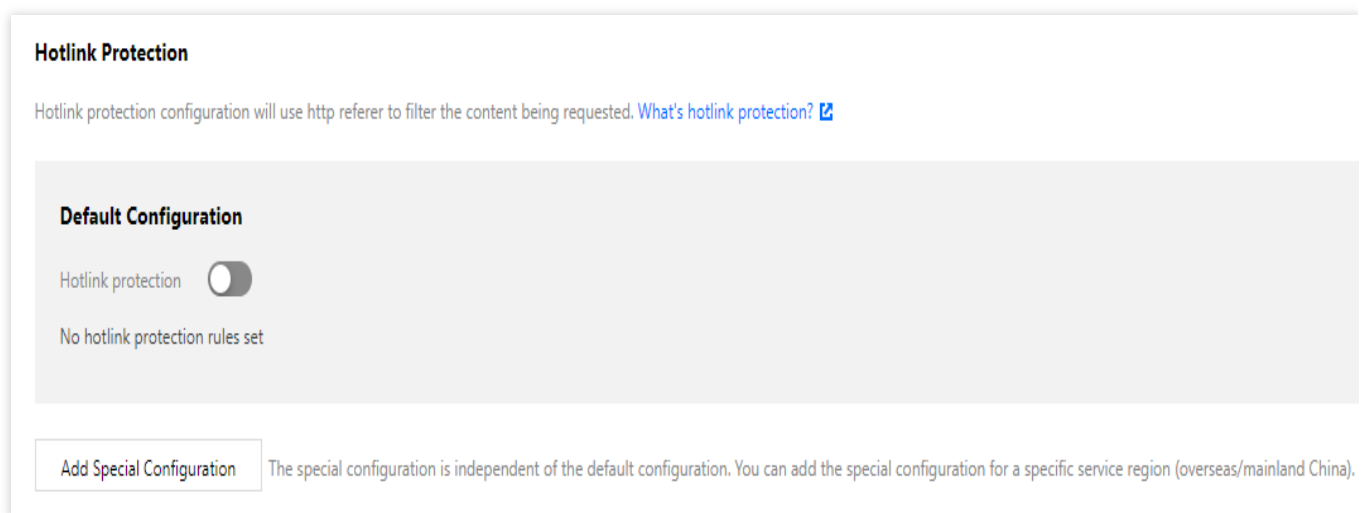
To control the source of access to your business resources, you can use the referer hotlink protection feature in Tencent Cloud CDN.

By configuring an access control policy on the value of the referer field in the HTTP request header, you can control the access source to prevent hotlinking by malicious users.

Configuration Guide

Viewing the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. Open the **Access Control** tab to see the **Hotlink Protection Configuration** section. It is disabled by default.



Enabling the configuration

Toggle on the switch, select a hotlink protection type, tick **Allow blank referer** as needed, enter an IP or domain name in the input box, and click **OK**.

Modified Hotlink protection configuration ×

Exclude http://, line-feed break; one entry per line; no duplication.
If "Allow blank referer" is not checked and no contents are entered,
referer hotlink protection feature is not enabled.

Hotlink protection type ☐ referer blacklist ☒ referer whitelist

☐ Allow blank referer ⓘ

Please enter domain (www.test.com) or IP (203.123.123.123). ;
supports front-end wildcards, example: *.test.com

Allowed to enter: 400.

OK

Cancel

Referer blacklist:

If the referer field of a request matches the string configured in the blacklist, 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 blacklist, CDN node will return the requested information.

If **Allow blank referer** is ticked, 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).

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 **Allow blank referer** 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).

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, e.g., if `*.qq.com` is configured, then both `www.qq.com` and `a.qq.com` will be matched.

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.

Hotlink Protection

Hotlink protection configuration will use http referer to filter the content being requested. [What's hotlink protection?](#)

Default Configuration

Hotlink protection

☐

refererWhitelist (Allow blank referer)

1.1.1.1

Add Special Configuration

The special configuration is independent of the default configuration. You can add the special configuration for a specific service region (overseas/mainland China).

Region-specific configuration

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

Hotlink Protection

Hotlink protection configuration will use http referer to filter the content being requested. [What's hotlink protection?](#)

Default Configuration

Hotlink protection ☐

No hotlink protection rules set

Add Special Configuration

The special configuration is independent of the default configuration. You can add the special configuration for a specific service region (overseas/mainland China).

Note:

Currently, region-specific configuration items cannot be deleted once added but can be disabled.

Configuration Sample

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

Hotlink Protection

Hotlink protection configuration will use http referer to filter the content being requested. [What's hotlink protection?](#)

Default Configuration

Hotlink protection ☒ [Edit](#)

refererWhitelist (Allow blank referer)

1.1.1.1

Overseas Region Configuration

Hotlink protection ☒ [Edit](#)

refererBlacklist (Allow blank referer)

1.1.1.1

Then the actual access will be 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, then a 403 status code will be returned.

IP Blocklist/Allowlist Configuration

Last updated : 2025-02-19 17:57:22

Overview

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, preventing hotlinking by malicious IPs, attacks, etc.

Directions

Viewing the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. Open the **Access Control** tab to find the **IP Blocklist/Allowlist Configuration** section. The **On/Off** switch is toggled off by default.

Enabling the configuration

To enable the IP blocklist/allowlist configuration, toggle on the **On/Off** switch. If you enable the IP blocklist/allowlist configuration for the first time and no rule is available, the Add Rule page pops up. The IP blocklist/allowlist configuration takes effect based on the priorities of the rules that you add. The rule at the bottom of the rule list has 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

In the **IP Blocklist/Allowlist Configuration** section, click **Add Rule** to add an IP blocklist/allowlist rule.

IP blocklist

If a client IP matches an IP or IP range in the blocklist, the accessed CDN node will directly return a 403 status code.

IP allowlist

If a client IP does not match any IP or IP range in the allowlist, the accessed CDN node will directly return a 403 status code.

Configuration limitations

When you add a rule, select **Allowlist** or **Blocklist** as **Rule type**. The IP blocklist and allowlist are mutually exclusive and cannot be configured at the same time.

All rules can support a total of 500 IP whitelist IP/IP segments and 200 blacklist IP/IP segments.

Do not add entries in the IP:Port format to the IP blocklist or allowlist.

Do not add reserved IPv4/IPv6 addresses or address ranges to the IP blocklist or allowlist.

The rule at the bottom of the rule list has the highest priority.

To modify a rule, click **Modify** on the right of the rule in the **Operation** column.

Adjusting the priority of a rule

To adjust the priority of a rule, click **Adjust priority** above the rule list. Then, click the upward or downward arrow on the right of the rule in the **Operation** column to adjust its priority, as shown in the following figure. If you click the upward arrow, the rule moves up one row. If you click the downward arrow, the rule moves down one row. After you adjust the priority of the rule, click **Save**.

Note:

The lower a rule is in the rule list, the higher its priority.

Deleting rules





To delete a rule, click **Delete** on the right of the rule in the **Operation** column. In the pop-up window, click **OK** to confirm the deletion. The rule is permanently deleted.

Disabling the configuration

To disable the IP blocklist/allowlist configuration, toggle off the **On/Off** switch. After the IP blocklist/allowlist configuration is disabled, you can still modify IP blocklist/allowlist rules. However, the modified rules are not immediately published to the production environment. The rules take effect only when you enable the IP blocklist/allowlist configuration.

Configuration Samples

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

	1.1.1.1		*
	1.1.1.1		/test

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 blocklist rule at the bottom of the rule list is matched. In this case, the access request is denied, and a 403 status code is returned.
2. If a user whose IP is 1.1.1.2 requests to access `https://www.test.com/test/vod.mp4` , the blocklist rule is not matched because the IP is not specified in the blocklist rule. The allowlist rule that is configured for the access resource allows access requests only from IP 1.1.1.1. In this case, the access request is denied due to an IP mismatch, and a 403 status code is returned.
3. If a user whose IP is 1.1.1.1 requests to access `https://www.test.com/vod.mp4` , the allowlist rule instead of the blocklist rule is matched. In this case, the access request is allowed, and the user can access the resource as expected.

IP Access Limit Configuration

Last updated : 2024-12-30 21:34:57

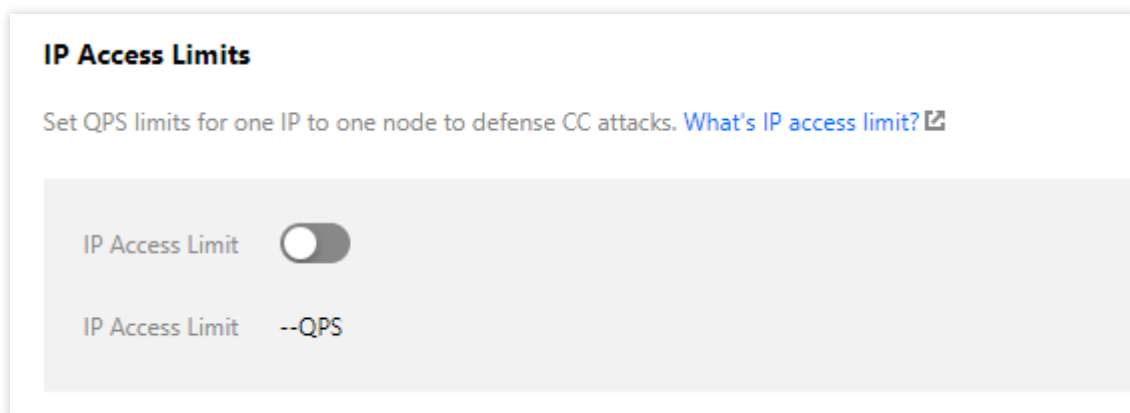
Configuration Overview

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 client IP, you can defend against high-frequency CC attacks and prevent hotlinking by malicious users.

Configuration Guide

Viewing the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. Open the **Access Control** tab to see the **IP Access Limit Configuration** section. It is disabled with no value set by default:



Enabling the configuration

Toggle on the switch, set the threshold, and click **OK**.

IP access limit ×

Setting an access limit for single IP can help resist part of CC attacks, however it may also block some normal accesses.

Threshold times/s

OK Cancel

Configuration description

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 a proper frequency limit according to your actual business conditions and use scenarios.

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.

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. When the switch is on, this configuration will take effect across the entire network:

IP Access Limits

Set QPS limits for one IP to one node to defense CC attacks. [What's IP access limit?](#)

IP Access Limit ☐

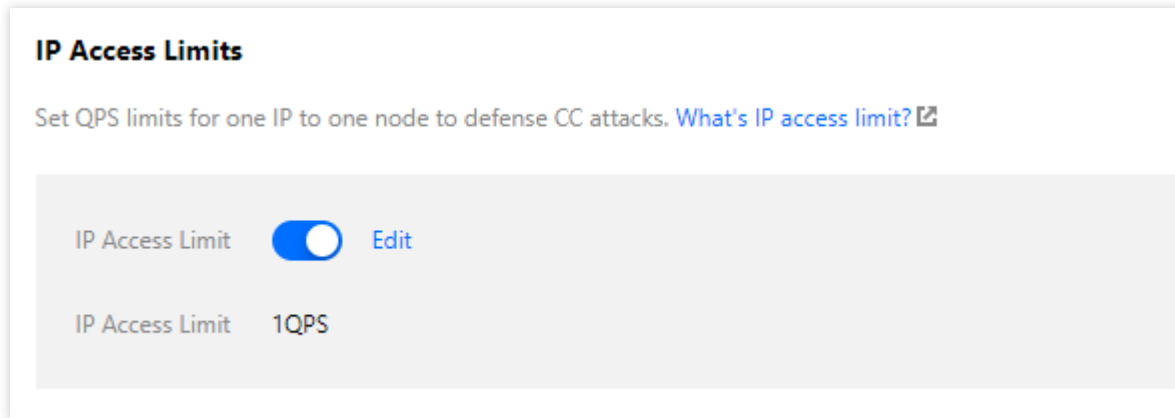
IP Access Limit 100QPS

Note:

If your acceleration domain name is configured for global acceleration, the IP access limit configuration will take effect globally. This configuration does not distinguish between requests from regions in and outside the Chinese mainland.

Configuration Sample

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



Then the actual access will be as follows:

1. A user with the client IP `1.1.1.1` requests the resource `http://www.test.com/1.jpg` for 10 times in one second, and all access requests are made to one server on CDN cache node A. 10 access logs will be generated on this server, 9 of which exceed the QPS limit. The status code "514" will be returned.
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 : 2024-12-30 21:35:04

Overview

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.

The Ignore Query String configuration should be enabled for video dragging. That is, the Ignore Query String of all rules in [Cache Key Rule Configuration(<https://www.tencentcloud.com/document/product/228/35316>)] should be configured as "Ignore All", and the origin server should support Range requests. Supported file formats are MP4, FLV, and TS.

File Type	Meta Information	Parameter Description (start)	Request Sample
MP4	For a video on the origin server, the meta information must be located in the file header. Videos with meta information located at the file end are not supported.	The parameter <code>start</code> specifies a time point (in seconds) and uses a decimal to specify a millisecond. For example, "start = 1.01" means that the start time is at 1.01s. CDN will locate the last keyframe before the time specified by <code>start</code> if <code>start</code> is not a keyframe.	<pre>http://www.test.com/demo.mp4?start=10</pre> indicates that the video will be played back starting from the 10th second.
FLV	The video on the origin server must have meta information.	The parameter <code>start</code> specifies a byte. CDN will automatically locate the last keyframe before the byte specified by <code>start</code> if <code>start</code> is not a keyframe.	<pre>http://www.test.com/demo.flv?start=10</pre> indicates that the video will be played back starting from the 10th byte.
TS	-	The <code>start</code> parameter defines a start byte. CDN	<pre>http://www.test.com/demo.ts?start=10</pre> indicates that the video is

		will automatically locate the beginning byte.	
--	--	---	--

Viewing the Configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and click a streaming VOD acceleration domain name to enter the configuration page. Open the **Access Control** tab to find the **Video Dragging** section.

Video dragging is disabled by default.

Video Dragging

By enabling this, you can specify the start point via "start". mp4, flv and ts files are supported. Query string should be ignored as well. [What's Video Dragging?](#)

Video Dragging: ☐

Authentication Configuration Instruction

Last updated : 2024-12-30 21:35:15

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.

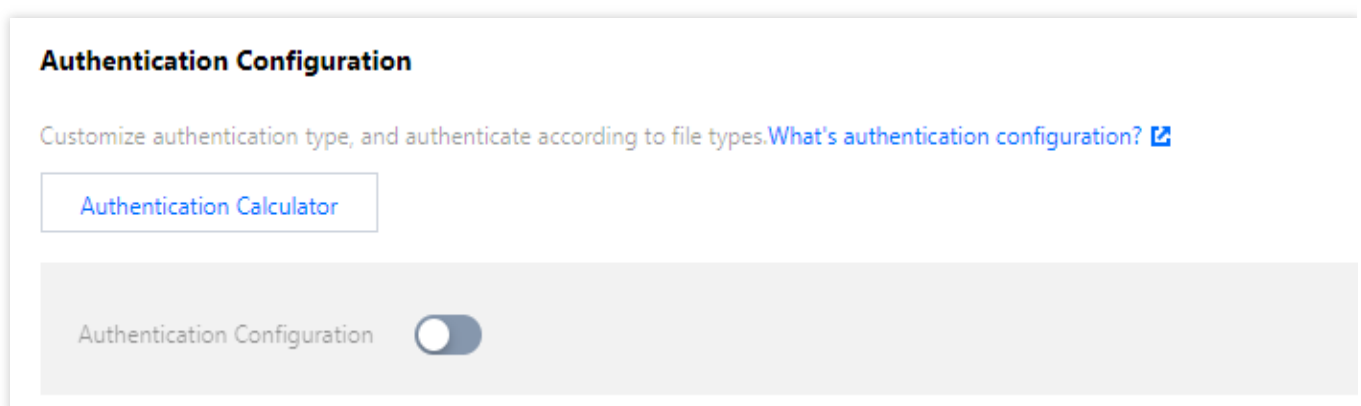
Note:

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** on the left sidebar, and click **Manage** on the right of the domain name to access its configuration page. Under the **Security Configuration** tab, find the authentication configuration, which is disabled by default:



Modifying configuration

1. Modify the configuration

CDN provides four authentication signature calculation models of your choice. You can use the **Authentication Calculator** provided to view these models. For more information on the configuration effect and algorithms, please see the specific algorithm documents for [TypeA](#), [TypeB](#), [TypeC](#), and [TypeD](#):

Configuration [X]

1 Type > 2 Configure > 3 Files

Type ☒ TypeA ☐ TypeB ☐ TypeC ☐ TypeD

Example http://[redacted]59-rsje9oyrj
ovvkmr8-0-d8f681081ff7fe5006a6ae2d1f793473

Next

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.

Authentication Configuration

Customize authentication type, and authenticate according to file types. [What's authentication configuration?](#)

[Authentication Calculator](#)

Authentication Configuration	<input checked="" type="checkbox"/>
Authentication Key	34yrkoayk7x
Signature Parameter Name	sign
Valid Time	1
Time Format	Decimal (Unix timestamp)
Authentication Scope	Authenticate the specified file types
Authentication Files	All

3. Add a region-specific configuration

If your acceleration domain name is configured for global acceleration and you want acceleration in and outside mainland China to have different authentication configurations, you can click **Add Special Configuration** under the configuration.

[Add Special Configuration](#)

The special configuration is independent of the default configuration. You can add the special configuration for a specific service region (overseas/Chinese mainland).

Note:

Currently, an added region-specific configuration item cannot be deleted but can only be disabled.

Configuration Sample

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

Authentication Configuration

Customize authentication type, and authenticate according to file types. [What's authentication configuration?](#)

Authentication Calculator

Default Configuration

Authentication Configuration ☐

Authentication Key 3nzn5ihrsewzz9yh

Signature Parameter Name sign

Valid Time 1

Time Format Decimal (Unix timestamp)

Authentication Scope Authenticate the specified file types

Authentication Files All

Overseas Region Configuration

Authentication Configuration ☒ [Edit](#)

Authentication Mode TypeC

Authentication Key tteeeee

Valid Time 111

Time Format Hexadecimal (Unix timestamp)

Authentication Scope Authenticate the specified file types

Authentication Files All

The actual effect will be as follows:

1. A user in mainland China can access the resource `http://cloud.tencent.com/1.jpg` by directly initiating a request.
2. A user outside Mainland China can access the resource `http://cloud.tencent.com/1.jpg` by initiating a request with a URL in the format of `http://cloud.tencent.com/509301d10da7b862052927ed7a947f43/5e561139/1.jpg`.

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 : 2024-12-30 21:35:22

You can add authentication to prevent hotlinking of your website. Tencent Cloud supports Type A, B, C and D authentication. This document describes details of 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.

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 in use), which defaults to 0.
md5hash	<p>A string containing 32 characters calculated based on the MD5 algorithm. It is calculated as follows:</p> <ul style="list-style-type: none"><code>md5hash = md5sum(uri-timestamp-rand-uid-pkey)</code> .<code>uri</code> : It is the resource access path and must start with a slash (/).<code>timestamp</code> : Its value is the above <code>timestamp</code> .<code>rand</code> : Its value is the above <code>rand</code> .<code>uid</code> : Its value is the above <code>uid</code> .<code>pkey</code> : It can contain 6 to 40 letters and digits. It should be kept private and disclosed to only the client and server.

Authentication logic description

After the CDN server receives a user request, it parses the `timestamp` parameter in the URL and the validity period of the authentication URL and compares it with the current time.

1.1 If the sum of `timestamp` and the validity period of the authentication URL is before the current time, the server judges that the URL has expired and is invalid and returns the HTTP error code 403.

1.2 If the sum of `timestamp` and the validity period of the authentication URL is after the current time, the server uses the MD5 algorithm to calculate the value of `md5hash` and it with the `md5hash` value passed in by the URL. If they are the same, the request will pass the authentication; otherwise, the HTTP error code 403 will be returned.

Configuration Directions

Here we take Type-A authentication as an example.

Field configuration

Authentication key: `dimtm5evg50ijsx2hvuwyfoiu65`

Signature parameter: `sign`

Validity period of the authentication URL: 1s

Authentication Configuration

✓ Select a mode

2 Configure Parameter

3 Configure Files

Primary key

Enter 6-40 characters containing letters and digits [Auto-create](#)

Secondary key

Enter 6-40 characters containing letters and digits [Auto-create](#)

Signature parameter

Valid Time

-

1

+

s

Time format

Decimal (Unix timestamp)

Back

Next

The time when the signature calculation server generates the authentication URL: 2020-02-27 16:10:32 (UTC+8). Its decimal integer value after conversion is 1582791032 (timestamp).

Requested origin address: http://www.mixcre.com/test/1.jpg

Generation process

Get authentication parameters:

Parameter	Value
URI	Resource access path, which 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 the authentication URL: http://www.mixcre.com/test/1.jpg?sign=1682234383-

YES3WZ57u91G3zA1YYzh5Y3aIy6U2i0K-0-57b80424b3e6f9da4027fe13c00c44a7

When the client uses the encryption URL for access, if the md5hash value calculated by the CDN server is the same as the md5hash value carried by the access request, which are both

3fbb88382c9356b6faaf9d68c7b2ae3a in this example, the request will pass the authentication; otherwise, the authentication will fail.

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:

As the authentication parameter will be automatically ignored, the cache keys of the files to be authenticated will be affected, and the priority here is higher than the cache key rules in **Cache Configuration > Cache Key Rule Configuration**.

For example, the Type A configuration here is as: "Authentication Parameter: sign "; "Authentication Scope:

`jpg` "; then the `sign` parameter will be automatically ignored for JPG files even though the configuration is as "All Files: Not Ignore" in **Cache Configuration -> Cache Key Rule Configuration**.

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
```

If the CDN node is not hit after successful authentication, it will initiate an origin-pull request, **which is in the same format as the access request with the `sign` parameter retained**. The origin server can ignore it or perform authentication again as needed.

TypeB

Last updated : 2024-12-30 21:35:28

Algorithm Description

Access URL format `http://DomainName/timestamp/md5hash/FileName`

Algorithm description

timestamp: A timestamp in the format of `YYYYMMDDHHMM` .

md5hash: MD5 (custom key + timestamp + file path).

Sample

request `http://cloud.tencent.com/202003032017/b91bad39a0f9c885ddebd6b6164de3c4/test.jpg`

Note:

When the MD5 value is calculated, if the request path is `http://cloud.tencent.com/test.jpg` , then the path used for MD5 calculation will be `/test.jpg` .

Configuration Guide

Parameter description

TypeB requires the following configurations:

Authentication Configuration

✓ Select a mode >

2 Configure Parameter >

3 Configure Files

Authentication Key

cqp7k0v7bl5p3l

Enter a key consisting of 6 to 40 digits, uppercase and lowercase letters. [Randomly generate](#)

Valid Time

–

2

+

Time Format

Decimal (YYYYMMDDHHMM)

Previous

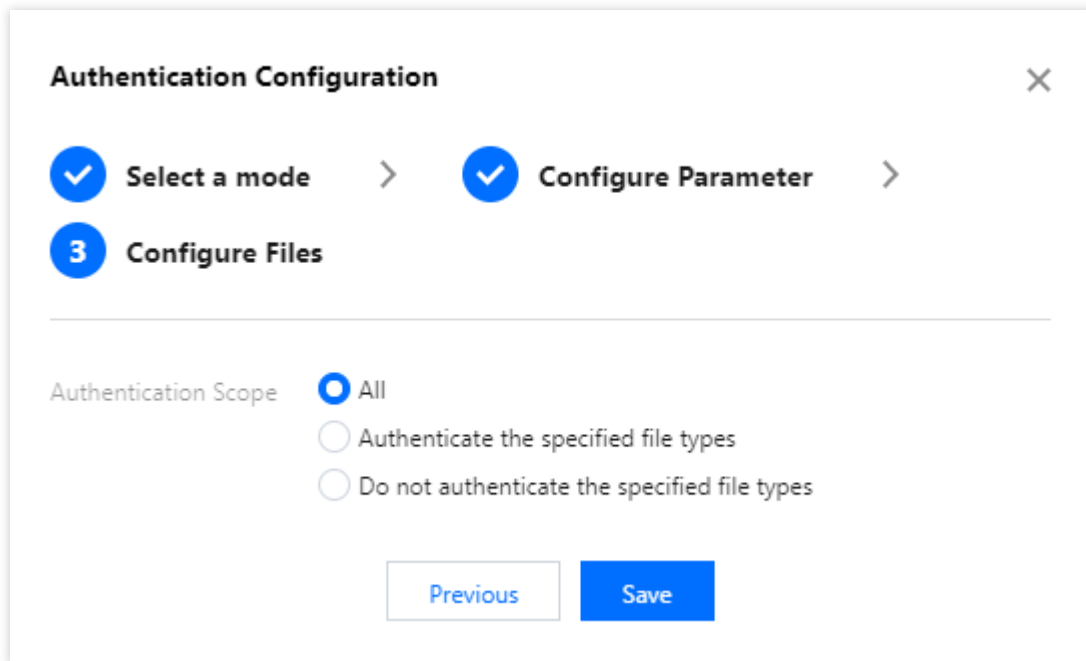
Next

Custom Authentication Key: it can contain 6 to 40 digits, uppercase and lowercase letters. It should be kept private and disclosed to only the client and server.

Custom Validity Period: the `timestamp` value in the request path plus the configured validity period is compared with the current time to determine whether the request has expired; if so, a 403 error will be directly returned.

Object

After configuring the key, parameter name, and validity period, you can specify the authentication object as needed. The following three authentication modes are supported:



Authentication Configuration

✓ Select a mode > ✓ Configure Parameter >

3 Configure Files

Authentication Scope

☒ All

☐ Authenticate the specified file types

☐ Do not authenticate the specified file types

Previous Save

All files under a specified domain name need to be authenticated.

All files except those of a specified type need to be authenticated.

Only files of a specified type need to be authenticated.

Notes:

Cache hit rate

If you have enabled TypeB authentication for a domain name, the signature and timestamp will be carried in the access URL path. When a CDN node caches a resource, it will automatically ignore the fields in the path and thus 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
```

If no hits are found on the CDN node after successful authentication, the node will initiate an origin-pull request, **in which the `md5hash` and `timestamp` will be removed from the path**. The origin server does not require any configuration.

TypeC

Last updated : 2024-12-30 21:35:35

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 TypeC authentication.

Algorithm Description

Access URL format `http://DomainName/md5hash/timestamp/FileName`

Note:

The access URL cannot contain any Chinese characters.

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	<p>A string containing 32 characters calculated based on the MD5 algorithm. It is calculated as follows:</p> <ul style="list-style-type: none">• There are no symbols between parameters in <code>md5hash = md5sum(pkeytimestampuri)</code>.• pkey: It can contain 6–40 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 (/).• timestamp: Its value is the above <code>timestamp</code>.

Authentication logic description

After the CDN server receives a user request, it parses the `timestamp` parameter in the URL and the validity period of the authentication URL and compares it with the current time.

1.1 If the sum of `timestamp` and the validity period of the authentication URL is before the current time, the server judges that the URL has expired and is invalid and returns the HTTP error code 403.

1.2 If the sum of `timestamp` and the validity period of the authentication URL is after the current time, the server uses the MD5 algorithm to calculate the value of `md5hash` and it with the `md5hash` value passed in by the URL. If they are the same, the request will pass the authentication; otherwise, the HTTP error code 403 will be returned.

Directions

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

The time when the signature calculation server generates the authentication URL: 2020-02-27 16:10:32 (UTC+8). Its decimal integer value after conversion is `1582791032` (timestamp).

Requested origin address: `http://cloud.tencent.com/test.jpg`

Generation process

Get authentication parameters:

Parameter	Value
URI	Resource access path, which is <code>/test.jpg</code> .
timestamp	<code>1582791032</code>
pkey	<code>dimtm5evg50ijsx2hvuwyfoiu65</code>

Concatenate the signature string: `dimtm5evg50ijsx2hvuwyfoiu651582791032/test.jpg`

Calculate the MD5 value of the signature string: `md5hash = md5sum(pkeytimestampuri)`

`=md5sum(dimtm5evg50ijsx2hvuwyfoiu651582791032/test.jpg) = ea68b93ac23ebbc6eebf7f163c6e9c4c`

Generate the authentication

URL: `http://cloud.tencent.com/ea68b93ac23ebbc6eebf7f163c6e9c4c/1582791032/test.jpg`

When the client uses the encryption URL for access, if the `md5hash` value calculated by the CDN server is the same as the `md5hash` value carried by the access request, which are both

`ea68b93ac23ebbc6eebf7f163c6e9c4c` in this example, the request will pass the authentication; otherwise, the authentication will fail.

