Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

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

Trademark Notice

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

Service Statement

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

Management Description
Domain Management
Domain Name Operations
Domain name search
Configuration Management
Configuration Overview
Basic Configurations
Basic Information
Origin Server Configuration
HTTPS Origin-pull algorithm description
Access Control
Hotlink Protection Configuration
IP Blacklist/Whitelist Configuration
IP Access Limit Configuration
Video Dragging Configuration
Authentication Configuration
Instruction
TypeA
TypeB
TypeC
TypeD
Cache Configuration
Ignore query string configuration
Cache Expiration Configuration
Status code cache configuration
HTTP Header Cache Configuration
Cache Configuration
Origin-pull Configuration
Range GETs Configuration
Follow 301/302 Configuration
Origin-pull timeout configuration
HTTPS Acceleration Configuration
HTTPS Configuration
HTTPS Acceleration Configuration Guide
HTTPS forced Redirect
HTTP2.0 configuration
OCSP binding configuration
FAQs about HTTPS
Advanced Configuration
  Bandwidth Cap Configuration
  HTTP Header Configuration
  SEO Optimization Configuration
  Smart Compression Configuration
Permission Management
  Policy creation
  Console Permissions
  Project-Level Permissions
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
  Cache Purge
  FAQs about Cache Purge
Log Management
  Log Download
  Real-Time Log
Service Query
  Entire Network Status Monitoring
  Operational Report
Diagnosis Tools
  Verify Tencent IP
  Self-Diagnosis Tool
Value-added Services
  Pornography Detection
Operation Scenario

After you connect a domain name to Tencent Cloud CDN, you can log in to the CDN Console and select Domain Management on the left sidebar to view, enable, or disable the acceleration domain name.

CDN allows you to customize the domain name list page to display multiple basic configuration items and adjust their order as needed. In addition, you can activate or disable in batches the acceleration service for domain names, improving business management efficiency.

List Operation Guide

Customizing the list display

Click the Customize icon to the right of the search box to display the customization option box:
You can choose to display or hide fields and adjust their display order:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>required and cannot be hidden.</td>
</tr>
<tr>
<td>Service type</td>
<td>static acceleration, download acceleration, or streaming VOD acceleration.</td>
</tr>
<tr>
<td>Status</td>
<td>domain name service status (activated, disabled, or deploying).</td>
</tr>
<tr>
<td>CNAME</td>
<td>CNAME record of the domain name.</td>
</tr>
<tr>
<td>Origin type</td>
<td>external origin server or COS origin server.</td>
</tr>
<tr>
<td>Service region</td>
<td>mainland China, outside mainland China, or global.</td>
</tr>
<tr>
<td>Project</td>
<td>name of the project to which the domain name belongs.</td>
</tr>
<tr>
<td>Primary origin</td>
<td>primary origin server address.</td>
</tr>
<tr>
<td>Backup origin</td>
<td>backup origin server address.</td>
</tr>
<tr>
<td>HTTPS configuration</td>
<td>configured or not configured.</td>
</tr>
<tr>
<td>Origin-pull protocol</td>
<td>HTTP, HTTPS, or follow protocol.</td>
</tr>
<tr>
<td>Origin domain</td>
<td>origin-pull domain name configuration.</td>
</tr>
</tbody>
</table>
• Ignore query string: enabled or disabled.

**Exporting the configuration list**

Click the **Export** icon to the right of the search box to export the domain name list as an Excel file.

- The exported content only contains the domain names and configuration items currently displayed on the domain name list page. It will not contain all domain names and basic configuration items.
- Up to 3,000 domain names can be exported at a time.

![Domain Name List](image)

**Domain Name Operation Guide**

On the CDN Console, you can activate, disable, and delete the acceleration service and modify the projects for acceleration domain names.

**Disabling the acceleration service**

After the acceleration service is disabled for a domain name, its configurations will be deactivated on cache nodes across the entire network. If access requests to the domain name are still redirected to CDN nodes, error 404 will be returned. Before disabling a domain name, make sure that its CNAME record is pointing to a non-CDN CNAME address.

- You can only disable activated acceleration domain names. Domain names in deployment cannot be disabled.
- Configurations of disabled domain names will be retained and take effect when the domain names are reactivated.
- Consumption will no longer be generated after the acceleration service is completely disabled.

You can click **Disable** in the "Operation" column on the right of the domain name to disable the service. You can also select multiple domain names in **Activated** status and disable them in batches.
Enabling the acceleration service

If a domain name is in Disabled status, you can activate the acceleration service to distribute its configuration to cache nodes across the entire network again:

You can click Activate in the "Operation" column on the right of the domain name to enable the service. You can also select multiple domain names in Disabled status and activate them in batches via More Actions at the top.

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

Deleting an acceleration domain name

If a domain name is in Disabled status, you can click More on the right to delete it. Note that once a domain name is deleted, its configuration will be cleared and cannot be restored and its statistical
data can no longer be viewed.
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.

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.
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

<table>
<thead>
<tr>
<th>Type</th>
<th>Input Format</th>
<th>Example</th>
<th>Search Box Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single keyword</td>
<td><strong>Keyword</strong></td>
<td><a href="http://www.test.com">www.test.com</a></td>
<td></td>
<td>Filters domain names containing <a href="http://www.test.com">www.test.com</a></td>
</tr>
<tr>
<td>Single domain name attribute</td>
<td><strong>Attribute:keyword</strong></td>
<td>Origin server:1.1.1</td>
<td></td>
<td>Filters domain names where the origin server contains 1.1.1</td>
</tr>
<tr>
<td>Multiple domain name attributes</td>
<td><strong>Attribute:keyword carriage return</strong></td>
<td>Domain name:test Origin server:1.1.1</td>
<td></td>
<td>Filters domain names where the domain name contains &quot;test&quot; and origin server contains &quot;1.1.1&quot;</td>
</tr>
<tr>
<td>Type</td>
<td>Input Format</td>
<td>Example</td>
<td>Search Box Example</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------</td>
<td>------------------</td>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Single domain name attribute with multiple keywords</td>
<td>**Attribute:keyword</td>
<td>keyword**</td>
<td>Project:test1</td>
<td>test2</td>
</tr>
<tr>
<td>Copied character</td>
<td>(Pasted character)</td>
<td>test abc</td>
<td></td>
<td>Filters domain names containing &quot;test&quot; or &quot;abc&quot;</td>
</tr>
</tbody>
</table>

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`. 
Configuration Management

Configuration Overview

Last updated: 2020-05-26 10:38:17

CDN supports various custom configurations that allow you to optimize your CDN acceleration service based on your business needs.

Basic Configuration

<table>
<thead>
<tr>
<th>Configuration Name</th>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td>You can change the domain name project, service region, and business type.</td>
</tr>
<tr>
<td>Origin Server Configuration</td>
<td>You can configure the basic information of the origin server, the origin-pull request protocol, the origin domain, and the hot backup origin server to ensure smooth origin-pull. You can configure the settings in/outside mainland China differently.</td>
</tr>
</tbody>
</table>

Access Control

<table>
<thead>
<tr>
<th>Configuration Name</th>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore Query String Configuration</td>
<td>You can specify whether a node will ignore the parameters after &quot;?&quot; in a user request URL.</td>
</tr>
<tr>
<td>Hotlink Protection Configuration</td>
<td>You can configure the HTTP referer blacklist/whitelist. You can configure the settings in/outside mainland China differently.</td>
</tr>
<tr>
<td>IP Blacklist/Whitelist Configuration</td>
<td>You can configure the IP blacklist/whitelist for access control.</td>
</tr>
<tr>
<td>IP Access Limit Configuration</td>
<td>You can configure the access limit of an IP to a single node.</td>
</tr>
<tr>
<td>Video Dragging Configuration</td>
<td>You can enable the video dragging configuration.</td>
</tr>
<tr>
<td>Authentication Configuration</td>
<td>You can configure the URL authentication. You can configure the settings in/outside mainland China differently.</td>
</tr>
</tbody>
</table>
Cache Expiration Configuration

<table>
<thead>
<tr>
<th>Configuration Name</th>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Expiration Configuration</td>
<td>You can configure the cache expiration rules for the specified resources.</td>
</tr>
<tr>
<td>Status Code Cache Configuration</td>
<td>You can configure the 403 and 404 status code cache period.</td>
</tr>
<tr>
<td>HTTP Header Cache Configuration</td>
<td>You can configure the header cache policy.</td>
</tr>
</tbody>
</table>

Origin-Pull Configuration

<table>
<thead>
<tr>
<th>Configuration Name</th>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range GETs Configuration</td>
<td>You can enable/disable Range GETs.</td>
</tr>
<tr>
<td>Follow 301/302 Configuration</td>
<td>You can configure whether requests should be redirected when the origin server returns the 301/302 status code.</td>
</tr>
<tr>
<td>Origin-Pull Timeout Configuration</td>
<td>You can configure the timeout periods for origin-pull TCP connection and data loading to ensure smooth origin-pull.</td>
</tr>
</tbody>
</table>

Advanced Configuration

<table>
<thead>
<tr>
<th>Configuration Name</th>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Cap Configuration</td>
<td>You can configure the bandwidth cap for domain names. When the cap is reached, the CDN service will be disabled and the access request will be forwarded to the origin server. You can configure the settings in/outside mainland China differently.</td>
</tr>
<tr>
<td>HTTPS Configuration</td>
<td>You can configure HTTPS to implement secure acceleration, which supports forced HTTPS redirection, HTTP2.0 access, and OCSP stapling.</td>
</tr>
<tr>
<td>SEO Optimization Configuration</td>
<td>You can enable SEO optimization configuration to ensure the stability of the search engine weights.</td>
</tr>
<tr>
<td>HTTP Header Configuration</td>
<td>You can add a HTTP header configuration.</td>
</tr>
</tbody>
</table>
Basic Configurations
Basic Information

Last updated: 2020-06-02 14:29:16

Configuration

For services that have been connected to Tencent Cloud CDN, you can view information such as domain name creation time, corresponding CNAME domain name, service region, project, service type, and supported protocols on the basic information module of the domain name. You can also modify information such as service 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, and click Manage on the right of the domain name to access its configuration page. The first module displays its basic information.

![Basic info]

- IPv6 is only supported in mainland China.
If you select "IPv4 + IPv6" when connecting the domain name, the node will support both IPv4 and IPv6 access requests.

**Modifying basic information**

1. **Modify the project**

Click **Modify** on the right of the project to modify the project to which the domain name belongs. Note that modifying the project will change the project statistics and sub-user permissions granted by the project.

To create a project or manage existing projects, go to the **Project Management** page.

2. **Modify the domain name service region**

**Definition of the domain name service region:**

- If a domain name is configured for global acceleration, requests will be scheduled to the nearest global CDN cache node. In general, nodes in and outside of mainland China serve users in and outside of mainland China, respectively.
- If a domain name is configured for acceleration in mainland China, access requests from global users will be served by cache nodes in mainland China.
- If a domain name is configured for acceleration outside mainland China, access requests from global users will be served by cache nodes outside mainland China.
You can click **Modify** on the right of the service region to modify it:

![Switch Service Region](image)

Acceleration services in and outside of mainland China are billed separately at different prices. For more information, please click [here](#).

### 3. Modify the service type

CDN optimizes acceleration performance based on the service type. For the best acceleration result, we recommend you select the service type similar to that of your actual services. If you want to adjust the service type, click **Modify** on the right:

- Modifying the service type will change the underlying CDN acceleration platform, which may generate a small number of failed requests and increase origin-pull bandwidth. We recommend you do this during off-peak hours.
- If you cannot find **Modify** next to your domain name, it may have special configuration. You can [contact us](#) for assistance.
Origin Server Configuration

Configuration

You can modify information such as domain name basic information, origin-pull request protocol, and origin domain in the origin server configuration module.

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 the domain name to access its configuration page. Under "Basic info", you can find the origin server configuration module.

Origin Server Type

- **External**: select this type if you already have your own stable business server (i.e., origin server). Enter the corresponding IP address list or domain name as the origin server address.
- **COS Origin**: if resources have already been stored in COS, the bucket can be selected as the origin server.

Origin Server Address

The origin server address can contain up to 511 characters and supports origin-pull for multiple IPs with one domain name.
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.

Origin Domain
The site domain name accessed on the origin server by a CDN node during origin-pull. For more information, please see Origin-Pull Domain Name Configuration.

Modifying the configuration

1. Modify the primary origin server configuration
Click Edit on the top-right corner to modify the configuration of the primary origin server:

Modify origin server info

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceleration Domain</td>
<td>chris9.elliotxing.com</td>
</tr>
<tr>
<td>Origin Type</td>
<td>External</td>
</tr>
<tr>
<td>Origin-pull Protocol</td>
<td>HTTP</td>
</tr>
<tr>
<td>Origin address</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>Host header</td>
<td>1.test.com</td>
</tr>
</tbody>
</table>

Modify the origin server address
If external origin server is selected, you can enter up to 511 characters for the origin server address. The following configuration modes are supported:
- **Multi-IP round-robin origin-pull:** if multiple IPs are entered for the origin server, round-robin origin-pull will be used. The origin server detection feature of CDN is enabled by default. When the number of failed origin-pulls of an IP exceeds the threshold, requests will no longer be forwarded to this address, which will be blocked for a period of time and then automatically resumed.

- **IPv6 origin server:** if you have IPv6 beta eligibility and selected "IPv4 + IPv6" as the request protocol of the domain name, you can enter an IPv6 address as the origin server.

- **Origin-pull to custom port:** "IP:port" format is supported. HTTP protocol supports the custom port between 1 and 65535. HTTPS protocol currently only supports port 443.

- **Weighed origin-pull:** "IP:port:weight" format is supported where the weight is between 1 and 100. The default port can be used.

- **Origin-pull to domain name:** enter only one independent domain name for the origin server (currently, origin-pull to IPv6 domain name is not supported).

### Modify the origin-pull protocol

You can configure origin-pull protocol for the domain name to HTTP, HTTPS, or follow protocol in the origin server configuration section:

- **HTTP:** HTTP origin-pull is used for access requests over both HTTP and HTTPS.
- **HTTPS:** HTTPS origin-pull is used for access requests over both HTTP and HTTPS.
- **Follow protocol:** HTTP requests use HTTP origin-pull, while HTTPS requests use HTTPS origin-pull.

- If you select HTTPS origin-pull or follow protocol, make sure the origin server supports HTTPS access. Otherwise, origin-pull will fail.
- Currently, you can still modify this configuration item on the certificate management page. However, it will be migrated in the future.

### Modify the origin domain

When a domain name is connected, the default origin domain will be the acceleration domain name. If a wildcard domain name is connected, it will be the default origin domain, while the actual origin domain will be the access domain name. You can modify it here as needed.

If COS is used as the origin server, the origin domain cannot be modified.

### 2. Configure the hot backup origin server

If your primary origin server is an external one, you can add a hot backup 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 and ensure the high availability of origin-pull.

You can configure origin-pull protocol and origin domain for the hot backup origin server differently from those for the primary origin server.

