Content Delivery Network
Management Description
Product Documentation
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
    Host Header Configuration
Access Control
  Ignore Query String Configuration
  Hotlink Protection Configuration
  IP Blacklist/Whitelist Configuration
  IP Access Limit Configuration
  Video Dragging Configuration
  Authentication Configuration
    Instruction
    TypeA
    TypeB
    TypeC
    TypeD
Cache Configuration
  Parameter cache configuration
  Node cache configuration
  Status code cache configuration
  Header cache configuration
Origin-pull Configuration
  Intermediate Node Configuration
  Range GETs Configuration
  Origin-pull follows 301amp 302 configuration
  Origin-pull timeout configuration
HTTPS Acceleration Configuration
  Notes on HTTPS acceleration configuration
  HTTPS acceleration configuration Guid
  HTTPS forced Redirect
  HTTP2.0 configuration
  OCSP binding configuration
Advanced Configuration
  Bandwidth Limit Configuration
  Customize response header configuration
  SEO optimized configuration
Intelligent compression configuration
HTTPS Configuration
SEO Optimization
Authentication Configuration
Configure HTTP Header
Permission Management
  Permission's explanation on the console
  Policy creation
  Project-level Permission explanation
CDN Permissions
Certificate Management
Statistical Analysis
  Realtime Monitoring
    Panel Configuration
    Data Comparison
    Access Monitoring
    Origin-Pull Monitoring
    Status codes description
Data Analysis
Purge and Prefetch
  Cache Purge
Log Management
  Log Management
  Real-time log
Service Query
  Entire Network Status Monitoring
  Monthly Operations Report
Diagnosis Tools
  Verify Tencent IP
  Self Troubleshooting Tool
Value-added Services
  Pornography Detection
We have revamped the domain management page and are now transiting from the legacy version to the new version.
If you see any discrepancies from the descriptions in this document, please see Domain Name Operations (Legacy).

Operation Scenarios

After you create a distribution, you can log in to the CDN Console and select Domain Management on the left sidebar to view the acceleration domain or activate/disable acceleration service.

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

Operation Guide

List operations

1. Customizing the list display

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

![Customize](image)

You can customize the following fields:

- **Domain**: this is required and cannot be hidden.
- **Service type**: static acceleration, download acceleration, or streaming VOD acceleration.
- **Status**: domain service status (activated, disabled, or deploying).
- **CNAME**: CNAME record of the domain.
- **Origin type**: external origin server or COS origin server.
- **Service region**: Mainland China, outside Mainland China, or global.
- **Project**: name of the project where the domain resides.
- **Primary origin configuration**: primary origin server address.
- **Backup origin configuration**: backup origin server address.
- **HTTPS configuration**: configured or not configured.
- **Origin-pull protocol**: HTTP, HTTPS, or follow protocol.
- **Origin domain**: origin-pull domain settings.
- **Ignore query string**: enabled or disabled.

### 2. Exporting the configuration list

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

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

In the CDN Console, you can activate, disable, and delete the acceleration service or modify projects for acceleration domains:

1. Disabling acceleration service

After the acceleration service is disabled for a domain, its configurations on the cache nodes across the entire network will be deactivated, and if access requests to it are still redirected to a CDN node, error 404 will be returned. Therefore, before disabling a domain, you should make sure that its CNAME record is pointing to a non-CDN CNAME address.

- You can only disable activated acceleration domains. Domains in deployment cannot be disabled.
- Configurations of disabled domains will be retained and take effect when the domains are reactivated.
- No more consumption will be generated after the acceleration service is completely disabled.

You can click Disable in the "Operation" column on the right of a domain to disable the service. You can also select multiple domains in Activated status and disable them in batches in More Actions at the top.

2. Enabling acceleration service

If a domain 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 a domain to enable the service. You can also select multiple domains in Disabled status and activate them in batches in More Actions at the top.

If there is no operation or consumption for an activated domain in 3 months, it will be considered to be inactive, and CDN will automatically disable its acceleration service.
3. Deleting acceleration domains

If a domain is in Disabled status, you can click More on the right to delete it. Please note that once a domain is deleted, its configuration will be cleared and cannot be restored. Its statistical data will also no longer viewable.
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><a href="http://www.test.com">www.test.com</a></td>
<td>Filters domain names containing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.test.com">www.test.com</a></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</td>
<td>**Attribute:**keyword</td>
<td>Origin server:1.1.1</td>
<td></td>
<td>Filters domain names where the origin server contains 1.1.1.1</td>
</tr>
<tr>
<td>Multiple domain name attributes</td>
<td>**Attribute:**keyword carriage return **Attribute:**keyword</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>Single domain name attribute with multiple keywords</td>
<td>**Attribute:**keyword</td>
<td>Project:test1</td>
<td>test2</td>
<td>Project:test1</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.
CDN supports various custom configurations, you can optimize your CDN acceleration 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>Modifies the domain’s project and service type</td>
</tr>
<tr>
<td>Origin Server Configuration</td>
<td>Configures hot backup origin server and modifies the origin server to ensure the success of origin-pull</td>
</tr>
<tr>
<td>Host Header Configuration</td>
<td>Specifies the domain name accessed by CDN during origin-pull</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>Specifies whether a node will ignore the parameters after &quot;?&quot; in a user request URL</td>
</tr>
<tr>
<td>Hotlink Protection Configuration</td>
<td>Configures HTTP referer blacklist/whitelist</td>
</tr>
<tr>
<td>IP Blacklist/Whitelist Configuration</td>
<td>Configures IP blacklist/whitelist for access control</td>
</tr>
<tr>
<td>IP Access Limit Configuration</td>
<td>Configures access limit of an IP to a single node</td>
</tr>
<tr>
<td>Video Dragging Configuration</td>
<td>Enables video dragging configuration</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>Configures cache expiration rules for the specified resources</td>
</tr>
<tr>
<td>Status Code Cache Configuration</td>
<td>Configures 404 status code cache period</td>
</tr>
<tr>
<td>HTTP Header Cache Configuration</td>
<td>Configures the header cache policy</td>
</tr>
</tbody>
</table>