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
```

If the CDN node is not hit after successful authentication, it will initiate an origin-pull request, **in which the**

md5hash and timestamp will be removed from the path. The origin server does not need to process the authentication information.

TypeD

Last updated : 2024-12-30 21:35:41

Algorithm Description

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

Algorithm description

`timestamp` : a decimal or hexadecimal timestamp in UNIX format.

`md5hash` : MD5 (custom key + file path + timestamp).

Sample request `http://cloud.tenloud.tencent.com/test.jpg?`

`sign=0f8201d814dfaf64cf54e74c5f7dbcb0&t=1582791032`

Note:

When the MD5 value is calculated, if the request path is `http://cloud.tencent.com/test.jpg` , then the path used for MD5 calculation will be `/test.jpg` .

Configuration Guide

Parameter Description

TypeD requires the following configurations:

Authentication Configuration

✓ Select a mode

2 Configure Parameter

3 Configure Files

Authentication Key

cqp7k0v7bl5p3l

Enter a key consisting of 6 to 40 digits, uppercase and lowercase letters. [Randomly generate](#)

Signature Parameter Name

sign

Timestamp Parameter Name

t

Valid Time

–

2

+

Time Format

☐ Decimal (Unix timestamp)

☒ Hexadecimal (Unix timestamp)

Previous

Next

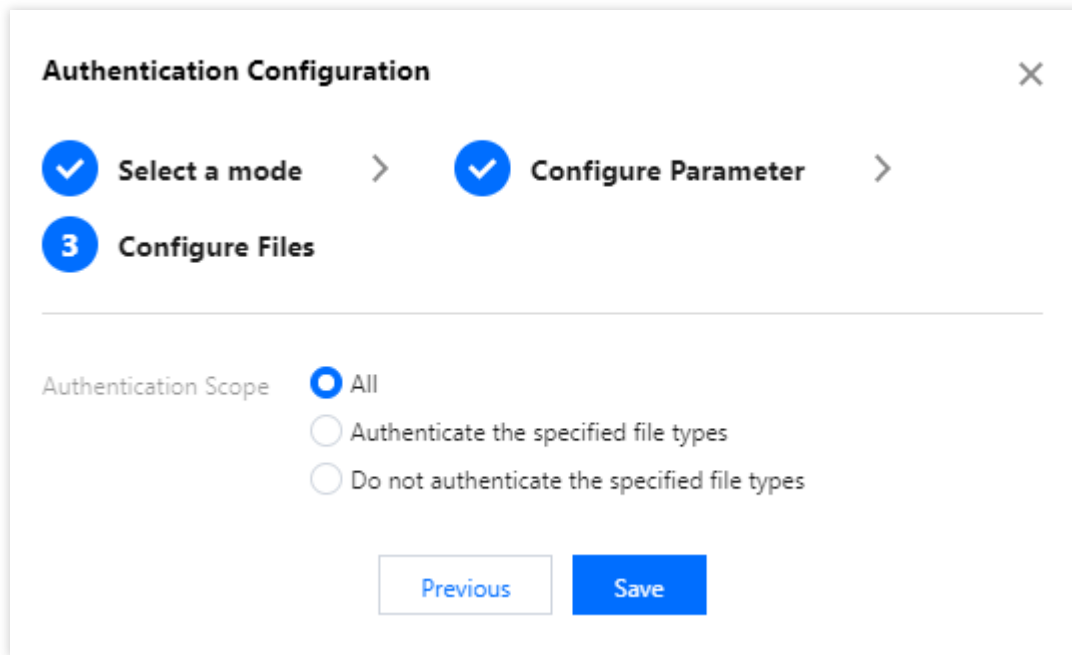
Custom authentication key: it contains 6 to 40 digits and uppercase and lowercase letters. The key should be kept private and known only to the client and server.

Custom authentication parameter name and timestamp parameter name: the `sign` in the example can be replaced with a parameter name containing 1 to 100 uppercase and lowercase letters, digits, and underscores. After CDN receives the request, it will read the value of the specified signature parameter and calculate the MD5 value. If the result matches the `md5hash` value passed in, the signature will be successfully verified. If not, a 403 error will be directly returned.

Custom validity period: the `timestamp` value in the timestamp parameter, plus the configured validity period, is compared with the current time to determine whether the request has expired. If yes, a 403 error will be directly returned. The validity period is in seconds.

Object

After configuring the key, parameter name, and validity period, you can specify the authentication object as needed. The following three authentication modes are supported:



All files under a specified domain name need to be authenticated.

All files except those in a specified type need to be authenticated.

Only files in a specified type need to be authenticated.

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 corresponding parameter and thus will not affect the cache hit rate.

Note:

As the corresponding parameter will be automatically ignored after the configuration, i.e., the configured authentication and timestamp parameters will be filtered, the cache keys of the files to be authenticated will be affected, and the priority here is higher than the cache key rules in **Cache Configuration > Cache Key Rule Configuration**.

For example, the TypeD configuration here is as: "Authentication Parameter: `sign`"; "Timestamp Parameter: `t`"; "Authentication Scope: `jpg`"; then the `sign` and `t` parameters will be automatically filtered for JPG files even though the configuration is as "All Files: Do Not Filter" in **Cache Configuration -> Cache Key Rule Configuration**.

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
```

If the CDN node is not hit after successful authentication, it will initiate an origin-pull request, **which is in the same format as the access request with the `sign/t` parameter retained**. The origin server can ignore it or perform

authentication again as needed.

UA Blocklist/Allowlist Configuration

Last updated : 2025-01-13 10:22:18

Configuration Overview

Tencent Cloud CDN supports configuring User-Agent (UA) blocklist/allowlist rules for access control.

CDN checks the `User-Agent` field in HTTP request headers based on the rules to allow or reject user access requests.

Configuration Guide

Configuration limitations

The blocklist and allowlist cannot be set at the same time. Please set either the blocklist rules or the allowlist rules.

Maximum number of blocklist/allowlist rules: 10

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.

Configuration instructions

Log in to the [CDN Console](#), select **Domain Management** on the left sidebar, and then click **Manage** on the right of a domain name to enter its configuration page. Select **Access Control** tab to find the UA blocklist/allowlist configuration, which is disabled by default:

UA Blocklist/Allowlist Configuration

Controlling access by setting the blocklist and allowlist for the User-Agent value in the request header.[What's UA blocklist/allowlist configuration?](#)

UA Blocklist/Allowlist ☐

The configuration below can be modified when it is disabled, but the configuration will not be deployed officially until it is enabled.

Add Rule

Rule Type	Rule Content	Effectiveness Type	Effectiveness Rule	Operation
No data yet				

When the switch is toggled off, click **Add Rule** to add blocklist/allowlist rules one by one:

Set UA Blocklist/Allowlist Rule

Rule Type

☒ Blocklist ☐ Allowlist

Rule Content

android

Effectiveness Type

☒ All Content ☐ File ext ☐ File Directory ☐ Specified File

Effectiveness Rule

*

Confirm

Cancel

Note:

1. Supports wildcard * and multiple values, such as curl*|*IE*|*Chrome*|*firefox*.*\$ represents an empty user agent. If the rule content contains an empty User-Agent, the following processing will be performed:

In a whitelist scenario, if the User-Agent in the request is empty, the request is allowed.

In a blacklist scenario, if the User-Agent in the request is empty, the request will be rejected.

2. If there is no * , all characters will be used for exact match.

The overall configuration will be disabled after a rule is added, so the ongoing services will not be affected:

UA Blocklist/Allowlist Configuration

Controlling access by setting the blocklist and allowlist for the User-Agent value in the request header.[What's UA blocklist/allowlist configuration?](#)

UA Blocklist/Allowlist ☐

The configuration below can be modified when it is disabled, but the configuration will not be deployed officially until it is enabled.

Add Rule

Rule Type	Rule Content	Effectiveness Type	Effectiveness Rule	Operation
Blocklist	*andriod*	All Content	*	Modify Delete

You can toggle the switch on to officially deploy the configured UA blocklist/allowlist.

UA Blocklist/Allowlist Configuration

Controlling access by setting the blocklist and allowlist for the User-Agent value in the request header.[What's UA blocklist/allowlist configuration?](#)

UA Blocklist/Allowlist ☒

The configuration below can be modified when it is disabled, but the configuration will not be deployed officially until it is enabled.

Add Rule

Rule Type	Rule Content	Effectiveness Type	Effectiveness Rule	Operation
Blocklist	*andriod*	All Content	*	Modify Delete

Configuration Samples

The UA blocklist/allowlist configuration of `cloud.tencent.com` is as follows:

UA Blocklist/Allowlist Configuration

Controlling access by setting the blocklist and allowlist for the User-Agent value in the request header.[What's UA blocklist/allowlist configuration?](#)

UA Blocklist/Allowlist ☒

The configuration below can be modified when it is disabled, but the configuration will not be deployed officially until it is enabled.

[Add Rule](#)

Rule Type	Rule Content	Effectiveness Type	Effectiveness Rule	Operation
Blocklist	*Chrome*	All Content	*	Modify Dele

If `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 : 2024-12-30 21:35:54

Overview

Tencent Cloud CDN supports downstream speed limit configuration for setting the maximum downstream throughput speed over one single URL on the server.

The downstream speed limit configuration can control the peak bandwidth of CDN to a certain degree. It is frequently used in scenarios such as ecommerce 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.

Directions

Viewing the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. Open the **Access Control** tab to find the **Downstream Speed Limit Configuration** section. The **Downstream Speed Limit** switch is toggled off by default.

Downstream Speed Limit Configuration

Setting the downstream speed limit on an URL can control the CDN access bandwidth.[What's downstream speed limit configuration?](#)

Downstream Speed Limit ☐

The configuration below can be modified when it is disabled, but the configuration will not be deployed officially until it is enabled.

[Add Speed Limiting Rule](#) [Adjust Priority](#)

Effectiveness Type	Effectiveness Rule	Speed Limiting Settings	Operation
No data yet			

Adding rules

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

Add Speed Limiting Rule

Rule Type ☒ All Content ☐ Specified File Type
☐ Specified Folder ☐ Specified File

Rule Content *

Speed Limiting Settings - 0 + KB/s

[Confirm](#) [Cancel](#)

Configuration limitations

Maximum number of downstream speed limit rules: 10

Unit: KB/s; value range: 1-1,000,000 (integers only)

Supported rule types: all content, specified file type, specified folder, and specified file. Regular matching is currently not supported.

Rules are executed from bottom to top. Rules at the bottom have higher priority.

Configuration Samples

The downstream speed limit configuration of `cloud.tencent.com` is as follows:

Downstream Speed Limit Configuration

Setting the downstream speed limit on a URL can control the CDN access bandwidth. [What's downstream speed limit configuration](#)

On/Off ☒ The configuration below can be modified when it is disabled, but the configuration will not be deployed officially until it is enabled

Add RuleAdjust priority

Effect Type	Effect Rule	Speed Limit Settings	Operation
All Content	*	400KB/s	Modify Delete
File Extension	mp4	200KB/s	Modify Delete

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.

Access Port Configuration

Last updated : 2024-12-30 21:36:09

Configuration Overview

By default, CDN supports port 80, 8080, and 443. You can disable any of them as needed.

Note:

Port configuration is now only available in the Chinese mainland. If a domain name is configured for global acceleration, then the configuration changes will take effect only in the Chinese mainland.

This feature may be unavailable in some platforms. We will complete server upgrade as soon as possible.


Configuration Guide

Viewing the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, click **Manage** on the right of a domain name to enter its configuration page. Open the **Access Control** tab to find the **Chinese Mainland Access Port Configuration** section.

Port 80, 8080, and 443 are enabled by default.

Chinese Mainland Access Port Configuration

The port 80, 8080, and 443 are enabled by default. You can disable specified ports as needed. [What's access port configuration?](#) 

Port 80  Port 8080  Port 443 

Modifying the configuration

You can disable and enable the ports as needed.

Modification limitations


If HTTPS access or forced HTTPS redirection is enabled for a domain name, Port 443 cannot be disabled.

Either Port 80 or 8080 must be opened.

Configuration Samples

If the **Chinese Mainland Access Port Configuration** of the acceleration domain name `www.test.com` is as follows:

Chinese Mainland Access Port Configuration

The port 80, 8080, and 443 are enabled by default. You can disable specified ports as needed. [What's access port configuration?](#) 

Port 80 ☒ Port 8080 ☐ Port 443 ☒

Then the actual access will be as follows:

CDN nodes deny all access requests from the port 8080.

If a domain name is configured for global acceleration, the configuration will only take effect in the Chinese mainland, which means that the CDN nodes will deny the access requests from the port 8080.

Cache Configuration

Cache Key Rule Configuration

Last updated : 2024-12-30 21:36:18

Configuration Overview

Tencent Cloud CDN uses the `Key-Value` format to map resources during caching, where `Key` is the cache key and a unique identifier of the cached resource. By configuring cache key rules, you can configure the Ignore Query String and Cache Ignore URL Case features for the content of different file types to optimize cache keys.

Ignore Query String

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 disable Ignore Query String and use a complete URL as the cache key to cache images and distinguish between resources.