3. Add the region-specific configuration

If your acceleration domain name is configured for global acceleration and you want to avoid cross-border traffic, you can click Add Special Configuration at the bottom to configure different origin servers for different service regions of the domain name:

Select regions that need different origin-pull policies and enter the corresponding origin server.
information:

- After the region-specific configuration is added, it currently cannot be directly deleted.
- If the region-specific configuration is the same as the basic configuration, they will automatically merge. You can configure them to be the same to delete the region-specific configuration.

Configuration Sample
Origin-pull domain name configuration

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

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

Suppose the CDN origin server and the acceleration domain name www.test.com are configured as follows:
The actual origin-pull will then be:

1. When a user in mainland China accesses the file http://www.test.com/test.txt and the node in mainland China 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 1.test.com, and then cache and return it to the user.

3. At this time, a user outside of mainland China accesses the file http://www.test.com/test.txt. As the node outside of mainland China 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 of mainland China fails to forward the request to the primary origin server outside of mainland China 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 of mainland China.
<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Algorithm</th>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDHE-RSA-AES256-SHA</td>
<td>ECDHE-RSA-AES256-SHA384</td>
<td>ECDHE-RSA-AES256-GCM-SHA384</td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES256-SHA</td>
<td>ECDHE-ECDSA-AES256-SHA384</td>
<td>ECDHE-ECDSA-AES256-GCM-SHA384</td>
</tr>
<tr>
<td>SRP-AES-256-CBC-SHA</td>
<td>SRP-RSA-AES-256-CBC-SHA</td>
<td>SRP-DSS-AES-256-CBC-SHA</td>
</tr>
<tr>
<td>DH-RSA-AES256-SHA</td>
<td>DH-RSA-AES256-SHA256</td>
<td>DH-RSA-AES256-GCM-SHA384</td>
</tr>
<tr>
<td>DH-DSS-AES256-SHA</td>
<td>DH-DSS-AES256-SHA256</td>
<td>DH-DSS-AES256-GCM-SHA384</td>
</tr>
<tr>
<td>DHE-RSA-AES256-SHA</td>
<td>DHE-RSA-AES256-SHA256</td>
<td>DHE-RSA-AES256-GCM-SHA384</td>
</tr>
<tr>
<td>DHE-DSS-AES256-SHA</td>
<td>DHE-DSS-AES256-SHA256</td>
<td>DHE-DSS-AES256-GCM-SHA384</td>
</tr>
<tr>
<td>CAMELLIA256-SHA</td>
<td>DH-RSA-CAMELLIA256-SHA</td>
<td>DHE-RSA-CAMELLIA256-SHA</td>
</tr>
<tr>
<td>PSK-3DES-EDE-CBC-SHA</td>
<td>DH-DSS-CAMELLIA256-SHA</td>
<td>DHE-DSS-CAMELLIA256-SHA</td>
</tr>
<tr>
<td>ECDH-RSA-AES256-SHA</td>
<td>ECDH-RSA-AES256-SHA384</td>
<td>ECDH-RSA-AES256-GCM-SHA384</td>
</tr>
<tr>
<td>ECDH-ECDSA-AES256-SHA</td>
<td>ECDH-ECDSA-AES256-SHA384</td>
<td>ECDH-ECDSA-AES256-GCM-SHA384</td>
</tr>
<tr>
<td>AES256-SHA</td>
<td>AES256-SHA256</td>
<td>AES256-GCM-SHA384</td>
</tr>
<tr>
<td>ECDHE-RSA-AES128-SHA</td>
<td>ECDHE-RSA-AES128-SHA256</td>
<td>ECDHE-RSA-AES128-GCM-SHA256</td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES128-SHA</td>
<td>ECDHE-ECDSA-AES128-SHA256</td>
<td>ECDHE-ECDSA-AES128-GCM-SHA256</td>
</tr>
</tbody>
</table>

HTTPS Origin-pull algorithm description

Last updated: 2020-04-13 20:19:39
<table>
<thead>
<tr>
<th>SSL/TLS Cipher Suite</th>
<th>ECDHE-RSA-AES256-SHA384</th>
<th>ECDHE-RSA-AES256-GCM-SHA384</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDHE-RSA-AES256-SHA</td>
<td>SRP-AES-128-CBC-SHA</td>
<td>SRP-DSS-AES-128-CBC-SHA</td>
</tr>
<tr>
<td>DP-API-DSS-AES128-SHA256</td>
<td>DH-RSA-AES128-SHA256</td>
<td>DH-RSA-AES128-GCM-SHA256</td>
</tr>
<tr>
<td>DP-API-DSS-AES128-SHA256</td>
<td>DH-DSS-AES128-SHA256</td>
<td>DH-DSS-AES128-GCM-SHA256</td>
</tr>
<tr>
<td>DP-API-DSS-AES128-SHA256</td>
<td>ECDH-RSA-AES128-SHA256</td>
<td>ECDH-RSA-AES128-GCM-SHA256</td>
</tr>
<tr>
<td>DP-API-DSS-AES128-SHA256</td>
<td>ECDH-ECDSA-AES128-SHA256</td>
<td>ECDH-ECDSA-AES128-GCM-SHA256</td>
</tr>
<tr>
<td>DP-API-DSS-AES128-SHA256</td>
<td>CAMELLIA128-SHA</td>
<td>DHE-RSA-CAMELLIA128-SHA</td>
</tr>
<tr>
<td>DP-API-DSS-AES128-SHA256</td>
<td>PSK-RC4-SHA</td>
<td>DHE-DSS-CAMELLIA128-SHA</td>
</tr>
<tr>
<td>AES128-SHA</td>
<td>AES128-SHA256</td>
<td>AES128-GCM-SHA256</td>
</tr>
<tr>
<td>SEED-SHA</td>
<td>DH-RSA-SEED-SHA</td>
<td>DH-DSS-SEED-SHA</td>
</tr>
<tr>
<td>DES-CBC3-SHA</td>
<td>DHE-RSA-SEED-SHA</td>
<td>DHE-DSS-SEED-SHA</td>
</tr>
<tr>
<td>IDEA-CBC-SHA</td>
<td>PSK-AES256-CBC-SHA</td>
<td>PSK-AES128-CBC-SHA</td>
</tr>
<tr>
<td>EDH-RSA-DES-CBC3-SHA</td>
<td>ECDH-RSA-DES-CBC3-SHA</td>
<td>ECDHE-RSA-DES-CBC3-SHA</td>
</tr>
<tr>
<td>EDH-DSS-DES-CBC3-SHA</td>
<td>ECDH-ECDSA-DES-CBC3-SHA</td>
<td>ECDHE-ECDSA-DES-CBC3-SHA</td>
</tr>
<tr>
<td>RC4-SHA</td>
<td>ECDH-RSA-RC4-SHA</td>
<td>ECDHE-RSA-RC4-SHA</td>
</tr>
<tr>
<td>RC4-MD5</td>
<td>ECDH-ECDSA-RC4-SHA</td>
<td>ECDHE-ECDSA-RC4-SHA</td>
</tr>
<tr>
<td>Cipher Suite 1</td>
<td>Cipher Suite 2</td>
<td>Cipher Suite 3</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-SHA</td>
<td>ECDHE-RSA-AES256-SHA384</td>
<td>ECDHE-RSA-AES256-GCM-SHA384</td>
</tr>
<tr>
<td>SRP-3DES-EDE-CBC-SHA</td>
<td>SRP-RSA-3DES-EDE-CBC-SHA</td>
<td>SRP-DSS-3DES-EDE-CBC-SHA</td>
</tr>
<tr>
<td>DH-DSS-DES-CBC3-SHA</td>
<td>DH-RSA-DES-CBC3-SHA</td>
<td>-</td>
</tr>
</tbody>
</table>
Access Control

Hotlink Protection Configuration

Configuration Scenario

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 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 enter its configuration page. Under the Access Control tab, find the hotlink protection configuration, which is disabled by default:

![Hotlink Protection Configuration](image)

Modifying configuration

1. **Modify the configuration**

Switch to select the hotlink protection type, enter the corresponding information, select whether to allow blank referer, and click OK to enable hotlink protection.
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 selected, 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 whitelist:

- If the referer field of a request matches the string configured in the whitelist, CDN node will return the requested information.
- If the referer field of a request does not match the string configured in the whitelist, CDN node will not return the requested information and a 403 status code will be returned.
- Once the whitelist is configured, CDN node can only return requests that match the string configured in the whitelist.
- If Allow empty referer is selected, 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 rules:

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

2. Disable the configuration

You can switch to disable the hotlink protection feature. When the switch is off, this feature will not take effect in the production environment even if there is an existing configuration. If the switch is on, a message will be displayed to confirm whether to enable this feature before the configuration takes effect across the entire network.

3. Add region-specific configuration

If your acceleration domain name is configured for global acceleration and you want different referer hotlink protection configurations for acceleration in and outside of Mainland China, click Add Special
After a region-specific configuration item is added, it cannot be directly deleted for the time being. You can only disable it.

Configuration Sample

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

The actual access status will be as follows:

1. If a user in Mainland China whose referer is 1.1.1.1 initiates a request, the whitelist configured for Mainland China will be hit and the requested content will be directly returned.
2. If a user outside Mainland China whose referer is empty initiates a request, the blacklist configured for regions outside Mainland China will be hit and a 403 code will be returned.
IP Blacklist/Whitelist Configuration

Last updated: 2020-04-13 19:42:02

Configuration Scenario

To control the source of access to your business resources, you can use the IP blacklist/whitelist 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.

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 enter its configuration page. Under the Access Control tab, find the IP blacklist/whitelist configuration, which is disabled by default:

Modifying configuration

1. Modify the configuration

Switch to select "IP Blacklist" or "IP Whitelist", enter the list of IPs or IP ranges, and click OK to enable IP blacklist/whitelist configuration:
IP blacklist
If a client IP matches an IP or IP range in the blacklist, the accessed CDN node will directly return a 403 status code.

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

Blacklist/Whitelist rules
- The IP blacklist and whitelist are mutually exclusive and cannot be configured at the same time.
- Only IP ranges /8, /16, and /24 are supported.
- The blacklist/whitelist does not support entries in IP:port format and can contain up to 50 entries.

2. Disable the configuration
You can switch to disable the IP blacklist/whitelist feature. When the switch is off, this feature will not take effect in the production environment even if there is an existing configuration. When the switch is on, a message will be displayed to confirm whether to enable this feature before the configuration
takes effect across the entire network.

If your acceleration domain name is configured for global acceleration, the IP blacklist/whitelist will take effect globally. This configuration does not distinguish between requests from and outside of Mainland China.

Configuration Sample

Suppose the IP blacklist/whitelist configuration of the acceleration domain name www.test.com is as follows:
The actual access status will be as follows:

1. A user with client IP 1.1.1.1 accesses the resource http://www.test.com/test.txt. As the IP matches an IP in the whitelist, the requested content will be returned.
2. A user with client IP 2.1.1.1 accesses the resource http://www.test.com/test.txt. As the IP does not match any IP in the whitelist, a 403 status code will be returned.
IP Access Limit Configuration

Last updated : 2020-04-13 19:42:03

Configuration Scenario

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

Configuration Guide

Viewing configuration

Log in to the CDN Console, select Domain Management on the left sidebar, and click Manage on the right of the domain name to enter its configuration page. Under the Access Control tab, find the IP access limit configuration. It is disabled by default, and the threshold is left empty:

![IP Access Limits](image)

Modifying configuration

1. Modify the configuration
Enter the frequency threshold and click **OK** to enable IP access limit.

### 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 the proper threshold 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.

### 2. Disable the configuration

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

Configuration Sample

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

```
<table>
<thead>
<tr>
<th>IP Access Limit</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Access Limit</td>
<td>1QPS</td>
</tr>
</tbody>
</table>
```

The actual access status will be as follows:

1. A user with 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 client IP 2.2.2.2 requests the resource http://www.test.com/1.jpg for 2 times 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: 2019-12-02 15:31:51

- Video dragging generally happens during on-demand video. When a user drags the video progress bar, a request similar to the one as shown below will be sent to the server:
  

  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.

- When enabling video dragging, you need to enable the ignore query string feature too, and the origin server must support range requests. Files in MP4, FLV and TS are supported:

<table>
<thead>
<tr>
<th>File Type</th>
<th>meta Information</th>
<th>start Parameter Description</th>
<th>Sample Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>MP4</td>
<td>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.</td>
<td>The start parameter specifies a time (in seconds) and uses decimal to specify a millisecond (for example, start = 1.01 means that the starting time is at 1.01s). CDN will locate the last key frame before the time specified by the start parameter (if start is not a key frame).</td>
<td><img src="http://www.test.com/demo.mp4?start=10" alt="http://www.test.com/demo.mp4?start=10" /> The video will be played back starting from the 10th second</td>
</tr>
<tr>
<td>FLV</td>
<td>The video on the origin server must have meta information.</td>
<td>The start parameter specifies a byte. CDN will automatically locate the last key frame before the byte specified by the start parameter (if start is not a key frame).</td>
<td><img src="http://www.test.com/demo.flv?start=10" alt="http://www.test.com/demo.flv?start=10" /> The video will be played back starting from the 10th byte</td>
</tr>
</tbody>
</table>
## File Type | meta Information | start Parameter Description | Sample Request
--- | --- | --- | ---
TS | No special requirements | The start parameter specifies a time (in seconds) and uses decimal to specify a millisecond (for example, start = 1.01 means that the starting time is at 1.01s). CDN will locate the last key frame before the time specified by the start parameter (if start is not a key frame) | http://www.test.com/demo.ts?start=10. The video will be played back starting from the 10th second |

### Configuration Guide

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

2. Find the domain name you want to edit and click **Manage** in the operation column.

3. Click the **Access Control** tab and configure the **Video Dragging** module. Video dragging is disabled by default.

4. Toggle the video dragging switch on. If the **Ignore Query String** feature is disabled, enabling video dragging will automatically enable that feature.
The CDN server will ignore all parameters after “?” in the URL. What's Filter Parameter?

Ignore Parameters

Hotlink Protection  Edit
Hotlink protection configuration will be set.
No hotlink protection rules set

Modify Video Dragging Configurations

You need to enable Filter Parameters first to enable Video Dragging. Click “Confirm” to enable both, or “Cancel” to discard this operation.

Confirm  Cancel

IP Blacklist & Whitelist  Edit
Set an IP blacklist and whitelist to filter.
No IP blacklist/whitelist rules set

IP Access Limits
Set an access frequency limit for a single IP to resist CC attacks. What's IP access limit?

IP access limit

IP access limit: 10QPS  Edit

1. The threshold defaults to the average daily accesses of an IP of this domain name.
2. Setting an access frequency for single IP can help resist CC attacks, however it may also block some normal accesses.

Video Dragging
By enabling this, you can specify the start point via “start”. mp4, flv and ts files are supported. Filter Parameter should be enabled as well. What's Video Dragging?
Authentication Configuration

Instruction

Last updated: 2020-05-26 10:38:17

Configuration

Generally, content 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 blacklist/whitelist, IP blacklist/whitelist, and IP access frequency limit.