### Origin Configuration
## Configuration Name | Feature Description
--- | ---
Intermediate Node Configuration | Specifies whether to use intermediate nodes
Range GETs Configuration | Enables/disables range GETs
Follow 302 Configuration | Configures whether requests should be redirected when the origin server returns the 302 status code

### Security Configuration

## Configuration Name | Feature Description
--- | ---
Authentication Configuration | Configures URL authentication

### Advanced Configuration

## Configuration Name | Feature Description
--- | ---
Bandwidth Cap Configuration | Configures 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
HTTPS Configuration | Configures HTTPS to implement secure acceleration where forced HTTPS redirection is supported
SEO Optimization Configuration | Enables SEO optimization configuration to ensure stability of the search engine weights
HTTP Header Configuration | Adds an HTTP header configuration

### Cross-border Direct Connect Configuration

## Configuration Name | Feature Description
--- | ---
Cross-border Direct Connect Configuration (in beta) | Enables/disables cross-border direct connect lines during global CDN acceleration to ensure origin-pull quality
You can view the basic information of a domain name in the CDN Console, including its accelerated domain name, CNAME, creation time, project, and service type. You can also modify the **project** and **service type** as needed.

Changing the service type will also change the acceleration platform and optimization model. Please make sure that the modification matches your service type. If you are a Tencent Cloud VIP customer and have issues changing the service type manually, you can contact our pre-sales or after-sales customer service or submit a ticket.

**Configuration Guide**

1. Log in to the **CDN Console** and click **Domain Name Management** on the left sidebar to enter the management page. Find the domain name you want to edit and click **Manage** in the "Operation" column.

2. You can view the basic information of the domain name on the **Basic Configuration**. Click **Modify** on the right of the **project**.
Origin Server Configuration

Last updated: 2020-02-22 19:48:08

You can modify the configuration of the origin server for your domain name:

- **Multi-site active-active IPs**
  When multiple IPs are configured as the origin server, CDN uses a polling policy to randomly select an IP for origin-pull. It also performs origin server detection, so that when an origin server IP is found to be exceptional, it will be blocked for a period of time (60 seconds by default) and skipped during polling.

- **Domain name origin server**
  A specified domain name can be set as the origin server, which should be different from the accelerated domain name.

- **COS bucket origin server**
  A public domain name of the selected COS bucket can be used as an origin server for CDN origin-pull.

- **Slave origin server configuration**
  Tencent Cloud CDN supports configuring an external domain name as a hot backup slave origin server. When an origin-pull request to the master origin server fails (e.g., 4XX, 5XX, or TCP connection errors), it will be forwarded to the slave origin server. Configuring a slave origin server can effectively reduce origin-pull failure rate and improve the service quality. Hot backup slave origin server does not support HTTPS origin-pull for the time being; therefore, when you configure a certificate for a domain name with a slave origin server, do not select HTTPS origin-pull.

**Configuration Guide**

**Viewing the Configuration**

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. You will see the **Origin Server Information** module on the **Basic Configuration** Page. You can view the current origin server configuration of the domain name here.

### Modifying Origin Server

You can edit existing origin servers or add hot backup origins (only own origins supported). When the back-to-origin request failed, the hot backup origin server will be requested. To set up an origin server:

1. Click the **Origin server info** section.
2. Check the **Master origin server**.
3. Enter the **Origin type** and **Origin address**.
4. Click the + button to add a hot backup origin server.

---

©2013-2019 Tencent Cloud. All rights reserved.
1. Go to **Basic Configuration** to see the **Origin Server Information** module.

![Basic Configuration](image)

2. Click the **Edit** icon in the top-right corner of the master origin server to modify its type:

![Modify origin server info](image)

**External Origin**: The origin server address can be configured as multiple IPs or one single domain name. Origin-pull to the specified port is supported in the format of "domain name:PORT/IP:PORT" in the value range from 0 to 65535.

- If the origin server address is configured as IPs, the weight of the origin server IPs can be configured in the format of IP:PORT:WEIGHT in the value range from 0 to 1000.
  - The weight cannot be set for single origin server.
  - If the origin server is multiple IPs, it is not allowed to set origin-pull weight only for certain IPs.
  - If the origin server is in domain name format, the weight cannot be set. Only IP origin servers support weight configuration.
Weight can be configured in the format of IP:PORT:WEIGHT, where PORT can be omitted. In this case, the format is IP::WEIGHT.

Currently, only IPv4 addresses support weight configuration, while IPv6 addresses do not.

**COS Origin**: Specify a COS bucket as the origin server.

**Adding a Slave Origin Server**

1. If the origin server of a domain name is an **external origin**, you can add a hot backup slave origin server for it. When an origin-pull request to the master origin server fails (e.g., 4XX, 5XX, or TCP connection errors), it will be forwarded to the slave origin server.

2. A slave origin server can only be added for an external origin. The origin server address can be configured as multiple IPs or one domain name. Origin-pull to the specified port is supported in the port range from 0 to 65535.
Modifying Slave Origin Server

Once a slave origin server is added, master/slave switch can be easily performed in the console. You can also modify or delete the slave origin server.
Sample Case

A user requests http://www.test.com/1.jpg which is not hit on any node. The request is forwarded to the origin server.