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 enable Ignore Query String and use the URL part before "?" (i.e.,

```
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.

Cache Ignore URL Case

If the letter case of resource URL paths is relevant to the resource content in your business, you can disable "Cache Ignore URL Case".

If the letter case of resource URL paths is irrelevant to the resource content in your business, you can enable "Cache Ignore URL Case" to improve the hit rate.

Note:

The platform is being upgraded and Cache Ignore URL Case cannot be enabled currently.

Configuration Guide

Viewing the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. Select the **Cache Configuration** tab to find the **Cache Key Rule Configuration** section.

When adding an acceleration domain name, the Ignore Query String is enabled or disabled by default based on different acceleration business types.

If static acceleration is selected, the Ignore Query String is disabled by default. In the cache key configuration, the Ignore Query String of all file rules will be synced to **Not Filter**.

If downloading or streaming VOD acceleration is selected, the Ignore Query String is enabled by default. In the cache key configuration, the Ignore Query String of all file rules will be synced to **Filter All**.

Cache Key Rule Configuration

Configure the cache key rule to configure filtering parameters and ignore case for the content of different file types.[How to set the cache key rule?](#)

Add RuleAdjust Priority

Type	Content	Ignore Query String	Ignore URL Case	Operation
All Files	All Files	Reserve Specified Parameter version	No	Modify

Adding rules

You can add cache rules as needed.

Add Cache Key Rule

Type

Specified File Type

Content

jpg;png;css

Ignore Query String

☒ Not filter ☐ Filter All ☐ Reserve Specified Parameter

Ignore URL Case

☐ Yes ☒ No

Save

Cancel

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".

Ignore Query String - Reserve Specified Parameters.

All files: up to 6 parameter names can be entered; each one can contain up to 20 characters.

Specified file type/folder/full-path file: up to 5 parameter names can be entered; each one can contain up to 20 characters.

Separate each parameter name with ";". For example: key1;key2;key3.

Modifying rules

You can click **Modify** to modify the added cache key rules.

Note:

The default rules support modifying Ignore Query String and Cache Ignore URL Case configurations, while the type and content cannot be modified.

Deleting rules

You can click **Delete** to delete the added cache key rules (except the default ones).

Configuration Samples

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

Cache Key Rule Configuration				
Configure the cache key rule to configure filtering parameters and ignore case for the content of different file types. How to set the cache key rule?				
Add Rule Adjust Priority				
Type	Content	Ignore Query String	Ignore URL Case	Operation
All Files	All Files	Reserve Specified Parameter version	No	Modify
Specified File Type	jpg;png	Filter All	No	Modify Delete

Then the actual access will be as follows:

A client accessed the resources `www.test.com/abc.jpg?version=1&colour=red` and `www.test.com/abc.JPG?version=1&colour=red`, the two requests arrived at the CDN node X, on which

the resources are not cached.

The origin server will be pulled for the image `abc.jpg`, and the image will be cached on the CDN node X. As Ignore Query String is enabled and **Filter All** is selected, the URL part `www.test.com/abc.jpg` before "?" will be used as the cache key.

The client accessed the resource `www.test.com/abc.JPG?version=1&colour=red`, and as the Cache Ignore URL Case is disabled, the cached resource `www.test.com/abc.jpg` will not be hit, the origin server will be pulled for the image `abc.JPG`, the image will be cached on the CDN node X, and `www.test.com/abc.JPG` will be used as the cache key.

Node Cache Validity Configuration

Last updated : 2024-12-30 21:36:25

You can set the cache validity period of resources on the origin server on CDN nodes in **Node Cache Validity** to adjust the cache update frequency of origin server resources on the CDN nodes. You can configure the resource cache validity period by directory, file extension, and full file path based on your business needs.

Overview

CDN will determine whether a resource cached on a CDN node expires based on the cache validity period configured in **Node Cache Validity**.

If the cache of a resource accessed by an end user doesn't expire on the CDN node, the node will directly return the cached resource to the user.

If a resource accessed by an end user is not cached, or the resource cache has expired on the CDN node, the node will pull the latest resource from the origin server to cache it 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 [cache purge](#) feature to update unexpired caches on the CDN node, so as to ensure that resources cached on the CDN node and stored on the origin server are consistent.

Notes

As the cache validity period affects the origin-pull frequency, we recommend you set the resource cache validity period based on your business needs. If it is too short, CDN will perform origin-pull frequently, thereby increasing the bandwidth usage of the origin server. If it is too long, caches on CDN nodes will be updated slowly, making end users unable to get the latest resources.

CDN nodes cache resources based on the [CDN cache rule and priority](#). However, resources cached on a CDN node may be deleted from the node before the expiration time due to a low request frequency.

We recommend you use different filenames before and after updating a resource on the origin server. For example, name resources with different content by version numbers `img-v1.jpg` and `img-v2.jpg`, to prevent CDN nodes from returning the old but unexpired resource to the end user after the resource content is changed on the origin server.

If you still use the legacy version (in basic mode) of the node cache validity configuration, we recommend you submit the advanced mode configuration to upgrade the node cache validity configuration to the latest version so as to support more features. Note that after the upgrade to the advanced mode, you cannot restore to the basic mode. For

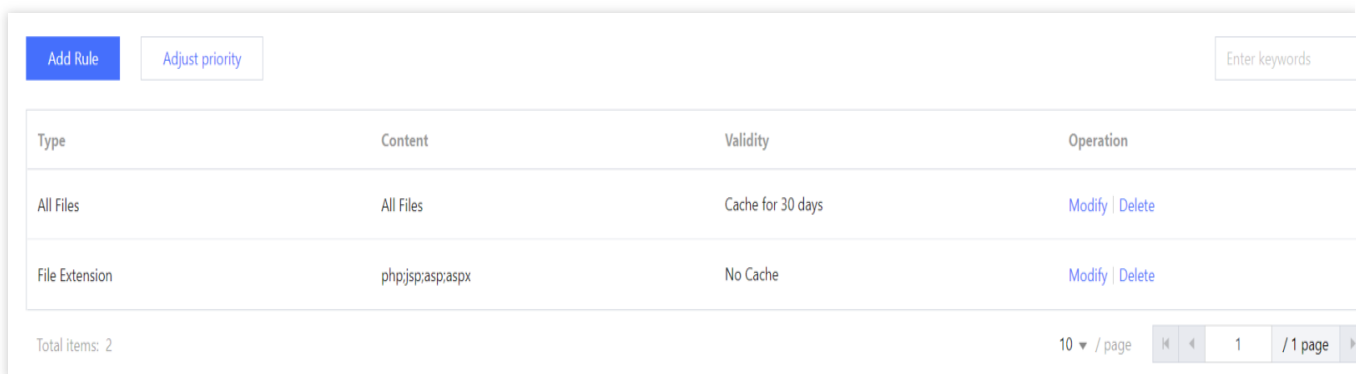
more information on the legacy version of the node cache validity configuration, see [Node Caching Rule Configuration \(Legacy\)](#).

The origin server can set the `Cache-Control` response header to control the cache validity period on CDN nodes (when **Cache Option** is **Follow Origin Server**). Then, CDN nodes will pass the `Cache-Control` header to the end user to control the browser cache validity period. If you want CDN nodes to set the browser cache validity period, you can modify the `Cache-Control` header returned by CDN nodes to the user in [Browser Cache Validity](#).

Configuration Description

Directions

1. Log in to the [CDN console](#).
2. Click **Domain Management** on the left sidebar to enter the domain name management list.
3. Select the target domain name and click **Manage** to enter the domain name configuration page.
4. Click **Cache Configuration** to switch to the **Cache Configuration** tab, and you can view the **Node Cache Validity**.



Add Rule		Adjust priority	<input type="text" value="Enter keywords"/>	
Type	Content	Validity	Operation	
All Files	All Files	Cache for 30 days	Modify Delete	
File Extension	php,jsp,asp,aspx	No Cache	Modify Delete	
Total items: 2		10 / page	1	/ 1 page

5. Click **Add Rule** to enter the **Add Rule** page and add a node cache validity rule.

Add Rule

×

Type

File Extension ▼

Content

jpg;png;css

Cache Option

Follow Origin Server ▼

Heuristic cache

☒ It takes effect when the origin server responds without Cache-Control or Expires

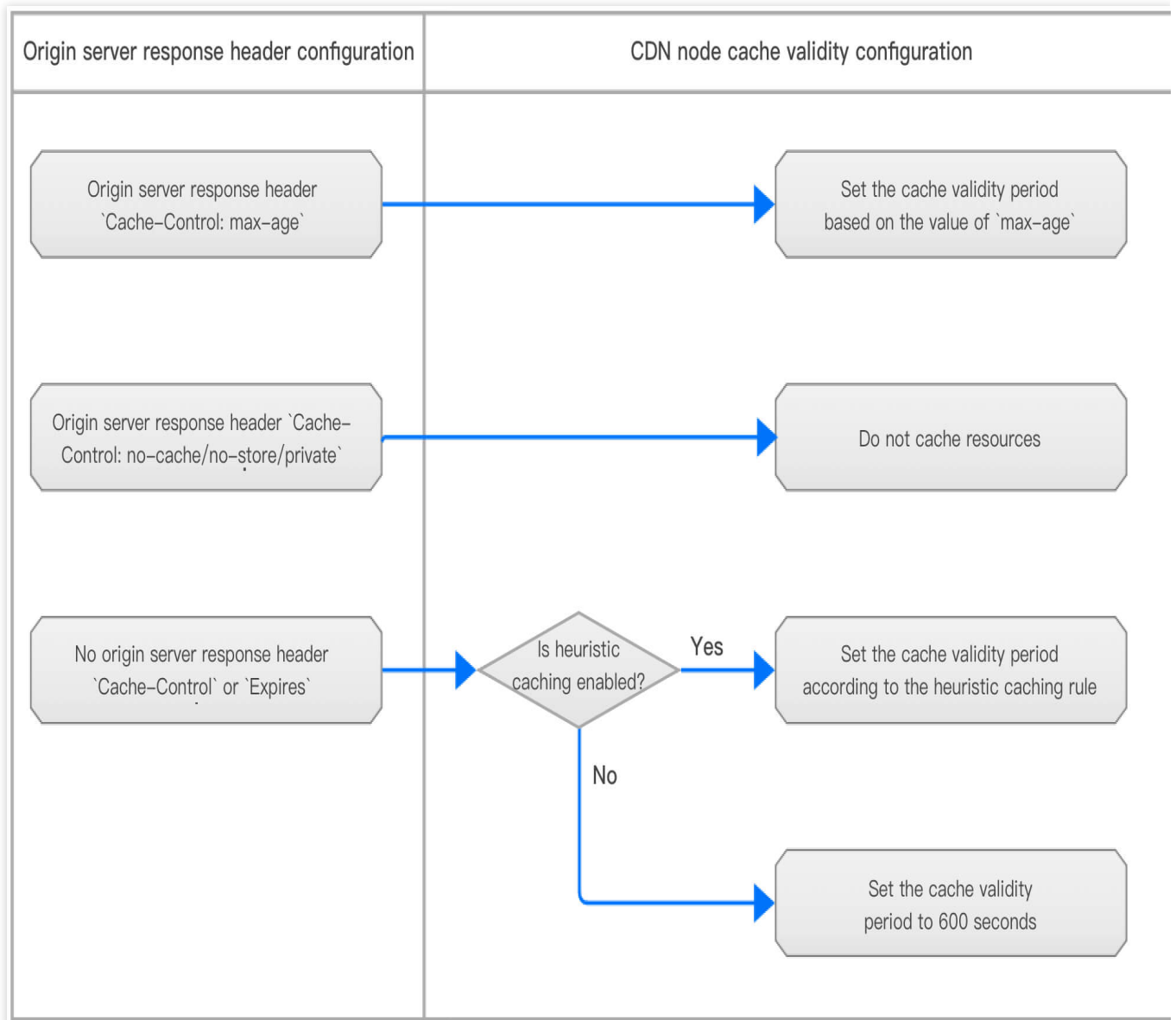
OK

Cancel

Configuration Item	Description
Type	You can select All Files, File Extension, File Directory, Full Path, or Homepage. All Files: Set the rule for all files. This is the default option. File Extension: Set the rule for the specified file extension. File Directory: Set the rule for the specified file directory. Full Path: Set the rule for the specified full file path. Homepage: Set the rule for the specified domain name root directory.
Content	Enter the content based on the selected file type.If Type is All Files, the content is fixed to all files.If Type is File Extension, you can enter one or multiple file extensions separated by ";", such as `jpg;png;css`.If Type is File Directory, you can enter one or multiple file directories separated by ";", and the entered content cannot end with "/", such as `/test;/a/b/c`.If Type is Full Path, you can enter one or multiple full file paths separated by ";", such as `/index.html;/test/.jpg`.
Cache Option	You can select Follow Origin Server, Cache, or Do not cache. Follow Origin Server: The CDN node cache validity period will be set based on the `Cache-Control` origin server header, and heuristic caching can be enabled.Cache: You can customize the CDN node cache validity period and enable force cache.Do not cache: CDN nodes will not cache any resources.

CDN cache rule and priority

Cache Option is Follow Origin Server



The cache validity period will be set on CDN nodes based on the `Cache-Control` origin server response header. If the field in the `Cache-Control` origin server response header is `max-age`, the CDN node cache validity period will be set based on the value of `max-age`. For example, if `Cache-Control: max-age=300` is configured, the cache validity period will be 300 seconds.

If the field in the `Cache-Control` origin server response header is `no-cache`, `no-store`, or `private`, the CDN node will not cache resources.

If there is no `Cache-Control` or `Expires` origin server response header, the cache rule will be set based on the heuristic caching status:

If heuristic caching is disabled and there is no `Cache-Control` or `Expires` origin server response header, the cache validity period will be 600 seconds.

If heuristic caching is enabled and there is no `Cache-Control` or `Expires` origin server response header, the heuristic cache validity period will be set according to the following rules:

i. **Default Configuration:** If there is the `Last-Modified` origin server response header, the cache validity period will be calculated as follows: $(\text{current time} - \text{Last-Modified}) * 0.1$. If there is no `Last-Modified` origin server response header, the cache validity period will be 600 seconds by default.

Add Rule

Type

File Extension

Content

jpg;png;css

Cache Option

Follow Origin Server

Heuristic cache

☒ It takes effect when the origin server responds without Cache-Control or Expires

Cache policy

☒ Default Configuration ☐ Custom policy

If the response header of the origin server Last-Modified exists, the cache time is (Current time - Last modified time) * 0.1. If it does not exist, the default cache time is 600s.

OK

Cancel

ii. **Custom Policy:** You can customize the heuristic cache validity period.

Add Rule ✕

Type

File Extension ▼

Content

jpg;png;css

Cache Option

Follow Origin Server ▼

Heuristic cache

☒ It takes effect when the origin server responds without Cache-Control or Expires

Cache policy

☐ Default Configuration ☒ Custom policy

Cache Time

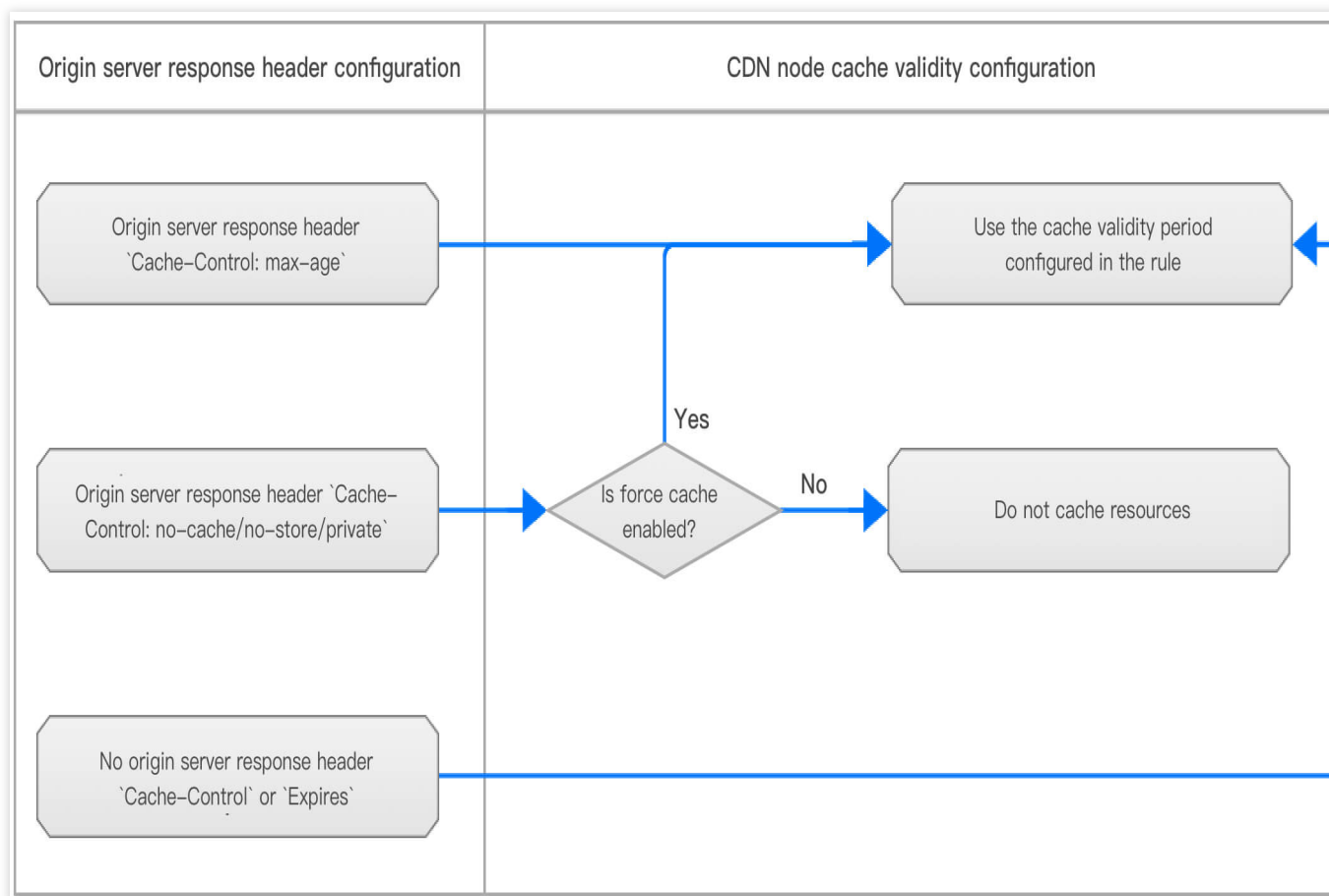
− 100 +

Seconds ▼

OK

Cancel

Cache Option is Cache



You can customize the cache validity period on the CDN node.

If force cache is disabled:

If the field in the `Cache-Control` origin server response header is `max-age` or there is no `Cache-Control` header, resources will be cached according to the custom CDN node cache rule.

If the field in the `Cache-Control` origin server response header is `no-cache`, `no-store`, or `private`, CDN nodes will not cache resources.

Add Rule ✕

Type

File Extension ▼

Content

jpg;png;css

Cache Option

Cache ▼

Cache Time

−

1

+

days ▼

Force cache ⓘ

☐ Yes ☒ No

OK

Cancel

If force cache is enabled: The `Cache-Control` origin server response header will be ignored, and resources will be cached according to the custom CDN node cache rule.

Add Rule ✕

Type

File Extension ▼

Content

jpg;png;css

Cache Option

Cache ▼

Cache Time

—

1

+

days ▼

Force cache ⓘ

☒ Yes ☐ No

OK

Cancel

Cache Option is Do not cache

CDN nodes are configured to not to cache resources. For each user request to access a resource, CDN nodes will directly perform origin-pull to get the resource and return it to the user.

Add Rule ✕

Type

File Extension ▼

Content

jpg;png;css

Cache Option

No Cache ▼

OK

Cancel

Priority of multiple cache rules

If multiple cache rules are configured, the lower the rule position, **the higher the priority**. You can click **Adjust Priority** to drag and drop cache rules to change their order and adjust the priority.

Add Rule Adjust priority

Enter keywords

Type	Content	Validity	Operation
All Files	All Files	Cache for 30 days	Modify Delete
File Extension	php;jsp;asp;aspx	No Cache	Modify Delete
File Extension	jpg	Cache for 10 days; Force Cache on	Modify Delete

Total items: 3

10 ▼ / page

⏮

⏪

1

⏩

⏭

/ 1 page

Recommended configuration

For seldom updated static files, such as images and large files, we recommend you set the cache validity period to 30 days.

For frequently updated static files, such as .js and .css files, we recommend you set the cache validity period based on the update frequency of your business.

For dynamic files, such as .php, .jsp, .asp, and .aspx files, **you need to set Cache Option to Do not cache.**

For other requests involving direct interaction with the origin server, such as **site login** (`/wp-admin` directory for WordPress backend login, for example) or **API-based query**, you need to set **Cache Option to Do not cache**; otherwise, an access error may occur.

Configuration limitations

You can add up to 100 cache rules for a domain name.

If there are multiple cache rules, the lower the rule position, the higher the priority.

If **Type** is set to **File Extension**, **File Directory**, or **Full Path**, you can enter up to 100 items and separate them by ";", such as `jpg;png` (when **Type** is set to **File Extension**).

If no rules are configured or the request fails to hit any configured rules, the cache validity period will be set on CDN nodes based on the `Cache-Control` origin server response header. If there is no `Cache-Control` header, CDN nodes will cache the resource for 600 seconds.

CDN nodes only cache content requested by GET and HEAD requests. Content requested by POST and OPTIONS requests won't be cached on CDN nodes.

Configuration Samples

Sample 1

The original cache rules specify that CDN doesn't cache .php, .jsp, .asp, and .aspx files and caches other files for 30 days.

Add Rule		Adjust priority	<input type="text" value="Enter keywords"/>	
Type	Content	Validity	Operation	
All Files	All Files	Cache for 30 days	Modify Delete	
File Extension	php;jsp;asp;aspx	No Cache	Modify Delete	
Total items: 2		10 / page	1 / 1 page	

You need to add a rule to cache .jpg and .png files for 10 days while ignoring the `Cache-Control` origin server response header (i.e., enabling force cache), and change **Cache Option** in the cache rule for **All Files** to **Follow Origin Server**.

1. Click **Add Rule**, set **Type** to **File Extension**, **Content** to `jpg;png`, **Cache Option** to **Cache**, **Cache Validity** to **10 days**, and **Force Cache** to **Yes**, and click **OK**.

Add Rule ✕

Type

File Extension ▼

Content

jpg

Cache Option

Cache ▼

Cache Time

−

10

+

days ▼

Force cache ⓘ

☒ Yes ☐ No

OK

Cancel

2. Select the cache rule for **All Files**, click **Modify**, change **Cache Option** to **Follow Origin Server**, and click **OK**.

Modify Rule

Type

All Files

Content

All Files

Cache Option

Follow Origin Server

Heuristic cache

☒ It takes effect when the origin server responds without Cache-Control or Expires

OK

Cancel

3. After the adjustment, the cache rules are:

.jpg and .png files will be cached for 10 days with force cache enabled.

.php, .jsp, .asp, and .aspx won't be cached.

Other files will be cached for 30 days.

Add RuleAdjust priority

Enter keywords

Type	Content	Validity	Operation
All Files	All Files	Follow Origin Server	Modify Delete
File Extension	php;jsp;asp;aspx	No Cache	Modify Delete
File Extension	jpg	Cache for 10 days; Force Cache on	Modify Delete

Total items: 3

10 / page

1 / 1 page

Below are actual caching results:

The `www.test.com/abc.jpg` resource will be cached on the node for 10 days, even though the field in the `Cache-Control` origin server response header is `no-cache`, `no-store`, or `private`.

The `www.test.com/def.php` resource won't be cached to the node.

Sample 2

Suggestions on configuring node cache validity rules for a site built based on WordPress:

For resources under the domain name `/wp-admin` directory for backend login, you need to set **Cache Option** to **Do not cache**; otherwise, backend login resources will be cached and login errors will occur. If there are any API resources, you also need to set **Cache Option** to **Do not cache** for them.

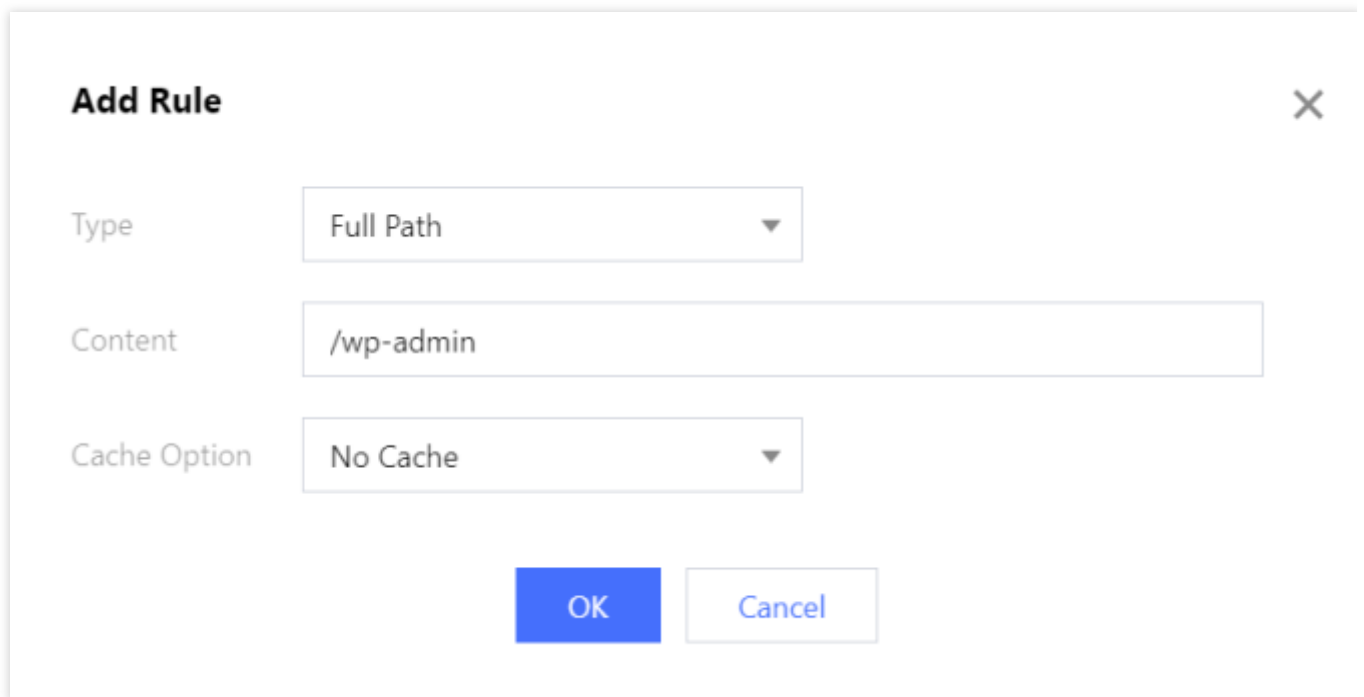
For .php, .jsp, .asp, and .aspx dynamic files, you need to set **Cache Option** to **Do not cache** (default cache rule of CDN).

As .html, .js, and .css files are updated frequently, you need to set the cache validity period based on the update frequency. We recommend you set the cache validity period to 7 days and disable force cache.

Other files are cached for 30 days (default cache rule of CDN).

Add cache rules while retaining the default CDN cache rules:

1. Click **Add Rule**, set **Type** to **File Directory**, **Content** to `/wp-admin`, and **Cache Option** to **Do not cache**, and click **OK**.



Add Rule ✕

Type

Content

Cache Option

2. Click **Add Rule**, set **Type** to **File Extension**, **Content** to `html;js;css`, **Cache Option** to **Cache**, **Cache Validity** to **7 days**, and **Force Cache** to **No**, and click **OK**.

Add Rule ✕

TypeFile Extension

Contenthtml;js;css

Cache OptionCache

Cache Time

7

days

Force cache ☐ Yes ☒ No

OKCancel

3. As the lower the rule position, the higher the priority, click **Adjust Priority** and drag and drop the rule of not caching files in the `/wp-admin` directory to the bottom to grant it the highest priority.

Add RuleAdjust priorityEnter keywords

Type	Content	Validity
All Files	All Files	Cache for 30 days
File Extension	php;js;asp;aspx	No Cache
Full Path	/wp-admin	No Cache
File Extension	html;js;css	Cache for 7 days

Define priority by the sequence of items in the list. The lower items are with higher priorities.

SaveCancel

4. After the adjustment, the cache rules are:

All resources under the `/wp-admin` directory will not be cached.

.html, .js, and .css files will be cached for 7 days.

.php, .jsp, .asp, and .aspx won't be cached.

Other files will be cached for 30 days.

[Add Rule](#) [Adjust priority](#)

Type	Content	Validity	Operation
All Files	All Files	Cache for 30 days	Modify Delete
File Extension	php;jsp;asp;aspx	No Cache	Modify Delete
File Extension	html;js;css	Cache for 7 days	Modify Delete
Full Path	/wp-admin	No Cache	Modify Delete

Total items: 4 10 / page 1 / 1 page

FAQs

If the file changes on the origin server, will the cache on CDN cache nodes be updated in real time?

How do I tell whether user access has hit the CDN cache?

Status Code Cache Configuration

Last updated : 2024-12-30 21:36:38

Configuration Overview

Normally, when a CDN node successfully pulls a requested resource from the origin server (with a 2XX status code returned), the node will process the resource based on the rules in the node cache validity configuration.

If the origin server is unable to process the non-2XX requests quickly, and you do not want all requests to be passed through to the origin server, you can configure the status code cache validity period. In this case, the CDN node will directly respond to non-2XX requests, helping reduce pressure on the origin server.

Currently supported status codes are as follows:

4XX: 400, 401, 403, 404, 405, 407, 414

5XX: 500, 501, 502, 503, 504, 509, 514

Note:

For now, some platforms only supports 404 and 403 codes. We will complete server upgrade as soon as possible.

Currently, only the status codes 404 and 403 are supported in regions outside the Chinese mainland. If the acceleration region of a domain name is "Global", then the status code cache rules except for 404 and 403 will only take effect in the Chinese mainland.

Configuration Guide

Viewing configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, click **Manage** on the right of a domain name to enter its configuration page, and switch to the **Cache Configuration** tab to find the **Status Code Cache** section.

There is a default rule, which will cache 404 requests for 10 seconds.

Status code cache

Set status code cache time [What's status code caching?](#)

New status code cache

Status Code	Cache Validity	Operation
404	10s	Modify Delete

Adding rules

You can click **Add Rule** to add status code cache rules as needed.

New status code cache

Status Code	Cache Validity	Operation
<div>403</div>	<div></div> <div>days</div>	

OK

Cancel

Configuration limitations

Each status code can only have one unique rule.

The cache time means not to cache content.

HTTP Header Cache Configuration

Last updated : 2024-12-30 21:36:44

Configuration Overview

Besides resources, Tencent Cloud CDN will also cache the following headers from the origin server and return them to users by default:

Access-Control-Allow-Origin

Timing-Allow-Origin

Content-Disposition

Accept-Ranges

If your origin server has special headers that need to be cached and returned to users by CDN, you can enable header cache.

Configuration Guide

Viewing the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. Open the **Cache Configuration** tab to find the **HTTP Header Cache Configuration** section. The configuration is enabled by default, and you can disable it as needed.

HTTP Header Cache

If it's on, all header information passed through from the origin is cached. And if it's off, only part of the key header information is cached. [What's HTTP header cache?](#)

Due to the node cache, if it needs to take effect immediately after turned on/off, please refresh the cache.

Cache all headers: ☒

Access URL Rewrite Configuration

Last updated : 2024-12-30 21:36:50

Configuration Overview

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** on the left sidebar, click **Manage** on the right of a domain name to enter its configuration page, and open the **Cache Configuration** tab to find the **Access URL Rewrite Configuration** section.

Access URL Rewrite Configuration is disabled by default.

Access URL Rewrite Configuration

Multiple access URL rewrite rules can be configured. [What's access URL rewrite configuration](#)

On/Off ☐ The configuration below can be modified when it is disabled, but the configuration will not be deployed officially until it is enabled

Add RuleAdjust priority

Current URL	Target Host	Target Path
No data yet		

Total items: 0

Adding rules

You can click **Add Rewrite Rule** to add rules as needed.

Add Rule



Matching Rule ☐ Full-path matching

If it's not selected, Prefix Matching is used by default

Current URL

Starting with "/"; supporting full-path matching (e.g., /test/a.jpg) and wildcard (*) matching (e.g., /test/*/*.jpg)

Target Host

"http://" or "https://" is required

Target Path

Starting with "/" (e.g., /newtest/b.jpg); the wildcard "*" can be caught with "\$n" (e.g., if n=1,2,3... then /newtest/\$1/\$2.jpg)

Save

Cancel

Configuration limitations

Each domain name can have up to 100 rewrite rules.

You can adjust the priority for multiple rules. Rules at the bottom of the list have higher priority.

Current URL: starting with /; supporting full-path matching (e.g., /test/a.jpg) and wildcard () matching (e.g., /test/./jpg).

If you want to specify a file directory, you cannot end the path with / (e.g., /test).

Target Host: it is the current domain name (starting with `http://`) by default. It can be modified to other domain names starting with `http://` or `https://` .

Target Path: starting with / (e.g., /newtest/b.jpg); the wildcard * can be captured with `$n` (e.g., if n=1,2,3... then /newtest/\$1/\$2.jpg). If you want to specify a file directory, you cannot end the path with / (e.g., /test).

Up to 5 `*` and 10 `$n` are supported.

The content can contain up to 1,024 characters and Chinese characters are not supported.

Configuration Samples

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

Access URL Rewrite Configuration

Multiple access URL rewrite rules can be configured. [What's access URL rewrite configuration](#)

On/Off ☒ The configuration below can be modified when it is disabled, but the configuration will not be deployed officially until it is enabled

Add RuleAdjust priority

Current URL	Target Host	Target Path
/test/a.jpg Full-path matching	http://www.test.com	/newtest/b.jpg
/test/*.png Full-path matching	http://www.newtest.com	/newtest/\$1.png

Total items: 2

Then the actual access will be as follows:

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

A client requests `www.test.com/test/a.png` and the CDN node returns `www.newtest.com/newtest/a.png`.

Browser Cache Validity Configuration

Last updated : 2024-12-30 21:36:57

Feature Overview

By configuring the browser cache validity, you can customize client browser cache policies to reduce origin-pull rate.

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 the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, click **Manage** on the right of a domain name to enter its configuration page. Open the **Cache Configuration** tab to find the **Browser Cache Validity Configuration** section.

Browser Cache Validity Configuration			
Browser cache validity configuration is a set of browser caching policies for user files, which can lower the origin-pull rate. How to set the browser cache validity configuration?			
Add Rule	Adjust Priority		
Type	Content	Cache Behavior	Operation
All Files	All Files	Follow Origin Server	Modify

Adding rules

Click **Add Rule** to add browser cache validity rules for specified file type, file directory, file path, and homepage.

Add Browser Cache Rule ✕

Specified File Type

Specified File Type ▼

Content

jpg;png;css

Cache Option

Follow Origin Server ▼

OK

Cancel

Follow origin server: follow the `Cache-Control` header of the origin server. If the origin server does not have a CC header or its CC header is `no-cache/no-store/private`, the browser will not cache resources.

Cache: if the CC header of the origin server is not `no-cache/no-store/private`, the browser cache validity rules will be applied; otherwise, the browser will not cache resources.

No cache: no resource is cached in a browser.

Configuration limitations

Each domain name can have up to 20 rules. Only one "All Files" and "Homepage" rule can be added.

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.

Chinese characters are not supported.

Default policies

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

When a user makes a request for a certain business resource, if the HTTP response header of the origin server contains the field `Cache-Control`, the `Cache-Control` will be followed.

If the HTTP response header of the origin server does not contain the field `Cache-Control`, then the resource cache validity on the browser will be 600 seconds.

When there are node cache validity rules configured (configuration guide: [Node Cache Validity Configuration \(New\)](#)) or matched:

If the HTTP response header of the origin server does not contain the field `Cache-Control`, then the browser will not cache resources.

If the HTTP response header of the origin server contains the field `Cache-Control` , then the browser cache will follow `Cache-Control` .

Cache Configuration FAQs

Last updated : 2024-12-30 21:37:03

What's node cache validity configuration?

Node cache validity configuration refers to a set of validity rules the CDN cache nodes should follow when caching your business contents.

All resources cached on CDN nodes have validity. For unexpired resources, when a request reaches the node, the node will directly return the requested resources to the user, so as to speed up the resource acquisition. For expired resources, the node will forward the user request to the origin server. If the resources have been updated on the origin server, they will be reacquired, cached to the node, and then returned to the user; otherwise, only the resource validity will be updated on the node. A proper cache validity can effectively improve the resource hit rate and lower the origin-pull rate, reducing bandwidth usage.

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](#).

I use my own server as the origin server of CDN. Can I configure CDN to not cache a specific type of files? Can I set the cache validity to "0" to disable caching?

You can configure different cache validity periods for different types of directories and files. If the cache validity is configured to "0", the CDN node will not cache the resource, in which case the CDN node needs to pull related resources from the origin server every time the users send access requests to the node. For more information on cache configurations, please see [Node Cache Validity Configuration \(Legacy\)](#).

What cache validity configuration does Tencent Cloud support?

Tencent Cloud CDN supports configuring cache actions and cache validity rules for various file types, and you can also adjust the priority of custom cache rules. Proper cache validity rules can effectively improve the resource hit rate and lower the origin-pull rate, reducing bandwidth usage. For more information, please see [Cache Configuration](#).

What is the default cache configuration of CDN?

When adding an acceleration domain name, default node cache validity rules are added based on different acceleration service types and can be modified as needed.

If static acceleration is selected, the general dynamic files (such as PHP, JSP, ASP, and ASPX files) will not be cached by default, and other files will be set to follow the origin server by default.

If download or streaming VOD acceleration is selected, the default cache validity of all files will be 30 days.

What are cache matching rules?

When multiple cache rules are set, the ones at the bottom of the list have higher priority. 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. 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.

Origin-pull Configuration

Range GETs Configuration

Last updated : 2024-12-30 21:37:10

If most of your files are large static files, enabling Range GETs can help increase the file response speed during origin-pull and improve the large file delivery efficiency.

Description

Range GETs refers to origin-pull based on range requests. `Range` is one of the HTTP request headers, which is used to get files in the specified range. You can use a range request to request only partial file content from the server. For example, if a request carries the HTTP header `range: bytes=0-999`, the first 1,000 bytes of the file will be returned to the user.

In CDN, after Range GETs is enabled, origin-pull requests will carry the `Range` header by default. If the partial file requested by a user is not cached on the node or its cache has expired, CDN will perform Range GETs to pull and cache the requested partial file to the node and return it to the user. After Range GETs is disabled, if the user request doesn't carry the `Range` header, CDN will still pull the entire file during origin-pull.

For large files such as APK, audio, and video files, you can use range requests to effectively improve the delivery efficiency of large files, shorten the response time, and reduce the pressure on the origin.

Notes

1. Before you enable Range GETs, make sure that the origin server supports range requests. Otherwise, origin-pull may fail.
2. After you enable Range GETs, resources are cached in shards on the nodes. These shards have the same cache validity period and follow the cache validity rule that you defined.
3. Origin-pull may fail if Range GETs is enabled for small static files, or if you enable Range GETs while using a COS origin server and data processing methods such as image processing. To ensure successful origin-pull in these cases, we recommend that you do not enable Range GETs.
4. We recommend that you enable Range GETs to cache large static files in the following cases: The origin server supports range requests, or you use a COS origin server and do not use any data processing methods such as image processing.

StreamLink Configuration

Configuration in domain management

1. Log in to the [CDN console](#).
2. Click **Domain Management** on the left sidebar to enter the domain name management list.
3. Select the target domain name and click **Manage** to enter the domain name configuration page.
4. Click the **Origin-pull Configuration** tab to view the Range GETs configuration items.

Range GETs Configuration

Enable Range GETs to reduce the consumption in file delivery during origin-pull and shorten the response time (the origin server must support Range requests). [What's Range GETs](#)

Note that the origin-pull may fail if it's enabled for small static files, or you enable it while using a COS origin server and data processing methods

Add Rule

Adjust priority

Type	Content	Range GETs	Operation
All Files	All Files	Disable	Modify

Total items: 1

10 / page

1 / 1 page

5. In Range GETs configuration, Range GETs is disabled for all files by default. You can also add multiple custom rules for files as needed. Range GETs rules can be matched by file extension, file directory, and full path.

Item	Description
Type	<p>You can select All Files, File Extension, File Directory, or Full Path:</p> <p>All Files: This Range GETs rule applies to all files. It is the default rule and cannot be deleted.</p> <p>File Extension: This Range GETs rule applies to the specified file extensions.</p> <p>File Directory: This Range GETs rule applies to the specified file directories.</p> <p>Full Path: This Range GETs rule applies to the specified file paths.</p>
Content	<p>Enter the content based on the selected file type:</p> <p>If Type is File Extension, you can enter one or multiple file extensions separated by ";".</p> <p>If Type is File Directory, you can enter one or multiple file directories separated by ";", and the entered content cannot end with "/", such as <code>/test;/a/b/c</code>.</p> <p>If Type is Full Path, you can enter one or multiple full file paths separated by ";", such as <code>/index.html;/test/*.jpg</code>. The file path supports the * wildcard.</p>
Range GETs	<p>Range GETs can be enabled or disabled.</p> <p>Enable: If Range GETs is enabled, range requests are used for origin-pull requests. After Range GETs is enabled, if the user request does not carry the <code>Range</code> header and the</p>

requested files are larger than 4 MB in size, the CDN node splits the origin-pull request into several sub-requests for origin-pull based on a shard size of 1 MB. If the requested files are smaller than 4 MB in size, the CDN node pulls complete files from the origin server. If the user request carries the `Range` header, the CDN node uses the `Range` header for origin-pull. Disable: If Range GETs is disabled, range requests are not used for origin-pull requests.

Recommended Configuration

If your files are larger than 4 MB in size, we recommend you enable Range GETs for such files. If only part of your files are large ones, we recommend you enable Range GETs for them through match by file type, file directory, or full path and disable Range GETs for other files.

Configuration limitations

You can configure up to 20 Range GETs rules. The lower the rule, the higher the priority. When a user requests a file, the file will be matched with rules in sequence by priority, and the rule with the highest priority will be executed preferentially after a successful match.

Configuration Samples

Sample 1

If Range GETs needs to be enabled for all files, configure Range GETs for the domain name

`cloud.tencent.com` as follows:

Enable Range GETs to reduce the consumption in file delivery during origin-pull and shorten the response time (the origin server must support Range requests). [What's Range GETs](#)

Note that the origin-pull may fail if it's enabled for small static files, or you enable it while using a COS origin server and data processing methods

Add RuleAdjust priority

Type	Content	Range GETs	Operation
All Files	All Files	Disable	Modify

Total items: 1

10 / page

1 / 1 page

User A requests for the resource `http://cloud.tencent.com/test.apk`. After the node receives the request and finds that the cached file `test.apk` has already expired, the node initiates an origin-pull request. Since Range GETs is enabled for all files in the current rule, the node uses a range request to obtain and cache the resource in shards. If user B also makes a range request for the same file to the same node and the shards that are

stored on the node match the specified byte segments in the range request, the resource is directly returned to user B even though the shards are not completely obtained.

Sample 2

If Range GETs needs to be enabled for only part of your files, configure Range GETs for the domain name

`cloud.tencent.com` as follows:

Range GETs Configuration

Enable Range GETs to reduce the consumption in file delivery during origin-pull and shorten the response time (the origin server must support Range requests). [What's Range GETs](#)

Note that the origin-pull may fail if it's enabled for small static files, or you enable it while using a COS origin server and data processing methods

Add RuleAdjust priority

Type	Content	Range GETs	Operation
All Files	All Files	Disable	Modify
File Extension	apk	Disable	Modify Delete

Total items: 2

10 / page

1 / 1 page

When user A makes a request for the `http://cloud.tencent.com/test.apk` resource, as the bottom rule has a higher priority than the top rule, Range GETs will be used for the request if the node resource is not hit or the cached resource has expired. If user B makes a request for the `http://cloud.tencent.com/test.jpg` resource, as it only matches the rule for all files, Range GETs won't be used when origin-pull is performed for the request.

Follow 301/302 Configuration

Last updated : 2024-12-30 21:37:16

Configuration

Tencent Cloud CDN does not cache 301/302 status codes by default. When an origin server returns a 301/302 request, the CDN node will return the response to the client by default, and the client will be redirected to the corresponding resource for access.

When the follow 301/302 redirect configuration is enabled, the CDN node will be redirected when receiving a 301/302 redirect request during origin-pull until it gets the required resource (up to 3 follows are supported). It will then return the actual resource to the client, which does not need to be redirected.

Configuration Guide

Log in to the [CDN Console](#), select **Domain Management** on the left sidebar, and click **Manage** to the right of the domain name to access its configuration page. Under the **Origin Configuration** tab, find **Follow 301/302 Configuration**, which is disabled by default:

Follow 301/302 Configuration

With "Follow 302" enabled, if code 301/302 is returned for node back-to-origin requests, requests will be redirected to get resources, instead of showing 301/302 to users. [What's Follow 301/302?](#)

Follow 301/302 ☐

Configuration Sample

Suppose the follow 301/302 redirect configuration for the domain name `cloud.tencent.com` is as follows:

Follow 301/302 Configuration

With "Follow 302" enabled, if code 301/302 is returned for node back-to-origin requests, requests will be redirected to get resources, instead of showing 301/302 to users. [What's Follow 301/302?](#)

Follow 301/302 ☒

User A requests a resource `http://cloud.tencent.com/1.jpg`. If the cache is not hit on the node, the node will request the resource from the origin server. If the HTTP response status code returned by the origin server is 302 and the redirect address is `http://cloud.tencent.com/1.jpg`, then:

1. After follow 301/302 redirect is enabled, the node will directly initiate a request to the redirect address when it receives the HTTP response with the 301/302 status code.
2. The resource will be obtained, cached to the node, and returned to the user.
3. At this time, if user B also sends a request for `http://cloud.tencent.com/1.jpg`, the cache will be hit on the node and the resource will be returned to the user.
4. After follow 301/302 redirect is enabled, up to 3 follows are allowed. If this limit is exceeded, the 301/302 status code will be returned to the user.

Suppose the follow 301/302 redirect configuration for the domain name `cloud.tencent.com` is as follows:

Follow 301/302 Configuration

With "Follow 302" enabled, if code 301/302 is returned for node back-to-origin requests, requests will be redirected to get resources, instead of showing 301/302 to users. [What's Follow 301/302?](#)

Follow 301/302 ☐

User A requests a resource `http://cloud.tencent.com/1.jpg`. If the cache is not hit on the node, the node will request the resource from the origin server. If the HTTP response status code returned by the origin server is 301/302 and the redirect address is `http://xxx.tencent.com/1.jpg`, then:

1. The node will directly return the HTTP response to the user.
2. When the user initiates a request for `http://xxx.tencent.com/1.jpg`, no acceleration will take effect if the domain name is not connected to CDN.
3. At this time, if user B also sends a request for `http://cloud.tencent.com/1.jpg`, the process above will be repeated.

Origin-pull timeout configuration

Last updated : 2024-12-30 21:37:24

Configuration Scenario

When Tencent Cloud CDN forwards a request to the origin server, the default timeout period for TCP connection is 5 seconds, and the default timeout period for data loading during origin-pull is 10 seconds. If the origin-pull duration exceeds the aforementioned time limits, failures will often occur.

You can adjust the timeout periods for origin-pull TCP connection and data loading according to your origin server data processing conditions and network environment so as to ensure normal origin-pull.

Configuration Guide

Viewing the configuration

Log in to the [CDN Console](#), select **Domain Management** on the left sidebar, and click the domain name to enter its configuration page. You will find the origin-pull timeout configuration on the **Origin Configuration** tab. By default:

The TCP connection timeout period is 5 seconds.

The origin-pull loading timeout period is 10 seconds.

Origin pull timeout configuration

According to the origin site status and service characteristics, customize the TCP connection timeout and load time for origin-pull requests. [What is the origin-pull timeout configuration?](#)

Default Configuration

TCP connection time 5 seconds [Edit](#)

Origin-pull load time 10 seconds [Edit](#)

Modifying the configuration

You can click **Edit** on the right to modify the corresponding timeout period as needed:

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

Modify origin-pull timeout time ✕

TCP connection time (unit: second)

TCP connection timeout time can be set to a positive integer between 5 and 60

OK Cancel

The origin-pull loading timeout period can be set to 5–60 seconds.

Modify origin-pull timeout time ✕

Origin-pull load time (unit: second)

Origin-pull load time can be set to a positive integer between 5 and 60

OK Cancel

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.

Request Header Configuration

Last updated : 2024-12-30 21:37:31

Configuration Overview

Tencent Cloud CDN supports adding origin-pull request headers:

Carries the real client IP to the origin server through the `X-Forwarded-For` header.

Carries the real client port to the origin server for analysis through the `X-Forward-Port` header.

Adds custom headers.

You can also set and delete custom origin-pull request headers.

Configuration Guide

Viewing the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and then click **Manage** on the right of a domain name to enter its configuration page. Select the **Origin-pull Configuration** tab to find the **Origin-pull Request Header Configuration** section. The feature is disabled and not pre-configured by default.

Origin-pull Request Header Configuration

Adding the header to carry the client IP, port, or to identify CDN service for origin-pull.[What's request header configuration?](#)

Request Header

The configuration below can be modified when it is disabled, but the configuration will not be deployed officially until it is enabled.

Add Origin-pull Header Rule

Adjust Priority

Rule Type	Rule Content	Header Parameter	Header Value	Operation
No data yet				

Operation

Operation	Description
Set	Sets the value of a specified request header parameter.

	<p>If the target header does not exist, a new one will be added.</p> <p>If the origin-pull request header parameter already exists, the new request header will overwrite the old one as duplicate headers are not allowed.</p>
Add	<p>Adds a specified origin-pull request header parameter.</p> <p>If the target header already exists, the new request header will overwrite the old one as duplicate headers are not allowed.</p>
Delete	<p>Deletes a specified request header parameter.</p>

Note:

Rules are executed from bottom to top, and the priority is meaningful for the same type of operations only, that is, the priorities of multiple "Set", "Add", and "Delete" rules are independent.

If an origin-pull request header parameter is configured with multiple rules of different operations, the operations will be conducted in the order of "Add", "Delete", and "Set". For example, if the header `X-CDN` is configured with rules of "Add", "Delete", and "Set", it will be added, then deleted, and finally set.

Header parameter

Header Parameter	Description
X-Forwarded-For	The header used to carry the real client IP. Its value defaults to <code>\$client_ip</code> variable, which cannot be modified.
X-Forward-Port	The header used to carry the real client port. Its value defaults to <code>\$remote_port</code> variable, which cannot be modified.
Custom header	<p>Key: 1 to 100 characters, including digits (0 - 9), lowercase letters (a - z), uppercase letters (A - Z), and hyphens (-).</p> <p>Value: 1 to 1000 characters. Chinese characters are not supported.</p> <p>Some standard headers cannot be set, added, or deleted by the user. For the detailed list, please see Notes.</p>

Note:

Up to 10 origin-pull request header rules can be configured.

Supported rule types: all content, specified file type, specified folder, and specified file. Regex match is currently not supported.

Configuration Samples

The origin-pull request header configuration of the acceleration domain name `cloud.tencent.com` is as follows:

Origin-pull Request Header Configuration

Adding the header to carry the client IP, port, or to identify CDN service for origin-pull. [What's request header configuration?](#)

Request Header ☒

The configuration below can be modified when it is disabled, but the configuration will not be deployed officially until it is enabled.

Add Origin-pull Header Rule

Adjust Priority

Rule Type	Rule Content	Header Parameter	Header Value	Operation
All Content	*	X-Forward-For	\$client_ip	Modify Delete
File ext	mp4	x-cdn	TencentCloud	Modify Delete
File Directory	/test	x-cdn	Tencent	Modify Delete

If the accessed resource is `http://cloud.tencent.com/test/test.mp4`, then:

1. It hits the `*` rule, so the header `X-Forwarded-For:$client_ip` will be added, and `$client_ip` will be replaced with the real client IP during origin-pull.
2. It hits both the `.mp4` file type rule and `/test` path rule. The two rules are of the same type, "Add". As the lower rule has the higher priority, the header `x-cdn:Tencent` is added.

Notes

In origin-pull request header rules, the following standard headers currently cannot be set, added, or deleted:

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
referrer-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 Rewrite Configuration

Last updated : 2024-12-31 14:19:23

Overview

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.

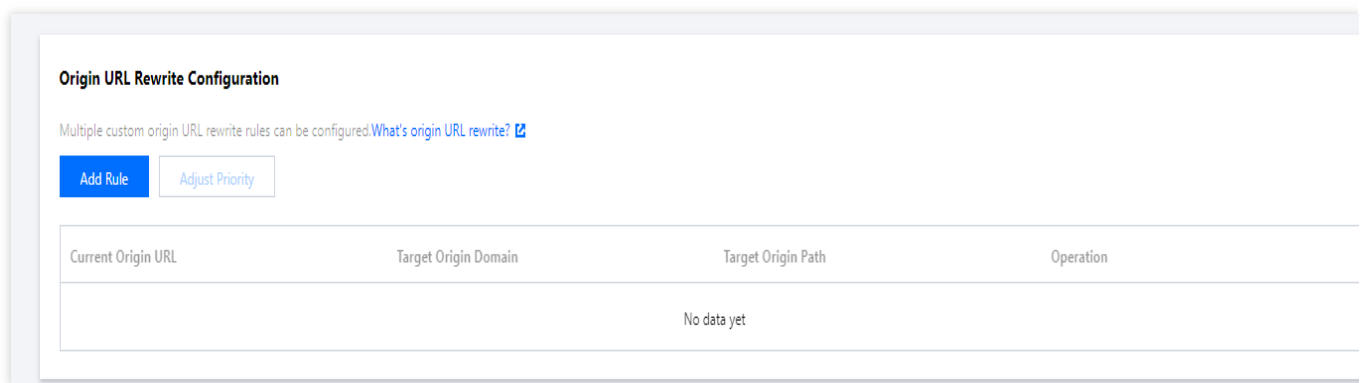
Note:

This feature is not available for ECDN domain name.

Directions

Viewing the configuration

Log in to the [CDN Console](#), select **Domain Management** on the left sidebar, click **Manage** on the right of a domain name to enter its configuration page, and switch to the **Origin-pull Configuration** tab to find the **Origin URL Rewrite Configuration** section.



Adding rules

You can click **Add Rule** to add rewrite rules as needed.

Add Origin URL Rewrite Rule ×

Current Origin URL

Starting with "/"; supporting full-path matching (e.g., /test/a.jpg) and wildcard (*) matching (e.g., /test/*/*.jpg).

Target Origin Domain

www.test.com

Please enter the target origin domain (excluding "http://" or "https://").

Target Origin Path

Starting with "/" (e.g., /newtest/b.jpg); the wildcard "*" can be caught with "\$n" (e.g., if n=1,2,3... then /newtest/\$1/\$2.jpg).

Save

Cancel

Configuration limitations

Each domain name can have up to 100 rewrite rules.

You can adjust the priority for multiple rules. Rules at the bottom of the list have higher priority.

Current Origin URL: starting with "/"; prefix matching is used by default; supporting full-path matching (e.g., /test/a.jpg) and wildcard (*) matching (e.g., /test/*/*.jpg). If you want to specify a file directory, you cannot end the path with "/" (e.g., /test).

Target Origin Domain: the current domain name is used by default (excluding "http://" and "https://"). You can modify it as needed.

Target Origin Path: starting with "/" (e.g., /newtest/b.jpg); the wildcard "*" can be captured with "\$n" (e.g., if n=1,2,3... then /newtest/\$1/\$2.jpg). If you want to specify a file directory, you cannot end the path with "/" (e.g., /test).

Up to 5 "*" and 10 "\$n" are supported.

The target origin domain can contain up to 250 characters. Other content can contain up to 1,024 characters.

Configuration Samples:

Suppose the **Origin URL Rewrite Configuration** of the acceleration domain name www.test.com is as follows:

The origin-pull will be rewritten as follows:

In case `www.test.com/images/1.jpg` is requested, the request hits the first, second and third rule. As rules are executed from the bottom to top, the URL will be re-written to `www.test.com/index.html`.

In case `www.test.com/images` is requested and the request hits the second rule, the URL will be rewritten to `www.test.com/goodboy.html`.

Origin-pull SNI

Last updated : 2024-12-30 21:38:34

Overview

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.

Note:

Only domain names accelerated in the Chinese mainland are supported.

This feature may be unavailable in some platforms. We will complete server upgrade as soon as possible.

Directions

Viewing the configuration

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

Editing the configuration

After it's enabled, you need to specify a domain name and the configuration will then take effect. When the configuration switch is off, the configuration will not be deployed.

Merging Requests

Last updated : 2024-12-30 21:39:18

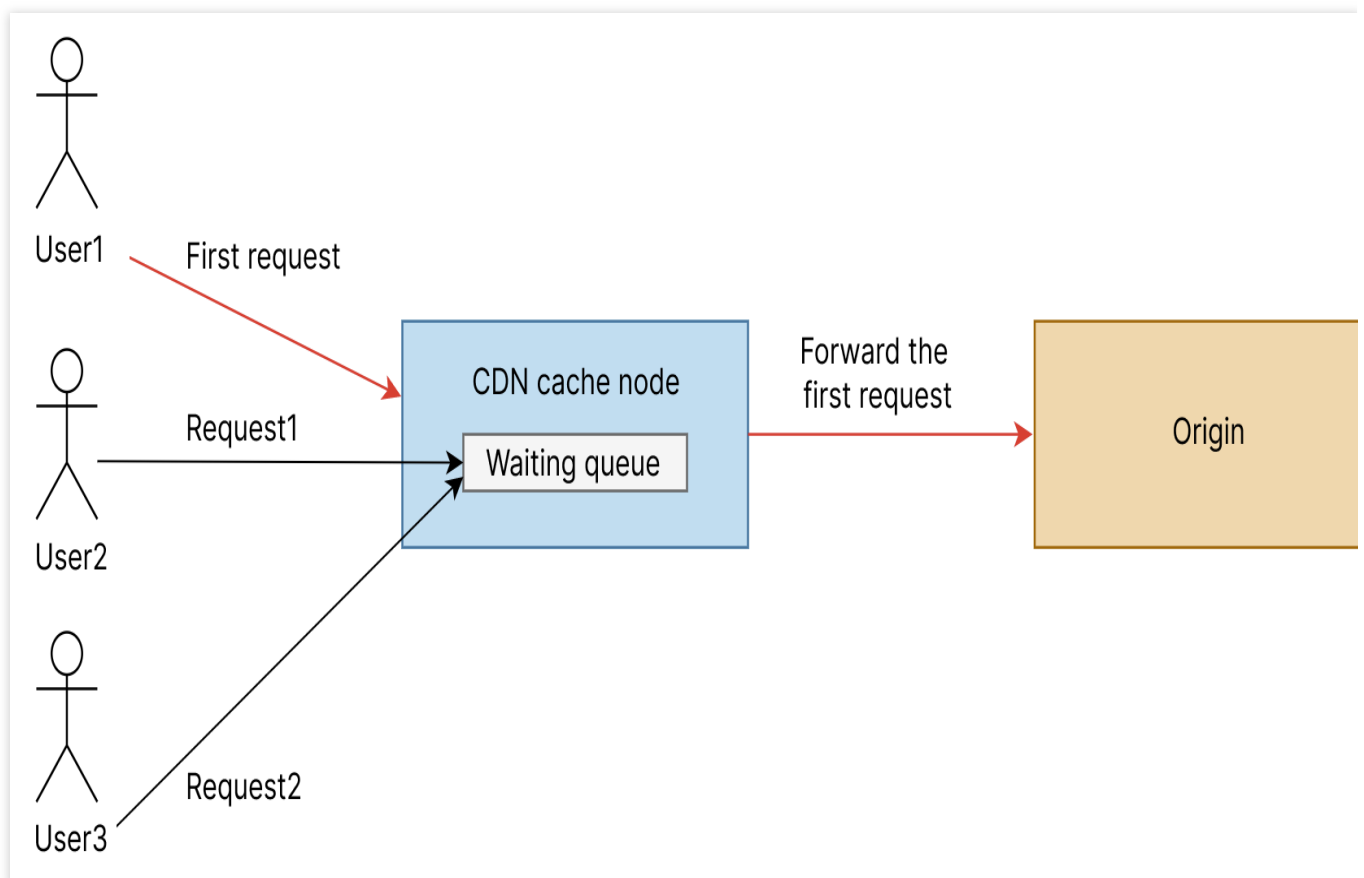
Origin-pull merging can help increase the cache hit rate, so as to lower the load pressure during peak hours like big online promotion events.

Description

When multiple users request for the same resource that is not cached on the cache node, all requests are forward to the origin, leading to soaring bandwidth and connections. A slow or failed origin response that could affect access experience may even occur if the origin server reaches the performance limit.

When origin-pull merge is enabled, only one request is forwarded to the origin to retrieve the requested resource. Other similar requests are hold till the resource is ready on the cache node.

The following figure shows how this feature works. Three requests are sent to the same cache node requesting for the same resource. The first request is forwarded to the origin. The resource is then returned to the requester and cached on the cache node. Now, other awaiting requests can get the resource from the cache.



Limits

1. It only supports response status code 200, 206 and 304.
2. Unsupported caching headers: "cache-control: no-cache", "no-store", "private" and "pragma: no-cache".
3. Unsupported data transfer methods: Chunked transfer encoding.
4. Supported HTTP request methods: GET.
5. "content-length" and "transfer-encoding" must be present in the HTTP response header.
6. Unsupported compression methods: Gzip and Brotli.

Configuration

1. Log in to the [CDN console](#).
2. Click **Domain Management** on the left sidebar to enter the domain name management list.
3. Select the target domain name and click **Manage** to enter the domain name configuration page.
4. Click the **Origin-pull Configuration** tab and find **Origin-pull merge**.
5. Origin-pull merge is disabled by default. You can enable it as needed.

Configuration Sample

The following configuration sample shows how to enable origin-pull merge.

HTTPS Configuration

HTTPS Configuration

Last updated : 2024-12-30 21:39:37

If you need to configure an existing certificate for your domain name, please see below. If the certificate you configure is from Tencent Cloud SSL Certificates Service, you can skip this step.

Uploading Certificate

Generally, CAs provide the following types of certificates, and **Nginx** is used by CDN.

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

Certificate

Common certificate extensions include ".pem", ".crt", and ".cer". Open the certificate file in a text editor and you can see content similar to the one shown 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
tTELMAkGA1UEBhMCVVMxZzAVBgNVBAAoTD1Zlcm1TdWduLmNvLnVzLnVzLnVzLnVz
ExZWZlZjU2LmNvLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVz
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMm
VmVyaVnVpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMmVmVyaVnVpZ24uY29tL3Jw
YSoAYykwOTEvMC0GA1UEAxMmVmVyaVnVpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMm
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
V2FzaGluZ3RvbjEQA4GA1UEBhMCVVMxZzAVBgNVBAAoTD1Zlcm1TdWduLmNvLnVzLnVz
bSBzBjbmMuRowGAYDVQQDFBFPYXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSo
AQEFAAQBJQAwYkCgYEA3Xb0EGea2d88QGEUwLcEpwGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8QwSAdk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wbFqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWn0uIVGdg76626gg0oJSaj48R2n0MnVcC
AwEAAaOCAdEwggHMAkGA1UdEwQCAAwCwYDVR0PBAQDAgMEUUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVlJTZW1Zlcm1TdWduLmNvLnVzLnVzLnVzLnVzLnVzLnVz
ZW1Zlcm1TdWduLmNvLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVz
BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBggrBgEFBQcDAjAFBgNVHSMEGDAwBS17wsRzsBBA6NKZ2B1shzgVy19
RzB2BggrBgEFBQcBAQRMGgwJAYIKwYBBQUHMAAGGh0dHA6Ly9vY3NwLnVzLnVzLnVz
aWduLmNvLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVzLnVz
aXNpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMmVmVyaVnVpZ24uY29tL3JwYSo
WDBWFglpbWFnZS9naWYwITAFMACGBSs0AwIaBBRLa7kolgYMu9BS0JsprEsHiyEF
GDAmFiRodHRwOi8vbG9nb3Z2ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
hvcNAQEFBQADggEBALpFBXeg782QsTtGwEE9zBcVCuKjrsL3dWK1dFq30P4y/Bi
ZBYEyw8t8zNuYFUE25Ub/zmvmp7p0G76tmQ8bRp/4qkJoISesHJvFgJ1mksr3IQ
3gaE1a2BSUIHxGLn9N4F09hYwwbeEZAcfBgBiLdEiodNwzcvGJ+2LLDWGJOGnNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcFA4uhwMDSe0nynbn
1qiWk450mCOnqH4ly4P41Xo02t4A/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 manually splice the server certificates and intermediate certificates 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.

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

A certificate chain from an intermediate CA comes in this format:

```

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

```

Private key

Common private key extensions include ".pem" and ".key". Open the private key file in a text editor and you will see content similar to the one shown below.

A ".pem" private key begins with "-----BEGIN RSA PRIVATE KEY-----" and ends with "-----END RSA PRIVATE KEY-----". Every line in between contains 64 characters, while the last line may have less than 64 characters.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAyZiSSSCHH67bmT8mFykAxQ1tKCYukwBiWZwk0StFEbTWHy8K
tTHSFD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A
Xw9SgrqFJMJC Lva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ
/fD0XXyuWoqaIePZtK9Qnjn957ZEPHjtUpVZuhS3409DDM/tJ3T18aaNYWhrPBc0
jNcz0Z6XQGf1rZG/Ve520GX6rb5dUYpdcfXzN5NM6xYg8a1L7UHDHHPi4AYsatdG
z5TMPnmEf8yZPUYudTLxgMVAovJr09Dq+5Dm3QIDAQBAoIBAGL68Z/nnFyRHRFi
laF6+Wen8ZvNqkm0hAMQwIJh1Vp1fL74//8Qyea/EvUtuJHyB6T/2PZQoNVhxe3S
cgQ93Tx424WGPcwUshSfxewFbAYGf3ur8W0xq0uU07BAxaKHnCMNG7dGyo1UowRu
S+yXLRpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2
06W/zHZ4YAxwkTYLKGHjoieYs111ahLAJvICVgTc3+LzG2pIpM7I+K0nHCSeswM
i5x9h/OT/ujZsyX9P0PaAyE2bqy0t080tGexM076Ssv0KVhKFvWjLUnhf6WcqFCD
xqhhxkECgYEA+PftNb6eyXl+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhqqHu0edU
ZXIHrJ9u6B1XE1arpijVs/WHmFhYSTm6DbdD7S1tLy0BY4cPTRhziFTKt8AkIXMK
605u0UiWsq0Z8hn1Xl4lox2cW9ZQa/Hc9udeyQotP4NsMJWgpBV7tC0CgYEAwvNf
0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzFEG8/AR3Md2rhmiZi
GnJ5fdfe7uY+JsQFX2Q5JjwTadlBW4led0Sa/uKRao4UzVgnYp2aJKxtuWfFvVbU
+kf728ZJRA6azSLvGmA8hu/GL6bgfU3fkSkw03ECgYBpYK7TT7JvvnAErMtJf2yS
ICRkQaB3gPSe/lCgzy1nhtaFOUbNxeuowLAZR0wrz7X3TZqHEDcYoJ7mK346of
QhGLITyoeHkbYkAUtq038Y04EKH6S/IzMzB0frXiPKg9s8UKQzkU+GSE7ootli+a
R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUHKIKcP/+xn
R3kVl06MZCfAdqirAjiQwApkh9Bxbp2eHCrB8lMFAWLRQSlOk79b/jVmTZMC3upd
EJ/iSWjZKPbw7hCFAeRtPhxyNTJ5idEiu9U8EQid811giPgn0p3sE0HpDI89qZX
aaIMEQKBgQDK2bsnzE9y0ZWhGTeu94vziKmFrSkJMGH8pLaTiliw1iRhRYWJysZ9
B0IDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcv0Bh5Hx0yy23m9hFRzfDeQ7z
NTKh193HHF1joNM81LHFyGRFEWWrroW5gfBudR6USRnR/6iQ11xZXw==
-----END RSA PRIVATE KEY-----
```

If your private key begins with "-----BEGIN PRIVATE KEY-----" and ends with "-----END PRIVATE KEY-----", we recommend you convert the format using OpenSSL with the following command:

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

Converting other formats to PEM

Currently, CDN only supports certificates in PEM format. Certificates in other formats need to be converted to PEM format. We recommend you use OpenSSL. The following shows how to convert some common formats to PEM.

DER to PEM

DER format is generally used on Java platforms.

Certificate conversion:

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

Private key conversion:

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

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 content of the PEM certificate.

Private key conversion: private keys can generally be exported on IIS servers.

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 certificate chain

When configuring a private certificate, you may encounter an issue that the **certificate chain cannot be completed**, as shown below.

In this case, you can paste the certificate content (in PEM format) issued by the CA after the domain name certificate (in PEM format) to complete the certificate chain. You can also submit a ticket for assistance.

Hosted Certificate

Tencent Cloud provides a certificate hosting service: [SSL Certificates Service](#). 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.

SSL Certificates Service provides you with 20 DV SSL certificates issued by TrustAsia free of charge.

HTTPS Configuration Guide

Last updated : 2024-12-30 21:39:54

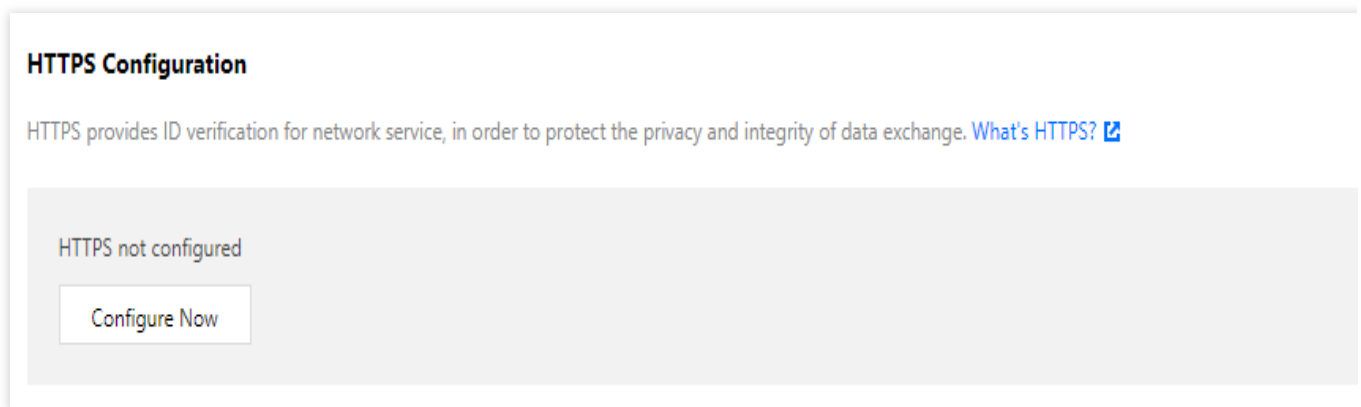
Configuration Overview

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.

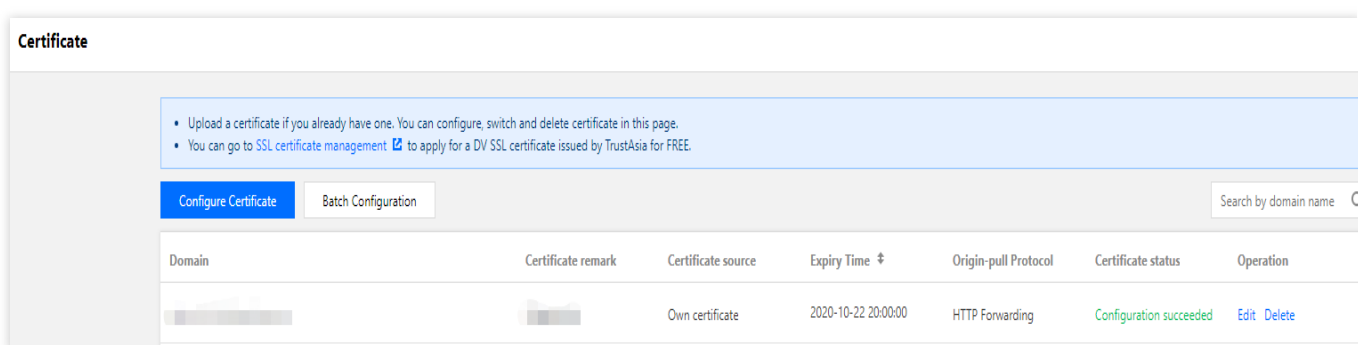
Configuration Guide

Viewing the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, click **Manage** on the right of a domain name to enter its configuration page, and open the **HTTPS Configuration** tab.



You can select **Certificate Management** on the left sidebar to view all domain names configured with HTTPS acceleration under your account.



Configuring a certificate

1. Select a domain name

On the **Certificate Management** page, click **Configure Certificate** and select the acceleration domain name to be configured with a certificate:

The status of the acceleration domain name needs to be "Deploying" or "Enabled". Disabled domain names cannot be configured with HTTPS acceleration.

Domain names suffixed with `.file.myqcloud.com` are the default acceleration domain names of Tencent Cloud COS and can use HTTPS acceleration without configuring any certificates.

Domain names suffixed with `.image.myqcloud.com` are the default acceleration domain names of Tencent Cloud CI and can use HTTPS acceleration without configuring any certificates.

The certificate can be deployed to the following domains. The new certificate will be deployed to all service regions of selected CDN domains.

Select the domain you want to configure certificate

Domain

Enter keywords/Select from dro... ▼

2. Select a certificate

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

CDN supports ECC certificate deployment.

The certificate content must be in PEM format. If not, please see [Converting other formats to PEM](#).

You can select a certificate hosted by Tencent Cloud for quick deployment.

Select a certificate

Certificate source

☒ Own certificate ☐ Tencent Cloud Hosting Certificate

Certificate Content

PEM code

[View examples](#)

Private key contents

PEM code

[View examples](#)

Remark (optional)

Please enter remark contents

Configuring in batches

Click **Batch Configuration** at the top. You can upload certificates to automatically match domain names for batch configuration:

1. Select a certificate

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

CDN supports ECC certificate deployment.

The certificate content must be in PEM format. If not, please see [Converting other formats to PEM](#).

You can select a certificate hosted by Tencent Cloud for quick deployment.

1 Upload Certificate

2 Associate domain name, select origin-pull protocol

3 Done

- The certificate can be deployed to the following domains. The new certificate will be deployed to all service regions of selected CDN domains.
- You can only configure certificates for acceleration domain in the status of "Deploying" and "Activated".

Certificate source

☒ Own certificate ☐ Tencent Cloud Hosting Certificate

Click [SSL certificate management](#) to view details of your hosting certificates or apply for a FREE one

Certificate Content

PEM code

[View examples](#)

Private key contents

PEM code

[View examples](#)

Remark (optional)

Please enter remark contents

Next

2. Select 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:

Select a bound domain name

Associate with Domain ☐ Display only domain names with SSL certificates

<input type="checkbox"/>	Domain	Certificate status	Expiry Time
No available domain names			
Selected 0 items, Total 0 items			

Changing a certificate

Modifying a certificate

Click **Edit** on the right of a certificate to update it for the specified domain name. You can also configure certificates in batches again to override the original certificate configurations.

Domain	Certificate remark	Certificate source	Expiry Time [⚙]	Origin-pull Protocol	Certificate status	Operation
		Own certificate	2020-10-22 20:00:00	HTTP Forwarding	Configuration succeeded	Edit Delete
		Own certificate	2020-10-22 20:00:00	HTTP Forwarding	Configuration succeeded	Edit Delete

Certificate updates will seamlessly take effect on nodes one by one across the entire network without affecting the HTTPS service in the production environment. You can also click **Delete** to cancel the HTTPS acceleration service.

Certificate expiration

Tencent Cloud will send you expiration reminders through SMS, email, and the Message Center 30, 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.

Region-specific configuration

If your domain name is configured for global acceleration, the configured HTTPS certificate will take effect globally.

Currently, the certificates configured for the regions in and outside the Chinese mainland must be the same.

If a domain name has different certificates in/outside the Chinese mainland, you will see Chinese mainland and outside Chinese mainland tags on the **Certificate Management** page, which indicate that the domain names with tags have different legacy configurations.

Under the **Advanced Configuration** tab of the domain name, you can also see two configurations:

Forced Redirection Configuration

Last updated : 2024-12-30 21:40:10

Configuration Overview

Tencent Cloud CDN supports HTTPS/HTTP forced redirection.

If a domain name is configured with a certificate for HTTPS acceleration, you can specify the 301/302 redirection method to force all HTTP requests at the CDN node to be HTTPS requests.

You can also specify the 301/302 redirection method to force all HTTPS requests at the CDN node to be HTTP requests.

Configuration Guide

Configuration limitations

HTTPS acceleration must be enabled for configuring HTTPS forced redirection.

Configuration instructions

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, click **Manage** on the right of a domain name to enter its configuration page, and open the **HTTPS Configuration** tab to find the **Forced Redirection** section. The feature is disabled by default.

Forced Redirection

Users' access requests will be forcibly redirected to HTTPS or HTTP as configured. [What's HTTPS forced redirection?](#)

Redirection Configuration



Toggle it on, and configure the redirection type, method:

Redirection Type Configuration ✕

Redirection Type

☒ **Https->Http** ☐ **Http->Https**

Redirection Method

☐ **301 Redirection** ☒ **302 Redirection**

Confirm

Cancel

Finally, click **Confirm** to deploy the configuration:

Forced Redirection

Users' access requests will be forcedly redirected to HTTPS or HTTP as configured.[What's HTTPS forced redirection?](#) 🔗

Redirection Configuration ☒ [Edit](#)

Redirection Type

Https->Http

Redirection Method

302 Redirection

HTTP2.0 configuration

Last updated : 2024-12-30 21:40:24

Configuration Overview

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 the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. Open the **HTTPS Configuration** tab to find the **HTTP2.0 Configuration**, which is enabled by default.