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 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 Security Configuration tab, find the authentication configuration, which is disabled by default:

Modifying the configuration
1. Modify the configuration

CDN provides four authentication signature calculation models of your choice. You can open the Authentication Calculator at the top 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:

![Authentication Calculator](image)

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.
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.

Currently, an added region-specific configuration item cannot be deleted, and 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:

Then, 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`.
Algorithm Description

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

**Algorithm description**
- timestamp: a decimal timestamp in UNIX format.
- rand: a random string consisting of 0–100 uppercase and lowercase letters and digits.
- uid: 0.
- md5hash: MD5 (file path-timestamp-rand-uid-custom key).

**Sample request**
http://cloud.tencent.com/test/test.jpg?sign=1582791032-im1acp76sx9sdqe601v-0-dd63f95e739ed4b47427a129d21ef4e3

When 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**
TypeA requires the following configuration:

**Custom Authentication Key**: it contains 6–32 uppercase and lowercase letters and digits. The key should be kept private and known only to the client and server.

**Custom Authentication Parameter Name**: the `sign` in the example can be replaced with a parameter name containing 1–100 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 request, 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.

**Object**

After configuring the key, parameter name, and validity period, you can specify the authentication object as needed. The following three 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 TypeA 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 authentication parameter and thus not affect the cache hit rate.

**Origin-pull policy**
The access format of a domain name with TypeA 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: 2020-04-27 14:28:23

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
```

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 configuration:

Modify origin-pull timeout time

```
Modify origin-pull timeout time

Origin-pull load time (unit: second)  10

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

OK  Cancel

Custom Authentication Key: it can contain 6–32 case-sensitive letters and digits. It should be kept
private and disclosed to only the client and server.

**Custom Validity Period:** the timestamp value in the request path and 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:

- 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.

**Precautions**

**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, which does 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, 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.
Algorithm Description

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

Algorithm description
- timestamp: a hex timestamp in UNIX format.
- md5hash: MD5 (custom key + file path + timestamp).

Sample request
http://cloud.tencent.com/8fe9b5597c809d7ace147468c7c7eadb/5e577978/test/test.jpg

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
TypeC requires the following configuration:

**Custom Authentication Key**: it contains 6–32 uppercase and lowercase letters and digits. The key should be kept private and known only to 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 yes, 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 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 TypeC authentication for a domain name, it 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.
Algorithm Description

**Access URL format**

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

**Algorithm description**

- timestamp: a decimal or hex timestamp in UNIX format.
- md5hash: MD5 (custom key + file path + timestamp).

**Sample request**

http://cloud.tenloud.tencent.com/test.jpg?sign=0f8201d814dfaf64cf54e74c5f7dbcb0&t=1582791032

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 configuration:

**Custom Authentication Key**: it contains 6-32 uppercase and lowercase letters and digits. 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 1-100 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.

**Object**
After configuring the key, parameter name, and validity period, you can specify the authentication object as needed. The following three 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 authentication parameter and thus not affect the cache hit rate.

**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.
Cache Configuration

Ignore query string configuration

Last updated: 2020-05-20 11:36:23

Configuration Scenario

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.

When a user accesses the resource through a URL, the access request may carry some parameters for special purposes. For example, the following links are used to represent two different images:

```text
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 image contents and distinguish between resources.

In an audio/video scenario, if you use the timestamp signature parameter for access authentication:

```text
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.

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 enter its configuration page. Under the **Access Control** tab, find the Ignore Query String configuration.

When you connect an acceleration domain name:

- If static acceleration is selected, Ignore Query String will be disabled by default.
- For download and streaming VOD acceleration, Ignore Query String is enabled by default.
Modifying configuration

You can switch to enable/disable Ignore Query String, and the configuration will take effect across the entire network in about 5 minutes:

- If your acceleration domain name is configured for global acceleration, the Ignore Query String configuration will take effect globally. This configuration does not distinguish between requests from and outside of Mainland China.
- Enabling Ignore Query String can effectively improve cache hit rate.
Cache Expiration Configuration

Last updated : 2020-05-22 10:58:29

Configuration Scenario

Resource cache in Tencent Cloud CDN is triggered by requests. When a user initiates an access request to a resource, if the CDN node receiving the request has not cached the requested resource, it will forward the request to the origin server to pull the resource. After the resource is successfully pulled by the node (with a 2XX status code returned), it will be cached on the node and returned to the user.

You cannot directly manage resources cached on CDN nodes. If you are worried that resources on the origin server change but CDN nodes still cache the legacy resources and return them to users, you can configure node cache rules.

Each cached resource on CDN node has an expiration time. If the requested cached resource has expired, it will be considered as invalid even if the resource is still cached on the node. The node will pull the resource from the origin server again. Node cache rule allows you to configure the cache validity period for resources in a specific type, directory, and path. You can configure these items based on actual business scenarios.

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 enter its configuration page. Under the Cache Configuration tab, find the cache validity configuration.

When you connect an acceleration domain name:

- If you select static acceleration, the default cache validity period of general dynamic files (such as .php, .jsp, .asp, .aspx) will be 0 (direct origin-pull without caching), and the validity period for all other types of files will be 30 days.
- If you select download acceleration or streaming VOD acceleration, the default cache validity period of all files will be 30 days.
Modifying configuration

1. Modify the configuration

CDN currently allows you to configure cache validity rules in the following four formats:

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

Configuration rules:
• You can configure up to 10 cache validity rules.
• If there are multiple cache validity rules, the one at the bottom has the highest priority.
• You can configure the validity period to up to 365 days.

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

2. Platform policies
When a user makes a request for a certain business resource and the origin server's HTTP response header includes the `Cache-Control` field, the default policy will be as follows:

• If the `Cache-Control` field is `Max-Age`, the cache validity period for this resource is subject to that configured for the node, rather than the value specified by `Max-Age`.
• If the `Cache-Control` field is `no-cache`, `no-store`, or `private`, the CDN node will not cache the resource.
• If the `Cache-Control` field does not exist, CDN will add the "Cache-Control:max-age = 600" header by default.

3. Advanced cache configuration
After advanced cache configuration is enabled, you can adjust the node cache validity period dynamically by configuring the `Max-Age` value in the HTTP response header `Cache-Control` of the origin server.

After advanced cache configuration is enabled, CDN will compare the configured node cache validity period with the `Max-Age` value and take the smaller one as the actual validity period.

• If `Max-Age` configured for `/index.html` of the origin server is 200 seconds and the cache validity period configured for CDN is 600 seconds, the actual cache validity period of the file will be 200 seconds.
• If `Max-Age` configured for `/index.html` of the origin server is 800 seconds and the cache validity period configured for CDN is 600 seconds, the actual cache validity period of the file will be 600 seconds.

After advanced cache configuration is enabled, if the origin server does not return the `Last-Modified` field, CDN will add it by default and change its value once every 10 minutes.
Configuration Sample

Suppose the cache validity rule configured for the acceleration domain name `cloud.tencent.com` is as follows:

![Cache Rules](image)

The actual cache validity period will be as follows:

1. 200 seconds for the `/test/abc.jpg` file.
2. 400 seconds for the `/test/def.jpg` file.
3. 300 seconds for the `/test/1.png` file.
Status code cache configuration

Configuration Scenario

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 cache validity period configured in the cache rule.

If a non-2XX status code is returned, the 404 status code indicates caching for 10 seconds by default, while all other status codes indicate no caching. If the origin server cannot immediately process the non-2XX status code and you do not want that all requests pass through the origin server, you can configure the status code cache validity period so the CDN node will directly respond to non-2XX status code, helping reduce pressure on the origin server.

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 enter its configuration page. Under the Cache Configuration tab, find the status code cache configuration.

Modifying configuration

Currently, you can configure the cache validity period for the following status codes for exceptions:

- 403
- 404
To cancel the configuration and directly perform origin-pull, you can configure the cache validity period to 0 or delete the configuration entry.

If your acceleration domain name is configured for global acceleration, the configured status cache validity period will take effect globally. This configuration does not distinguish between requests from and outside of Mainland China.
HTTP Header Cache Configuration

Last updated: 2020-05-22 10:59:27

Configuration Scenario

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 in and returned to users by CDN, you can enable header cache.

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 enter its configuration page. Under the Cache Configuration tab, find the HTTP header cache configuration, which is disabled by default.

![HTTP Header Cache Configuration](image)

Modifying configuration

You can directly switch to enable/disable HTTP header cache, and the configuration will take effect across the entire network in about 5 minutes:
If your acceleration domain name is configured for global acceleration, the header cache configuration will take effect globally. This configuration does not distinguish between requests from and outside of Mainland China.

The header cache configuration is being upgraded across the entire network. If an error message is displayed when you disable it, it may be caused by the upgrade. Please contact us to disable it on the backend.
Cache Configuration

Last updated: 2020-05-21 14:21:44

What is cache expiration configuration?

Cache expiration configuration refers to a set of expiration policies the CDN cache nodes should follow when caching your business contents.

All resources cached on CDN nodes have an expiration time. For unexpired resources, when a request reaches the node, the node will directly return the requested resource 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, reacquire the resource and cache it to the node, and then return it to the user. A reasonable cache validity period can effectively improve the resource hit rate and lower the origin-pull rate, reducing bandwidth usage.

What is cache configuration?

1. Log in to the CDN Console and click Domain Management on the left sidebar to enter the management page.

2. Locate and click the domain name you want.

3. In the Cache Configuration tab, find the Browser Cache Validity Configuration section and toggle on the Browser Cache switch to enable it.
4. The following results are then achieved.

When a user requests for a certain resource from the origin server and the Response HTTP Header includes the `Cache-Control` field with a value of `max-age=xxxx`, the cache validity period for the resource on the node take the lesser of the value of the set validity period or the `max-age` directive:

- For example, if the `max-age` set for the `/index.html` of the origin server is 200 seconds and the cache validity period set for CDN is 600 seconds, the actual cache validity period for the file will be 200 seconds.
- If the `max-age` set for the `/index.html` of the origin server is 800 seconds and the cache validity period set for CDN is 600 seconds, the actual cache validity period for the file will be 600 seconds.

> If the `Cache-Control` field does not exist in the response header of your origin server, the `Cache-Control:max-age=600` header will be used by default.

**How do I control the file cache time in a browser?**

Tencent Cloud CDN supports the `Cache-Control` configuration on the origin server by default, but configuration of the `Cache-Control` header is not supported. `max-age` cannot be configured on CDN nodes, but CDN nodes can inherit the origin server's `max-age`. To configure `max-age` on CDN nodes, you only need to configure the `max-age` on the origin server.

**How do I adjust the priority of cache configuration?**

For more information, please see the directions in Node Cache Configuration.
I use my own server as the origin server of CDN. Can I configure to not cache a specific type of files? Can I set the cache period to "0" to disable caching?

You can configure different cache validity periods for different types of directories and files. If the cache validity period 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 request to the node. For more information on cache configurations, please see Node Cache Configuration.

Which cache expiration configuration does Tencent Cloud support?

Tencent Cloud CDN supports cache validity period configuration at various dimensions, custom priority adjustment, and cache inheritance policies (advanced cache configuration). A reasonable cache validity period can effectively improve the resource hit rate and lower origin-pull rate, reducing bandwidth usage.

What is the default cache configuration of CDN?

Default configuration is as follows when a domain name is connected:

- External origin domain name connection: by default, the cache validity period for all files is 30 days, except for dynamic files (such as .php, .jsp, .asp, .aspx). The cache validity period for these dynamic files is 0 by default, which means any request for such files will be directly forwarded to the origin server.
- COS origin domain name connection: by default, the cache validity period for all files is 30 days.
- Advanced cache expiration configuration is disabled by default.

What are cache inheritance policies?

When a user makes a request for a certain business resource, the origin server's Response HTTP Header includes the Cache-Control field. The default policy is as follows:

- If the Cache-Control field is max-age, the cache validity period for this resource is subject to the period set for the resource, and will not inherit the value specified by max-age.
- If the Cache-Control field is no-cache or no-store, the CDN node does not cache the resource.

What are cache matching rules?

When multiple caching policies are set, the priorities of the entries are determined on a bottom-to-top basis, with the entry at the bottom of list having the highest priority and the one at the top having the lowest priority. For example, suppose the following caching policies are set for a domain name:

All files (30 days)
.php .jsp .aspx 0 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 entry. It is hit, so the cache validity period is 30 days.
2. Match with the second entry. It is not hit.
3. Match with the third entry. It is hit, so the cache validity period is 300 seconds.
4. Match with the fourth entry. It is hit, so the cache validity period is 400 seconds.
5. Match with the fifth entry. It is hit, so the cache validity period is 200 seconds.

The final cache validity period is subject to the last matching result, and so it will be 200 seconds.
Origin-pull Configuration
Range GETs Configuration

Last updated: 2020-06-02 14:29:17

Configuration

CDN will shard files to improve storage efficiency when caching resources. It also supports Range requests. For example, if a request carries HTTP header `Range: bytes = 0-999`, the first 1,000 bytes of the file will be returned to the user.

After Range GETs is enabled, if a partial file requested by a user has expired, CDN will perform Range GETs to pull and cache the required partial file and return it to the user. After Range GETs is disabled, even if a user only requests a partial file, CDN will pull the entire file and then cache it before returning the requested partial file to the user.

Enabling Range GETs can greatly increase the delivery efficiency of large files, improve the response time, and reduce the pressure on the origin server.

After Range GETs is enabled, resources will be cached in shards on the node. These shards have the same cache expiration time and follow the cache expiration rule defined by the user.

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 the domain name to access its configuration page. Under the Origin Configuration tab, find Range GETs configuration, which is disabled by default. However, it is enabled by default for domain names of COS origin servers:
Modifying the configuration

You can toggle the Range GETs switch to enable or disable this feature. To enable it, first confirm that the origin server supports Range requests. Otherwise, the operation may fail.

If your acceleration domain name is configured for global acceleration, the Range GETs configuration will take effect globally. It does not distinguish between requests from and outside of mainland China.

Configuration Sample

Suppose the Range GETs configuration of the domain name `cloud.tencent.com` is as follows:

User A makes a request for the `http://cloud.tencent.com/test.apk` resource. After the node receives the request and finds that the cached `test.apk` file has already expired, it will initiate a Range GETs request to get and cache the resource by shards. If user B also makes a Range request at this time and the shards stored on the node match the specified byte segments in the Range request, the resource will be directly returned to user B without waiting to obtain all shards.
Follow 301/302 Configuration

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

Viewing the configuration

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:

Modifying the configuration

You can toggle the follow 301/302 redirect configuration switch to enable or disable this feature:
If your acceleration domain name is configured for global acceleration, the follow 301/302 redirect configuration will take effect globally. It does not distinguish between requests from and outside of mainland China.

Configuration Sample

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

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.
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: 2020-04-27 14:28:23

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.