1. If the origin server is configured as follows:

If the resource is not cached on the server 1.1.1.1, a 404 error will be directly returned. In this case, after receiving the response, the CDN node at the origin-pull layer will directly return the request to the requesting client, and the client cannot obtain the image.
2. If the origin server is configured as follows:

If the resource is not cached on the server 1.1.1.1, a 404 error will be directly returned. In this case, after receiving the response, the CDN node at the origin-pull layer will request the resource again to the slave origin server 2.2.2.2. If 2.2.2.2 returns a 200 status code, the node will send the successfully obtained content to the requesting client, and the client will successfully obtain the image.
The algorithms supported by HTTPS Origin-pull are shown in the following table (in no order):

<table>
<thead>
<tr>
<th>ECDHE-RSA-AES256-SHA</th>
<th>ECDHE-RSA-AES256-SHA384</th>
<th>ECDHE-RSA-AES256-GCM-SHA384</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>SRP-AES-128-CBC-SHA</td>
<td>SRP-RSA-AES-128-CBC-SHA</td>
<td>SRP-DSS-AES-128-CBC-SHA</td>
</tr>
<tr>
<td>DH-RSA-AES128-SHA</td>
<td>DH-RSA-AES128-SHA256</td>
<td>DH-RSA-AES128-GCM-SHA256</td>
</tr>
<tr>
<td>Cipher</td>
<td>Cipher</td>
<td>Cipher</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-SHA</td>
<td>ECDHE-RSA-AES256-SHA</td>
<td>ECDHE-RSA-AES256-GCM-SHA384</td>
</tr>
<tr>
<td>DH-DSS-AES128-SHA</td>
<td>DH-DSS-AES128-SHA256</td>
<td>DH-DSS-AES128-GCM-SHA256</td>
</tr>
<tr>
<td>DHE-RSA-AES128-SHA</td>
<td>DHE-RSA-AES128-SHA256</td>
<td>DHE-RSA-AES128-GCM-SHA256</td>
</tr>
<tr>
<td>DHE-DSS-AES128-SHA</td>
<td>DHE-DSS-AES128-SHA256</td>
<td>DHE-DSS-AES128-GCM-SHA256</td>
</tr>
<tr>
<td>ECDH-RSA-AES128-SHA</td>
<td>ECDH-RSA-AES128-SHA256</td>
<td>ECDH-RSA-AES128-GCM-SHA256</td>
</tr>
<tr>
<td>ECDH-ECDSA-AES128-SHA</td>
<td>ECDH-ECDSA-AES128-SHA256</td>
<td>ECDH-ECDSA-AES128-GCM-SHA256</td>
</tr>
<tr>
<td>CAMELLIA128-SHA</td>
<td>DH-RSA-CAMELLIA128-SHA</td>
<td>DHE-RSA-CAMELLIA128-SHA</td>
</tr>
<tr>
<td>PSK-RC4-SHA</td>
<td>DH-DSS-CAMELLIA128-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>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>
Host Header Configuration

What Is a Host Header?

A host header refers to the website domain name accessed at the origin server by a CDN node during origin-pull. Please make sure that the configured host header domain name can be accessed; otherwise, origin-pull may fail. The host header can be customized according to your business.

- Origin server and host header: The IP/domain name configured at the origin server allows a CDN node to find the corresponding origin server during origin-pull. There can be multiple websites on the server, and the host header indicates on which website a resource resides.
- According to applicable regulations, if an origin server uses a Tencent Cloud CVM’s accelerated domain name, the domain name configured to be the host header should have completed ICP filing through Tencent Cloud.

Configuration Guide

Viewing the Configuration

1. Log in to the CDN Console and click Domain Management on the left sidebar to enter the management page.
2. In the list, find the domain name you want to edit and click Manage in the operation column.
3. At the bottom of the basic configuration page, you can view the host header configuration information.

By default, the host header of a sub-domain name is the configured accelerated domain name, while that of a wildcard domain name is the access domain name:
If the accelerated domain name connected is www.test.com, when a node sends an origin-pull request to a resource under this domain name, the host field in the request HTTP header is www.test.com.

If the accelerated domain name connected is a wildcard domain such as *.test.com and the access domain name is abc.test.com, then the host header is abc.test.com.

Modifying a Host Header

You can click Edit in the origin configuration section on the same page to adjust the host header configuration. Host header can be customized only for your own origin servers but not COS origin servers.

Sample Case

The user access domain name is www.test.com, the origin server is configured as domain name origin.test.com, and the A record corresponding to origin.test.com is 1.1.1.1.

The user request is: http://www.test.com/1.jpg.
1. If the configuration is as follows:

By default, the host header is the accelerated domain name, and the actual request is sent to 1.1.1.1 during origin-pull.

The resource obtained is: http://www.test.com/1.jpg.

2. If the configuration is as follows:

The host header is origin.test.com, and the actual request is sent to 1.1.1.1 during origin-pull.

The resource obtained is: http://origin.test.com/1.jpg.
Access Control
Ignore Query String Configuration

Last updated: 2020-01-19 16:40:23

CDN provides an Ignore Query String switch, which allows you to control whether to filter the parameters after "?" in user requests' URLs during caching. You can use this feature for flexible version control or token-based authentication.

If different parameters in your resource URL represent the same content, we recommended you enable the ignore query string feature to effectively improve the cache hit rate.

Configuration Guide

1. Log in to the CDN Console and click Domain Management on the left sidebar to enter the management page. Find the desired domain name and click Manage in the "Operation" column.

2. Click the Access Control tab and configure the ignore query string feature in the "Ignore Query String" module.

If your accelerated business type is download or video on-demand, the ignore query string feature is enabled by default. If the accelerated type is static content, it is disabled by default.

Sample Case
When CDN caches resources on the node storage structure, it uses cache_key as an index to search for stored resources.

1. If the configuration is as follows:

   ![Access Control Table]

   - User A requests a resource with URL `http://www.test.com/1.jpg?version=1.1`. When a node stores the resource, the corresponding cache_key is `www.test.com/1.jpg` with the parameters after `?` ignored.
   - User B requests a resource with URL `http://www.test.com/1.jpg?version=1.2`, which will also be looked up with cache_key as `www.test.com/1.jpg`, so the content can be directly hit because it is the same as that requested by user A.

2. If the configuration is as follows:

   ![Access Control Table]

   - User A requests a resource with URL `http://www.test.com/1.jpg?version=1.1`. When a node stores the resource, the corresponding cache_key is `www.test.com/1.jpg?version=1.1` with the parameters after `?` ignored.
   - User B requests a resource with URL `http://www.test.com/1.jpg?version=1.2`, which will be looked up with cache_key as `www.test.com/1.jpg?version=1.2`. Because there is no hit, the corresponding content will be obtained from the origin server again for caching.
Hotlink Protection Configuration

Configuration Guide

1. Log in to the CDN Console and click Domain Management on the left sidebar to enter the management page. Find the desired domain name and click Manage in the "Operation" column.