HTTP2.0 Configurations

Please configure a HTTPS certificate first to enable this configuration. [What's HTTP2.0?](#) 


HTTP2.0



Modifying the configuration

Toggle the switch to enable or disable HTTP2.0. If the domain name certificate is deleted, HTTP2.0 will be automatically disabled.

HTTP2.0 Configurations

Please configure a HTTPS certificate first to enable this configuration. [What's HTTP2.0?](#) 

HTTP2.0



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 Configuration

Last updated : 2024-12-30 21:40:39

Overview

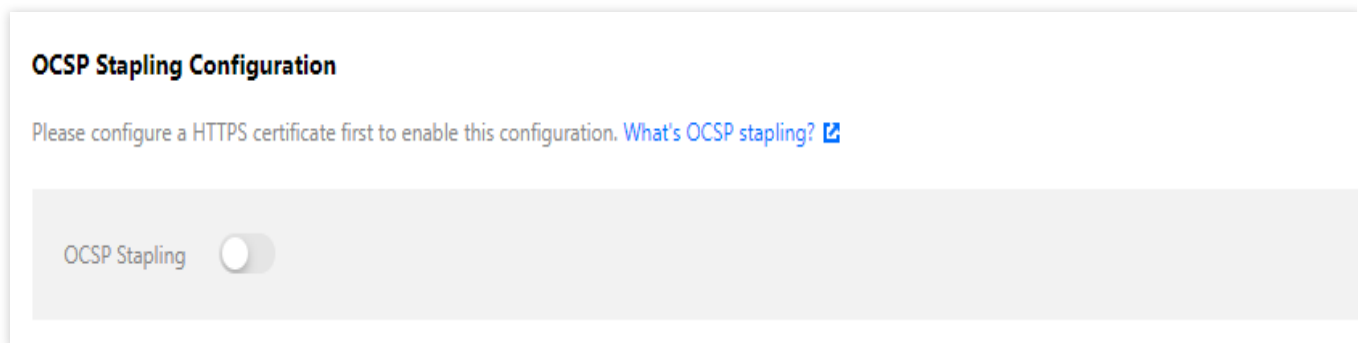
After OCSP stapling (a TLS certificate status query extension) is enabled, the server will send a pre-cached Online Certificate Status Protocol (OCSP) response during the TLS handshake for user verification, so that the user does not need to send a query request to the certificate authority (CA). OCSP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

Tencent Cloud CDN allows you to enable/disable OCSP stapling.

Directions

Viewing the configuration


Log in to the [CDN Console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of the domain name to access its configuration page. Under the **HTTPS Configuration** tab, find **OCSP Stapling Configuration**, which is disabled by default:



Modifying the configuration

If a domain name has been configured with HTTPS acceleration, you can directly toggle the OCSP stapling switch to enable/disable this feature. After the certificate configuration is deleted, OCSP stapling will automatically be invalidated:

OCSP Stapling Configuration

Please configure a HTTPS certificate first to enable this configuration. [What's OCSP stapling?](#) 

OCSP Stapling



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.

HSTS Configuration

Last updated : 2024-12-30 21:40:54

Configuration Overview

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.

Configuration Limitations

`expireTime` can range from 0 to 365 days and is configured in seconds.

Check `includeSubDomain` if you need to include sub-domain names.

To enable HSTS configuration, HTTPS acceleration configuration must be completed first.

After the HSTS configuration is enabled, we recommend enable [Forced Redirection Configuration](#) to redirect HTTP requests to HTTPS requests. Otherwise the browser will not create HSTS cache for HTTP requests.

Configuration Guide

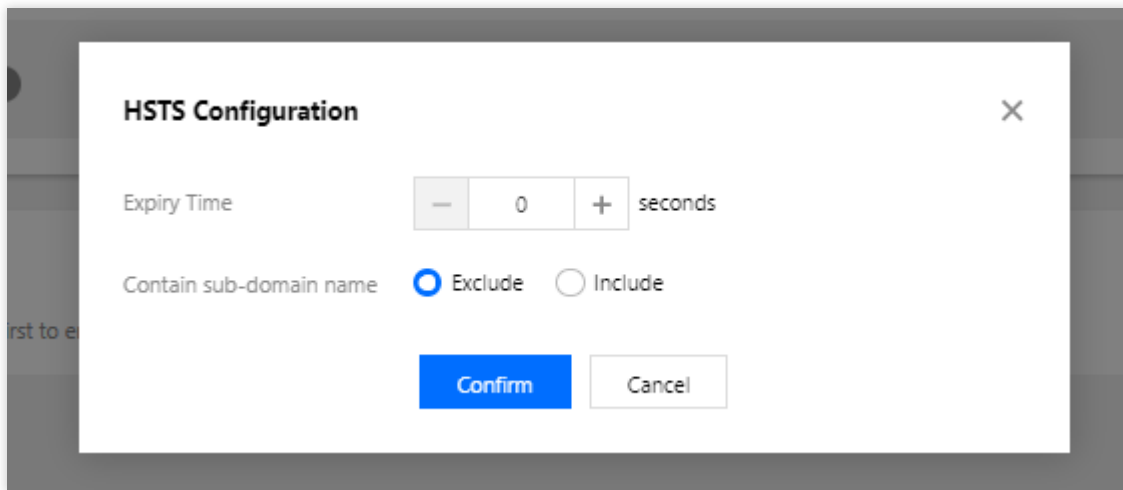
Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. Open the **HTTPS Configuration** tab to find the **HSTS Configuration** section. It is disabled by default.

HSTS Configuration

Enabling HSTS configuration as needed. After enabling it, the header Strict-Transport-Security will be added to CDN response.[What's HSTS configuration?](#) 

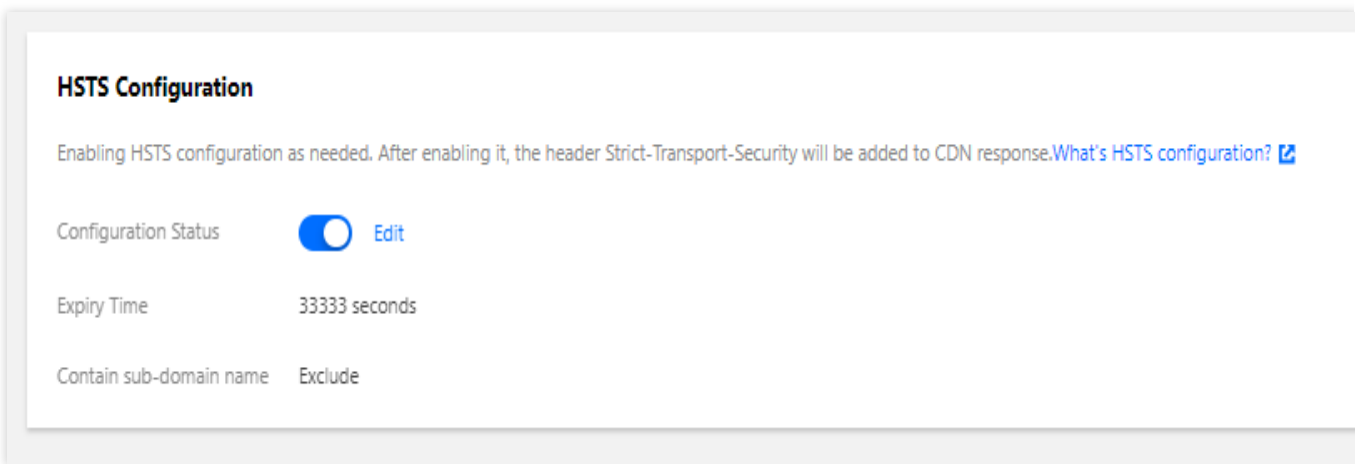
Configuration Status ☐

Toggle it on and configure accordingly:



The screenshot shows a modal dialog titled "HSTS Configuration" with a close button (X) in the top right corner. Inside the dialog, there are three configuration options: "Expiry Time" with a numeric input field set to "0" and a "seconds" label, "Contain sub-domain name" with two radio buttons, "Exclude" (which is selected) and "Include", and two buttons at the bottom: "Confirm" (in blue) and "Cancel" (in white with a grey border).

Click **Confirm** to apply the configuration to the response header. You can click **Edit** to modify it later.



The screenshot shows a settings page titled "HSTS Configuration". Below the title is a descriptive text: "Enabling HSTS configuration as needed. After enabling it, the header Strict-Transport-Security will be added to CDN response. [What's HSTS configuration?](#)". Below this text are three rows of configuration details: "Configuration Status" with a blue toggle switch and an "Edit" link, "Expiry Time" with the value "33333 seconds", and "Contain sub-domain name" with the value "Exclude".

Configuration Sample

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

HSTS Configuration

Enabling HSTS configuration as needed. After enabling it, the header Strict-Transport-Security will be added to CDN response. [What's HSTS configuration?](#)

Configuration Status ☒ Edit

Expiry Time 2 seconds

Contain sub-domain name Exclude

The response header is:

x	Headers	Preview	Response	Initiator	Timing
	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 : 2024-12-30 21:41:11

Feature Overview

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:

Make sure the HTTPS certificate is properly configured.

TLS version configuration is now only available in the Chinese mainland regions. If the acceleration region of a domain name is "Global", then the configuration changes will take effect only in the Chinese mainland.

This feature may be unavailable in some platforms. We will complete server upgrade as soon as possible.


Configuration Guide

Viewing configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, click **Manage** on the right of a domain name to enter its configuration page, and open the **HTTPS Configuration** tab to find the **TLS Version Configuration** section.

By default, TLS 1.0/1.1/1.2 are enabled and TLS 1.3 is disabled.

TLS Version Configuration

CDN enables TLS 1.0/1.1/1.2 by default. You can disable or enable TLS versions as needed.[What's TLS version configuration?](#) 

TLS 1.0 Enabled | TLS 1.1 Enabled | TLS 1.2 Enabled | TLS 1.3 Not enabled

[Modify Configuration](#)

Modifying configuration

Open **Modify Configuration** to enable and disable TLS versions as needed.

Modify TLS Version Configuration ✕

i Only a single version or multiple successive ones can be enabled, i.e., skipping version 1.1 to enable 1.0 and 1.2 is not allowed. At least one version must be enabled.

Select desired versions to enable: ☒ TLS 1.0 ☒ TLS 1.1 ☒ TLS 1.2 ☐ TLS 1.3

OK

Cancel

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.

At least one version must be enabled.

QUIC

Last updated : 2024-12-30 21:42:57

Announcement :

Tencent Cloud CDN will officially launch QUIC support on January 5, 2022.

QUIC support is billed based on the number of QUIC requests. For more details, see [Billing Overview](#).

We will notify you in advance of your subscription being billed. Please pay attention to our announcements in the console and documentation.

Feature Overview

Quick UDP Internet Connections (QUIC) is a common network protocol, which guarantees network security and reduces the latency in transfer and connections to prevent network congestion. You can enable QUIC protocol for clients to access CDN nodes with enhanced data transfer security and access efficiency.

For now, the supported QUIC versions include draft h3-28, h3-Q050, h3-Q046, h3-Q043, Q046, and Q043.

Directions

1. Enable QUIC:

After adding a domain name, you can click **Domain Management** on the left sidebar, in the domain name details page, select **HTTPS Configuration > QUIC configuration**. QUIC is disabled by default, and you can enable it manually.

Note: An HTTPS certificate is required to enable QUIC.

QUIC Charged

Quick UDP Internet Connections (QUIC) guarantees network security and reduces the latency in transfer and connections to prevent network congestion. [What's QUIC](#)

This is a value-added item. It's billed based on the number of QUIC requests. [Billing description](#)

QUIC ☒ Enable it to access CDN over QUIC

Note:

Switching service types concerns resource scheduling between platforms. We recommend not switching service types for domain names after enabling QUIC.

QUIC requests cannot be forwarded to the origin.

QUIC is only partially supported for now.

Use Limits:

QUIC is now not available for on-demand video streaming acceleration.

QUIC cannot be enabled for any domain names with IPv6 enabled.

2. Disable QUIC:

You can go to **Domain Management** > **HTTPS Configuration** > **QUIC**, and disable QUIC.

Billing

QUIC support 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 Overview](#).

FAQs about HTTPS

Last updated : 2024-12-30 21:43:15

What is HTTPS?

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

Does CDN support HTTPS configuration?

Yes. Tencent Cloud CDN fully supports HTTPS configuration. You can either upload your own certificate for deployment or go to the [SSL Certificate Service console](#) to apply for a free third-party certificate provided by TrustAsia.

How do I configure an HTTPS certificate?

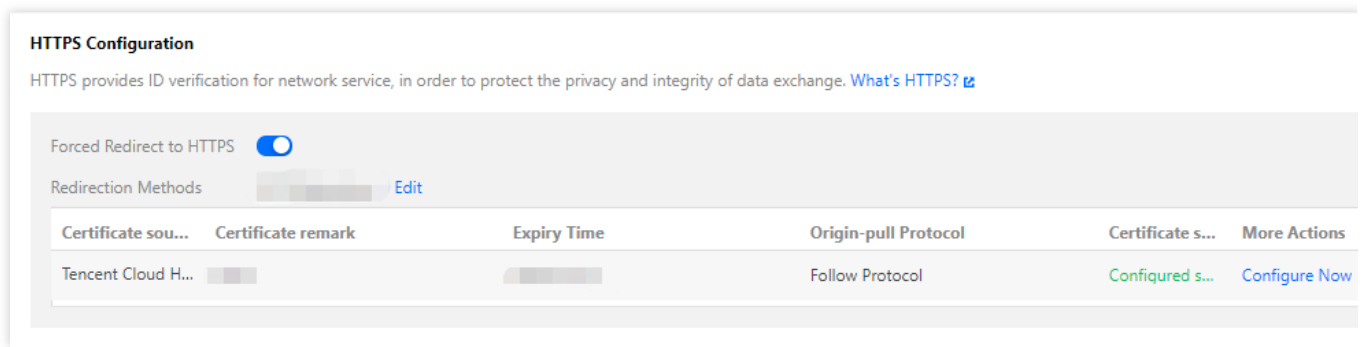
You can configure an HTTPS certificate in the [CDN console](#). For detailed directions, please see [HTTPS Configuration Guide](#).

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.

Can I deny HTTP access and allow HTTPS access only?

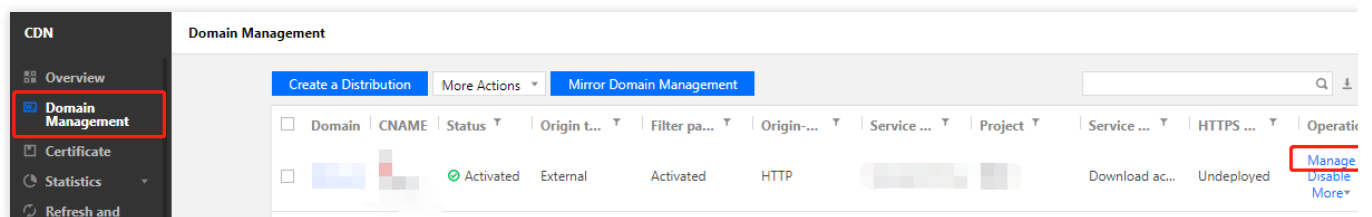
Yes. After successfully configuring an HTTPS certificate, you can use the [Forced Redirection](#) feature. HTTP requests from users will be forcibly redirected to HTTPS requests.



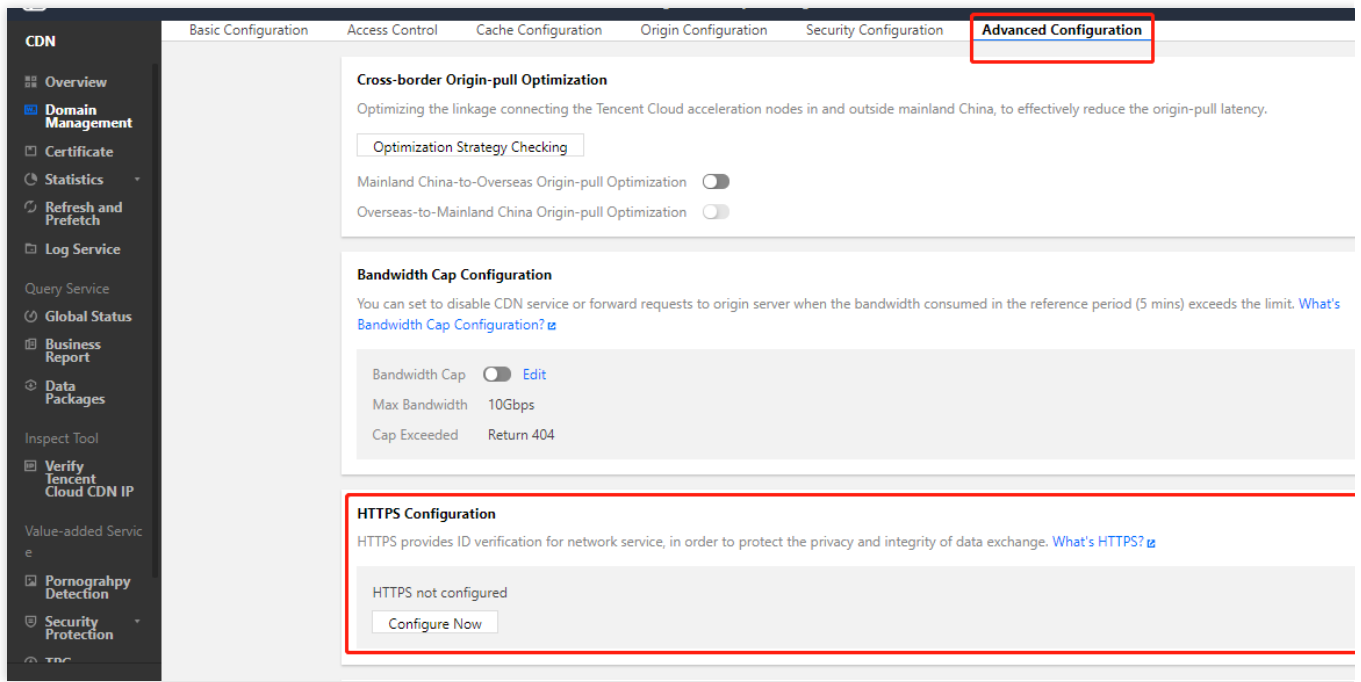
Why does HTTPS access not work after CDN is configured?

For HTTPS access, please configure it as instructed:

1. Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its management page.



2. Open the **Advanced Configuration** tab to find the **HTTPS Configuration** section, and click **Configure Now** to go to the **Certificate Management** page. For configuration directions, please see [HTTPS Configuration Guide](#).



HTTPS access can be enabled after the certificate is successfully configured.

Advanced Configuration

Usage Limit Configuration

Last updated : 2024-12-30 21:44:46

Overview

If you worry about high fees incurred by high bandwidth or traffic usage due to hotlinking by malicious users, you can use the usage limit feature to control the usage.

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 bandwidth cap is exceeded, you can disable CDN to avoid incurring more CDN service fees.

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 Prevention Solutions](#).

Directions

Viewing the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. You will find the **Usage Limit Configuration** on the **Advanced Configuration** tab, which is disabled by default.

Usage Limit Configuration

You can disable the CDN service when the resource usage in the sampling period exceeds the threshold. [About Usage Limit](#)

On/Off	<input checked="" type="checkbox"/> Edit
Type	Instantaneous bandwidth usage limit
Sampling period	Per 5 minutes
Threshold	10Gbps
Cap Exceeded	Return 404
Custom threshold	-


Detailed configuration items

1. Enabling the configuration

Toggle the switch on and configure the items:

Configure Usage Limit ×

×

- CDN service will be suspended if the consumption generated in the sampling period exceeds the threshold. You can activate the domain name again on the domain management page to recover the CDN service.
- The configuration may take effect in about 10 minutes, during which the traffic that exceeds the limit will incur charges. For more details, see [Attack Prevention Solutions](#) .
- For Tencent Cloud COS origins, you can only select "Return 404 (indicating CDN is disabled)"
- If you set a cumulative usage limit, usage data will be accumulated during a sampling period, and the collected data will be cleared once a new sampling period begins.

Statistic Type


☒ Instantaneous usage ☐ Cumulative usage

Accumulate the resource usage within the sampling period

Sampling period

Per 5 minutes


Threshold

Bandwidth 

−

10

+

Gbps 

Enter an integer in the range 1-10000.

You are now billed by traffic. It is recommended to set a traffic limit.

Limit Reached

☒ Return 404 (indicating CDN is deactivated)

CDN service will be suspended if the resource used by the domain name exceeds the threshold. You need to activate the domain name again on the domain management page to recover the CDN service.

Custom threshold

☐ Enable

The value can be 10% to 90%. When the ratio of Access bandwidth

The value can be 10% to 90%. When the ratio of actual bandwidth used/limit reaches this value, CDN will send an alarm message.

OK

Cancel

Statistic Type:

Instantaneous usage: It collects statistics on the traffic/bandwidth usage once every five minutes.

Cumulative usage: Compared with instantaneous usage, it supports a longer statistical period (every hour or calendar day).

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, or per day (before 24:00 of the day).

Note:

A statistical period starts from 5 minutes before the configuration time:

For example, if the rule is configured during 09:05:01–09:09:59, the statistical period will start from 09:05:00.

If **Per hour** is selected as the statistical period, (1) the first statistical period will be less than one hour; (2) starting from the next statistical period, usage statistics will be collected once every hour.

For example, if the rule is configured at 09:23:10 on January 13, 2022, the first statistical period will be 9:20:00–9:59:59, and the next one will be 10:00:00–10:59:59.

If **Before 24:00 of the day** is selected as the statistical period, the statistical period will be 09:20:00–23:59:59 on January 13, 2022.

Limit: Instantaneous usage supports both **Traffic** and **Bandwidth** options, while cumulative usage supports only **Traffic**.

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.

Unblocking period: **Scheduled unblocking** and **Never unblock** are supported.

Scheduled unblocking: 60 minutes, 12 hours, 24 hours, or 3 days.

For example, if the domain name `ex.com` is set to return 404 (CDN is disabled) after the limit is exceeded, and the automatic unblocking period is set to 60 minutes, then after the configured cumulative usage limit is exceeded, CDN will be disabled, and the acceleration domain name will be deactivated and will be automatically unblocked after 60 minutes.

Never unblock: If you worry that your domain name may be susceptible to high-traffic or high-bandwidth attacks, you can configure **Never unblock**. If the domain name is set to return 404 (CDN is disabled) after the limit is exceeded,

then after the configured cumulative usage limit is exceeded, the domain name will be deactivated, and you should manually enable domain name acceleration in the console if needed.

When cap is exceeded:

Return 404: After the cap is exceeded, CDN will be directly disabled for the domain name. In this case, you can go to the **Domain Management** page to activate the domain name again to resume the CDN service.

Note: If the **Origin Type** is **COS Origin** or **Third-Party Object Storage Origin**, only **Return 404** (CDN is disabled) is supported.

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:

If the detected domain name bandwidth (traffic) exceeds the threshold, the **Return 404** configuration needs to be delivered node by node across the entire network; therefore, there will be a certain delay for the configuration to take effect.

If the alarm threshold is enabled, as the scan interval is five minutes, if the usage surges or the configured percentage value is large, it may happen that the alarm threshold is not triggered during the previous scan, and the bandwidth cap is directly reached during the next scan. In this case, CDN will send alarm notifications of the percentage and the bandwidth cap successively.

2. Adding a region-specific configuration

If your acceleration domain name is configured for global acceleration and you want to configure different usage limits for acceleration in and outside the Chinese mainland, you can click **Add Special Configuration**.

Add Special Configuration

The special configuration is independent of the default configuration. You can add the special configuration for a specific service region (overseas/Chinese mainland).

Note:

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

Region-specific configuration is not supported for domain names with the acceleration type of dynamic content or dynamic & static content.

Configuration examples

Suppose the domain name `cloud.tencent.com` is configured for global acceleration, and a region-specific usage limit configuration (for regions outside the Chinese mainland) is added as follows:

Usage Limit Configuration

You can disable the CDN service when the resource usage in the sampling period exceeds the threshold. [About Usage Limit](#)

Chinese Mainland Configuration

On/Off ☒ [Edit](#)

Type Instantaneous bandwidth usage limit

Sampling period Per 5 minutes

Threshold 10Gbps

Cap Exceeded Return 404

Custom threshold -

Overseas Region Configuration

On/Off ☒ [Edit](#)

Type Instantaneous bandwidth usage limit

Sampling period Per 5 minutes

Threshold 15Gbps

Cap Exceeded Return 404

Custom threshold -

Mutual independence of configurations for regions in and outside the Chinese mainland: If **Outside Chinese mainland** is selected for the region-specific configuration, the initial configuration will take effect in the Chinese mainland. After the traffic from the Chinese mainland reaches 4 GB during a statistical period (5 minutes), the 404 error will be returned for all requests from the Chinese mainland, without affecting the service outside the Chinese mainland; after the traffic from outside the Chinese mainland reaches 11 GB during a statistical period (before 24:00 of the day), the 404 error will be returned for all requests from outside the Chinese mainland, without affecting the service in the Chinese mainland.

Acceleration region switch: If the acceleration region of a domain name is switched from global to Chinese mainland, the usage limit configuration for outside the Chinese mainland will be disabled by default and cannot be edited.

3. Disabling the configuration

You can toggle off the usage limit feature. Then, even if there is existing configuration at the bottom, it will not take effect in the production environment. If you toggle the switch on, a message will be displayed asking you whether to enable this feature before the configuration takes effect across the entire network.

HTTP Response Header

Last updated : 2024-12-30 21:45:03

Configuration Overview

When an end user requests a business resource, you can add a custom header in the returned **response message** to implement cross-origin resource sharing.

Response header configuration is of the domain name dimension, therefore, once the configuration takes effect, it will be synced to the response message of each resource under the domain name. Response header configuration only makes changes to the client (browser) response but not to the CDN node cache.

Directions

Viewing the configuration

Log in to the [CDN Console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. Open the **Advanced Configuration** tab to find the **Response Header Configuration** setting, which is disabled by default. You can click **Add Rule** to add HTTP response header rules.

Response Header Configuration

The configuration of response header may affect the responses from client programs (browser).[What's response header configuration?](#)

Configuration Status ☐

The configuration below can be modified when it is disabled, but the configuration will not be deployed officially until it is enabled.

Add Rule

Adjust Priority

Header Operation	Header Parameter	Header Value	Operation
No data yet			

Operation type

Operation	Description
Set	<p>Changes the value of a specified response header parameter.</p> <p>If the target header does not exist, it will be added after the change operation.</p> <p>If the header parameter already exists, all the duplicates will be changed and merged into one header. For example, after the rule "Set - <code>x-cdn: value1</code> " is configured, if a</p>

	request contains multiple <code>x-cdn</code> headers, the headers will be changed and merged into one header <code>x-cdn: value1</code> .
Delete	Deletes a specified response header parameter.

Note:

Some headers cannot be set or deleted in a self-service manner. For the detailed list, see [Notes](#).

Up to 10 HTTP response header rules can be configured.

Rule priority can be adjusted. Rules at the bottom of the list have higher priority. If a header parameter is configured with multiple rules, the bottom rule will take effect as rules are executed from bottom to top.

Header parameter

Header Parameter	Description
Access-Control-Allow-Origin	Cross-origin resource sharing (CORS) header, which specifies the domain allowed to access resources. If a source request host is configured as a header parameter value, it will be filled in to the response header. You can also set it as * to allow all domains to access resources. For more information, see Access-Control-Allow-Origin Match Mode Description . The wildcard *, domain names, and IPs are supported. http:// or https:// must be contained. Please separate multiple ones with ,, and up to 1000 characters are supported. E.g., http://test.com,http://1.1.1.1.
Access-Control-Allow-Methods	Specifies the CORS HTTP request method and supports multiple methods at the same time: Access-Control-Allow-Methods: POST, GET, OPTIONS.
Access-Control-Max-Age	Specifies the validity period (in seconds) of a preflight request. For a non-simple CORS request, an HTTP query request, namely the preflight request, is needed before the official communication to check whether the CORS request is secure to be accepted. A CORS request is non-simple if it is: Not a GET, HEAD, or POST request, or it is a POST request but its request data type is application/xml, text/xml or any other data type except application/x-www-form-urlencoded, multipart/form-data, and text/plain. For example, if a custom request header is Access-Control-Max-Age:1728000, there will not be another CORS preflight request sent within 1,728,000 seconds (20 days).
Access-Control-Expose-Headers	Specifies which headers can be exposed to clients as a part of responses. By default, these 6 headers can be exposed to clients: Cache-Control, Content-Language, Content-Type, Expires, Last-Modified, and Pragma. If you want to make other headers accessible to clients, you can separate multiple headers with ,, e.g., Access-Control-Expose-Headers: Content-Length,X-My-Header. In this way, clients can access the two headers Content-Length and X-My-Header.

Content-Disposition	Activates download in the browser and sets the default filename of the downloaded resource. When a server sends files to a client browser, with the file types such as TXT and JPG supported by the browser, the files will be directly opened in the browser by default. If you want the user to save the files, you can configure the Content-Disposition field to override the browser's default behavior. The common configuration is as follows: Content-Disposition: attachment; filename=FileName.txt
Content-Language	Specifies the language code used on the page. The common configuration is as follows: Content-Language: zh-CN Content-Language: en-US
Custom	Supports custom header and key-value pair settings. A custom header parameter supports 1-100 characters of uppercase and lowercase letters, digits, and hyphens (-). The parameter value supports 1-1000 characters excluding Chinese characters.

Access-Control-Allow-Origin match mode introduction

Match Mode	Origin Value
Full match	*
Fixed match	<code>http://cloud.tencent.com</code> <code>https://cloud.tencent.com</code> <code>http://www.b.com</code>
Second-level wildcard domain name match	<code>https://*.tencent.com</code>
Port match	<code>https://cloud.tencent.com:8080</code>

--	--

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.