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) 5
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) 10
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.
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-----
MIIEIcTCCAygAwIBAgIQCQ6H1XKr48ioTW1s2A2krTANBgkqhkiG9w0BAQUFADBh
TELMwkgAlUEh8MVUeKzAeABgMB0AAGM5E4YQDQWQL
ExIwNjOaI1nbiU8C85Vz90BZtX03b13jM2swOQD+nLizZUJ1CycyvBZi81z71lg
YQGvR8Bc0MvE93Y3d5c2udVyaXn2jZ2Jy9h9l3iwAYAwbOQTVWh0Ca0EAvAh
Vt1YFvN2ZgQ7ZLx3MgyB7y11n1gUYAvyYI6B1c09RizhQw67A+SFRZ4
MVdWd1wCWDhG8WboDAlAQI7H6XbcQVYQivGxhVNU+BTBEGUXECBMK
V2ZxLzr3eDjFqJ8AEU1B8EJQ+2UJvdvH8zTeBYBbGAbQ+eNg1h9uLjMw
bJSJmmM8zwGAYDQDQFBFlW0vYu1ie9m9YuXzdzLmXbTBCznAMBGkvki9i69w0B
AQEEAFAOB8yuYkCqYAgA3kb0E0G0z2d880GEUcLcEpz6QGwEHKUyZeLMG1LrU3JZeeN
3wFZht8s0w54d2zcgr/RwYvXptDcYjRkmn8jymkScm/Q7d7CuwLW+S/P0wFqjWM
X9G4Jc/evJ0m6F5AsuxC8jtg0wlyy/C3Hw0oUzTvGd7G2Ggg0s1Sacy48R2nNwCc
Av5eAaaODCAdEwqG/HMMkALUdEwQOoAMAoYdVR0PBAD4DqAgWgMEUAgUidQHQ+MDw
O4aDoGCH9oDHAGL9y9TVJITJ7Z4nc1MUrRZyY31sL21m1caZwaDmLmHvbS9TVJIT
Zu1m1tVM55csmw5AAYDvRq8bd0WzOSAbgRtgknhBhFAQXvAaQcCgcCgcCAQGF
BwIFhE0xhIioLXiomvL3d33y2ZxJpc21nBl5jD02wCnEOhMB6G4UIUQJOQMBQcSCG
AQUFWBMBBqrBbrFBEQcdAIJFQBNVNSMEDAMg65S17wsRsbS5AB6KNZ2BtshzgVY19
Rz2B9r9brB6FBQ8BqAQrMw9Yi5KwY7B87X1AGGGG9H6HAGL9y9V3L2n1cmQz
akLsUwNw787Ba6Br8gBEffmXyQmRcY1IoBCa03F3EvYJNAEF
oXnP4zYy29t781LBD0wLYw7o2yLcYLMlNcJj5BbQgQbEQFCQBDARML7C70KhdFeo
WODMWg5JGBfF3S29oMVWTAMACBr5Q0Anz6BRA7xkojLYMwAB5QDmrEsHEyEF
QRhdfmRodfRwib8vbCgnh52z2Xjpc21n15jD20vDnSb2zsHM5SnwWvnOYJTKoZ2
hucNAQFEBQD8aqEBALfbEx6G72Gq3GwCwEE987y8CcyKjrs1DnkWf1Q3p40y7
ZB7Y6rWy8z8nYuFUEZ51b/znwpmpe70pGh7m8QHn8F4ckO3j3Ses3HvJg1Mhks3r
3IQ
3egEAOuN2UDS5HtqON0F99hYywe0BZcaT5gFXgbIldE0tdcMwvzCJ0LD1WQ30GwIR
NM565xjzhjPCxYX8bUClBD4kKzu0CtItzQ/L5YuGEW507u6xwJ88v6v9F768EBfTeS
R7KCC17F5cSrRaeQyG5jJxbrx1m9Fb/fmsdnc1s5ves-----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.
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. 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.cer -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 outcertificate.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 Acceleration Configuration Guide

Last updated: 2020-06-02 11:48:58

Configuration

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, and click Manage on the right of a domain name to access its configuration page. You can find the HTTPS configuration of the specified domain name under the Advanced Configuration tab.

You can access the Certificate Management page 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 "Activated". Disabled domain names cannot be configured with HTTPS acceleration.
- The `.file.myqcloud.com` suffix is the default acceleration domain name of Tencent Cloud COS and can use HTTPS acceleration without configuring any certificates.
- The `.image.myqcloud.com` suffix domain name is the default acceleration domain name of Tencent Cloud CI and can use HTTPS acceleration without configuring any certificates.

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 Tencent Cloud-hosted certificate for quick deployment.
3. Origin-pull method

In addition to setting the origin-pull mode in the origin server configuration module or when connecting the acceleration domain name, you can also adjust the origin-pull protocol when configuring a certificate. CDN supports the following three origin-pull protocols:

- **HTTP origin-pull**: all requests use HTTP origin-pull.
- **HTTPS origin-pull**: all requests use HTTPS origin-pull.
- **Follow protocol**: the origin-pull mode is based on the request protocol. HTTP requests use HTTP origin-pull, while HTTPS requests use HTTPS origin-pull.
When configuring follow protocol or HTTPS origin-pull, you need to deploy a valid certificate on the origin server. Otherwise, origin-pull will fail.

HTTPS origin-pull currently only supports port 443. If you specify another port for the origin server, the configuration will fail.

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 Tencent Cloud-hosted certificate for quick deployment.
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:
3. Origin-pull method

In addition to setting the origin-pull mode in the origin server configuration module or when connecting the acceleration domain name, you can also adjust the origin-pull protocol in batches when configuring certificates in batches. CDN supports the following three origin-pull protocols:

- HTTP origin-pull: all requests use HTTP origin-pull.
- HTTPS origin-pull: all requests use HTTPS origin-pull.
- Follow protocol: the origin-pull mode is based on the request protocol. HTTP requests use HTTP origin-pull, while HTTPS requests use HTTPS origin-pull.

After the configurations are submitted in batches, the selected domain names will be deployed with a certificate one by one. If an exception occurs, the list page will display the "Failed to update" status, and the original configuration will continue to take effect.

If the update fails, you can click Edit on the right to configure it again.
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.

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 acceleration domain name is configured for global acceleration, the configured HTTPS certificate will take effect globally. Currently, the certificates configured for mainland China and outside mainland China must be the same.

If a domain name has different certificates in/outside mainland China, you will see mainland China and outside mainland China 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:
If your acceleration domain name has different certificate configurations and you want to change one of the certificates, please submit a ticket for assistance.
HTTPS forced Redirect

Last updated: 2020-04-13 20:19:42

Configuration Scenario

CDN supports configuration of forced HTTPS redirect. If a domain name has been configured with the certificate for HTTPS acceleration, you can specify the 301/302 redirect method to force redirect all HTTP requests at the CDN node to HTTPS requests.

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 enter its configuration page. If the domain name has been configured with an HTTPS certificate, you can find Forced Redirect to HTTPS switch under the Advanced Configuration tab. It is disabled by default:

Modifying configuration

You can click Edit on the right to switch 301/302 redirect or directly disable the configuration.
If your domain name is configured for global acceleration, the forced HTTPS redirect configuration will take effect globally. This configuration does not distinguish between requests from and outside of Mainland China.
HTTP2.0 configuration

Last updated: 2020-04-13 20:19:43

Configuration Scenario

If a domain name has been configured with a certificate for HTTPS acceleration, you can enable HTTP2.0 support.

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

Configuration Guide

Viewing configuration

Log in to the CDN Console, select Domain Management on the left sidebar, and click Manage on the right of the domain name to enter its configuration page. Under the Advanced Configuration tab, find HTTP2.0 Configurations, which is enabled by default:

Modifying configuration

Switch to enable or disable HTTP2.0. After the certificate configuration is deleted, HTTP2.0 configuration will be automatically invalidated:
If your domain name is configured for global acceleration, HTTP2.0 configuration will take effect globally. This configuration does not distinguish between requests from and outside of Mainland China.
OCSP binding configuration

Last updated: 2020-06-02 14:29:18

Configuration

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.

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 the domain name to access its configuration page. Under the Advanced Configuration tab, find OCSP Stapling Configuration, which is disabled by default:

![OCSP Stapling Configuration](image)

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
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 of mainland China.
FAQs about HTTPS


1. What is HTTPS?
HTTPS refers to Hypertext Transfer Protocol Secure, which is 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 the certificate for the domain name and deploy it on the CDN nodes across the network to implement the encrypted data transfer across the network.

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

3. How do I configure HTTPS certificate?
You can configure the HTTPS certificate in the CDN Console. For more information, see HTTPS Configuration.

4. Do the HTTPS certificates on CDN nodes need to be synchronized with HTTPS certificate updates on origin server?
This depends on your origin-pull method.
HTTP Forwarding: Synchronization is not needed.
HTTPS Forwarding: When the certificate on origin server is updated, the certificates on the CDN nodes need to be updated synchronously. The certificate between client and node must be identical to the one between node and origin server. Otherwise, a failure of origin-pull will occur.

5. Is there any way for users to allow only HTTPS access and forbid HTTP access?
You can use Forced HTTPS Redirection. After the certificate is configured successfully, the Forced Redirect option appears. When it’s enabled, even if you initiate an HTTP request, it will be changed
to an HTTPS request.

### HTTPS Configuration

HTTPS provides ID verification for network service, in order to protect the privacy and integrity of data exchange. [What's HTTPS?](#)

<table>
<thead>
<tr>
<th>Certificate source</th>
<th>Certificate remark</th>
<th>Expiry Time</th>
<th>Origin-Pull method</th>
<th>Certificate status</th>
<th>More Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Own certificate</td>
<td></td>
<td></td>
<td>Follow protocol</td>
<td>Configuration succ...</td>
<td>Configure Now</td>
</tr>
</tbody>
</table>
Advanced Configuration

Bandwidth Cap Configuration

Configuration Scenario

Tencent Cloud CDN is pay-as-you-go. If you are concerned about excessive bandwidth usage and fee surges due to hotlinking by malicious users, you can set a bandwidth cap to control usage. This feature is only applicable to bill-by-bandwidth users.

Bandwidth cap configuration can detect the bandwidth generated in a statistical period (at a 5-minute granularity) and perform forced origin-pull according to the configuration or disable the CDN service (a 404 error will be returned for all requests) if the threshold is exceeded. This will avoid incurring additional CDN acceleration fees.

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 bandwidth cap configuration on the Advanced Configuration tab. It is disabled by default:

Modifying the configuration

1. Modify the configuration
You can toggle the switch to configure the bandwidth threshold:

- For COS origin server domain names, returning a 404 error is the only option when the threshold is reached.
- If the detected domain name bandwidth exceeds the threshold, origin-pull or return of the 404 error for access needs to be implemented across the entire network node by node; therefore, there may be a certain delay for the configuration to take effect.

2. Disable the configuration

You can toggle the bandwidth cap 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.
3. Add region-specific configuration

If your acceleration domain name is configured for global acceleration and you want to configure acceleration in and outside Mainland China with different bandwidth cap settings, you can click Add Special Configuration.

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

Configuration Sample

Suppose the bandwidth cap configuration of the acceleration domain name cloud.tencent.com is as follows:
### Capped Bandwidth Configuration

You can set to disable CDN service or forward requests to origin server when the bandwidth consumed in the reference period (5 min) exceeds the limit. [What’s Capped Bandwidth?](#)

<table>
<thead>
<tr>
<th>Default Configuration</th>
<th>Overseas Region Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Cap</td>
<td>Bandwidth Cap</td>
</tr>
<tr>
<td>Max Bandwidth</td>
<td>Max Bandwidth</td>
</tr>
<tr>
<td>Cap Exceeded</td>
<td>Cap Exceeded</td>
</tr>
</tbody>
</table>

The access status will be as follows:

If the bandwidth reaches 11 Gbps in Mainland China and 4 Gbps outside Mainland China, a 404 error will be returned for access requests from all users in Mainland China, while users outside Mainland China can still enjoy the acceleration service.
HTTP Header Configuration

Last updated : 2020-05-22 11:03:48

Configuration Scenario

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

As the HTTP header configuration is for a specified domain name, once the configuration takes effect, the configured header will be added to the response messages of user requests for any resource under this domain name. HTTP header configuration affects only response of the client (such as browser) rather than CDN node's caching behaviors.

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 response header configuration on the Advanced Configuration tab. It is disabled by default.

Modifying the configuration

1. Modify the configuration

Toggle the switch and add HTTP header configuration. Currently, the following headers can be configured. You can also add custom headers:

- Access-Control-Allow-Origin: it specifies the sources of cross-origin requests allowed to access the resource.
- **Access-Control-Allow-Methods**: it specifies the allowed methods of cross-origin requests.
- **Access-Control-Max-Age**: it specifies the validity period for caching the returned result of preflight request for a particular resource when a cross-origin request is initiated.
- **Access-Control-Expose-Headers**: it specifies the headers visible to the client when a cross-origin request is initiated.
- **Content-Disposition**: it activates download in the browser and sets the default filename of the downloaded file.
- **Content-Language**: it specifies the language code used by the webpage.
- **Custom**: you can add a custom header.