2. Click the Access Control tab and configure the Hotlink Protection module.

Hotlink protection is disabled by default with no blacklist or whitelist. Referer-based blacklist and whitelist are incompatible with each other and cannot coexist. You can enter up to 400 entries, separated by line breaks and one entry per row.

- 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.

Referer Whitelist

1. Click the Edit icon in the hotlink protection configuration section and select Referer Whitelist to configure the whitelist.

   If you configure a referer whitelist for the domain name www.test.com with content as www.abc.com and do not check
Allow blank referer, you only allow requests where the referer value is www.abc.com to access, and a 403 error will be returned for other requests.

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

Referer Blacklist

1. Click the Edit icon in the hotlink protection configuration section and select Referer Blacklist to configure the blacklist.
   - If you configure a referer blacklist for the domain name www.abc.com with content as www.test.com and do not check Allow blank referer, a 403 error will be returned for all requests where the referer value is www.test.com, and all other requests will return the requested information.

2. Configuration Notes:
   - If the referer field of a request matches the string configured in the blacklist, the 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, the CDN node will return the requested information.
   - If Allow blank referer is checked, the 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).
Sample Case

If the domain name referer is configured as follows:
• If a user requests a resource with URL \[\text{http://www.test.com/1.jpg?version=1.1}\] from a browser and the request referer field is empty, then the requested information will be returned.

• If a user requests a resource with URL \[\text{http://www.test.com/1.jpg?version=1.1}\] and the request referer \[\text{www.abcd.com}\] is not in the whitelist, then a 403 error will be returned.
IP Blacklist/Whitelist Configuration

Last updated : 2020-01-19 17:04:46

CDN supports IP blacklist/whitelist configuration, allowing you to create filtering policies for source IPs of user requests based on business needs and preventing hotlinking or attacks from malicious IPs.

Configuration Guide

1. Log in to the CDN Console and click Domain Management on the left sidebar to enter the management page. Find the desired domain name and click Manage in the “Operation” column.

2. Click the Access Control tab and then IP Blacklist & Whitelist Configuration. The IP blacklist/whitelist feature is disabled by default.

- IP blacklist and whitelist are incompatible with each other and cannot coexist. You can enter up to 100 entries in the blacklist or up to 50 entries in the whitelist, separated by line breaks and one entry per row.
- Currently, only IP ranges in the following formats are supported: /8, /16, and /24. If both IP blacklist and whitelist are empty, blacklist/whitelist feature is disabled.

Whitelist Configuration

1. Click Edit and IP Whitelist will be selected by default. You can now configure the whitelist. Enter IPs in the input box and submit them to enable the IP whitelist. The requested content will be returned only if
the source IP matches an IP address or IP range in the whitelist; otherwise, a 403 error will be returned.

2. After the configuration is completed, the feature is on and effective IP whitelist configuration information will be displayed below. You can click **Edit** to change the configuration information.

3. After the **IP Blacklist/Whitelist** feature is off, the configuration information below will become invalid, i.e., the IP blacklist/whitelist feature is disabled. It can be enabled again manually.
Blacklist Configuration

1. Click **Edit** and select **IP Blacklist** to configure the blacklist.
   Enter IPs in the input box and submit them to enable the IP blacklist. If the source IP matches an IP address or IP range in the blacklist, a 403 error will be returned; otherwise, the requested content will be returned.

2. After the configuration is completed, the feature is on and effective IP blacklist configuration information will be displayed below. You can click **Edit** to change the configuration information.
3. After the **IP Blacklist/Whitelist** feature is off, the configuration information below will become invalid, i.e., the IP blacklist/whitelist feature is disabled. It can be enabled again manually.

Sample Case
If the IP blacklist/whitelist configuration of the domain name www.test.com is as follows:

![Switch on IP Blacklist & Whitelist]

Then:

- When a user with IP 1.1.1.1 accesses the resource http://www.test.com/1.jpg, the IP matches an IP in the whitelist, the requested content will be returned.
- When a user with IP 2.2.2.2 accesses the resource http://www.test.com/1.jpg, as the IP does not match any IP in the whitelist, a 403 error will be returned.
IP Access Limit Configuration

©2013-2019 Tencent Cloud. All rights reserved.

CDN supports configuring the IP access frequency limit to protect against CC attacks by limiting the number of access requests per second to a node allowed for a client. After the configuration is enabled, a 514 error will be returned for requests that exceed the QPS limit. Setting a lower limit may affect the normal usage of high-frequency users. Please set the limit according to your actual business needs.

Configuration Guide

Viewing the Configuration

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 IP Access Limits module.

The “IP Access Limits” feature is disabled by default.
Modifying the IP Access Limits

1. Go to the **IP Access Limits** module and toggle the switch on. The system will automatically input a default limit based on the average single-IP access requests in the last 30 days. You can view this limit in the **IP Access Limit** field below.

   The default limit is calculated as follows: The number of access requests by a single IP at each of the 288 statitical points per day (one point per 5 minutes) is calculated, and the 30 highest values in the last 30 days are averaged as the default limit. The default minimum limit is 10 QPS and for reference only. We recommend setting the limit based on your business fluctuations.

2. Click **Edit**.

3. Set the IP access limit and click **OK**.
Sample Case

If the domain name www.test.com is configured with the following IP access limit:

Then:

- If a user with IP 1.1.1.1 requests the resource http://www.test.com/1.jpg for 11 times in one second, and all the access requests are made to one server on the CDN cache node A, then there will be 11 access logs generated on this server, one of which exceeds the QPS limit, and the status code “514” will be returned.
- If a user with IP 2.2.2.2 requests the resource http://www.test.com/1.jpg for 11 times in one second, and the access requests are evenly distributed on multiple CDN cache nodes, then each node will return the content.
Video Dragging Configuration

- 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:
  
  \[
  \text{http://www.test.com/test.flv?start=10}
  \]

  In this case, data will be returned starting from the 10th byte. Video files in VOD scenarios are all cached on various CDN nodes; therefore, the nodes can directly respond to such requests once this configuration is enabled.