Notes

The headers below are not supported and will not take effect if configured:

```
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 : 2024-12-30 21:45:18

Overview

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 changed frequently, Tencent Cloud CDN can only guarantee that most but not all search engine IPs can be identified.

The SEO configuration feature is available only when the connected domain name is an [external origin](#). After this feature is enabled, if a domain name has multiple origin server addresses, the first one will be the default origin-pull address.


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.

Directions

Viewing the configuration

Log in to [CDN Console](#), select **Domain Management** on the sidebar, and click **Manage** on the right of a domain name to enter its configuration page. You will find the SEO configuration on the **Advanced Configuration** tab. It is disabled by default:

SEO optimization

Enable Pull Source for Search Engine to ensure stable search engine weights. [What's SEO configuration?](#) 


Pull Source for Search Engine



Modifying the configuration

You can toggle the switch to enable or disable SEO configuration:

SEO optimization

Enable Pull Source for Search Engine to ensure stable search engine weights. [What's SEO configuration?](#) 

Pull Source for Search Engine



Smart Compression Configuration

Last updated : 2024-12-30 21:45:36

Overview

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. This configuration does not distinguish between requests from the Chinese mainland and from outside the Chinese mainland.

The file type (content-type) and Brotli compression are currently not available in regions outside the Chinese mainland.

Directions

Viewing the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. Open the **Advanced Configuration** tab to find the **Smart Compression** section. This configuration 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.

Auto Compression

Enable the smart compression service to save transmission traffic. [What is smart compression?](#)

Auto Compression	<input checked="" type="checkbox"/> Edit
Compression object	.js;.html;.css;.xml;.json;.shtml;.htm
File Size	256B ~ 2048KB
Compression method	Gzip

Modifying the configuration

Click **Modify** to modify the compression rules:

Auto Compression Configuration

File ext

Please enter a file suffix, separated by ";" for example: .jpg; .html; .css

File Size

Byte ~

KB

Set a size range. Files in this range will be compressed before being transferred

Compression method☒ Gzip ☐ Brotli ⓘ

Save

Cancel

Configuration limitations

Type: supports **All Files**, **File Extension**, and **File Content-Type**. It is set to **File Extension** by default. If **File Extension** is selected, the maximum content length is 200 characters.

If **File Content-Type** is selected, the default content is as follows: `text/html, text/xml, text/plain, text/css, text/javascript, application/json, application/javascript, application/x-javascript, application/rss+xml, application/xmltext, image/svg+xml, image/tiff`. You can edit the content as needed. Note that you can enter up to 100 groups of content separated with semicolons (;). Each group can have up to 50 characters.

Some platforms are being upgraded and do not support the file type (content-type) and Brotli compression.

Note:

The configuration can be modified when disabled, but will not be officially deployed until it is enabled.

If Gzip and Brotli are both selected, the compressed files will be returned according to the request compression header.

If Brotli is selected only and the request compression header does not support it, the original resources will be returned without being compressed.

Custom Error Page

Last updated : 2024-12-30 21:45:50

Feature Overview

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, and 451

5XX: 500, 501, 502, 503, and 504

Note:

This feature may be unavailable on some platforms. We will complete the server upgrade as soon as possible.

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 the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, click **Manage** on the right of a domain name to enter its configuration page, and switch to the **Advanced Configuration** tab to find the **Custom Error Page Configuration** section.

The custom error page configuration is disabled by default.

Custom Error Page Configuration

After it is configured, the request to which the specified status code could have been returned will be redirected to the specified target address. The host of the target address should be the same as the current domain name.[What's custom error page configuration?](#)

Custom Error Page ☐ The configuration below can be modified when it is disabled, but the configuration will not be deployed officially until it is enabled.

[Add Rule](#)

Status Code	Redirect	Destination URL	Operation
No data yet			

Adding rules

You can click **Add Rule** to add custom error page rules as needed.

Add Custom Error Page Rule

Status Code

400

Redirect

☒ 301 ☐ 302

Destination URL

"http://" or "https://" is required; the host should be the same as the current domain name.

OK

Cancel

Configuration limitations

Each status code can only have one unique rule.

Redirect: 301 or 302.

Destination URL: `http://` or `https://` is required.

The content can contain up to 1,024 characters and Chinese characters are not supported.

POST Request Size Configuration

Last updated : 2024-12-30 21:46:06

Feature Overview


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

Viewing the configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, click **Manage** on the right of a domain name to enter its configuration page, and open the **Advanced Configuration** tab to find the **POST Request Size Configuration** section. The limited request size can be configured as up to **200 MB**.

POST Request Size Configuration

The default maximum POST request size is 32 MB, and you can adjust it. [What's POST request size configuration?](#) 

Maximum POST Request Size 32MB [Edit](#)

Note:

On some platforms, there is no size limit on POST requests, and the feature is not supported for some domain names.

Image Optimization

Last updated : 2024-12-30 21:46:20

Overview

When distributing mass images with Tencent Cloud CDN, you can enable image optimization. This feature can compress images that meet specified requirements into WebP, Guetzli, and TPG formats, while drastically reducing downstream traffic and costs.

Directions

Log in to the [CDN console](#), select **Domain Management** on the left sidebar. Click **Manage** on the right of a domain name configured with a COS origin. On the page that appears, select **Image Optimization**.

Only domain names that are configured with a COS V5 origin are supported.

If the CI service is not yet activated before this feature is enabled, you can quickly complete the activation in the CDN console.

If the CI service is already activated, you can use this feature directly.

Note:

[Tencent Cloud CI](#) provides you a secure, stable and efficient cloud data processing service. When images (Webp, Guetzli, TPG) are processed, charges for the CI service will be incurred. For more billing details, see [Billing Overview](#).

WebP adaptation

When WebP adaptation is enabled, images that meet the following compression requirements will be processed and returned. If these requirements are not met, the original images will be returned.

The HTTP Accept header contains `image/webp`.

The image is in JPG, JPEG, BMP, GIF, or PNG format.

Note:

The charges incurred are included in the billable item "Basic Image Processing" of your CI bill.

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 input animated image, the total number of pixels (Width x Height x Number of frames) cannot exceed 100 million pixels (GIF frame limit: 300).

Guetzli adaptation

The CI-launched Guetzli image compression feature is visually lossless. It compresses JPG images at a high ratio to reduce the downstream traffic and increase the download speed. By taking advantage of human beings' insensitivity toward specific color gamuts and details, Guetzli discards specific details to reduce download traffic by 35% to 50% without changing quality.

When Guetzli adaptation is enabled, images that meet the following compression requirements will be processed and returned.

The HTTP Accept header contains `image/guetzli` .

The image is in JPG or JPEG format.

Note:

The charges incurred are included in the billable item "Guetzli Compression" of your CI bill.

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 adaption is a CI-launched advanced image compression feature. It converts images into TPG format with smaller image size, greatly reducing the download traffic and improving the page load speed.

When TPG adaption is enabled, images that meet the following compression requirements will be processed and returned.

The HTTP Accept header contains `image/tpg` .

The image is in JPG, JPEG, BMP, GIF, PNG, or WebP format.

Note:

The charges incurred are included in the billable item "Image Advanced Compression" of your CI bill.

Must-knows

After image optimization is enabled, the cache key of the request URL will change and conflict with the configured cache key rules. In this case, the cache key rules take higher priority.

For example, when image optimization is enabled for JPG files, the request URL

`http://www.test.com/a.jpg?colour=red` changes to `http://www.test.com/a.jpgxxxxxx ? colour=red` , which conflicts with the configured cache key rule that ignores all parameters for all files. In this case, the rule will be executed, and the request URL will eventually change to `http://www.test.com/a.jpgxxxxxx` .

Statistical Analysis

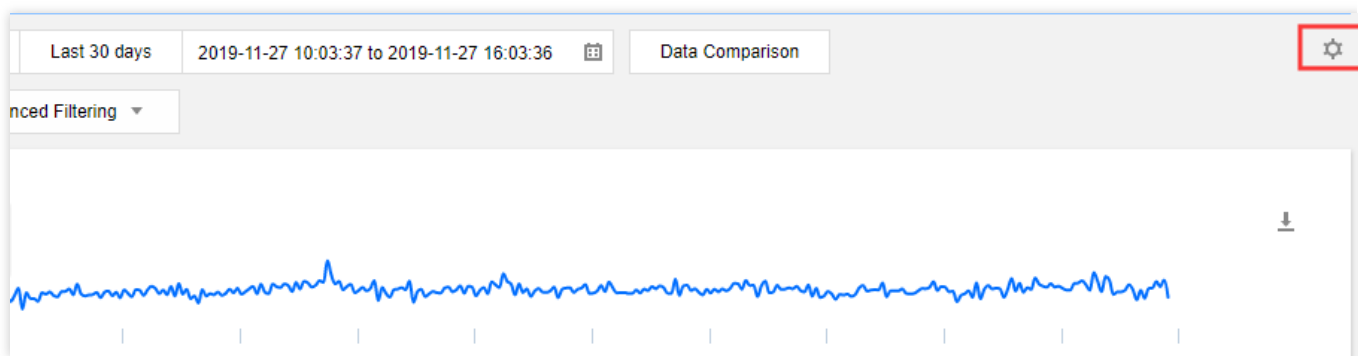
Realtime Monitoring

Panel Configuration

Last updated : 2024-12-30 21:46:43

The new **Instance Monitoring** page allows you to adjust the metrics panel as needed to view the data curves of desired metrics.

1. Log in to the [CDN Console](#) and select **Statistics > Realtime Monitoring** on the left sidebar to enter the management page.
2. Click the configuration icon on the right to enter the configuration page.



3. Select data metrics to be displayed on the overview page as needed: Selected metrics will be displayed directly. If you un-select a metric, it will no longer be displayed by default.

You can customize the panel via real-time monitoring of **Access Monitoring** and **Origin-Pull Monitoring** overview pages.

Custom display module ✕

▶	<input type="checkbox"/> Usage
▶	<input checked="" type="checkbox"/> Total Requests
▶	<input checked="" type="checkbox"/> Status Code

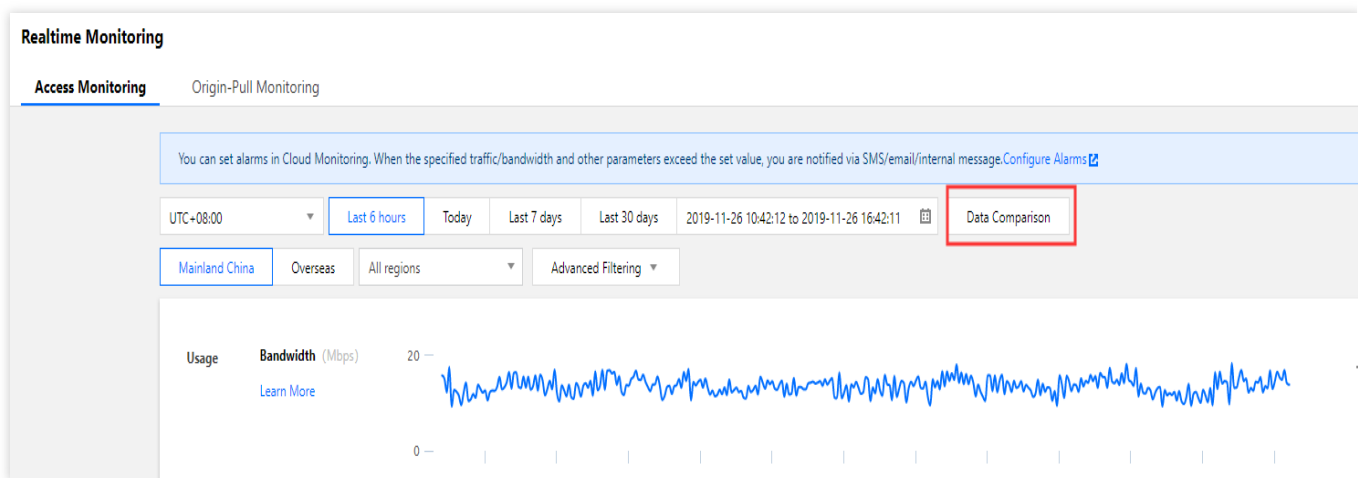
OK Cancel

Data Comparison

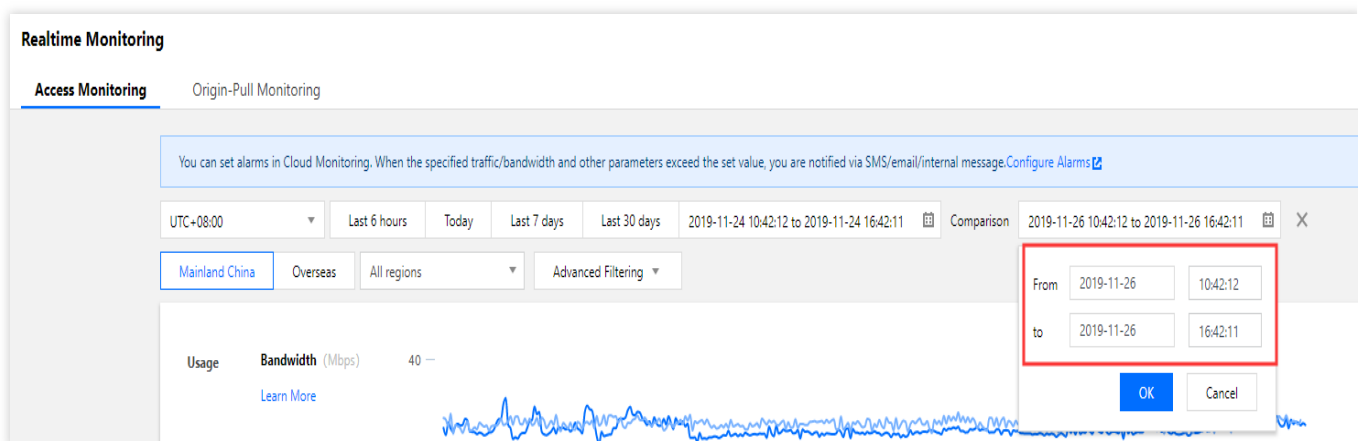
Last updated : 2024-12-30 21:47:00

Tabs on the new **Real-Time Monitoring** page all support data curve comparison.

1. Log in to the [CDN Console](#) and select **Statistics > Real-Time Monitoring** on the left sidebar to enter the management page.
2. Query the data curve of a specified time period, click **Data Comparison**, and specify another time period to start data comparison.



To facilitate your use, the system will automatically fill the start or end time accordingly after you specify the end or start time, ensuring the two time periods for comparison are of the same length.



Access Monitoring

Last updated : 2024-12-30 21:47:15

This document describes the new version of the console. It provides more comprehensive and detailed statistics and is used as the basis for billing. We recommend you use the new version.

Metrics Descriptions

Metrics on the overview page

Log in to the [CDN Console](#) and select **Statistics > Realtime Monitoring** on the left sidebar to enter the management page. The **Access Monitoring** tab is displayed by default. The monitoring curves of all domain names with a 1-minute granularity in the last 6 hours will be returned, 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 code: Percentage chart of status codes (2XX/3XX/4XX/5XX) returned within the selected time period.

2XX request status codes: Status codes generated by 2XX status code monitoring will be counted.

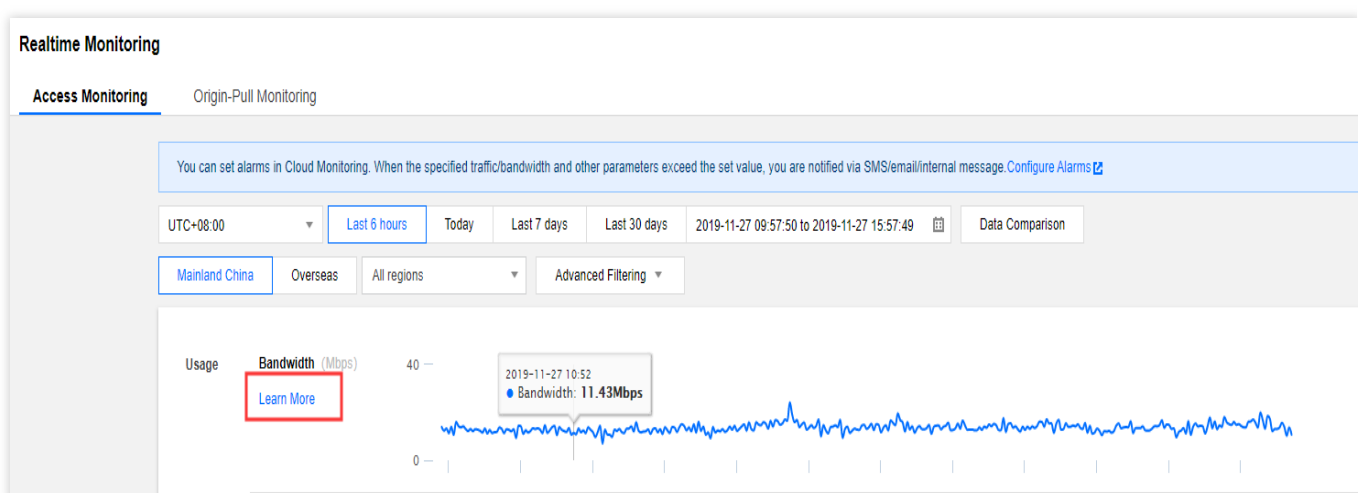
3XX request status codes: Status codes generated by 3XX status code monitoring will be counted.

4XX request status codes: Status codes generated by 4XX status code monitoring will be counted.

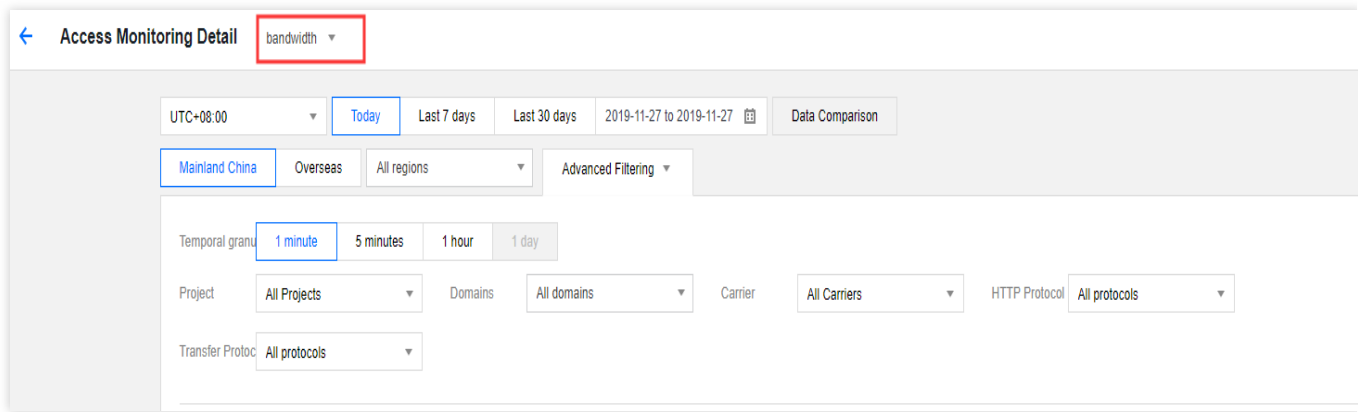
5XX request status codes: Status codes generated by 5XX status code monitoring will be counted.

Data on the details page

Click **View Details** under each metric to enter the metric details page.



You can also switch to another metric by selecting it from the drop-down list on the top-left corner of the details page.



On the details page, you can view the following metric data:

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 number of requests, curve of real-time request count, request count rankings of domain names (from high to low), and request count rankings of URLs (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 on the overview page

The monitoring page provides options to display data curves at a 1-minute, 5-minute, 1-hour, or 1-day granularity. The minimum time granularity can be displayed varies by the selected time period.

Time period \leq 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 \leq 24 hours: The minimum time granularity is 5 minutes. The latency for displaying 5-minute curve is about 5–10 minutes.

24 hours < time period \leq 31 days: The minimum time granularity is 1 hour.

Time period > 31 days: The minimum time granularity is 1 day.

Granularity on the details page

The time granularity options on the metric details page are as follows:

Time period \leq 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 \leq 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 time period for query is 90 days.

Aggregation Description

The method for aggregating 1-minute data into 5-minute, 1-hour, or 1-day data varies by data metric.

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: Based on the selected granularity, the traffic hit rate is calculated by using the formula "(total downstream traffic - origin-pull traffic) / total downstream traffic" rather than taking the average of 1-minute data values.

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 collected based on the downstream bytes in the log of an acceleration domain name is data at the application layer, while traffic generated during actual data transfers over the network is 5–15% more than application-layer data.

Consumption by TCP/IP headers: In TCP/IP-based HTTP requests, each packet has a maximum size of 1,500 bytes, including TCP and IP headers of 40 bytes, 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% packets are lost on the internet, and the server will re-transmit the lost parts. This traffic cannot be counted by the application layer, which 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 **statistical district** or **ISP** option is not selected as a filter, all queried data will be billable data.

If **statistical district** or **ISP** option is selected as a filter, the data needs to be matched for calculation by client IP in the access log, and all queried data will be log data.

Filter Description

Currently, query by both **statistical district** and **ISP** is not supported. You can only query all ISPs by district or query all districts by ISP.

Currently, origin-pull monitoring does not support filtering by statistical area or ISP.

Currently, origin-pull monitoring does not support filtering by HTTPS/HTTP request.

Origin-Pull Monitoring

Last updated : 2024-12-30 21:47:29

Note:

Origin-pull data query is not available for ECDN domain names now.

Metric Description

Metrics on the overview page

Log in to the [CDN Console](#) and select **Statistics > Realtime Monitoring** on the left sidebar to enter the management page. The **Access Monitoring** tab is displayed by default. You can click **Origin-Pull Monitoring** on the right to enter the origin-pull monitoring metrics page. The monitoring curves of all domain names with a 1-minute granularity in the last 6 hours will be returned, including the following metrics:

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 conditions will be counted as failing origin-pull requests:

Timeout in receiving origin-pull data.

Timeout in sending origin-pull request.

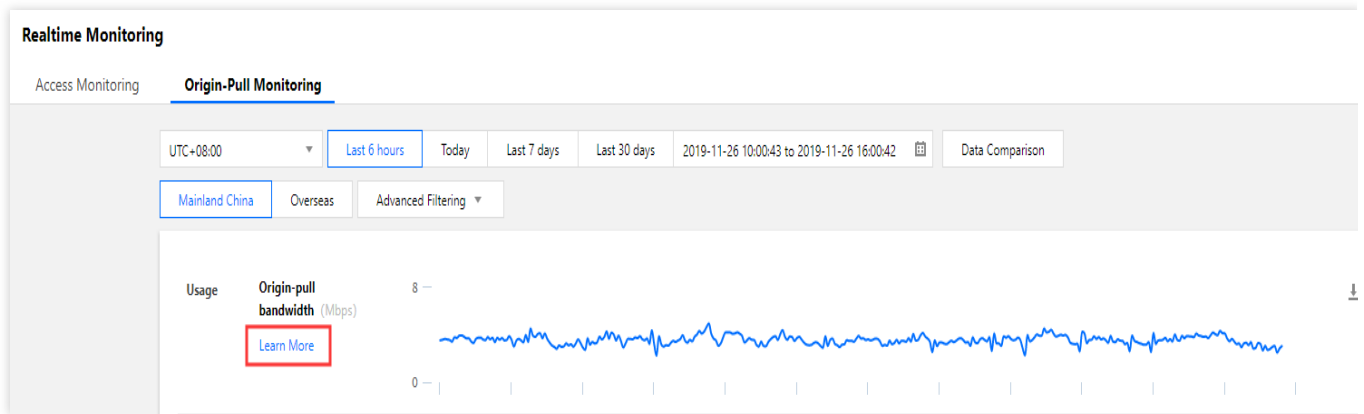
Timeout in establishing a TCP connection for origin-pull.

The origin server actively closes the connection.

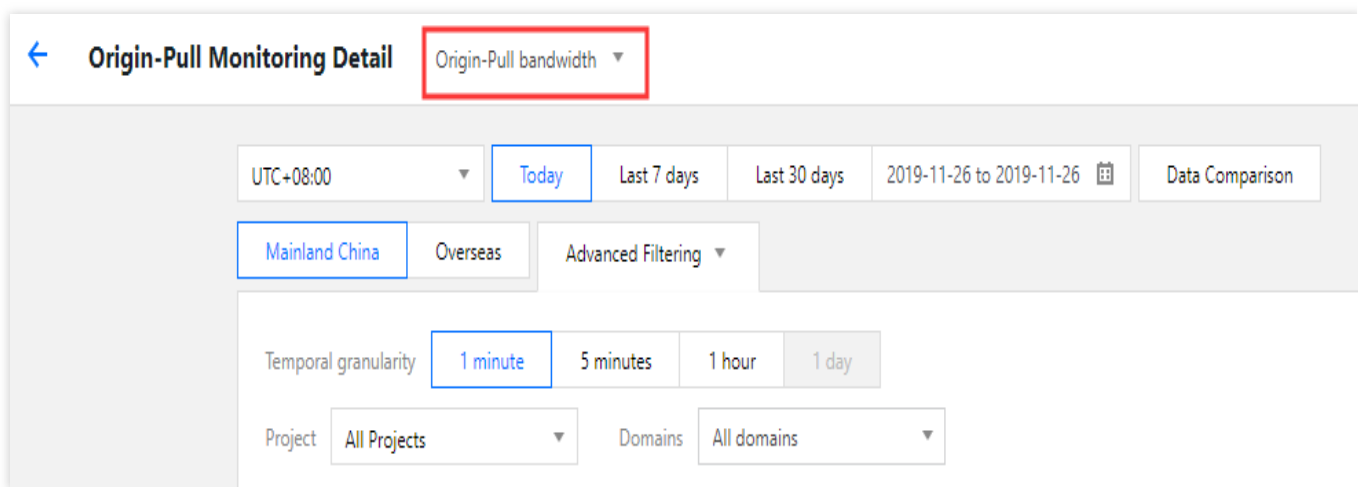
HTTP protocol compatibility error of the origin server.

Data on the details page

Click **Learn More** under each metric to enter the metric details page.



You can also switch to another metric by selecting it from the drop-down list on the top-left corner of the details page.



Granularity Description

Granularity on the overview page

The monitoring page provides options to display data curves at a 1-minute, 5-minute, 1-hour, or 1-day granularity. The minimum time granularity can be displayed varies by the selected time period.

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.

Granularity on the details page

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 data collected at a 1-minute granularity can be queried only in the new version of the console. For historical data, the minimum granularity for query is 5 minutes.

The maximum time period for query is 90 days.

Aggregation Description

The method for aggregating 1-minute data into 5-minute, 1-hour, or 1-day data varies by data metric.

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 : 2024-12-30 21:47:45

The table below explains the status codes of CDN.

Status Code	Meaning	Suggestion
0	The request ends before the status code is obtained	Check whether the client disconnects the request early, or whether the origin-pull fails.
400	HTTP request syntax error The server cannot parse the request	Check whether the request syntax is correct.
403	Request is rejected	Check whether the request is blocked by access controls such as referer blocklist/allowlist, IP blocklist/allowlist, and authentication.
404	Server cannot return correct information	Check whether the origin server is running normally, and whether the origin server information or origin domain configurations are changed. For more information, see the topic about how to troubleshoot the status code 404 that is returned when a CDN domain name is accessed.
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 CC attack	Contact Us or submit a ticket to unblock it.
514	IP access frequency exceeds the limit	Check the IP access frequency control configuration in the CDN Console.

524	Access traffic of the platform is overloaded	Business request surges may trigger a traffic overload on the platform. Estimate and report the business volume to Tencent Cloud. If you have any questions, please contact after-sales service.
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	Contact Us with the X-NWS-LOG-UUID information or submit a ticket for troubleshooting.
563	Connection timeout in the HTTPS request	Contact Us with the X-NWS-LOG-UUID information or submit a ticket for troubleshooting.
564	Origin-pull in the HTTPS request failed	If HTTP is configured as the origin-pull protocol, check the load and bandwidth utilization or access limit of the origin server. If the protocol-follow method is configured, check the port 443 status and certificate configuration of the origin server. If no error is found in the origin server, contact us with the X-NWS-LOG-UUID information or submit a ticket for troubleshooting.
567	Response times out when the	Contact Us with the X-NWS-LOG-UUID information or

node receives files

[submit a ticket](#) for troubleshooting.

The table below explains the [HTTP response status codes](#) of the webpage server.

Status code	Meaning
100	The server received the request headers, and the client should proceed to send the request body (in the case of a request for which a body needs to be sent; for example, a POST request). The client should ignore the response if the request is already complete. The server must send a final response to the client after the request is complete. To have the server check the request headers, the client must send <code>Expect: 100-continue</code> as a header in its initial request and receive a <code>100 Continue</code> status code in the response before sending the body. The status code 417 Expectation Failed indicates that the client should not continue with the request.
101	The server understood the request of the client and will notify the client by using the <code>Upgrade</code> header to use a different protocol to finish the request. After sending the last blank line of this response, the server will switch to the protocol that is defined in the <code>Upgrade</code> header. The server should switch protocols only if it is advantageous to do so. For example, switching to a newer version of HTTP, such as HTTP/2, has advantages over older versions, or switching to a real-time and synchronous protocol, such as WebSocket, helps transfer resources that use related features.
102	A WebDAV request may contain many sub-requests that involve file operations, requiring a long time to complete the request. This status code indicates that the server has received and is processing the request, but no response is available yet. This prevents the client from timing out and assuming that the request was lost.
103	This status code is used to return some response headers before the final HTTP message.
200	The request has succeeded, and the response headers or body expected by the request will be returned with this response. If the client made a GET request, the response will contain an entity corresponding to the requested resource. If the client made a POST request, the response will contain an entity that describes or contains the result of the action.
201	The request has been fulfilled by the server, resulting in the creation of a new resource. The URI of the resource has been returned with the <code>Location</code> header. If the required resource cannot be created in a timely manner, the <code>202 Accepted</code> status code should be returned.
202	The server has accepted the request but has not processed it. The request might or might not be eventually acted upon, and may be disallowed when processing occurs.
203	The server is a transforming proxy (such as a web accelerator) that received a 200 OK from its origin, but is returning a modified version of the response of the origin.
204	The server successfully processed the request of the client and is not returning any content.

	In the captive portal feature, when a Wi-Fi device is connected to a Wi-Fi access point that requires web authentication, if the device accesses a website that can generate an HTTP 204 response and receives an HTTP 204 response normally, web authentication is not required. Otherwise, the authentication interface will pop up on the web browser for the user to complete authentication and login.
205	The server successfully processed the request of the client and is not returning any content. Unlike the 204 response, this response requires the client to reset the document view.
206	The server successfully processed part of the GET request. HTTP download tools, such as FlashGet or Thunder, use this type of response to implement checkpoint restart or split a large file into multiple fragments for simultaneous download.
207	The message body that follows is an XML message and may contain a number of separate response codes, depending on how many sub-requests were made.
208	The members of a DAV binding have already been enumerated in a preceding part of the multi-status response, and will not be included again.
226	The server has fulfilled the request of the client for a given resource, and the response is a representation of the result of one or more instance manipulations applied to the current instance.
300	Multiple options are available for the requested resource, each with its own specific address and browser-driven negotiation information. The user or browser can choose a preferred address to redirect itself.
301	This status code indicates that the requested resource has been permanently moved to the new URI contained in the response. A browser automatically redirects to the new URL. All future requests should be directed to the new URI.
302	This status code is similar to the status code 301, but it indicates that the requested resource has been temporarily moved and the client should still use the original URI.
303	The response to the request can be found under another URI. When the response is received in response to a POST, PUT, or DELETE request, the client should assume that the server has received the data and should issue a new GET request to the given URI.
304	The requested resource has not been modified since the version that is specified by the If-Modified-Since or If-None-Match request header. In the case where this status code is returned, the resource does not need to be retransmitted because the client still has a previously downloaded copy.
305	The requested resource can be accessed only through the specified proxy. The Location field contains the URI information of the specified proxy. The receiver needs to issue a new request to access the requested resource through the proxy.
306	This status code is no longer used in the latest version of HTTP specifications. It originally

	meant that subsequent requests should use the specified proxy.
307	This status code indicates that the request should be repeated by using another URI and that future requests should still use the original URI. This is different from how the status code 302 was historically implemented, in that the request method cannot be changed when the original request is reissued. For example, a POST request should be repeated by using another POST request.
308	The request and all future requests should be repeated by using another URI. Status codes 307 and 308 are similar to the behaviors of status codes 302 and 301, but 307 and 308 do not allow the HTTP method to be changed. For example, submitting a form to a permanently redirected resource may continue smoothly.
401	This status code is similar to the status code 403 except that it is specifically used when required authentication has failed or has not yet been provided by the client.
405	The request method specified in the request-line cannot be used to request the resource. The server must generate an Allow header field in a 405 status code response. The field must contain a list of methods that the resource currently supports.
406	The content property of the requested resource does not meet the conditions in the request headers. Therefore, no response entity can be generated. The request is not acceptable.
407	This status code is similar to the status code 401, but it indicates that the client must authenticate itself with the proxy.
408	The server timed out while waiting for the request from the client. According to HTTP specifications: "The client did not produce a request within the time that the server was prepared to wait. The client MAY repeat the request without modifications at any later time."
409	This status code indicates that the request could not be processed because of conflict in the current state of the resource, such as an edit conflict between multiple simultaneous updates.
410	This status code indicates that the resource requested was previously in use but is no longer available and will not be available again. This should be used when a resource has been intentionally removed and the resource should be purged. Upon receiving a status code 410, the client should not request the resource in the future. Most servers use the status code 404 instead of this status code.
411	The server refuses to accept the request without a defined <code>Content-Length</code> header. The client can re-submit the request after adding a valid <code>Content-Length</code> header that describes the length of the message body to the request.
412	One or more preconditions given in the request header fields evaluated to false when verified on the server. This status code allows the client to place preconditions on the request metadata in the request header fields when it requests for a resource. This prevents the request method from being applied to resources that are not requested by the client.

415	The Internet media type submitted in the request for the resource by using the current request method is not supported by the server. As a result, the server refuses the request. For example, the client uploads an image in the SVG format, but the server requires images to be uploaded in the JPG format.
416	The client asked for a portion of the file, but the server cannot supply that portion. For example, this status code is returned if the client asked for a portion of the file that lies beyond the end of the file.
417	The server cannot meet the expectation given in the Expect header of the request.
500	This is a generic error message returned to the client when the server encounters an unexpected condition that prevents it from fulfilling the request. No specific error information is provided.
501	The server does not support the functionality required to fulfill the request. This is the appropriate response when the server does not recognize the request method and is not capable of supporting it for any resource.
505	The server does not support or refuses to support the HTTP version used in the request. The server is indicating that it is unable or unwilling to complete the request by using the same version as the client. The response should contain an entity that describes the reason why that version is not supported and the other protocols that are supported by the server.
508	The server encountered an infinite loop while processing the request.
510	The policy for accessing the resource has not been met in the request.

Data Analysis

Last updated : 2024-12-30 21:47:57

You can check your end-user distribution and resource usage on the **Data Analysis** page.

Log in to the [CDN console](#) and select **Statistics > Data Analysis** on the left sidebar to access the **Data Analysis** page.

The maximum time period for query is 31 days. Historical data is retained for 90 days.

You can query historical data generated in the last three months.

Note:

ECDN does not support displaying the number of unique IP access requests and user access region distribution currently.

Data Overview

Data overview in your specified report dimension is displayed.

The data overview varies according to the billing method.

For bill-by-traffic, total traffic, average traffic hit rate and total requests are displayed.

For bill-by-bandwidth, peak bandwidth, peak origin-pull bandwidth, and total requests are displayed.

User Access District Distribution

The user access district distribution is displayed in your specified report dimension. Based on the source client IP, the user access district can be determined, and displayed in a map or list, allowing you to view the district distribution of your users. You can view statistics of provinces in the Chinese mainland and regions outside the Chinese mainland.

Traffic

Traffic curve in your specified report dimension is displayed. You can choose to view the curve of billed traffic or origin-pull traffic.

Bandwidth

Bandwidth curve in your specified report dimension is displayed. You can choose to view the curve of billable bandwidth or origin-pull bandwidth. The peak bandwidth curve is supported.

Requests

Total request curve in your specified report dimension is displayed.

Error Codes

Numbers and proportions of error codes in your specified report dimension are displayed.

TOP10 URLs

The top 10 URLs in your specified report dimension are displayed. You can sort them by usage or total requests.

TOP 10 Projects

The top 10 projects in your specified report dimension are displayed.

TOP 10 Domain Names

The top 10 domain names in your specified report dimension are displayed.

Unique IP Access Requests

The unique IP access requests in the specified time period are counted by deduplicating the access client IPs in the log:

If the time range is less than or equal to one day, a deduplicated IP curve with a 5-minute granularity will be provided.

Domain name statistics are counted by deduplicating the active quantity in a full day. If there are multiple domain names, projects or accounts, the statistics are counted by accumulating the daily active quantity of each one with a 5-minute granularity.

Note:

Only data for the last 30 days can be queried.

User ISP Distribution

Based on the source client IP, the user ISP can be determined and displayed in a pie chart or list, allowing you to view the ISP distribution of your users.

FAQs about Statistical Analysis

Last updated : 2024-12-30 21:48:11

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 traffic data and displays the bandwidth statistics by dividing the total traffic by the duration of use.

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 in the monitoring information different from that in the log?

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.

Consumption by TCP/IP headers: in TCP/IP-based HTTP requests, each packet has a maximum size of 1,500 bytes and includes TCP and IP headers of 40 bytes, 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, which accounts for 3–7% of the total traffic.

As an industry standard, the billable traffic is the sum of the application-layer traffic and the overheads described above. Tencent Cloud CDN takes 10% as the overheads proportion, so the monitored traffic is around 110% of the logged traffic.

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?

Check whether the cache is purged: cache purge clears the specified content on the node, leading to a temporarily low traffic hit rate.

Check whether new resources have been put onto the origin server: high numbers of new resources may cause origin-pulls by CDN nodes, leading to a low traffic hit rate.

Check whether the origin server works properly: if it is malfunctioning with multiple 4XX or 5XX errors, the traffic hit rate will be affected.

Check whether the cache expiration policy is correctly configured: check the "Cache Rules" section on the Cache Configuration tab in the console. The cache expiration policies are displayed in ascending order by priority, i.e., a policy takes precedence over the one above it.

Check whether Range GETs is enabled: check the "Range GETs Configuration" section on the Origin Configuration tab in the console. If it is disabled, files will be pulled in their entirety instead of multiple parts as requested during origin-pull, which increases the origin-pull traffic and lowers the hit rate.

Check whether Ignore Query String is enabled: check the "Ignore Query String" section on the Access Control tab in the console. If it is disabled, caching will be performed based on the full path. In this case, if the same resource is requested by different parameters, it cannot be matched and will be cached multiple times, lowering the 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 question #2 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 automatically purged.

What should I do if my CDN traffic has an exception or is under DDoS or CC attacks?

If you believe your business traffic is unusually high, you can download logs to check your business access conditions and set access restrictions accordingly. CDN does not know your business logic, so it will not restrict access requests by default. Therefore, you need to configure the restrictions based on your business conditions. For more information, please see [Log Download](#).

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 Configuration](#).
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 cycle (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 Cache

Last updated : 2024-12-30 21:49:05

Overview

CDN is capable of configuring basic cache. Cache validity can be configured according to rules such as specified service types, directories, and specific URLs to regularly purge resources cached on nodes, pull the latest resources from the origin server, and cache them again.

In addition, CDN can purge cache for specified URLs or directories in batches:

Purge URL: this deletes the cache of the corresponding resources on all CDN nodes.

Purge directory: if you select **Purge updated resources**, when an end user accesses a resource under the corresponding directory, the `Last-Modify` information of the resource will be pulled from the origin server. If it is the same as that of the cached resource, the cached resource will be directly returned; otherwise, the updated resource will be pulled from the origin server and cached again. If you select **Purge all resources**, when the user accesses a resource under the corresponding directory, the latest version of the resource will be directly pulled from the origin server and cached again.

Note:

After a purge is successfully executed, the corresponding resource on the node will not have a valid cache. When the user initiates an access request again, the node will pull the required resource from the origin server and cache it on the node. If you submit a large number of purge tasks, many caches will be cleared, resulting in a surge in origin-pull requests and high pressure on the origin server.

Application Scenarios

New resource releases

When a resource is overwritten by a new resource with the same name on the origin server, you can submit a request to purge the URL/directory and clear all caches so users can directly access the latest version of the resource. This will prevent users from accessing the legacy version of the resource cached on the node.

Illegal resource cleanup

When illegal resources (such as resources related to pornography, drug, or gambling) are found on your origin server, they may still be accessible even after you delete them on the origin server because of node cache. To protect your network environment security, you can delete the cached resources through URL purge.

Operation Guide

Log in to the [CDN console](#), click **Purge and Prefetch** on the left sidebar, and submit a **Purge URL** or **Purge Directory** task:

CDN and ECDN URLs/directories can be purged together.

Task can be submitted by direct input or TXT file upload.

Content specifications

Check whether the submitted content meets the following specifications:

URLs must contain a protocol identifier "http://" or "https://", such as `http://www.test.com/test.html`, and should be entered 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.

URLs in the format of "http://*.test.com/" cannot be submitted. Even if you connect a wildcard domain name to CDN, you need to submit the corresponding subdomain names.

Wildcards are not allowed in URLs to purge.

For a URL with Chinese characters, enable "URL Encode" to encode the Chinese characters.

Submission limit

URL purge:

Up to 10,000 URLs can be purged per day for each account. For users who use CDN service outside the Chinese mainland, up to 10,000 global URLs can be purged per day, which is independent of the URL purge quota for the Chinese mainland.

Up to 1,000 URLs can be submitted at a time by direct input.

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.

Note:

When you are running out of daily purge quota, you can increase it on your own in the Tencent Cloud CDN console. The new quota will take effect immediately. The page will be refreshed automatically. You don't need to click the refresh button frequently.

Each quota can only be increased once a day.

Each quota is increased independently for each region.

Directory purge:

Up to 100 directories can be purged per day for each account. For users who use CDN service outside the Chinese mainland, up to 100 global directories can be purged per day, which is independent of the directory purge quota for the Chinese mainland.

Up to 20 directories can be submitted at a time by direct input.

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.

By default, URLs will be purged by acceleration regions of domain names in the URLs. If the domain names are accelerated globally, quotas for regions both in and outside the Chinese mainland will be consumed.

To query your operation records, please see [History](#).

Sub-user permissions configuration

URL purge, directory purge, and purge history query have been integrated within the permission system which supports permission configuration at the resource (domain name) level. For more information, see [Console Permissions](#).

Examples

Directory purge - purge updated resources

The acceleration domain name is `purge-test-1251991073.file.myqcloud.com`, the origin server is Tencent Cloud Object Storage (COS), and resources on the origin server are as follows:

1. Initiate requests to access resources `1.txt` and `2.txt` respectively. Nodes to be hit can be determined based on `X-Cache-Lookup: Hit From Disktank3` and `Server: NWS_SPMid`, resources will be directly returned by the nodes:

```
curl http://purge-test-1251991073.file.myqcloud.com/fileTest/1.txt
* Trying 14.215.85.233...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (14.215.85.233) port 80 (#0)
> GET /fileTest/1.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: NWS_SPMid
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:20:46 GMT
< Cache-Control: max-age=600
< Expires: Wed, 04 Sep 2019 23:30:46 GMT
< Last-Modified: Wed, 04 Sep 2019 23:01:37 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 19
< X-NWS-UUID-VERIFY: 72e4a2dbd2e9e5304c17d2beb0bf39d5
< X-NWS-LOG-UUID: 5673286006122774168 b5f0e763fad18324d85b241a7e6695c4
< X-Cache-Lookup: Hit From Disktank3
< Accept-Ranges: bytes
< X-Daa-Tunnel: hop_count=1
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```



```

curl http://purge-test-1251991073.file.myqcloud.com/fileTest/2.txt
* Trying 14.215.85.233...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (14.215.85.233) port 80 (#0)
> GET /fileTest/2.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: NWS_SPMid
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:22:03 GMT
< Cache-Control: max-age=600
< Expires: Wed, 04 Sep 2019 23:32:03 GMT
< Last-Modified: Wed, 04 Sep 2019 23:01:37 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 19
< X-NWS-UUID-VERIFY: e7112793c4a1bdde407954fb943e43fb
< X-NWS-LOG-UUID: 14628995741359757299 b5f0e763fad18324d85b241a7e6695c4
< X-Cache-Lookup: Hit From Disktank3
< Accept-Ranges: bytes
< X-Daa-Tunnel: hop_count=1
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact

```

2. On the origin server, replace `1.txt` with a file that has the same name, and the file's last modified time changes, while `2.txt` stays the same:

Basic Information

Object Name	1.txt
Object Size	258B
Last Modified	2019-12-11 17:12:12
ETag	"3f4989383498b548700c122d56a708ed"
Specified Domain	Default CDN Accelerati...
Object Address	https://examplebucket1-1259222427.file.myqcloud.com/fileTest/1.txt
Temporary Link	Copy Temporary Link Download Objects Refresh

The temporary link carries the signature parameter, and the temporary link can be used to access the object during the validity period of the signature, and the signature is valid for 1 hour (2019-12-11 18:12:51). Be sure to avoid leaking the temporary link, otherwise your objects may be accessed by other users.

Basic Information

Object Name	1.txt
Object Size	240B
Last Modified	2019-12-11 17:30:21
ETag	"282ba0ab22810e2eb79aa52fcdacccb"
Specified Domain	<input type="text" value="Default CDN Accelerati..."/>
Object Address	https://examplebucket1-1258222427.file.myqcloud.com/fileTest/1.txt
Temporary Link	Copy Temporary Link Download Objects Refresh

The temporary link carries the signature parameter, and the temporary link can be used to access the object during the validity period of the signature, and the signature is valid for 1 hour (2019-12-11 18:30:25).

Be sure to avoid leaking the temporary link, otherwise your objects may be accessed by other users.

3. Initiate requests again. As the cache has not expired, the legacy content of the `1.txt` resource will be accessed:

```
curl http://purge-test-1251991073.file.myqcloud.com/fileTest/1.txt
* Trying 113.105.165.187...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (113.105.165.187) port 80 (#0)
> GET /fileTest/2.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: NWS_SPMid
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:34:19 GMT
< Cache-Control: max-age=600
< Expires: Wed, 04 Sep 2019 23:44:19 GMT
< Last-Modified: Wed, 04 Sep 2019 23:01:37 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 19
< X-NWS-UUID-VERIFY: 72e4a2dbd2e9e5304c17d2beb0bf39d5
< X-NWS-LOG-UUID: 5673286006122774168 b5f0e763fad18324d85b241a7e6695c4
< X-Cache-Lookup: Hit From Disktank3
< Accept-Ranges: bytes
< X-Daa-Tunnel: hop_count=1
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```

4. Submit a directory purge task, select **Purge updated resources**, and wait for the purge to complete:

5. After the purge is complete, because `Last-Modified` of `1.txt` has been changed, the request will be forwarded to the origin server. As `2.txt` has not been changed, even after a directory purge task is submitted, it will still be hit and returned:

```
curl http://purge-test-1251991073.file.myqcloud.  
fileTest/1.txt -sv  
* Trying 113.105.165.187...  
* TCP_NODELAY set  
* Connected to purge-test-1251991073.file.myqcloud.com (113.105.165.187) port 80 (#0)  
> GET /fileTest/1.txt HTTP/1.1  
> Host: purge-test-1251991073.file.myqcloud.com  
> User-Agent: curl/7.54.0  
> Accept: */*  
>  
< HTTP/1.1 200 OK  
< Server: tencent-cos  
< Connection: keep-alive  
< Date: Wed, 04 Sep 2019 23:33:22 GMT  
< Last-Modified: Wed, 04 Sep 2019 23:24:17 GMT  
< Content-Type: text/plain; charset=utf-8  
< Content-Length: 23  
< X-NWS-UUID-VERIFY: 6a4ea0410342aee319550d46b866cd37  
< Accept-Ranges: bytes  
< ETag: "325daac4e71e82db89ee26922d7435b7"  
< x-cos-request-id: NWQ2ZmQ5NDJfMjZiMjU4NjRfMzY0Y181MmU1YWU1YWI=  
< X-Daa-Tunnel: hop_count=2  
< X-NWS-LOG-UUID: 14013390993447302634 2107abdde3874148ff95a672f195831b  
< X-Cache-Lookup: Hit From Upstream  
< X-Cache-Lookup: Hit From Upstream  
<  
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```

```
curl http://purge-test-1251991073.file.myqcloud.com/fileTest/2.txt
* Trying 113.105.165.187...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (113.105.165.187) port 80 (#0)
> GET /fileTest/2.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: NWS_SPMid
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:34:19 GMT
< Cache-Control: max-age=600
< Expires: Wed, 04 Sep 2019 23:44:19 GMT
< Last-Modified: Wed, 04 Sep 2019 23:01:37 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 19
< X-NWS-UUID-VERIFY: e7112793c4a1bdde407954fb943e43fb
< X-NWS-LOG-UUID: 1690084127387779050 2107abdde3874148ff95a672f195831b
< X-Cache-Lookup: Hit From Disktank3
< Accept-Ranges: bytes
< X-Daa-Tunnel: hop_count=1
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```

Prefetch Cache

Last updated : 2024-12-30 21:49:20

Feature Overview

After a domain name is connected to the CDN service, it initially has no resources on CDN cache nodes across the entire network. Resources will be cached once triggered by a user request. If the requested resources are expired or not cached on the cache node, CDN intermediate node will be pulled for the resources. If they are expired or not cached on the intermediate node neither, the user's origin server will be pulled.

CDN prefetch feature allows you to submit a resource list for loading resources to cache nodes without user requests. When a node loads a resource, if there is a valid (not expired) resource with the same name already cached on the node, the resource will not be loaded. We recommend purging resources entirely across the network before you update any resource with the same name.

Nodes load resources from the origin server, of which the bandwidth will increase after a large number of prefetch tasks are submitted.

Acceleration domain name services are deployed in a double-layer acceleration mechanism by default. Prefetching resources in the Chinese mainland, resources are loaded to intermediate nodes within the Chinese mainland by default, while prefetching resources in the regions outside the Chinese mainland, resources are loaded to edge servers outside the Chinese mainland by default.

Note:

Prefetching resources in the regions outside the Chinese mainland, resources are loaded to edge servers outside the Chinese mainland by default, and the traffic incurred on the edge layer is charged.

Use Cases

Installation package releases

Before releasing any new edition or update of installation packages, you can prefetch the resources to CDN cache nodes. After packages are officially released, massive download requests from users will be taken over by CDN cache nodes, increasing download speed and reducing the pressure on the origin server.

Marketing events

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.

Operations Guide

How to use

1. Log in to the [CDN console](#), click **Purge and Prefetch** on the left sidebar, open the **Prefetch URL** tab to submit a task.

2. You can specify a target region to prefetch resources.

For acceleration domain names in the Chinese mainland, only **Chinese Mainland** can be specified for acceleration. For acceleration domain names outside the Chinese mainland, only **Overseas** (i.e., the regions outside the Chinese mainland) can be specified for acceleration.

For global acceleration domain names, **Global**, **Chinese Mainland**, and **Overseas** (i.e., the regions outside the Chinese mainland) can be specified for acceleration.

The screenshot shows the 'Purge and Prefetch' interface in the Tencent Cloud CDN console. The 'Prefetch URL' tab is selected. The interface includes a 'Prefetch Area' section with three buttons: 'Global' (selected), 'Chinese Mainland', and 'Overseas'. Below this is a large text input field for 'URL' with a placeholder: 'Enter URL of the object you want to prefetch (include http:// or https://); one per line'. A character count '0/20' is visible at the bottom right of the input field. Below the input field, there is a note: 'Wildcards are not supported now.' and two lines of status information: 'Available prefetch URLs for today: 1000 (Mainland)' and 'Available prefetch URLs for today: 1000 (Overseas)'. At the bottom, there is a blue button labeled 'Submit and Prefetch'.

3. In the **History** tab, you can query prefetch tasks by a specified time period and term. Term queries only support querying with a domain name or a complete URL:

Purge and Prefetch

[Purge URL](#) [Purge Directory](#) [Prefetch URL](#) **[History](#)**

Select a date2020-12-15 00:00:00 ~ 2020-12-15 23:59:59 ⓘ (UTC+08:00)

Search termEnter a domain name, or a complete URL (includes Scheme)

Query type☐ Purge URL ☐ Purge Directory ☒ Prefetch URL

Query

Purge Records	Purge Time	Status ▾
No record		

Total items: 010 / page1 / 1 page

Precautions

Prefetch limits

Up to 1,000 URLs can be prefetched per day for each account in each acceleration region, and up to 20 URLs can be prefetched at a time. After a global prefetch task is conducted, the quota for regions in and outside the Chinese mainland will be used at the same time.

You need to add the `http://` or `https://` protocol identifier when submitting a prefetch task.

URLs in the format of `http://*.test.com` cannot be prefetched.

URLs containing Chinese characters cannot be prefetched.

Sub-user permissions configuration

URL prefetch and prefetch history query have been integrated to the latest permission system and support permission configuration at the resource (domain name) level.

For the permission assignment method, please see [Console Permissions](#).

History

Last updated : 2024-12-30 21:49:49

Description

After submitting purge and prefetch tasks, you can view detailed records and status of resource purge and prefetch in **History** page.

Directions

How to use

1. Log in to the [CDN console](#), click **Purge and Prefetch** on the left sidebar, and click **History**.
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.

The screenshot shows the 'History' page interface. At the top, there is a 'Date' range selector set to '2023-02-24 00:00:00 ~ 2023-02-24 23:59:59' with a calendar icon and '(UTC+08:00)'. Below this is a 'Search Term' input field with the placeholder 'Enter a domain name, or a complete URL (includes Scheme)'. The 'Query Type' section has three radio buttons: 'Purge URL' (selected and circled in red), 'Purge Directory', and 'Prefetch URL'. A blue 'Search' button is located below the search term field. Below the search buttons is a 'Submit again' button. The main content area is a table with columns 'Purge Records', 'Purge Time', and 'Status'. The table is currently empty, displaying 'No record'. At the bottom, there is a pagination bar showing 'Total items: 0', '10 / page', and a page number '1 / 1 page'.

Notes

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.

Purge and Prefetch FAQs

Last updated : 2025-01-24 09:25:28

When do I need to purge 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 are the differences between purge 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.

What are requirements for purge and prefetch? How long do they take to take effect?

Purge Cache

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 20 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.

Prefetch Resource

URL prefetch: A maximum of 1,000 URLs can be prefetched each day, and a maximum of 20 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.

Will the cache on CDN nodes be updated in real time?

No. The cached content on CDN cache nodes are updated based on the [cache validity](#) you configured in the console. If you need to update a file's cache in real time, use [cache purge](#).

How do I view the purge and prefetch history?

You can check the purge and prefetch history in the CDN console. For more information, see [History](#).

Can I prefetch with custom request headers?

No.

Log Management

Log Service

Last updated : 2025-05-06 17:47:18

Notice :

Field value "HTTP/3" for the HTTP protocol identifier (the 14th field in the offline log) in general logs will be in beta from September 13, 2021, which will not affect the CDN console and APIs. Please note that getting log data from offline log packages may require adjustment.<

QUIC access has been in beta. For more details, see [QUIC](#).

Features

After a domain name is connected to CDN, all requests will be scheduled to a CDN node. If the requested resource is cached on the node, the resource will be returned directly; otherwise, the request will be passed to the origin server to pull the requested resource.

CDN nodes respond to most of the user requests. To facilitate access analysis, CDN packages access logs of the entire network at an hourly granularity and retains them for 30 days by default. These logs can also be downloaded.

Note:

Currently origin-pull logs are not provided. Only node access logs are provided.

ECDN domain name offline logs cannot be queried by regions for now. For more information, see [Log Management](#).

Use Cases

Access behavior analysis

You can download access logs and analyze popular resources and active users.

Service quality monitoring

By downloading access logs, you can stay on top of the service status of all CDN nodes and calculate the average response time, average download speed, and other metrics.

Directions

How to use

Log in to the [CDN console](#), click **Log Service** on the left sidebar, and select a domain name and time range to query access logs. You can select multiple log packages and download them in batches:

Note:

The access logs are packaged by hour by default. If there is no request to the domain name for the hour, no log package will be generated for this hour.

For the same domain name, logs of accesses from within and outside the Chinese mainland are packaged separately. Log packages are named in the format of "[time]-[domain name]-[acceleration region]".

The access logs are collected from each CDN cache node, so the delay may vary. Generally, the delay for querying and downloading log packages is about 30 minutes. Log packages will be added continuously and will stabilize after around 24 hours.

The access log packages of a domain name are retained for 30 days. You can use an SCF function to transfer the log packages to COS as instructed in [Regularly Storing CDN Logs](#) for permanent storage.

Fields

The fields (from left to right) in the logs are listed as below:

No.	Fields
1	Request time
2	Client IP
3	Domain name
4	Request path
5	Number of bytes accessed this time, including the size of the file itself and the size of the request header.
6	Province numbers for Chinese mainland logs; region numbers for logs outside the Chinese mainland (see the mapping table below).
7	ISP numbers for Chinese mainland logs; <code>-1</code> will be used for logs outside the Chinese mainland (see the mapping table below).
8	HTTP status code
9	Referer information
10	Response time (in milliseconds), which refers to the time it takes for a node to return all packets to the client after receiving a request.
11	User-Agent information
12	Range parameter

13	HTTP method
14	HTTP protocol identifier
15	Cache hit/miss. A hit in a CDN edge server or parent node will be marked as hit.

Region/ISP mappings

Chinese mainland provinces

Region ID	Region	Region ID	Region	Region ID	Region
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	Xizang	4	Guangdong	173	Guangxi
1441	Hainan	0	Other	1	Hong Kong (China), Macao (China), and Taiwan (China)
-1	Outside the Chinese mainland				

Chinese mainland ISPs

ISP ID	ISP	ISP ID	ISP	ISP ID	ISP
2	China Telecom	26	China Unicom	38	CERNET

43	Great Wall Broadband Network	1046	China Mobile	3947	China Mobile Tietong
-1	ISPs outside the Chinese mainland	0	Other ISPs		

Regions outside the Chinese mainland

Region ID	Region	Region ID	Region	Region ID	Region
2000000001	Asia Pacific Zone 1 (service area)	765	Slovakia	1613	Angola
2000000002	Asia Pacific Zone 2 (service area)	766	Serbia	1617	Ivory Coast
2000000003	Asia Pacific Zone 3 (service area)	770	Finland	1620	Sudan
2000000004	Middle East (service area)	773	Belgium	1681	Mauritius
2000000005	North America (service area)	809	Bulgaria	1693	Morocco
2000000006	Europe (service area)	811	Slovenia	1695	Algeria
2000000007	South America (service area)	812	Moldova	1698	Guinea
2000000008	Africa (service area)	813	Macedonia	1730	Senegal
-20	Asia (client area)	824	Estonia	1864	Tunisia
-21	South America (client area)	835	Croatia	1909	Uruguay
-22	North America (client area)	837	Poland	1916	Greenland
-23	Europe (client area)	852	Latvia	2026	Taiwan (China)
-24	Africa (client area)	857	Jordan	2083	Myanmar
-25	Oceania (client area)	884	Kyrgyzstan	2087	Brunei
35	Nepal	896	Ireland	2094	Sri Lanka
57	Thailand	901	Libya	2150	Panama

73	India	904	Armenia	2175	Colombia
144	Vietnam	921	Yemen	2273	Monaco
192	France	926	Belarus	2343	Andorra
207	United Kingdom	971	Luxembourg	2421	Turkmenistan
208	Sweden	1036	New Zealand	2435	Laos
209	Germany	1044	Japan	2488	East Timor
213	Italy	1066	Pakistan	2490	Tonga
214	Spain	1070	Malta	2588	Philippines
386	United Arab Emirates	1091	Bahamas	2609	Venezuela
391	Israel	1129	Argentina	2612	Bolivia
397	Ukraine	1134	Bangladesh	2613	Brazil
-	-	1158	Cambodia	2623	Costa Rica
417	Kazakhstan	1159	Macao (China)	2626	Mexico
428	Portugal	1176	Singapore	2639	Honduras
443	Greece	1179	Maldives	2645	El Salvador
471	Saudi Arabia	1180	Afghanistan	2647	Paraguay
529	Denmark	1185	Fiji	2661	Peru
565	Iran	1186	Mongolia	2728	Nicaragua
578	Norway	1195	Indonesia	2734	Ecuador
669	United States	1200	Hong Kong (China)	2768	Guatemala
692	Syria	1233	Qatar	2999	Aruba
704	Cyprus	1255	Iceland	3058	Ethiopia
706	Czech	1289	Albania	3144	Bosnia and Herzegovina
707	Switzerland	1353	Uzbekistan	3216	Dominican

708	Iraq	1407	San Marino	3379	South Korea
714	Netherlands	1416	Kuwait	3701	Malaysia
717	Romania	1417	Montenegro	3839	Canada
721	Lebanon	1493	Tajikistan	4450	Australia
725	Hungary	1501	Bahrain	4460	Chinese mainland
726	Georgia	1543	Chile	-15	Asia - other
731	Azerbaijan	1559	South Africa	-14	South America - other
734	Austria	1567	Egypt	-13	North America - other
736	Palestine	1590	Kenya	-12	Europe - other
737	Türkiye	1592	Nigeria	-11	Africa - other
759	Lithuania	1598	Tanzania	-10	Oceania - other
763	Oman	1611	Madagascar	-2	Outside the Chinese mainland - other

ISPs outside the Chinese mainland

ISP ID	ISP
-1	ISPs outside the Chinese mainland

Notes

The traffic/bandwidth data calculated based on the number of bytes recorded in the fifth field of an access log is different from the billable CDN traffic/bandwidth data for the following reason:

Only application-layer data can be recorded in access logs. During actual data transfer, the traffic generated over the network is around 5-15% more than the application-layer traffic, including the following two parts:

Consumption by TCP/IP headers: in TCP/IP-based HTTP requests, each packet has a maximum size of 1,500 bytes and includes TCP and IP headers of 40 bytes, 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% to 10% of packets are lost on the Internet and retransmitted by the server. This type of traffic, which accounts for 3-7% of the total traffic, cannot be counted at the application layer.

As an industry standard, the billable traffic is the sum of the application-layer traffic and the overheads described above. Tencent Cloud CDN takes 10% as the overheads proportion, so the monitored traffic is around 110% of the logged traffic.

Examples

Sample log of accesses from within the Chinese mainland

Sample log of accesses from outside the Chinese mainland

Real-time Logs

Last updated : 2024-12-30 21:50:36

Real-time Logging

Tencent Cloud CDN provides the real-time log feature. This feature collects and publishes access logs in real time, enabling fast retrieval and analysis of log data. You can quickly access comprehensive, stable, and reliable one-stop logging services such as log collection, log storage, and log search in the CDN console.

Use Cases

You can access log data to view or analyze business conditions in multiple dimensions in real time.

Directions

Log in to the [CDN console](#), click **Log Service** in the left sidebar, and then click the **Real-time Logs** tab.

Enabling logging

To use this feature, you need to activate [Logging Service \(CLS\)](#) and grant CDN the permissions to create a logset.

Note:

We recommend that you use the root account to enable this feature. If you use a sub-account or are a collaborator, enable the real-time log feature as instructed in [Activate Real-time Logging as Sub-account/Collaborator](#).

When you enable the real-time log feature, CDN creates a logset for each region to host CDN logs.

A logset is a billable item as a part of CLS. However, the publish of CDN logs is free. For more information about the billing rules, see [Billing Overview](#).

At present, log shipping is supported in Shanghai, Beijing, Chengdu, Chongqing, Nanjing, Guangzhou, and Singapore.

Creating a log topic

Create a log topic in a logset, and ship the access logs of the target accelerated domain name to [CLS](#).

Note:

A logset can contain up to 500 log topics.

The topic name must be unique.

You cannot bind both CDN and ECDN domain names to the same log topic.

Logs of CDN domain names in the Chinese mainland can be shipped to Shanghai, Beijing, Chengdu, Chongqing, Nanjing, and Guangzhou. The logs of CDN domain names outside the Chinese mainland can be shipped to only the Singapore region.

ECDN domain names do not support log publishing to regions outside the Chinese mainland.

Log search

Log search supports various search and analysis methods and chart types. For more information, see [Search and Analysis](#).

You can search for logs by log topic. To do so, select a log topic as needed and click **Search** to access the log search page.

Managing log topics and logsets

You can manage log topics in the CDN console. The following operations are supported:

Manage: Update the list of domain names bound to a log topic

Disable: Stop shipping logs of bound domain names to the log topic. . Received logs are retained.

Enable: Ship logs of bound domain names to the log topic.

Delete: After a log topic is deleted, the log topic no longer accepts new log shipping of the bound domain names, and completely clears all logs it contains.

For more logset managing operations, such as renaming a logset, you can go to the [CLS](#) console.

Real-time Log Fields

Log Field	Raw Log Type	Log Service Type	Description
app_id	Integer	long	Tencent Cloud account <code>APPID</code>
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	ISP

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 all packets to the client after receiving a request.
remote_port	String	long	A port connecting the client and CDN nodes. This field will be displayed as <code>-</code> if the port does not exist.
rsp_size	Integer	long	Number of returned bytes
time	Integer	long	Request timestamp in UNIX format (in seconds)
ua	String	text	<code>User-Agent</code> information
url	String	text	Request path
uuid	String	text	Unique request ID
version	Integer	long	CDN real-time log version

Glossary

Logset

A logset is a project management unit in the log service. It is used to distinguish between logs of different projects and corresponds to an item or application. The CDN logset has the following basic attributes:

Region: The [region](#) to which a logset belongs.

Note:

At present, log shipping is supported in Shanghai, Beijing, Chengdu, Chongqing, Nanjing, Guangzhou, and Singapore.

Logset name: Name of the logset.

Retention period: Retention period of data in the logset.

Creation time: Logset creation time.

Log topic

A log topic is the basic management unit in the log service. One logset can contain multiple log topics, and one log topic corresponds to one type of application or service. We recommend you collect similar logs on different machines into the same log topic. For example, if a business project has three types of logs: operation log, application log, and access log, you can create a log topic for each type of log.

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. You need to configure corresponding rules first after creating a log topic before you can 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.

Ship logs to other platforms based on log topics.

Download and consume logs from log topics.

Note:

For more information, see [CLS documentation](#).

FAQs

Some of my logsets and log topics in the CLS console are not displayed in the CDN console. Why is that?

The CDN console displays only the logs created by the CDN service role, which are real-time logs exclusive to CDN. Other logsets and log topics are not synchronized to the CDN console.

I cannot retrieve the data I want in the real-time logs. Are they lost?

It may be because your log data volume is large, but the corresponding log topic has only a single partition, or automatic splitting is disabled for it. When you create a log topic, the default number of partitions is 1, and automatic splitting is enabled by default.

We recommend you estimate the number of required partitions based on your log volume and configure it in the advanced options in the [CLS](#) console. For more information, see [Topic Partition](#).

Can I delete CLS logsets?

Yes. To delete a CDN logset, go to the CLS console, delete all log topics in the logset, and then delete the logset. The deletion will be synchronized to the CDN console. You can create new logsets and log topics in the CDN console later.

EdgeOne

Last updated : 2024-12-30 21:50:53

With globally distributed edge nodes, [Tencent Cloud EdgeOne](#) offers CDN acceleration combined with comprehensive edge security services, including DDoS mitigation, web protection, bot management and custom rules, enabling more flexible and more robust protection capabilities.

To protect your domain names connected to CDN, migrate your service to EdgeOne as follows.

Directions

Step 1: Decide the protection scope

As EdgeOne service is provided based on [sites](#), you should determine how many sites needed for your domain names. See examples below:

CDN Domain Name	EdgeOne Site
<code>www.example.com</code> <code>test.example.com</code> <code>image.example.com</code>	<code>example.com</code>
<code>www.example.com</code> <code>test.example.com</code> <code>www.site.com</code>	<code>example.com</code> <code>site.com</code>

Step 2: Add sites and acceleration domain names

Go to the [EdgeOne console](#) to add your site and acceleration domain name. For detailed steps, see [Quick Start](#).

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

Custom security policies such as IP blocklist/allowlist, regional blocking and web protection rules can be created to suit your needs. For configuration details, see the documents below:

[DDoS Mitigation](#)

[Web Protection](#)

[Bot Management](#)

CDN Refund

To return unused CDN resources, submit your purchase records via [a ticket](#). Fees will be sent back based on the percentage of remaining usage.

Service Query

Entire Network Status Monitoring

Last updated : 2024-12-30 21:51:09

Feature Overview

CDN can monitor the latency and availability status of ISP in each province in Mainland China and each region outside Mainland China. It continues to send requests to monitoring files at selected nodes around the world and collects the response data of these requests. You can view real-time status and details of the entire network in the CDN Console.

The entire network monitoring feature monitors the service status of the CDN platform, not the actual service status of your business.

Directions

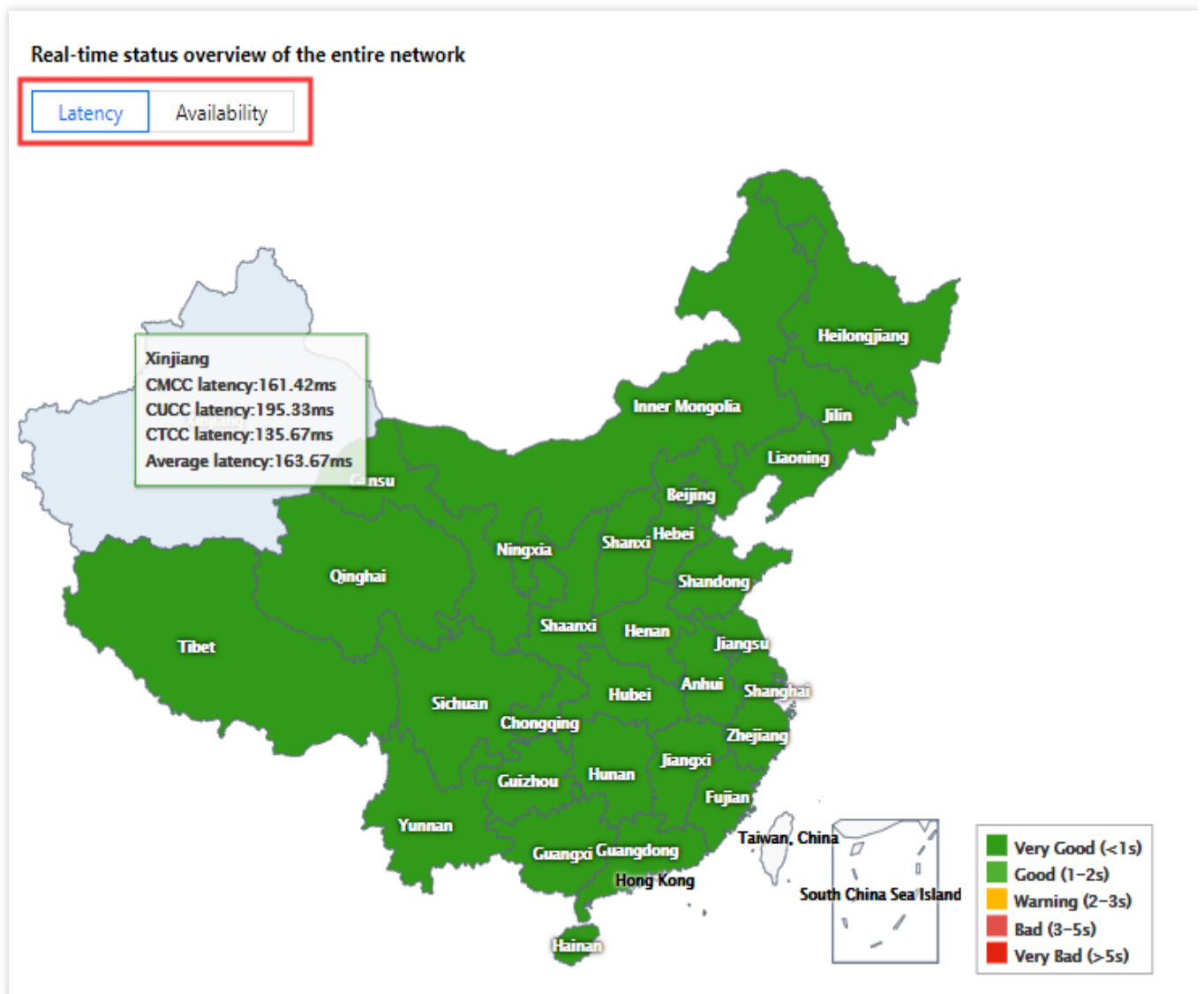
Log in to the [CDN Console](#) and click **Global Status** on the left sidebar to enter the real-time status overview of the entire network page.

Real-time status overview of the entire network

In **Real-time status overview of the entire network**, you can view the latency and availability status of ISP in each province in Mainland China and each region outside Mainland China. You can hover over a region in the map to view the corresponding data.

Real-time data in the map is updated every minute.

1. Mainland China



Hover over a province to see the data of three major ISPs (China Mobile, China Unicom, and China Telecom). Small and medium-sized ISPs are included when calculating the average latency or availability.

2. Outside Mainland China

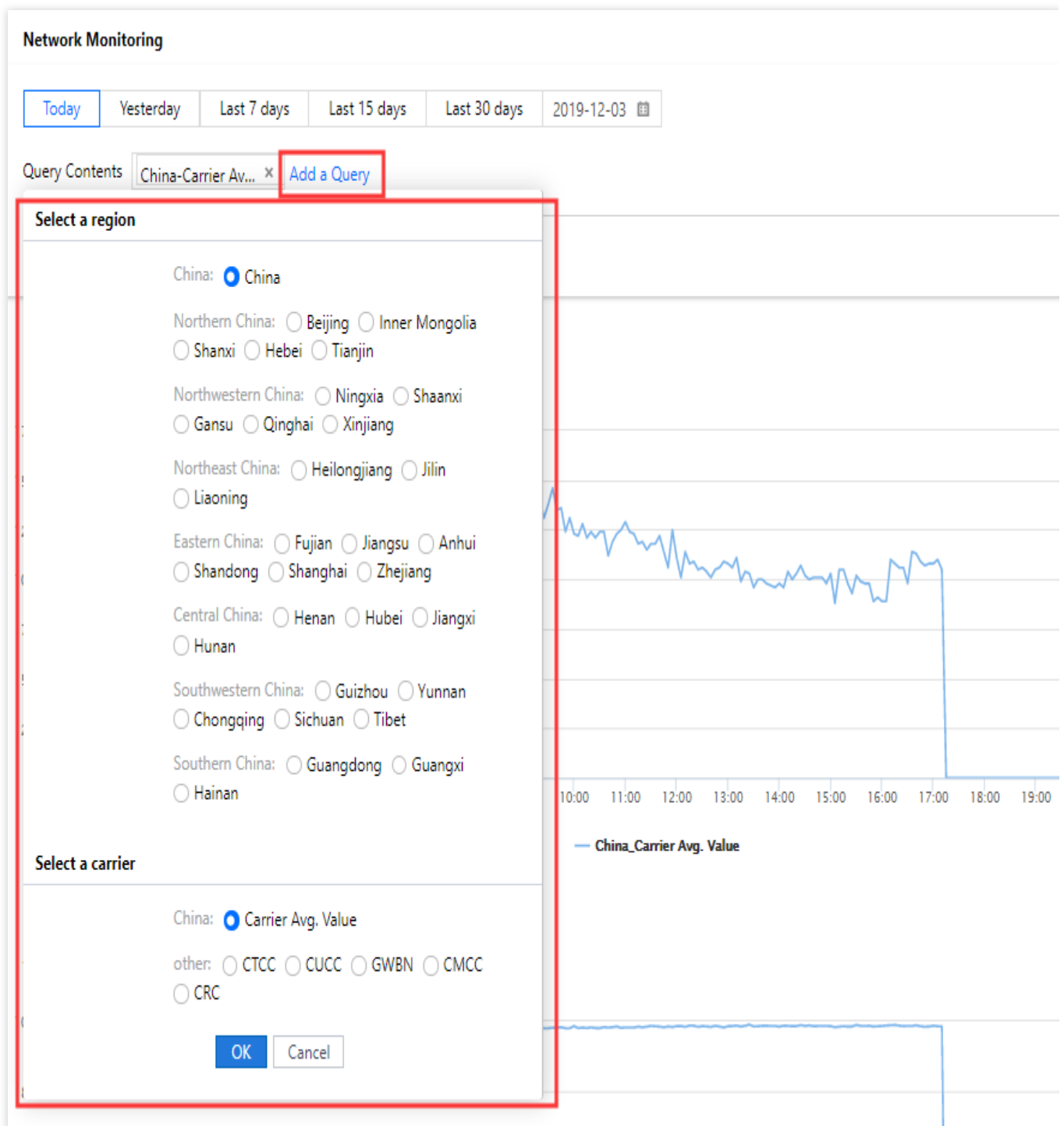
Entire network status details

In **Network Monitoring**, you can view the historical latency and availability curves of a specified region or ISP in Mainland China or a specified region outside Mainland China for a specified time period.

Time period: you can query the access statistics for the last 30 days with a maximum time span of 30 days.

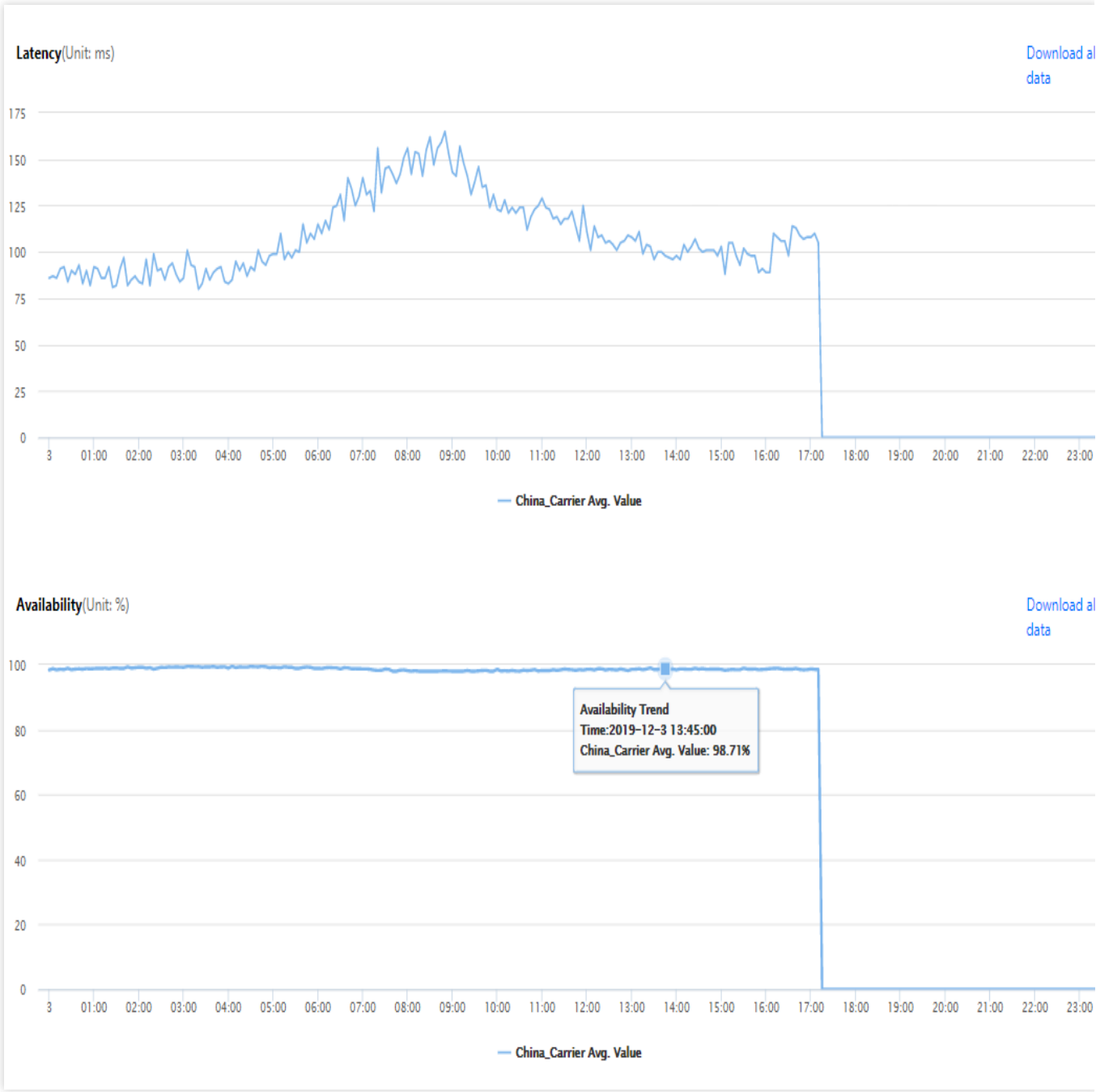
1. Mainland China

You can add multiple query criteria at a time to view multiple curves.



2. Outside Mainland China

You can select multiple regions at a time to view multiple curves.



Verify Tencent IP

Last updated : 2024-12-30 21:51:39

Feature Overview

CDN offers a tool for querying IP ownership. This tool can be used to verify whether a specified IP is of a CDN global cache node, and check the IP's acceleration service region, district, and ISP.

Overview

This tool can be used for troubleshooting. When there is an access exception, you can query the IP accessed in the following ways:

If the IP is not of a Tencent Cloud CDN node, the problem may be caused by domain name resolution exception.

Please go to your DNS service provider and check whether the CNAME configuration is correct;

If the IP is of a Tencent Cloud CDN node, you can check the node service status to see whether requests are interrupted by node activation/deactivation.

Operation Guide

Query Method

Log in to the [CDN console](#) and select **Inspect Tool -> Verify Tencent Cloud CDN IP** on the left sidebar.

The screenshot displays the 'Verify Tencent Cloud CDN IP' interface. At the top, the title 'Verify Tencent Cloud CDN IP' is shown. Below it, there is a section labeled 'Verify Server IP'. Inside this section, there is a text input field with the placeholder text 'Enter IP addresses you want to query (up to 20, one per line)'. Below the input field is a button labeled 'Verify'. At the bottom of the section, there is a small note: 'Verify whether the specified IP is a Tencent Cloud CDN server IP; support IPv6 format IP'.

Use Limits

Enter the IP addresses to be verified in the text box (one address per line).

Up to 20 IP addresses can be verified at a time.

Verification of IPv4 and IPv6 addresses is supported.

Verification is supported for global cache nodes. For nodes in the Chinese mainland, data of the ISP in the corresponding district will be returned; for nodes outside the Chinese mainland, data of the corresponding country/region will be returned.

You can view the node service status **for the last 3 hours**. If there were activation/deactivation status changes, the corresponding operation time will be displayed.

Use Cases

Nodes in the Chinese mainland

Verify Tencent Cloud CDN IP

Verify Server IP

124.232.162.187

Verify

Verify whether the specified IP is a Tencent Cloud CDN server IP; support IPv6 format IP

IP	Whether a Tencent Cloud CDN server	Service Region Distribution	Region	Service status ⓘ
124.232.162.187	Yes	China		Normal Service

Nodes outside the Chinese mainland

Verify Tencent Cloud CDN IP

Verify Server IP

211.152.130.101

Verify

Verify whether the specified IP is a Tencent Cloud CDN server IP; support IPv6 format IP

IP	Whether a Tencent Cloud CDN server	Service Region Distribution	Region	Service status ①
211.152.130.101	Yes	International	<div></div>	Normal Service

Origin-pull Node Query

Last updated : 2024-12-30 21:51:54

Description

Tencent Cloud CDN allows you to query the IPs or IP ranges of origin-pull nodes by specifying an acceleration domain name.

Use Cases

You can query the IPs or IP ranges of origin-pull nodes based on your requirements for business access control.

Directions

Log in to the [CDN console](#) and choose **Service Query > Verify Origin-pull Node** on the left sidebar.

Verify Origin-pull Node

① The origin-pull node query tool can access the origin-pull node IP through accelerated domain name query, and supports two types: IP address and IP segment. If your origin server has IP access restrictions, you can add the queried IP segment to the origin server I

Acceleration domain name

Queried Region ☒ Chinese mainland ☐ Overseas ☐ Global

Query Type ☒ IP range ☐ IP address

Use instructions:

Specify a valid acceleration domain name that is connected to CDN and enabled.

When you configure the **Queried Region** parameter, select the acceleration region that corresponds to your acceleration domain name.

Specify whether to query the IPs or IP ranges of origin-pull nodes based on your actual business needs.

ISP information is not supported if you select **Overseas** as **Queried Region**.

You can download the query results to your local device.

Content Compliance

Last updated : 2024-12-30 21:52:30

Feature Overview

Contents delivered through Tencent Cloud CDN must be compliant with the related laws and regulations. Restricted contents will be banned. You can check these contents and more details in **Content Compliance** page.

View Configuration

Log in to the [CDN console](#) and select **Inspect Tool > Content Compliance**.

Content Compliance

Content Compliance Instructic

The content on CDN must be compliant with the Chinese national laws and regulations. If you have any non-compliant content on the public delivery network, the Tencent Cloud compliance team will handle it.

Today

Yesterday

Last 7 Days

Last 30 days

2020-11-15 ~ 2020-12-14

Enter URL keyword to search.

URL	Reason	Time
No data yet		

Total items: 0

10 / page

1 / 1 page

Quota Management

Last updated : 2024-12-30 21:52:45

Overview

Quota management is a feature that enables you to view and manage quotas in the CDN console. The following quota types can be requested on a temporary or permanent basis: URL purge quota, directory purge quota, and URL prefetch quota.

Use Cases

Temporary quota is a quota that can be applied on a temporary basis and used within a validity period. When it expires, the quota type will end up as permanent.

Permanent quota is a quota that can be used for an indefinite period. As the permanent quota application takes a long time to process, we recommend requesting a temporary quota to meet your needs.

Operation Guide

Viewing quotas

To view quotas, log in to the [CDN console](#), and then select **Quota Management > Quota Details** on the left sidebar.

Coverage Area

Global

Enter the quota name

Quota name	Description	Coverage Area	Permanent quota	Temporary quota	Current quota	Used amount	Unit	Operation
Quota of URL purge li...	Daily URL purge limit	Chinese Mainland	10000	-	10000	0 <div></div>	PCS	Apply Application reco
Quota of URL purge li...	Daily URL purge limit	Overseas	10000	-	10000	0 <div></div>	PCS	Apply Application reco
Quota of directory pu...	Daily directory purge l...	Chinese Mainland	100	-	100	0 <div></div>	PCS	Apply Application reco
Quota of directory pu...	Daily directory purge l...	Overseas	100	-	100	0 <div></div>	PCS	Apply Application reco
Quota of URL prefetch...	Daily URL prefetch limit	Chinese Mainland	1000	-	1000	0 <div></div>	PCS	Apply Application reco
Quota of URL prefetch...	Daily URL prefetch limit	Overseas	1000	-	1000	0 <div></div>	PCS	Apply Application reco

Total items: 6

10 / page

1 / 1 page

Note:

Current quota indicates the maximum limit. If you have more than one temporary quotas, the current quota will be the maximum of all your quotas.

The temporary quota takes effect between 00:00-24:00 (UTC+8). After it expires, the quota type will turn permanent. URL purge quota, directory purge quota and URL prefetch quota all take effect on a daily basis and reset every day at 00:00 (UTC+8).

Quotas for regions in and outside the Chinese mainland are independent of each other and need to be applied separately.

Applying for quotas

To apply for a quota, click **Apply**. Complete and submit the application form.


Quota application

Quota name

Quota of URL purge limit

Quota description

Daily URL purge limit

Coverage Area	Chinese Mainland
Used amount	0
Increase Quota *	<input type="text" value="10001"/> Range: [10001, 10000000]
Quota type *	<div>Temporary quota ▼</div>
Validity period *	<div>2022-04-18 ~ 2022-04-19 </div> <p>For temporary quotas, the maximum validity period is 90 days, and the maximum application period is 7 days. Once your temporary quota runs out, the quota type will end up as permanent.</p>
Reason *	<div></div>
<div><div>Submit</div><div>Cancel</div></div>	

Note:




A temporary quota must be between a permanent quota +1 and 10000000.

For temporary quotas, the maximum validity period is 90 days, and the maximum application period is 7 days.

To request a quota successfully, you are encouraged to set an appropriate quota value and state the reason for your application.

Viewing application records

To view your application records, click **Application records** on the **Quota Details** page, or select **Quota Management > Application Records** on the left sidebar.

Application time 2022-03-20 ~ 2022-04-18 								Enter the quota name
Quota name	Coverage Area	Increase Quota	Quota type	Validity period	Status	Application result	Application time	Approval comment
Quota of directory purge limit	Overseas	101	Temporary quota	2022-04-18-2022-04-19	-	Pending approval	2022-04-18 12:05	-
Quota of URL purge limit	Chinese Mainland	10001	Temporary quota	2022-04-18-2022-04-19	Activated	Passed	2022-04-18 12:05	Application is approved
Total items: 2							10 ▾ / page	  1 / 1 page

Note:

When the application result is **Passed**, your application is accepted. If you failed to apply for a permanent quota, you can change your quota limit and reason for application before submitting again, or request a temporary quota instead. 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.

Offline Cache

Last updated : 2024-12-30 21:53:19

Overview

When your origin 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:

Offline cache is supported only for acceleration domain names in the Chinese mainland.

This feature may be unavailable in some platforms. We will complete server upgrade as soon as possible.

Directions

Viewing the configuration

Offline cache is disabled by default. You can enable it as needed.