### General configuration: Content-Disposition

Content-Disposition is used to activate download in the browser and set the default filename of the downloaded resource. When the server sends a file to the client browser, if it is in a type supported by the browser, such as TXT or JPG, it will be directly opened in the browser by default. If you want to ask the user to save the file, 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
```

### General configuration: Content-Language

Content-Language specifies the language code used by the webpage. Common configurations are as follows:
Cross-origin configuration: Access-Control-Allow-Origin

Cross-origin access refers to a scenario where a resource under a domain name, such as `www.abc.com`, initiates a request to another resource under another domain name, such as `www.def.com`. As the resource domain names are different, **cross-origin access** will occur. Using different protocols or ports can cause cross-origin access. You need to add configuration related to cross-origin access in the response header to make the first resource get the desired data.

- Feature overview:
  - **Access-Control-Allow-Origin** is used to solve the problem of cross-origin permissions of resources. Up to 10 values of origins allowed to access a resource can be configured. If a source request's host is in the configured domain name list, the corresponding value will be directly populated into the returned header. You can also set the wildcard `*` to allow all origins to access the resource.

- Match mode overview

<table>
<thead>
<tr>
<th>Match Mode</th>
<th>Origin Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full match</td>
<td><code>*</code></td>
<td>If it is set to <code>*</code>, the following header will be added to the response: <code>Access-Control-Allow-Origin:*</code></td>
</tr>
<tr>
<td>Fixed match</td>
<td><code>http://cloud.tencent.com</code></td>
<td>The source <code>https://cloud.tencent.com</code> hits the list, so the following header will be added to the response: <code>Access-Control-Allow-Origin:</code></td>
</tr>
<tr>
<td>Fixed match</td>
<td><code>https://cloud.tencent.com</code></td>
<td><code>https://cloud.tencent.com</code></td>
</tr>
<tr>
<td>Fixed match</td>
<td><code>http://*.tencent.com</code></td>
<td>The source <code>https://cloud.tencent.com</code> hits the list, so the following header will be added to the response: <code>Access-Control-Allow-Origin:</code></td>
</tr>
<tr>
<td>Fixed match</td>
<td><code>http://*.tencent.com</code></td>
<td><code>https://cloud.tencent.com</code></td>
</tr>
<tr>
<td>Fixed match</td>
<td><code>http://*.tencent.com</code></td>
<td><code>https://cloud.tencent.com</code></td>
</tr>
<tr>
<td>Fixed match</td>
<td><code>http://*.tencent.com</code></td>
<td><code>https://cloud.tencent.com</code></td>
</tr>
<tr>
<td>Fixed match</td>
<td><code>http://*.tencent.com</code></td>
<td><code>https://cloud.tencent.com</code></td>
</tr>
<tr>
<td>Fixed match</td>
<td><code>http://*.tencent.com</code></td>
<td><code>https://cloud.tencent.com</code></td>
</tr>
<tr>
<td>Second-level wildcard domain name match</td>
<td><code>http://*.tencent.com</code></td>
<td>The source <code>https://cloud.tencent.com</code> does not hit the list, so the response will not change.</td>
</tr>
<tr>
<td>Match Mode</td>
<td>Origin Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Port match | https://cloud.tencent.com:8080 | The source https://cloud.tencent.com:8080 hits the list, so the following header will be added to the response: Access-Control-Allow-Origin:https://cloud.tencent.com:8080
The source https://cloud.tencent.com does not hit the list, so the response will not change. |

If there are special ports, you need to enter the relevant information in the list. Arbitrary port match is not supported, and you must specify the ports.

**Cross-origin configuration: Access-Control-Allow-Methods**

Access-Control-Allow-Methods is used to specify the HTTP request methods allowed for cross-origin access. Multiple methods can be set as follows:

Access-Control-Allow-Methods: POST, GET, OPTIONS

**Cross-origin configuration: Access-Control-Max-Age**

Access-Control-Max-Age specifies the validity period of a preflight request. For a non-simple cross-origin request, before the formal communication, an HTTP query request called "preflight request" needs to be made to check whether the cross-origin request is secure and acceptable. The following requests are considered as non-simple cross-origin requests:

- The request is initiated in a method other than GET, HEAD, and POST or is initiated by using POST with a data type other than application/x-www-form-urlencoded, multipart/form-data, and text/plain (such as application/xml or text/xml).
- A custom request header is used.

Access-Control-Max-Age is measured in seconds. Below is a configuration sample:

Access-Control-Max-Age: 1728000

This indicates that no more preflight requests will be sent for the cross-domain access to this resource within 1,728,000 seconds (20 days).

**Cross-origin configuration: Access-Control-Expose-Headers**

Access-Control-Expose-Headers specifies which headers can be exposed to the client as part of the response. By default, the following six types of headers can be exposed to the client:
If you want the client to access other header information, you can use the following setting and separate multiple headers with ";".