- 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>
</table>
| MP4       | For a video on the origin server, the meta information must be located in the file header. Videos with meta information located at the file end are not supported | The 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.mp4?start=10  
  The video will be played back starting from the 10th second |
| FLV       | The video on the origin server must have meta information | 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) | http://www.test.com/demo.flv?start=10  
  The video will be played back starting from the 10th byte |
| 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.
Configure the scene

In general, the content distributed on CDN defaults to public resources, and users can use Access after they get the URL. In order to prevent malicious users from stealing your content for profit, in addition to Access control strategies such as referer Blacklist/Whitelist, IP Blacklist/Whitelist, IP Access frequency limit, you can also protect against theft by setting advanced timestamp authentication.

After configuring timestamp and Hotlink protection Prevent hotlinking, the client needs to calculate the signature according to the configuration and carry it to the server when initiating the request, and the CDN node verifies it at the server end, and then pass continues after the verification is passed.

Configuration Guid

View Settings

Login CDN console Select "Domain name Management" in the menu bar, and click "manage" on the right side of the domain name to enter the domain name configuration page. You can see the authentication configuration in "Security configuration". By default, authentication configuration is disabled.

Change Settings

1. Change Settings

CDN provides four authentication signature calculation methods for you to choose from. You can also view different authentication modes and the final results after configuration through the [Authentication Calculator] above. For more information on the algorithm, please see the specific algorithm description document /

2. Turn off configuration

You can use the authentication configuration switch to close the configuration with one button. When the switch is off, the network will not take effect even if the configuration exists below. The next time you click enable, the configuration will be confirmed twice in advance. It will not take effect from publish to entire network immediately.

3. Regional special configuration

If your accelerated domain name service region is global acceleration, and you want to make different authentication configurations for domestic and overseas acceleration regions, click add Special configuration below configuration to set it.
After the zone special configuration is added, it cannot be deleted directly for the time being. You can disable it by turning off the configuration.

**Configuration example**

If the domain name `cloud.tencent.com` For a globally accelerated domain name, the authentication configuration is as follows.

The actual effective scenarios are as follows:

1. **Actual Access resources of users in China**  
   [http://cloud.tencent.com/1.jpg](http://cloud.tencent.com/1.jpg) The request can be initiated directly.

2. **Actual Access resources for users outside China**  
   [http://cloud.tencent.com/1.jpg](http://cloud.tencent.com/1.jpg) The request URL format is 
   [http://cloud.tencent.com/509301d10da7b862052927ed7a947f43/5e561139/1.jpg](http://cloud.tencent.com/509301d10da7b862052927ed7a947f43/5e561139/1.jpg) .
Algorithm description

Access URL format

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

Algorithm description

- Timestamp: decimal (UNIX timestamp).
- Rand: random string, 0-100 bit random string, consisting of uppercase and lowercase letters and numbers.
- Uid: 0
- Md5hash: MD5 (file path-timestamp-rand-uid- custom key).

Request Sample

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

When calculating MD5, if the request path is http://cloud.tencent.com/test.jpg The path when calculating MD5 is /test.jpg.

Configuration Guid

Parameter description

The required configurations for TypeA are as follows:

- **Custom authentication key** It is composed of 6-32 bits uppercase and lowercase letters and numbers. The key needs to be kept secret and is known only to the client and the server.
- **Custom authentication parameter name** Replace the sign in the example with a parameter name consisting of any 1-100 uppercase and lowercase letters, numbers or underscores. After receiving the request, CDN takes out the corresponding value according to the specified signature parameters and performs MD5 calculation. If the passed md5hash value is matched, the signature verification is passed. If the verification fails, 403 is returned directly.
- **Custom effective time** Use the timestamp, carried in the request plus the configured valid time to compare it with the current time to determine whether the request is Expire. If Expire, it will directly return 403.

Effective object

After configuring the key, parameter name and Expire time, you can specify the authentication object as needed, and the following three modes are supported:

- Authentication verification is required for all files under the specified domain name.
- It is supported that files of the specified type are not authenticated. Other files need to be authenticated.
- Specified type files are supported for authentication verification.
Notes

Cache hit rate
For a domain name with TypeA authentication mode enabled, Access URL will carry authentication parameters. When caching resources on CDN nodes, the corresponding parameters will be automatically ignored and cached, which will not affect the hit rate of domain name cache.

Origin-Pull Policy
The domain name with TypeA authentication mode enabled. The format of Access is:

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

After the authentication is passed, if the CDN node is missed, the node will initiate Origin-pull request. The format is consistent with Access's request, and the sign parameter will be retained. Real server can ignore or re-check as needed.
TypeB
Last updated: 2020-03-19 17:57:02

Algorithm description

**Access URL format**

http://DomainName/timestamp/md5hash/FileName

**Algorithm description**

- Timestamp: timestamp, format is YYYYMMDDHHMM.
- Md5hash: MD5 (Custom key + timestamp + File path).

**Request Sample**

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

When calculating MD5, if the request path is http://cloud.tencent.com/test.jpg, The path when calculating MD5 is /test.jpg.

Configuration Guid

**Parameter description**

The required configurations for TypeB are as follows:

- **Custom authentication key:** It is composed of 6-32 bits uppercase and lowercase letters and numbers. The key needs to be kept strictly secret and is known only to the client and the server.
- **Custom valid time:** By comparing the timestamp value in the request path and the configured valid time with the current time, we can determine whether the request is Expire. If Expire, we will return 403 directly.

**Effective object**

After configuring the key, parameter name and Expire time, you can specify the authentication object as needed, and the following three modes are supported:

- Authentication verification is required for all files under the specified domain name.
- It is supported that files of the specified type are not authenticated. Other files need to be authenticated.
- Specified type files are supported for authentication verification.

**Notes**

**Cache hit rate**

For a domain name with TypeB authentication mode enabled, Access will carry his signature and timestamp in the URL path. When the CDN node carries out resource caching, it will automatically ignore the fields in the path for caching, which will not affect the domain name cache hit rate.
**Origin-Pull Policy**

The domain name with TypeB authentication mode enabled. The format of Access is:

http://DomainName/timestamp/md5hash/FileName

After the authentication is passed, if the CDN node is missed, the node will initiate Origin-pull request. **Origin-pull request will remove md5hash and timestamp from the path.** Real server does not need to do any special treatment.
TypeC

Last updated: 2020-03-19 17:57:02

Algorithm description

Access URL format

http://DomainName/md5hash/timestamp/FileName

Algorithm description

- Timestamp: hexadecimal (UNIX timestamp).
- Md5hash:MD5 (Custom key + File path + timestamp).

Request Sample

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

When calculating MD5, if the request path is http://cloud.tencent.com/test.jpg The path when calculating MD5 is /test.jpg.

Configuration Guid

Parameter description

The required configurations for TypeC are as follows:

** Custom authentication key: ** It is composed of 6-32 bits uppercase and lowercase letters and numbers. The key needs to be kept strictly secret and is known only to the client and the server.

** Custom valid time: ** By comparing the timestamp value in the request path and the configured valid time with the current time, we can determine whether the request is Expire. If Expire, we will return 403 directly.

Effective object

After configuring the key, parameter name and Expire time, you can specify the authentication object as needed, and the following three modes are supported:

- Authentication verification is required for all files under the specified domain name.
- It is supported that files of the specified type are not authenticated. Other files need to be authenticated.
- Specified type files are supported for authentication verification.

Notes

Cache hit rate

Domain names with TypeC authentication mode enabled will be carried in Access’s URL path. When caching resources on CDN nodes, the authentication path will be automatically ignored for caching, which will not affect the hit rate of domain name cache.
Origin-Pull Policy
The domain name with TypeC authentication mode enabled. The format of Access is:

http://DomainName/md5hash/timestamp/FileName

After the authentication is passed, if the CDN node is missed, the node will initiate Origin-pull request. **Origin-pull request will remove the md5hash and timestamp paths from the path.** Real server does not need to do any special treatment.
**Algorithm description**

**Access URL format**

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

**Algorithm description**

- Timestamp: decimal / hexadecimal (UNIX timestamp) is optional.
- Md5hash: MD5 (Custom key + File path + timestamp).

**Request Sample**

http://cloud.tenloud.tencent.com/test.jpg?sign=0f8201d814dfaf64af64e74c5f7dbcb0&t=1582791032

When calculating MD5, if the request path is http://cloud.tencent.com/test.jpg, the path when calculating MD5 is /test.jpg.

**Configuration Guid**

**Parameter description**

The required configurations for TypeD are as follows:

**Custom authentication key:** It is composed of 6-32 bits uppercase and lowercase letters and numbers. The key needs to be kept strictly secret and is known only to the client and the server.

**Custom authentication parameter name and timestamp parameter name:** Replace the sign in the example with a parameter name consisting of any 1-100-digit uppercase and lowercase letters, numbers or underscores. After receiving the request, CDN takes out the corresponding value according to the specified signature parameters and performs MD5 calculation. If the passed md5hash value is matched, the signature verification is passed. If the verification fails, 403 is returned directly.

**Custom valid time:** The timestamp value is taken out through the parameter configuration of timestamp, and the valid time of the configuration is compared with the current time to determine whether the request is Expire. If Expire, it will be returned directly.

**Effective object**

After configuring the key, parameter name and Expire time, you can specify the authentication object as needed, and the following three modes are supported:

- Authentication verification is required for all files under the specified domain name.
- It is supported that files of the specified type are not authenticated. Other files need to be authenticated.
- Specified type files are supported for authentication verification.
Notes

**Cache hit rate**
For a domain name with TypeD authentication mode enabled, Access URL will carry authentication parameters. When caching resources on CDN nodes, the corresponding parameters will be automatically ignored and cached, which will not affect the hit rate of domain name cache.

**Origin-Pull Policy**
The domain name with TypeD authentication mode enabled. The format of Access is:

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

After the authentication is passed, if the CDN node is missed, the node will initiate Origin-pull request. **The format is consistent with Access's request, and the sign/t parameter will be retained.** Real server can ignore or re-check as needed.
Cache Configuration
Parameter cache configuration

Configure the scene

Tencent Cloud CDN uses Key-Value format for resource mapping when caching, in which Key is the cache key, which is the unique identity of the cached resource.

When you use URL to source Access, you may bring some special parameters, such as using the following link to represent two different images:

http://cloud.tencent.com/1.jpg?version=1
http://cloud.tencent.com/1.jpg?version=2

In this scenario, parameter filtering needs to be turned off, and the complete URL is used as the cache key to cache the image content to distinguish resources.

In an audio / video scenario, if you use the signature parameter of timestamp to perform Access and Verification:

http://cloud.tencent.com/1.mp4?sign=XXXXXX

This kind of scenario needs to turn on parameter filtering, which is determined by "?" Previous link http://cloud.tencent.com/1.mp4. As a cache key, the node caches only one resource. Even if timestamp's signature is constantly changing, it can directly hit the cache after signature verification.

Configuration Guid

View Settings

Login CDN console Select "Domain name Management" in the menu bar, and click "manage" on the right side of the domain name to enter the domain name configuration page. Ignore Query String configuration can be seen in "Access Control" in the second column.

When connecting to an accelerated domain name:

- If you select static acceleration type, Ignore Query String is disabled by default.
- Download and streaming Video on-demand business type, Ignore Query String is enabled by default.
Change Settings

You can directly click the switch button to turn off or enable the parameter cache configuration. The effective time of configuring deliver and entire network is about 5 minutes:

- If your accelerated domain name service region is global acceleration, the parameter cache configuration will take effect globally, and domestic and overseas differentiated configurations are not supported.
- Enabling parameter cache configuration can effectively improve the cache hit rate.
Configure the scene

Tencent Cloud's CDN cache resource is triggered. When a user initiates Access for a resource, if the CDN node that the request reaches does not cache the resource, the user real server pulls the resource and successfully pulls the resource (2XX status code), then caches it on the node and returns it to the user.