```
Access-Control-Expose-Headers: Content-Length, X-My-Header
```

This indicates that the client can access `Content-Length` and `X-My-Header`.

**Custom header**

You can add a custom header and customize key-value settings:
Currently, the following headers cannot be added:

- Date
- Expires
- Content-Type
- Content-Encoding
- Content-Length
- Transfer-Encoding
- Cache-Control
- If-Modified-Since
- Last-Modified
- Connection
- Content-Range
If multiple identical headers are added, the lower the position, the higher the priority, and the header below will overwrite the header above it.

2. Disable the configuration

You can toggle the HTTP header switch to disable this feature. When the switch is off, existing configurations will not take effect in the production environment.

If your domain name is configured for global acceleration, the response header configuration will take effect globally. This configuration does not distinguish between requests from Mainland China and from outside Mainland China.
SEO Optimization Configuration

Last updated: 2020-05-22 11:00:16

Configuration Scenario

SEO optimization 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.

- As search engine IPs are updated very frequently, Tencent Cloud CDN can only guarantee that most but not all search engine IPs can be identified.
- The SEO optimization configuration feature is available only when the connected domain name is your own. After this feature is enabled, if a domain name has multiple origin server addresses, the first one will be the default origin-pull address.

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 SEO optimization configuration on the Advanced Configuration tab. It is disabled by default:

![SEO optimization configuration](image)

Modifying the configuration
Toggle the switch to enable or disable SEO optimization configuration:

If your domain name is configured for global acceleration, the SEO optimization configuration will take effect globally once enabled. This configuration does not distinguish between requests from Mainland China and from outside Mainland China.
Smart Compression Configuration

Last updated : 2020-04-27 14:28:26

Configuration Scenario

With the aid of smart compression, Tencent Cloud CDN can compress the returned resources with Gzip or Brotli according to set rules, which effectively reduces the size of transferred content and costs.

- When a new resource is requested for the first time, as the CDN node does not have it, the request will be forwarded to the origin server, and the uncompressed version of the resource will be returned (uncompressed on the origin server). In subsequent requests, the compressed version of the resource processed by the node will be returned.
- Smart compression currently is supported only for two service types: static acceleration and download acceleration.

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 smart compression configuration on the Advanced Configuration tab:

- After an acceleration domain name is connected, resources 256 bytes–2,048 KB in size with file extensions .js, .html, .css, .xml, .json, .shtml, and .htm will be compressed with Gzip by default.
Modifying the configuration

You can click Edit on the right to specify the file extensions and size range of files to be compressed:

Configuration description

- Gzip can compress files 0–30 MB in size.
- Currently, compression with Brotli is being upgraded and cannot be enabled.
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 Mainland China and from outside Mainland China.
Permission Management
Policy creation

Last updated: 2020-06-02 14:29:18

To make it easier for you to configure domain name queries and manage permissions at a higher level of granularity, the CDN permission policies have been completely upgraded. This allows you to grant permissions at the domain name level through custom policy statements.

1. Log in to the CAM Console and click Policies to access the policy management page. Then, click Create Custom Policy:

2. Select Create by Policy Generator:

3. Select CDN in the service drop-down list and select the actions to be authorized. If you want to grant full read/write permission, check Action Name to select all actions. To map specific actions with console features, please see Console Permissions.

4. Enter the domain name to be authorized as the resource. Then, click Add Statement and Next to create a policy. Then, associate the created policy with existing users and user groups for further authorization:
   - All domain names: enter * for resource description.
   - One/multiple domain names: you need to enter them in the six-segment CDN resource format (qcs::cdn::$account:domain/$domain) where $account is described using uin, i.e., the account ID of the root account. Take the domain names www.test1.com and www.test2.com as examples:
     - One domain name: qcs::cdn::uin/123456789:domain/www.test1.com
     - Multiple domain names: separate them with ,, such as qcs::cdn::uin/123456789:domain/www.test1.com,qcs::cdn::uin/123456789:domain/www.test2.com
When you have specified both Action and Resource to create a custom policy, you can call APIs to perform operations for desired resources. This document describes the mappings between console features and Action.

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

Service Overview

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

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

Domain Name Management

<table>
<thead>
<tr>
<th>Feature</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain name list and query</td>
<td>DescribeDomains</td>
<td>Basic configuration items of a domain name can be queried, displayed, and downloaded To get all detailed configuration items, DescribeDomainsConfig should be authorized</td>
</tr>
<tr>
<td>Feature</td>
<td>Authorized Action</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Adding domain name</td>
<td>DescribeDomains</td>
<td>Domain names can be added in any acceleration service region</td>
</tr>
<tr>
<td>Disabling domain name</td>
<td>StopCdnDomain</td>
<td>-</td>
</tr>
<tr>
<td>Enabling domain name</td>
<td>StartCdnDomain</td>
<td>-</td>
</tr>
<tr>
<td>Deleting domain name</td>
<td>DeleteCdnDomain</td>
<td>-</td>
</tr>
<tr>
<td>Modifying domain name project</td>
<td>UpdateDomainConfig</td>
<td>The domain name project is in the domain name configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All configuration items of a domain name can be modified after authorization</td>
</tr>
<tr>
<td>Domain name configuration management</td>
<td>UpdateDomainConfig</td>
<td>All configuration items of a domain name can be viewed/modified after authorization</td>
</tr>
<tr>
<td></td>
<td>DescribeDomainsConfig</td>
<td></td>
</tr>
</tbody>
</table>

### Certificate Management

<table>
<thead>
<tr>
<th>Feature</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Querying certificate list</td>
<td>DescribeDomainsConfig</td>
<td>All configuration items of a domain name can be viewed after authorization</td>
</tr>
<tr>
<td>Configuring certificate</td>
<td>UpdateDomainConfig</td>
<td>All configuration items of a domain name can be modified after authorization</td>
</tr>
<tr>
<td>Batch configuring certificates</td>
<td>UpdateDomainsHttps</td>
<td>This is used to configure certificates in batches</td>
</tr>
</tbody>
</table>

### Statistical Analysis

<table>
<thead>
<tr>
<th>Feature</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Querying detailed access data</td>
<td>DescribeCdnData</td>
<td>All access data metrics under a domain name can be queried after authorization</td>
</tr>
<tr>
<td>Feature</td>
<td>Authorized Action</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Querying detailed origin-pull data</td>
<td>DescribeOriginData</td>
<td>All origin-pull data metrics under a domain name can be queried after authorization</td>
</tr>
<tr>
<td>Querying top traffic/requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Querying top domain names</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Querying rankings of domain name status codes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Querying usage rankings by province in Mainland China</td>
<td>ListTopData</td>
<td>Rankings of different data metrics and dimensions can be queried after authorization</td>
</tr>
<tr>
<td>Querying usage rankings by ISP in Mainland China</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Querying usage rankings outside Mainland China</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Querying number of unique IPs</td>
<td>DescribelpVisit</td>
<td>-</td>
</tr>
</tbody>
</table>

**Purge and Prefetch**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Authorized Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submitting URLs for purge</td>
<td>PurgeUrlsCache</td>
</tr>
<tr>
<td>Submitting directories for purge</td>
<td>PurgePathCache</td>
</tr>
<tr>
<td>Querying purge records</td>
<td>DescribePurgeTasks</td>
</tr>
<tr>
<td>Submitting prefetch tasks</td>
<td>PushUrlsCache</td>
</tr>
<tr>
<td>Querying prefetch records</td>
<td>DescribePurgeTasks</td>
</tr>
</tbody>
</table>

**Log Service**
<table>
<thead>
<tr>
<th>Feature</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Querying log download link</td>
<td>DescribeCdnDomainLogs</td>
<td></td>
</tr>
</tbody>
</table>

### Network Status Overview

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

### Operational Report

<table>
<thead>
<tr>
<th>Feature</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Querying detailed access data</td>
<td>DescribeCdnData</td>
<td>All access data metrics under a domain name can be queried after authorization</td>
</tr>
<tr>
<td>Querying detailed origin-pull data</td>
<td>DescribeOriginData</td>
<td>All origin-pull data metrics under a domain name can be queried after authorization</td>
</tr>
<tr>
<td>Querying top traffic/requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Querying top domain names</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Querying rankings of domain name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>status codes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Querying usage rankings by province</td>
<td></td>
<td></td>
</tr>
<tr>
<td>in Mainland China</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Querying usage rankings by ISP in</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mainland China</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Querying usage rankings outside</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mainland China</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Querying number of unique IPs</td>
<td>DescribeIpVisit</td>
<td>-</td>
</tr>
</tbody>
</table>

Rankings of different data metrics and dimensions can be queried after authorization.
Traffic Package Management

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

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

IP Ownership Query

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

Self-Diagnosis Tool

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

If you need to grant different project-level permissions such as those for data query, purge and prefetch, and domain name management to different sub-accounts, you can create a policy as follows:

1. Log in to the CAM Console and click Policies on the left sidebar.
2. Click **Create Custom Policy** and select **Create by Product Feature or Project Permission**:
3. Enter the policy name as required and select **CDN** as the service type below:

![Policy Configuration Screen](image)

4. Enable the operation set to be authorized as needed and associate them with desired projects (the default project cannot be authorized). Then, associate them with sub-users:
Resource-Level and Project-Level

Currently, categories of operation sets and their corresponding OPEN API2.0 and OPEN API3.0 APIs are as shown below. Sub-users with operation set permissions can call a 2.0 or 3.0 API in the following list for any domain name in an authorized project:

<table>
<thead>
<tr>
<th>Permission Set</th>
<th>API2.0</th>
<th>API3.0</th>
<th>Authorizaton Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query usage data and statistics</td>
<td>DescribeCdnHostInfo&lt;br&gt;DescriptionCdnHostDetailedInfo&lt;br&gt;GetCdnStatusCode&lt;br&gt;GetCdnStatTop&lt;br&gt;GetCdnProvIspDetailStat</td>
<td>DescribeCdnData&lt;br&gt;DescribeOriginData&lt;br&gt;ListTopData&lt;br&gt;DescribedIpVisit</td>
<td>Yes</td>
</tr>
<tr>
<td>Query domain name information</td>
<td>GetHostInfoById&lt;br&gt;GetHostInfoByHost</td>
<td>DescribeDomains&lt;br&gt;DescribeDomainsConfig</td>
<td>Yes</td>
</tr>
</tbody>
</table>

![CDN Configuration](image)
<table>
<thead>
<tr>
<th>Permission Set</th>
<th>API2.0</th>
<th>API3.0</th>
<th>Authorization Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query a CDN log download link</td>
<td>GenerateLogList</td>
<td>DescribeCdnDomainLogs</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>GetCdnLogList</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add a domain name</td>
<td>AddCdnHost</td>
<td>AddCdnDomain</td>
<td>Yes</td>
</tr>
<tr>
<td>Launch/Deactivate a domain name</td>
<td>OnlineHost OfflineHost</td>
<td>StartCdnDomain StopCdnDomain</td>
<td>Yes</td>
</tr>
<tr>
<td>Delete a domain name</td>
<td>DeleteCdnHost</td>
<td>DeleteCdnDomain</td>
<td>Yes</td>
</tr>
<tr>
<td>Modify domain name configuration</td>
<td>UpdateCdnConfig</td>
<td>UpdateDomainConfig</td>
<td>Yes</td>
</tr>
<tr>
<td>Purge and prefetch</td>
<td>RefreshCdnDir RefreshCdnUrl</td>
<td>PurgeUrlsCache PurgePathCache</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>GetCdnRefreshLog CdnPusherV2</td>
<td>DescribePurgeTasks PushUrlsCache</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GetPushLogs CdnOverseaPushser</td>
<td>DescribePushTasks</td>
<td></td>
</tr>
<tr>
<td>Query service</td>
<td>QueryCdnIp (no authorization required)</td>
<td>DescribeCdnIp</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Console Permissions**

- View usage data and statistics: if **View usage data and statistics** is enabled in the policy and associated with a project, the sub-user can view the following modules in the console:
  - Overview page: data display module
  - Statistical analysis: real-time monitoring
  - Statistical analysis: data analysis
  - Data monitoring over the entire network
- Query domain name information: if the policy enables **Query domain name information** and is associated with a project, the sub-user can view the domain name list and detailed configuration information of the authorized project on the **Domain Name Management** page in the console.
- Query a CDN log download link: if the policy enables **Query a CDN log download link** and is associated with a project, the sub-user can query a log download link on the **Log Service** page in
the console.

- Add a domain name: if the policy enables **Add a domain name** and is associated with a project, the sub-user can add a domain name to the specified project.

- Launch/deactivate a domain name: if the policy enables **Launch/deactivate a domain name** and is associated with a project, the sub-user can launch/deactivate an acceleration domain name in the specified project.

- Delete a domain name: if the policy enables **Delete a domain name** and is associated with a project, the sub-user can delete an acceleration domain name in the specified project. As only deactivated domain names can be deleted, if the sub-user wants to delete a launched domain name, they need to have the permission to **launch/deactivate a domain name**.

- Modify domain name configuration: if the policy enables **Modify domain name configuration** and is associated with a project, the sub-user can modify the configuration of an accelerated domain name in the specified project.

- Purge and prefetch: if **Purge and prefetch** is enabled in the policy and associated with a project, the sub-user can submit corresponding purge or prefetch (whitelist) tasks and query their execution status on the **Cache Purge** page.
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

- Usage
- Total Requests
- Status Code
Data Comparison

Last updated: 2020-01-14 10:11:53

Tabs on the new **Realtime Monitoring** page all support data curve comparison.

1. Log in to the **CDN Console** and click **Statistics > Realtime 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: 2020-01-20 09:42:10

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 ≤ 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 ≤ 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 ≤ 1 day: The minimum time granularity is 1 minute. The latency for displaying the 1-minute curve is about 5–10 minutes.
• 1 day < time period ≤ 31 days: The minimum time granularity can be 5 minutes, 1 hour, or 1 day.
• Time period > 31 days: The minimum time granularity is 1 day.

- 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.

• 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: 2020-01-20 09:44:33

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. 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 chart 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.

![Realtime Monitoring](image)

You can also switch to another metric by selecting it from the drop-down list on the top-left corner of the details page.

![Origin-Pull Monitoring Detail](image)

**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 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 $\leq 24$ hours: The minimum time granularity is 1 minute. The latency for displaying the 1-minute curve is about 3 minutes.
- $24 \text{ hours} < \text{time period} \leq 31 \text{ days}$: The minimum time granularity can be 5 minutes, 1 hour, or 1 day.
- Time period $> 31 \text{ days}$: The minimum time granularity is 1 day.

- 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.
The table below explains the internal status codes of CDN.

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Meaning</th>
<th>Suggestion</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>HTTP request syntax error The server cannot parse the request</td>
<td>Check whether the request syntax is correct.</td>
</tr>
<tr>
<td>403</td>
<td>Request is rejected</td>
<td>Check whether access controls such as referer blacklist/whitelist, IP blacklist/whitelist, or authentication are configured.</td>
</tr>
<tr>
<td>413</td>
<td>Content length of the POST request exceeds the limit</td>
<td>Check the content size of the POST request from the client (the maximum size is 32 MB by default).</td>
</tr>
<tr>
<td>414</td>
<td>URL length exceeds the limit</td>
<td>The maximum URL size is 2 KB by default.</td>
</tr>
<tr>
<td>423</td>
<td>Looping request</td>
<td>Check the 301/302 configuration, HTTPS origin-pull, and rewriting method of the origin server.</td>
</tr>
<tr>
<td>499</td>
<td>The client closes the connection</td>
<td>Check the client status and timeout configuration.</td>
</tr>
<tr>
<td>502</td>
<td>Gateway Error</td>
<td>Check whether the business origin server is normal.</td>
</tr>
<tr>
<td>503</td>
<td>COS frequency control is triggered</td>
<td>Check the cache configuration or whether the COS origin server returns no-cache/no-store.</td>
</tr>
<tr>
<td>509</td>
<td>Blocked due to CC attack</td>
<td>Contact Us or submit a ticket to unblock it.</td>
</tr>
<tr>
<td>514</td>
<td>IP access frequency exceeds the limit</td>
<td>Check the IP access frequency control configuration in the CDN Console.</td>
</tr>
<tr>
<td>531</td>
<td>Error resolving the origin-pull domain name in the HTTP request</td>
<td>Check the domain name resolution configuration of the origin server.</td>
</tr>
<tr>
<td>Status Code</td>
<td>Meaning</td>
<td>Suggestion</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>532</td>
<td>Failed to establish a connection with the origin server in the HTTPS request</td>
<td>Check the port 443 status of the origin server, certificate configuration, or availability of the origin server.</td>
</tr>
<tr>
<td>533</td>
<td>Origin-pull connection timeout in the HTTPS request</td>
<td>Check the port 443 status of the origin server, certificate configuration, or availability of the origin server.</td>
</tr>
<tr>
<td>537</td>
<td>Origin server data reception timeout in the HTTPS request</td>
<td>Check the stability of the business origin server.</td>
</tr>
<tr>
<td>538</td>
<td>SSL handshake of HTTPS request failed</td>
<td>Check the compatibility between the origin server protocol and algorithm.</td>
</tr>
<tr>
<td>539</td>
<td>Certificate validation of HTTPS request failed</td>
<td>Check whether the certificate of the origin server is correctly configured (validity period and completeness of the certificate chain).</td>
</tr>
<tr>
<td>540</td>
<td>Certificate domain name validation of HTTPS request failed</td>
<td>Check whether the certificate of the origin server is correctly configured.</td>
</tr>
<tr>
<td>562</td>
<td>Failed to establish a connection in the HTTPS request</td>
<td>Contact Us with the X-NWS-LOG-UUID information or submit a ticket for troubleshooting.</td>
</tr>
<tr>
<td>563</td>
<td>Connection timeout in the HTTPS request</td>
<td>Contact Us with the X-NWS-LOG-UUID information or submit a ticket for troubleshooting.</td>
</tr>
<tr>
<td>564</td>
<td>Origin-pull in the HTTPS request failed</td>
<td>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.</td>
</tr>
</tbody>
</table>
Data Analysis

Last updated: 2020-01-14 12:23:38

The **Data Analysis** page displays various types of charts by analyzing user sources based on access logs to help you understand your user distribution and business usage.