You cannot directly manage the cached resources on the CDN node. If you are worried that the real server resource may change and the CDN node still caches the old resource back to the user, you can control it to a certain extent by configuring node cache rules.

The cache resource on every CDN node has the concept of "Expire time". If the requested cache resource has expired, it will be determined to be invalid even if the node still has a cache, and Origin-pull will pull it again. Node cache rule configuration supports specifying the cache Expire time of resources of a certain type, Directory and path in the node, which can be configured according to the actual business scenario.

Configuration Guid

View Settings

Login CDN console Select "Domain name Management" in the menu bar, and click "manage" on the right side of the domain name to enter the domain name configuration page. The cache Expire configuration can be seen in the "Cache configuration" in the third column.

When connecting to an accelerated domain name:

- If you select the static acceleration type, the default cache time for regular dynamic files (such as .php .jsp .asp .aspx) is 0 (no cache for direct Origin-pull), and the default Expire time for all other file types is 30 days.
- If you choose download acceleration and streaming Video on-demand acceleration, the default Expire cache time for all files is 30 days.

Change Settings
1. Change Settings

CDN currently supports the following four types of cache Expire rule configurations:

- **File type**: cache Expire time setting according to the file suffix entered. The format is `.jpg` Form, used between different suffixes; Interval.
- **Folder**: cache Expire time according to the filled Directory path, in the format of `/test` Form, there is no need to use `/` At the end, between different Directory; Interval.
- **Full-path file**: specify a complete file path to cache Expire time, in the format of `/index.html` The full path plus file type matching pattern is supported, such as `/test/*.jpg`.
- **Home page**: set the cache Expire time for the root Directory.

### Configuration rules:

- You can configure up to 10 cache Expire rules.
- The priority among multiple cache Expire rules is the bottom first.
- The cache time for Expire can be set up to 365 days.

If your accelerated domain name service region is global acceleration, the set cache Expire time will take effect globally, and differential configuration between domestic and overseas is not supported.

2. Platform strategy

When a user requests a business resource, the Cache-Control field exists in the HTTP Response Header corresponding to real server. The default platform policy is as follows:

- The Cache-Control field indicates that the cache time of Max-Age, for this resource is mainly based on the configured node cache Expire time, and does not inherit the time specified by Max-Age.
- The Cache-Control field is no-cache, no-store, or private,. At this time, the CDN node does not cache this resource.
- If there is no Cache-Control field, CDN will be added by default: `Cache-Control:max-age = 600` Head.

3. Advanced cache configuration
Enable advanced cache configuration. Users can adjust the node cache time dynamically by adjusting the Max-Age value in real server's HTTP Response Header Cache-Control.

When enabled, CDN compares the configured node cache time with the Max-Age value, and takes the smaller one as the actual effective node cache time:

- User real server configuration /index.html If the Max-Age of the CDN is 200s and the configured cache time of CDN is 600s, the actual Expire time of the file on the node is 200s.
- User real server configuration /index.html If the Max-Age of the file is 800s, and the cache time of CDN is 600s, the actual Expire time of the file on the node is 600s.

Advanced cache configuration is enabled. If real server does not return the Last-Modified field, CDN will add the Last-Modified field by default and change it every 10 minutes.

Configuration exampl

If you accelerate the domain name cloud.tencent.com The configuration of Expire rules for caching is as follows:

<table>
<thead>
<tr>
<th>Type</th>
<th>Content</th>
<th>Purge Time</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>All</td>
<td>30 days</td>
<td>Modify</td>
</tr>
<tr>
<td>File ext</td>
<td>php, js, jpg, uuid, etc</td>
<td>0 days</td>
<td>Modify</td>
</tr>
<tr>
<td>File ext</td>
<td>.png</td>
<td>5 minutes</td>
<td>Modify</td>
</tr>
<tr>
<td>Full path</td>
<td>/test/*</td>
<td>400 seconds</td>
<td>Modify</td>
</tr>
<tr>
<td>Full path</td>
<td>/test/abc.jpg</td>
<td>200 seconds</td>
<td>Modify</td>
</tr>
</tbody>
</table>

The actual cache time is as follows:

1. /test/abc.jpg The file node cache Expire time is 200s.
2. /test/def.jpg The file node cache Expire time is 400 seconds.
3. /test/1.png The file node cache Expire time is 300 seconds.
Configure the scene

Normally, the CDN node successfully pulls the requested resource (2XX status code) from real server, and the node processes it according to the Expir time configured by the cache rules.

If a non-2XX status code is returned, the other status codes will not be cached by default, except that the 404 status code will be cached by default for 10 seconds. If real server cannot quickly solve the non-2XX status codes and does not want all requests for pass through to go back to the origin server, you can configure the status codes to cache Expir's time, and the CDN node can directly respond to the non-2XX status codes to reduce the pressure on real server.

Configuration Guid

View Settings

Login CDN console Select “Domain name Management” in the menu bar, and click "manage" on the right side of the domain name to enter the domain name configuration page. The status code cache configuration can be seen in "Cache configuration" in the third column:

<table>
<thead>
<tr>
<th>Status code</th>
<th>Cache Validity</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>404</td>
<td>10s</td>
<td>Modify/</td>
</tr>
</tbody>
</table>

Change Settings

The following exception status code cache Expir configuration is supported

- four hundred and three
- four hundred and four

You can cancel the cache Expir time configuration by modifying the cache time to 0 or deleting the corresponding configuration entry, and directly Origin-pull.
If your accelerated domain name service region is global acceleration, the status code cache Expire time set will take effect globally, and differentiated configurations within and outside China are not supported.
Configure the scene

In addition to the resource content, Tencent Cloud CDN caches the following headers from real server by default and returns them to users:

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

If your real server has a special header that needs to be cached by CDN and returned to the user, you can do this by enabling the header cache configuration.