Log in to the [CDN Console](#) and select **Statistics > Data Analysis** on the left sidebar to enter the **Data Analysis** page.

- You can query data generated within a maximum time period of 31 days. Historical data is retained for 90 days.
- You can query historical data generated in the last three months.

### Unique IP access requests

The number of unique IP access requests in the specified time period is calculated by deduplicating 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.

### User access district distribution

The district of the access requester can be identified via the source client IP, which can be displayed in a map or list, allowing you to view the district distribution of your users.

### User ISP distribution

The ISP of the access requester can be identified via the source client IP, which can be displayed in a pie chart or list, allowing you to view the ISP distribution of your users.
FAQs about Statistical Analysis

How is 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 \( \frac{6 \times 8}{60} = 0.8 \text{ Mbps} \).
- As the usage for bill-by-bandwidth is calculated based on the statistics with 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 only about the data at the application layer, while the traffic generated by the actual data transferring over the network is around 5% to 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, including TCP and IP headers of 40 bytes, which generate traffic during transfer but cannot be counted by the application layer. The overheads of this part is around 3%.
- TCP retransmission: During normal data transfer over the network, around 3% to 10% packets are lost on the internet, and the server will retransmit the lost ones. This type of traffic cannot be counted by the application layer, which accounts for 3% to 7% of the total traffic.

As an industry standard, the billable traffic is the sum of the application-layer traffic and the overheads as 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 is counted as a CDN node hit.

Traffic hit rate = \( \frac{\text{total downstream traffic} - \text{origin-pull traffic}}{\text{total downstream traffic}} \).

How do I fix the low traffic hit rate issue?
- Check whether the cache is purged: Cache purge clears the specified content on the node, leading to temporarily low traffic hit rate.
• Check whether new resources are put into the origin server: High amounts of new resources may cause origin-pulls by CDN, leading to low traffic hit rate.

• Check whether the origin server works properly: If it is malfunctioning with a lot of 4XX or 5XX error, the traffic hit rate will be affected.

• Check whether the cache expiration policy is correctly configured: View the **Cache Expiration Configuration** section on the Cache Configuration page in the console. The cache expiration policies are displayed in ascending order in terms of priority, i.e., a policy takes precedence over the one above it.

• Check whether Range GETs is enabled: Check the **Range GETs** section on the Origin-pull Configuration page 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: View the **Ignore Query String** section on the Access Configuration page in the console. If it is disabled, caching will be performed based on the full path. In this case, if the same resource are requested by different parameters, it cannot be matched and will cached multiple times, which lowers the traffic hit rate.

**Do status code statistics include all the 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 varies from the billable data when **all districts** or **all ISPs** is selected. For details, see **question #2 above**.
Purge and Prefetch

Cache Purge

Last updated: 2020-04-27 14:28:29

Feature Overview

CDN is capable of configuring basic cache. Cache expiration time can be configured according to rules such as specified service types, directories, and specific URLs to regularly purge resources cached on nodes, pull 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 obtained from origin-pull. If it is the same as that of the currently 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.

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.

Use Cases

**New resource release**

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

How to use

Log in to the CDN Console, click Purge and Prefetch on the left sidebar, and submit a Purge URL or Purge Directory task:
In the **History** tab, you can query tasks by specified time period, term, and purge task type. Term queries only support querying a domain name or a complete purged URL/directory:

The console can return up to 10,000 operation records at a time, which can be exported to Excel. If you have a high number of purge tasks, please query and export them in batches.
Precautions

**URL purge:**

- Up to 10,000 URLs can be purged per day for each account, and up to 1,000 URLs can be submitted for purge at a time. For overseas CDN users, up to 10,000 global URLs can be purged per day. This quota is independent of the Mainland China URL purge quota.
- You need to add the `http://` or `https://` protocol identifier when submitting a purge task.
- URLs in the format of `http://*.test.com/` cannot be purged. Even if you connect a wildcard domain name to CDN, you need to submit the corresponding sub-domain names for purge.
- When submitting URLs for purge, domain names should have already been connected to CDN; otherwise, the submission will fail.
- URLs containing Chinese characters cannot be purged.
- By default, URLs will be purged by acceleration regions of domain names in the URLs.

**Directory Purge:**

- Up to 100 directories can be purged per day per account, and up to 20 directories can be submitted for purge at a time. For overseas CDN users, up to 100 global directories can be purged per day. This quota is independent of the Mainland China directory purge quota.
- You need to add the `http://` or `https://` protocol identifier when submitting a purge task.
- Directories in the format of `http://*.test.com/` cannot be purged. Therefore, even if you connect a wildcard domain name to CDN, you need to submit the corresponding sub-domain names for purge.
- When submitting URLs for purge, domain names should have already been connected to CDN; otherwise, the submission will fail.
- URL directories containing Chinese characters cannot be purged.

**Sub-user permissions configuration:**

- Directory purge, URL purge, and purge history query have been integrated to the latest permission system and support permission configuration at the resource (domain name) level.
- For learn how to grant permissions, please see Console Permissions.

Use Cases

**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 Distank3 and Server: NWS_SPMid, resources will be directly returned by the nodes:
2. On the origin server, replace \texttt{1.txt} with a file that has the same name, and the file’s last modified time changes, while \texttt{2.txt} stays the same:
3. Initiate requests again. As the cache has not expired, the legacy content of the `1.txt` resource will be accessed:
4. Submit a directory purge task, select **Purge updated resources**, and wait for the purge to complete:

5. After the purge is completed, 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 a cache hit and returned:
curl http:// purge-test-1251991073 .file .myqcloud.com/fileTest/1 .txt –svn
* 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 15:33:22 GMT
< Last-Modified: Wed, 04 Sep 2019 15:24:17 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 23
< X-NWS-UUID-VERIFY: 6a4ea0410342aee319558d46b866cd37
< Accept-Ranges: bytes
< ETag: "325daac4e71e82db89ee26922d7435b7"
< x-cos-request-id: NWQ2ZmQ5NDJFMjZ1MjU4NjRfMzY0Y181MmU1YWIt
< X-Daa-Tunnel: hop_count=2
< X-NWS-LOG-UUID: 14813390993447302634 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 –svn
* 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 15:34:19 GMT
< Cache-Control: max-age=600
< Expires: Wed, 04 Sep 2019 15:44:19 GMT
< Last-Modified: Wed, 04 Sep 2019 15:01:37 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 19
< X-NWS-UUID-VERIFY: e7112793c4a1bdde407954f943e43fb
< X-NWS-LOG-UUID: 1690884127387779050 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
FAQs about Cache Purge

Last updated: 2020-05-21 15:08:08

What is cache purge?

Cache purge includes URL purge, directory purge, and URL prefetch. (For more information, please see Cache Purge.)

- URL purge means to purge the cache on a file-by-file basis.
- Directory purge means to purge all files under a directory on a file-by-file basis.
- URL prefetch means to prefetch resources on a file-by-file basis.

Purge vs. 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 the requirements for cache purge? How long does it take effect?

Cache purge includes URL purge, directory purge, and URL prefetch.

- 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.
- URL prefetch: This feature is only available for key CDN customers. If the resource has already been cached to the node and has not expired, it will not be updated to the latest one. If you need to update the resources on all CDN nodes to the latest ones, you can purge them before prefetch. A maximum of 1,000 URLs can be prefetched each day and a maximum of 20 URLs are allowed to be submitted for each prefetch. It takes about 5 to 30 minutes for the prefetch to take effect, depending on the file size.

Will the cached content on CDN cache nodes be updated in real time?
No. The cached content on CDN cache nodes are updated based on the Cache Configuration you configured in the console. If you need to update a file's cache in real time, use Cache Purge.

**Does CDN support directory purge?**

Yes. CDN supports URL purge, directory purge, and URL prefetch.
Method 1: Purge Directory in the CDN Console. For more information, please see Cache Purge.
Method 2: Purge URL by calling the API. For more information, please see Purge URL.

**How to view the purge cache history?**

You can check the purge cache history in the CDN Console. For more information, please see History.

**Why doesn't directory prefetch or purge take effect?**

Please check whether Last-Modified of the origin server has changed; if so, the origin-pull will fail. If you are unable to solve the problem, please submit a ticket for troubleshooting.
Feature Overview

After a domain name is connected to CDN, a user's resource request will be scheduled to a CDN node for response. If the node has the resource cached, it will directly return the resource content; otherwise, it will pass through the request to the origin server to pull the requested resource.

As CDN nodes respond to most user requests, to help you analyze user access, 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.

Currently, only node access logs are provided.

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:
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.

Overseas access logs and Mainland China access logs of the same domain name 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, log packages can be queried and downloaded after about 30 minutes. Log packages will be added continuously and will stabilize after 2–3 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 here for permanent storage.

**Fields**

The fields (from left to right) in the logs are listed as below:

<table>
<thead>
<tr>
<th>No.</th>
<th>Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Request time</td>
</tr>
<tr>
<td>2</td>
<td>Client IP</td>
</tr>
<tr>
<td>3</td>
<td>Domain name</td>
</tr>
<tr>
<td>4</td>
<td>Request path</td>
</tr>
<tr>
<td>5</td>
<td>Number of bytes accessed this time, including the size of the file itself and the size of the request header</td>
</tr>
<tr>
<td>No.</td>
<td>Fields</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
</tr>
<tr>
<td>6</td>
<td>Province numbers for Mainland China logs; region numbers for overseas logs (see the mapping table below)</td>
</tr>
<tr>
<td>7</td>
<td>ISP numbers for Mainland China logs; <code>-1</code> will be used for overseas logs (see the mapping table below)</td>
</tr>
<tr>
<td>8</td>
<td>HTTP status code</td>
</tr>
<tr>
<td>9</td>
<td>Referer information</td>
</tr>
<tr>
<td>10</td>
<td>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</td>
</tr>
<tr>
<td>11</td>
<td>User-Agent information</td>
</tr>
<tr>
<td>12</td>
<td>Range parameter</td>
</tr>
<tr>
<td>13</td>
<td>HTTP method</td>
</tr>
<tr>
<td>14</td>
<td>HTTP protocol identifier</td>
</tr>
<tr>
<td>15</td>
<td>Cache hit/miss. A hit in a CDN edge server or parent node will be marked at hit</td>
</tr>
</tbody>
</table>

### Region/ISP mappings

#### Mainland China provinces

<table>
<thead>
<tr>
<th>Region ID</th>
<th>Region</th>
<th>Region ID</th>
<th>Region</th>
<th>Region ID</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Beijing</td>
<td>86</td>
<td>Inner Mongolia</td>
<td>146</td>
<td>Shanxi</td>
</tr>
<tr>
<td>1069</td>
<td>Hebei</td>
<td>1177</td>
<td>Tianjin</td>
<td>119</td>
<td>Ningxia</td>
</tr>
<tr>
<td>152</td>
<td>Shaanxi</td>
<td>1208</td>
<td>Gansu</td>
<td>1467</td>
<td>Qinghai</td>
</tr>
<tr>
<td>1468</td>
<td>Xinjiang</td>
<td>145</td>
<td>Heilongjiang</td>
<td>1445</td>
<td>Jilin</td>
</tr>
<tr>
<td>1464</td>
<td>Liaoning</td>
<td>2</td>
<td>Fujian</td>
<td>120</td>
<td>Jiangsu</td>
</tr>
<tr>
<td>121</td>
<td>Anhui</td>
<td>122</td>
<td>Shandong</td>
<td>1050</td>
<td>Shanghai</td>
</tr>
<tr>
<td>1442</td>
<td>Zhejiang</td>
<td>182</td>
<td>Henan</td>
<td>1135</td>
<td>Hubei</td>
</tr>
</tbody>
</table>
### Regions

<table>
<thead>
<tr>
<th>Region ID</th>
<th>Region</th>
<th>Region ID</th>
<th>Region</th>
<th>Region ID</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>1465</td>
<td>Jiangxi</td>
<td>1466</td>
<td>Hunan</td>
<td>118</td>
<td>Guizhou</td>
</tr>
<tr>
<td>153</td>
<td>Yunnan</td>
<td>1051</td>
<td>Chongqing</td>
<td>1068</td>
<td>Sichuan</td>
</tr>
<tr>
<td>1155</td>
<td>Tibet</td>
<td>4</td>
<td>Guangdong</td>
<td>173</td>
<td>Guangxi</td>
</tr>
<tr>
<td>1441</td>
<td>Hainan</td>
<td>0</td>
<td>Other</td>
<td>1</td>
<td>Hong Kong (China), Macao (China), and Taiwan (China)</td>
</tr>
<tr>
<td>-1</td>
<td>Outside Mainland China</td>
<td>-1</td>
<td>Other ISPs</td>
<td>-1</td>
<td>Other ISPs</td>
</tr>
</tbody>
</table>

### Mainland China ISPs

<table>
<thead>
<tr>
<th>ISP ID</th>
<th>ISP</th>
<th>ISP ID</th>
<th>ISP</th>
<th>ISP ID</th>
<th>ISP</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>China Telecom</td>
<td>26</td>
<td>China Unicom</td>
<td>38</td>
<td>CERNET</td>
</tr>
<tr>
<td>43</td>
<td>Great Wall Broadband Network</td>
<td>1046</td>
<td>China Mobile</td>
<td>3947</td>
<td>China Mobile Tietong</td>
</tr>
<tr>
<td>-1</td>
<td>ISPs outside Mainland China</td>
<td>0</td>
<td>Other ISPs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Regions outside Mainland China

<table>
<thead>
<tr>
<th>Region ID</th>
<th>Region</th>
<th>Region ID</th>
<th>Region</th>
<th>Region ID</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000000001</td>
<td>Asia Pacific Zone 1 (service area)</td>
<td>765</td>
<td>Slovakia</td>
<td>1613</td>
<td>Angola</td>
</tr>
<tr>
<td>2000000002</td>
<td>Asia Pacific Zone 2 (service area)</td>
<td>766</td>
<td>Serbia</td>
<td>1617</td>
<td>Ivory Coast</td>
</tr>
<tr>
<td>Region ID</td>
<td>Region</td>
<td>Region ID</td>
<td>Region</td>
<td>Region ID</td>
<td>Region</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------</td>
<td>-----------</td>
<td>----------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>2000000003</td>
<td>Asia Pacific Zone 3 (service area)</td>
<td>770</td>
<td>Finland</td>
<td>1620</td>
<td>Sudan</td>
</tr>
<tr>
<td>2000000004</td>
<td>Middle East (service area)</td>
<td>773</td>
<td>Belgium</td>
<td>1681</td>
<td>Mauritius</td>
</tr>
<tr>
<td>2000000005</td>
<td>North America (service area)</td>
<td>809</td>
<td>Bulgaria</td>
<td>1693</td>
<td>Morocco</td>
</tr>
<tr>
<td>2000000006</td>
<td>Europe (service area)</td>
<td>811</td>
<td>Slovenia</td>
<td>1695</td>
<td>Algeria</td>
</tr>
<tr>
<td>2000000007</td>
<td>South America (service area)</td>
<td>812</td>
<td>Moldova</td>
<td>1698</td>
<td>Guinea</td>
</tr>
<tr>
<td>2000000008</td>
<td>Africa (service area)</td>
<td>813</td>
<td>Macedonia</td>
<td>1730</td>
<td>Senegal</td>
</tr>
<tr>
<td>-20</td>
<td>Asia (client area)</td>
<td>824</td>
<td>Estonia</td>
<td>1864</td>
<td>Tunisia</td>
</tr>
<tr>
<td>-21</td>
<td>South America (client area)</td>
<td>835</td>
<td>Croatia</td>
<td>1909</td>
<td>Uruguay</td>
</tr>
<tr>
<td>-22</td>
<td>North America (client area)</td>
<td>837</td>
<td>Poland</td>
<td>1916</td>
<td>Greenland</td>
</tr>
<tr>
<td>-23</td>
<td>Europe (client area)</td>
<td>852</td>
<td>Latvia</td>
<td>2026</td>
<td>Taiwan (China)</td>
</tr>
<tr>
<td>-24</td>
<td>Africa (client area)</td>
<td>857</td>
<td>Jordan</td>
<td>2083</td>
<td>Myanmar</td>
</tr>
<tr>
<td>-25</td>
<td>Oceania (client area)</td>
<td>884</td>
<td>Kyrgyzstan</td>
<td>2087</td>
<td>Brunei</td>
</tr>
<tr>
<td>35</td>
<td>Nepal</td>
<td>896</td>
<td>Ireland</td>
<td>2094</td>
<td>Sri Lanka</td>
</tr>
<tr>
<td>57</td>
<td>Thailand</td>
<td>901</td>
<td>Libya</td>
<td>2150</td>
<td>Panama</td>
</tr>
<tr>
<td>73</td>
<td>India</td>
<td>904</td>
<td>Armenia</td>
<td>2175</td>
<td>Colombia</td>
</tr>
<tr>
<td>144</td>
<td>Vietnam</td>
<td>921</td>
<td>Yemen</td>
<td>2273</td>
<td>Monaco</td>
</tr>
<tr>
<td>192</td>
<td>France</td>
<td>926</td>
<td>Belarus</td>
<td>2343</td>
<td>Andorra</td>
</tr>
<tr>
<td>207</td>
<td>United Kingdom</td>
<td>971</td>
<td>Luxembourg</td>
<td>2421</td>
<td>Turkmenistan</td>
</tr>
<tr>
<td>Region ID</td>
<td>Region</td>
<td>Region ID</td>
<td>Region</td>
<td>Region ID</td>
<td>Region</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------</td>
<td>-----------</td>
<td>-------------------</td>
<td>-----------</td>
<td>-------------------</td>
</tr>
<tr>
<td>208</td>
<td>Sweden</td>
<td>1036</td>
<td>New Zealand</td>
<td>2435</td>
<td>Laos</td>
</tr>
<tr>
<td>209</td>
<td>Germany</td>
<td>1044</td>
<td>Japan</td>
<td>2488</td>
<td>East Timor</td>
</tr>
<tr>
<td>213</td>
<td>Italy</td>
<td>1066</td>
<td>Pakistan</td>
<td>2490</td>
<td>Tonga</td>
</tr>
<tr>
<td>214</td>
<td>Spain</td>
<td>1070</td>
<td>Malta</td>
<td>2588</td>
<td>The Philippines</td>
</tr>
<tr>
<td>386</td>
<td>United Arab Emirates</td>
<td>1091</td>
<td>Bahamas</td>
<td>2609</td>
<td>Venezuela</td>
</tr>
<tr>
<td>391</td>
<td>Israel</td>
<td>1129</td>
<td>Argentina</td>
<td>2612</td>
<td>Bolivia</td>
</tr>
<tr>
<td>397</td>
<td>Ukraine</td>
<td>1134</td>
<td>Bangladesh</td>
<td>2613</td>
<td>Brazil</td>
</tr>
<tr>
<td>398</td>
<td>Russia</td>
<td>1158</td>
<td>Cambodia</td>
<td>2623</td>
<td>Costa Rica</td>
</tr>
<tr>
<td>417</td>
<td>Kazakhstan</td>
<td>1159</td>
<td>Macao (China)</td>
<td>2626</td>
<td>Mexico</td>
</tr>
<tr>
<td>428</td>
<td>Portugal</td>
<td>1176</td>
<td>Singapore</td>
<td>2639</td>
<td>Honduras</td>
</tr>
<tr>
<td>443</td>
<td>Greece</td>
<td>1179</td>
<td>Maldives</td>
<td>2645</td>
<td>El Salvador</td>
</tr>
<tr>
<td>471</td>
<td>Saudi Arabia</td>
<td>1180</td>
<td>Afghanistan</td>
<td>2647</td>
<td>Paraguay</td>
</tr>
<tr>
<td>529</td>
<td>Denmark</td>
<td>1185</td>
<td>Fiji</td>
<td>2661</td>
<td>Peru</td>
</tr>
<tr>
<td>565</td>
<td>Iran</td>
<td>1186</td>
<td>Mongolia</td>
<td>2728</td>
<td>Nicaragua</td>
</tr>
<tr>
<td>578</td>
<td>Norway</td>
<td>1195</td>
<td>Indonesia</td>
<td>2734</td>
<td>Ecuador</td>
</tr>
<tr>
<td>669</td>
<td>US</td>
<td>1200</td>
<td>Hong Kong (China)</td>
<td>2768</td>
<td>Guatemala</td>
</tr>
<tr>
<td>692</td>
<td>Syria</td>
<td>1233</td>
<td>Qatar</td>
<td>2999</td>
<td>Aruba</td>
</tr>
<tr>
<td>704</td>
<td>Cyprus</td>
<td>1255</td>
<td>Iceland</td>
<td>3058</td>
<td>Ethiopia</td>
</tr>
<tr>
<td>706</td>
<td>Czech</td>
<td>1289</td>
<td>Albania</td>
<td>3144</td>
<td>Bosnia and Herzegovina</td>
</tr>
<tr>
<td>707</td>
<td>Switzerland</td>
<td>1353</td>
<td>Uzbekistan</td>
<td>3216</td>
<td>Dominican</td>
</tr>
<tr>
<td>708</td>
<td>Iraq</td>
<td>1407</td>
<td>San Marino</td>
<td>3379</td>
<td>South Korea</td>
</tr>
</tbody>
</table>
### Region ID and Region

<table>
<thead>
<tr>
<th>Region ID</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>714</td>
<td>Netherlands</td>
</tr>
<tr>
<td>717</td>
<td>Romania</td>
</tr>
<tr>
<td>721</td>
<td>Lebanon</td>
</tr>
<tr>
<td>725</td>
<td>Hungary</td>
</tr>
<tr>
<td>726</td>
<td>Georgia</td>
</tr>
<tr>
<td>731</td>
<td>Azerbaijan</td>
</tr>
<tr>
<td>734</td>
<td>Austria</td>
</tr>
<tr>
<td>736</td>
<td>Palestine</td>
</tr>
<tr>
<td>737</td>
<td>Turkey</td>
</tr>
<tr>
<td>759</td>
<td>Lithuania</td>
</tr>
<tr>
<td>763</td>
<td>Oman</td>
</tr>
</tbody>
</table>

### Precautions

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:

**ISPs outside Mainland China**

<table>
<thead>
<tr>
<th>ISP ID</th>
<th>ISP</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>ISPs outside Mainland China</td>
</tr>
</tbody>
</table>

**Precautions**

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. The traffic generated during actual data transfer over the network is around 5-15% more than 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. This includes TCP and IP headers which accounts for 40 bytes and 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 traffic is the sum of the application-layer traffic and the overheads as described above. Tencent Cloud CDN takes 10% as the overheads proportion, so the monitored traffic is around 110% of the logged traffic.

Use Cases

Sample Mainland China access log

```
20170719174306 10.10.10.10 www.test.com /test.png 77487 3 2 0 NULL 1408 "Mozilla/
20170719174407 10.10.10.10 www.test.com /test2.png 72488 5 2 200 NULL 13569 "Mozi
20170719174520 10.10.10.10 www.test.com /test3.png 74864 4 1 200 NULL 9474 "Mozi"
20170719174544 10.10.10.10 www.test.com /test4.png 81453 2 2 200 NULL 9218 "Mozi"
20170719174552 10.10.10.10 www.test.com /test5.png 54678 7 2 200 NULL 9041 "Mozi"
```

Sample overseas access log
Real-Time Log

Last updated: 2020-04-27 17:32:19

Feature Overview

CDN can collect and publish 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.

Currently, the real-time logging service of CDN is in beta. You can submit an application to try this feature. Applications will be reviewed within seven business days.

Use Cases

This feature can be used to view and analyze user access in real time.

Basic Concepts

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:

- Logset name: cdn_logset
- Region: the region to which a logset belongs.
- Retention period: the retention period of data in the current 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 for and analyze logs by log topics.
- Ship logs to other platforms based on log topics.
- Download and consume logs from log topics.

**Operation Guide**

Log in to the CDN Console, click Log Service on the left sidebar, and select Real-Time Log to access the real-time log page and create real-time log shipping.

**Creating a log topic**

Click Create to create a log topic.

Up to 10 log topics can be created under one logset.

**Configuring a log topic**

Enter the name of the new log topic and select the domain names to be bound to this topic.

- The name of the new log topic cannot be the same as the name of any existing log topic.
- A domain name can be bound to only one log topic.
- After the configuration information is saved, it takes about 15 minutes for the configuration to take effect.

**Managing a log topic**

After successfully configuring a log topic, you can perform log topic management. Specifically, you can stop/start shipping logs to the log topic, search for logs in log topic, manage the log topic, and delete the log topic.
Stopping/Starting log shipping

You can manually stop/start shipping logs to a log topic.

- After a log topic is stopped, all logs of the domain names bound to the log topic will no longer be shipped to it. Logs that have already been shipped to it will be retained. This operation will take effect in about 5–15 minutes.
- After a log topic is started, all logs of the domain names bound to the log topic will be shipped to it. This operation will take effect in about 5–15 minutes.

Search

You can search for logs by log topic. Select a desired log topic and click Search to access the log search page.

- Time Range: You can search for log data recorded today, during a 24 hour interval (one of the last 7 days), and during the last 7 days.
- Sort: You can sort logs in descending or ascending order by log time.
- Search: You can conduct full-text search, key-value search, and fuzzy keyword search. For more information, please see Syntax and Rules.

Log data description

<table>
<thead>
<tr>
<th>Log Field</th>
<th>Raw Log Type</th>
<th>Log Service Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>app_id</td>
<td>Integer</td>
<td>long</td>
<td>Tencent Cloud account APPID</td>
</tr>
<tr>
<td>client_ip</td>
<td>String</td>
<td>text</td>
<td>Client IP</td>
</tr>
<tr>
<td>file_size</td>
<td>Integer</td>
<td>long</td>
<td>File size</td>
</tr>
<tr>
<td>hit</td>
<td>String</td>
<td>text</td>
<td>Cache hit/miss. Both hits on CDN edge servers and parent nodes are marked as hit</td>
</tr>
<tr>
<td>Log Field</td>
<td>Raw Log Type</td>
<td>Log Service Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td>text</td>
<td>Domain name</td>
</tr>
<tr>
<td>http_code</td>
<td>Integer</td>
<td>long</td>
<td>HTTP status code</td>
</tr>
<tr>
<td>isp</td>
<td>String</td>
<td>text</td>
<td>ISP</td>
</tr>
<tr>
<td>method</td>
<td>String</td>
<td>text</td>
<td>HTTP method</td>
</tr>
<tr>
<td>param</td>
<td>String</td>
<td>text</td>
<td>Parameter carried in URL</td>
</tr>
<tr>
<td>proto</td>
<td>String</td>
<td>text</td>
<td>HTTP protocol identifier</td>
</tr>
<tr>
<td>prov</td>
<td>String</td>
<td>text</td>
<td>ISP province</td>
</tr>
<tr>
<td>referer</td>
<td>String</td>
<td>text</td>
<td>Referer information, i.e., HTTP source address</td>
</tr>
<tr>
<td>request_range</td>
<td>String</td>
<td>text</td>
<td>Range parameter, i.e., request range</td>
</tr>
<tr>
<td>request_time</td>
<td>Integer</td>
<td>long</td>
<td>Response time (in milliseconds), which refers to the time it takes for a node to respond to a client with all return packets after receiving a request</td>
</tr>
<tr>
<td>Log Field</td>
<td>Raw Log Type</td>
<td>Log Service Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>rsp_size</td>
<td>Integer</td>
<td>long</td>
<td>Number of returned bytes</td>
</tr>
<tr>
<td>time</td>
<td>Integer</td>
<td>long</td>
<td>Request timestamp in UNIX format</td>
</tr>
<tr>
<td>ua</td>
<td>String</td>
<td>text</td>
<td>User-Agent information</td>
</tr>
<tr>
<td>url</td>
<td>String</td>
<td>text</td>
<td>Request path</td>
</tr>
<tr>
<td>uuid</td>
<td>String</td>
<td>text</td>
<td>Unique request ID</td>
</tr>
<tr>
<td>version</td>
<td>Integer</td>
<td>long</td>
<td>Version protocol</td>
</tr>
</tbody>
</table>

**Management**

You can manage a created log topic and update the list of domain names bound to it.

The new configuration will take effect in 5-15 minutes.

**Deletion**

You can delete log topics manually.

After a log topic is deleted, all logs of the domain names bound to the log topic will no longer be shipped to it, and the logs that have already been shipped to the log topic will be completely cleared. This operation will take effect in about 5-15 minutes.
Service Query

Entire Network Status Monitoring

Last updated: 2020-04-27 18:22:08

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.

![Network Monitoring]

2. Outside Mainland China
You can select multiple regions at a time to view multiple curves.
Operational Report

Last updated: 2020-04-27 18:22:09

Feature Overview

Tencent Cloud CDN provides multi-dimensional reports to show and help you analyze your business status.

Directions

Log in to the CDN Console and click Business Report on the left sidebar to enter the corresponding page.

Report filter

In this module, you can specify the report dimensions and data to be displayed.

- **Area:** select mainland China or overseas.
- **Project:** select all projects or a specified project.
- **Domains:** select all domain names or a specified domain name under the selected project.
- **Report Type:** select daily, weekly, or monthly.
- **Select a time:** select a day, week or month based on the selected report type.
- **Modules:** select one or more desired data report items, including overview, traffic distribution, traffic, bandwidth, total requests, error code, and top 10 URLs.

Data overview description

Data Overview

Data overview in your specified report dimension is displayed.

1. The displayed data overview varies by billing mode. 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.

2. The time span for data comparison varies by report type. Day-on-day data is displayed in daily report, week-on-week in weekly report, and month-on-month in monthly report.

Traffic Distribution

Traffic distribution chart for a corresponding region is displayed in your specified report dimension. You can view statistics of provinces in Mainland China and regions outside Mainland China.
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 billed bandwidth or origin-pull bandwidth. Peak bandwidth curve can be displayed.

Total Requests
Total request curve in your specified report dimension is displayed.

Error Code
Numbers and proportions of error codes in your specified report dimension are displayed.

Top 10 URL
Top 10 URLs in your specified report dimension are displayed. You can sort them by usage or total requests.
Features

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.

Applicable Scenarios

This tool can be used for troubleshooting. When there is access exception, you can query the IP accessed in the following ways:

- If the IP is not of a CDN node, domain name resolution may be exceptional. Please go to your DNS service provider and check whether the CNAME configuration is correct;
- If the IP is of a CDN node, you can check the node service status to see whether node activation/deactivation operations have led to request interruptions.

Operation Guide

Query Method

Log in to the CDN Console and select **Inspect Tool > Verify Tencent IP Tool** on the left sidebar.

Usage Constraints

- 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 Mainland China, data of the ISP in the corresponding district will be returned; for nodes outside Mainland China, data of the corresponding country/region will be returned.
• You can view the node service status for the past 3 hours. If there were online/offline status changes, the corresponding operation time will be displayed.

Use Cases

Nodes in Mainland China

Nodes Outside Mainland China
Self-Diagnosis Tool

Last updated: 2020-05-09 15:01:20

CDN provides a self-diagnosis tool to help you troubleshoot URL access failure. The self-diagnosis process includes detection of DNS resolution, linkage quality, node status, origin server, and data access consistency, enabling you to identify problems and offering relevant solutions.

The resource URL to be diagnosed should be an activated domain name under your account. The bandwidth incurred in the diagnosis process is billable bandwidth. We recommend the diagnosed resource to be no more than 200 MB in size.

Fault Diagnosis

Diagnosis process

If a resource URL cannot be accessed, you can initiate diagnosis through Fault Diagnosis in the following steps:

1. Log in to the CDN Console and select Inspect Tool > Fault Self-diagnosis.

2. On the Fault Self-diagnosis page, enter the URL to be diagnosed. The URL should begin with http:// or https://. 
3. Click **Get a diagnosis link** and the link address will appear on the page.

4. Click the link to open the diagnosis page where diagnosis information will be collected. Do not close the page during the diagnosis progress. You can manually close it after the diagnosis is completed.
5. You can also send the diagnosis link to others for local fault diagnosis. After the diagnosis is completed, you need to close the webpage manually.

- The diagnosis link is valid for 24 hours and supports up to 10 fault diagnoses.
- You can copy the available diagnosis links on the **Diagnostic Report** page.

**Diagnostic Report**

**Viewing the report**

1. After the diagnosis is completed, click **Diagnostic Report** to view the reports, which are displayed in a table in chronological order. The contents in the table include:

   - The URL for which a diagnosis link is generated.
   - The diagnosis link corresponding to the URL.
- Time when the diagnosis link was generated.

- A countdown to the expiration of the diagnosis link.

- Number of remaining available diagnoses of the diagnosis link.

2. Click **Expand** in the operation column to view the report generated by each diagnosis and the diagnosis results.
3. The diagnostic reports will make an overall assessment based on the diagnosis for each step as shown below:
   - Normal
   - Abnormal
   - Page abnormally closed. This happens generally when the page is closed before diagnosis is completed.

4. Click **View Report** to view the diagnosis details and suggestions.

**Report interpretation**

1. The first part of the report displays diagnosis information, including:
   - Diagnostic report ID.
   - URL to be diagnosed.
   - Time when diagnosis was triggered.
2. The second part gives an overview of the diagnosis process and the results of each diagnosis module. Exceptional modules are clearly identified. Diagnosis modules include:

- Client information detection result.
- DNS detection result.
- CNAME detection result.
- Network linkage detection result.
- Access node detection result.
- Origin-pull node detection result.
- Origin server detection result.
3. The third part elaborates on the diagnosis results.

**Section 1. Client information**

Information such as client IP, district/ISP, and User-Agent, Referer, and Request Mode of the initiated HTTP/HTTPS request are obtained. Without client information, some subsequent detections cannot be conducted.

**Section 2. DNS detection**

The client's DNS IP is collected and checked against the client IP, to determine whether exceptions in local DNS configuration are causing issues in scheduling requests to the optimal cache nodes.
Section 3. CNAME detection

The CNAME configuration of the domain name is obtained. The CNAME resolution of the domain name needs to be configured with the correct domain name suffixed with *.cdn.dnsv1.com (default); otherwise, requests will be unable to reach CDN nodes.

If CNAME configuration detection fails, the requests will not reach CDN nodes and subsequent diagnoses will not be conducted.

Section 4. Network linkage detection

Multiple websites are checked locally to obtain the client's network status. If a website cannot be accessed due to local proxy configuration, the network linkage detection will fail, and subsequent diagnoses will not be conducted.
Section 5. Access node detection

After a client request reaches a CDN node, node information will be collected, including node IP, node district/ISP, status code returned by node, hit status, and resource MD5.

- If a resource has already been cached on a CDN node, it will directly be hit, and origin-pull node detection will not be conducted.

- In case of a cache miss, origin-pull node detection will ensue.

- If the status code returned by the URL is 301, 302, or 504, node detection information will not be obtained, and the subsequent detection will not be conducted.

- If an ACL has been configured for the domain name, the access node will directly return 403, and the hit status is **hit**.
Section 6. Origin-pull node detection

i. If the resource is directly returned by a CDN node, the hit status of both the access node and the origin-pull node is **hit**, and CDN will proceed to detect the origin server to help check whether the status codes and contents returned from the origin server are the same as those of the node.

2. If the resource is not directly returned by a CDN node, the hit status of both the access node and the origin-pull node is **missed**, and the contents will be returned by the origin server.

3. If an exceptional status code is generated at this time, you can compare the origin server status code and file MD5 value against those returned by the access module to determine whether the exception is caused by a CDN node or by the origin server, and then fix the problem accordingly.

If the diagnostic report cannot help you solve the problem, please submit a ticket or contact Tencent Cloud technical support.
Value-added Services
Pornography Detection

Last updated: 2020-01-14 15:01:39

Feature Overview

Leveraging the deep learning image recognition technology of Tencent YouTu, CDN supports pornography detection to intelligently scan images distributed across the internet and identify pornographic information. This service protects your business from getting involved in distributing pornographic information. This service is currently in beta test.

The pornography detection service scans images distributed by CDN, scores each image based on its pornographic rating, and then classifies them as "suspicious images", "pornographic images", or "normal images".

- Pornography detection service can keep the processing history of pornographic images for one month.
- Currently, pornography detection is only available to images distributed within Mainland China.

Use Cases

Avoiding the risk of image violation

The pornography detection service intelligently scans the image resources distributed across the internet by CDN, mark and collect statistics on "suspicious images" and "pornographic images" for you to confirm and manage, helping you avoid the risk of getting involved in distributing pornographic images and ensuring business compliance.

Operation Guide

1. Log into the CDN Console and click Pornography Detection on the left sidebar to enter the detection management page.
2. The Suspicious Images module is displayed by default in the console. You can switch to another module by clicking Pornographic Images or Normal Images.
Suspicious Images

When the pornography detection service scans and finds that your business resources contain suspected pornographic images, it will notify you via SMS, email, or internal message.

1. The Suspicious Images module is displayed by default in the console. You can click the icon in the top-right corner to switch to thumbnail or list mode.

   You can click Normal Images or Pornographic Images under an image and CDN will automatically mark it as a "normal" or "pornographic" image.

   CDN will also automatically block images classified as pornographic. If you want to unblock them, follow the steps in Unblocking Images below.

3. Automatic Management
   If you don't manually confirm a suspected pornographic image within 24 hours after the scan, CDN will automatically block it. You can click Pornographic Images on the top to switch to the "Pornographic Images" module and view the image. The blocking method is Automatic.

Pornographic Images

When the pornography detection service of CDN scans and finds that your business resources contain pornographic images, it will directly block them to protect your business from getting
involved in distributing pornographic information and your users will not be able to obtain them through CDN. You will be notified via SMS, email, or internal message.

1. The **Suspicious Images** module is displayed by default in the console. You can switch to another module by clicking **Pornographic Images**.

   “Pornographic images” can be filtered by image status (not appealed, appeal in process, appeal rejected) and managed as needed.

2. Unblocking Images

   If you want to unblock an image, click **Appeal** at the bottom-right corner to initiate an appeal. The pornography detection service team of Tencent Cloud will manually verify the image. If it is incorrectly classified by CDN, the team will unblock it and notify you via SMS, email, or internal message.

**Normal Images**
If your business resources are classified as "normal images", CDN will not block them temporally. However, they will be manually verified by the service team and entered into the sample library to optimize the pornography detection algorithm.

The **Suspicious Images** module is displayed by default in the console. You can switch to another module by clicking **Normal Images**. You can view the confirmation status of each image in the "Normal Images" module.