Configuration Guid

View Settings

Login CDN console Select "Domain name Management" in the menu bar, and click "manage" on the right side of the domain name to enter the domain name configuration page. You can see the HTTP header cache configuration in the "Cache configuration" in the third column, which is disabled by default.

Change Settings

You can directly click the switch button to turn off or enable the HTTP header cache configuration. The effective time of deliver and entire network is about 5 minutes:
- If your accelerated domain name service region is global acceleration, the parameter cache configuration will take effect globally, and domestic and overseas differentiated configurations are not supported.
- The header cache configuration is in the process of being upgraded by entire network. If you click close, you will get an error, which may be caused by the upgrade. Contact Us Close the Backend Background configuration item.
Origin-pull Configuration
Intermediate Node Configuration

Last updated: 2020-03-03 15:07:22

An intermediate server is an origin-pull server located at the intermediate layer between a business server (i.e., origin server) and a CDN edge server (or GCD edge server in GCD scenarios). When a user initiates a request, the request will reach the CDN edge server first. If the edge server does not have the required resource, it will initiate a resource request to the intermediate server. If the intermediate server does not have the resource, it will initiate a resource request to the origin server.

To improve the acceleration result, starting on October 15, 2018, the intermediate server had been enabled for all newly connected domain names by default and cannot be manually disabled. After the intermediate source configuration was enabled by default, corresponding configuration item became hidden in the console.

Configuration Guide

Log in to the CDN Console and click Domain Management on the left sidebar to enter the management page. Find the domain name you want to edit and click Manage in the “Operation” column.

Click Origin-Pull Configuration and if you don't see the "Intermediate Server Configuration" module, an intermediate server has been enabled for your domain name by default. User requests will be converged to the intermediate server, which will perform origin-pulls in a unified manner, improving the CDN acceleration result and alleviating the access pressure on your origin server.

For legacy connected domain names, if you see that the intermediate server configuration is disabled in Origin-pull Configuration, we recommend you manually enable this feature to improve the acceleration result. Once enabled, this configuration item will be hidden and cannot be disabled.

Sample Case

- The user request will reach an edge server first. If the requested resource is missed on the edge server, the request will be forwarded to a parent node. If there is still a miss, the request will be forwarded to the origin server. The CDN
architecture is as shown below:

- The user request will reach an edge server first. If the requested resource is missed on the edge server, it will be pulled from the origin server directly. The CDN architecture is shown in the figure:
Range GETs Configuration

Last updated: 2020-01-20 09:39:04

- CDN supports Range GETs configuration, where Range is the HTTP request header used for the request of a specified part of a file. For example, `Range: bytes = 0-999` can be used to request the first 1,000 bytes of a file. Enabling Range GETs configuration can increase the delivery efficiency and response speed of large files.
- The origin server needs to support Range requests, or origin-pull will fail.
- When Range GETs configuration is enabled, resources will be cached in segments on the node, and these segments have the same cache expiration time and follow user-defined cache expiration rule.

Configuration Guide

1. Log in to the CDN Console and click **Domain Management** on the left sidebar to enter the management page. Find the desired domain name and click **Manage** in the "Operation" column.

2. Click **Origin Configuration** and you will see the **Range GETs Configuration** module. The feature is enabled by default.

Sample Case
If the Range GETs configuration of the www.test.com domain name is as follows:

When user A makes a request for the http://www.test.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 obtain and cache the resource by segments; if user B also makes a Range request at this time and the segments stored on the node match the specified byte segments in the Range request, the resource will be directly returned to the user without having to wait until all segments are obtained.

If the Range GETs configuration of the www.test.com domain name is as follows:

When user A makes a request for the http://www.test.com/test.apk resource, after the node receives the request and finds that the cached test.apk file has already expired, it will initiate an origin-pull request to directly obtain the entire resource from the origin server and then return it to the user.
Configuration Scenario

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 follow 301/302 redirect configuration is enabled, the CDN node will redirect to the specified address when receiving a 301/302 redirect request during origin-pull until it gets the required resource (through up to 3 follows) and then return the actual resource to the client. Thus, the client 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 enter its configuration page. You will find the Follow 301/302 Configuration section in the Origin Configuration tab. It is disabled by default.

Modifying configuration

Toggle the switch to enable or disable follow 301/302 redirect:

If your acceleration domain name is configured for global acceleration, the follow 301/302 redirect configuration will take effect globally. This configuration does not distinguish between requests from Mainland China and from outside Mainland China.
Configuration Sample

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

- **Follow 301/302 Configuration**

User A requests a resource http://cloud.tencent.com/1.jpg. If there were no cache hits in the node, the node will request it from the origin server. If the HTTP response status code returned by the origin server is 301/302, and the redirect address is http://cloud.tencent.com/1.jpg, then:

1. As 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. After getting the required resource, the node will cache it and return it to the user.
3. At this time, user B also sends a request for http://cloud.tencent.com/1.jpg, which will result in a cache hit on the node and the resource will be returned to the user.
4. When follow 301/302 redirect is enabled, up to 3 follows are allowed. When the limit is exceeded, the 301/302 status code will be returned to the user.

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

- **Follow 301/302 Configuration**

User A requests a resource http://cloud.tencent.com/1.jpg. If there were no cache hits in the node, the node will request it from the origin server. If the HTTP response status code returned by the origin server is 301/302, and the redirect address is http://xxx.tencent.com/1.jpg, then:

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

Configure the scene

When Tencent Cloud CDN returns user real server, by default, the TCP connection timeout is 5 seconds, and the Origin-pull load data timeout is 10 seconds. If Origin-pull exceeds the above time setting, Origin-pull will often fail.

You can adjust Origin-pull 's TCP connection timeout and Origin-pull 's loading data timeout according to real server's data processing and network conditions to ensure normal Origin-pull.

Configuration Guid

View Settings

Login [CDN console] Select “Domain name Management” in the menu bar, and click “manage” on the right side of the domain name to enter the domain name configuration page. Origin-pull timeout configuration can be seen in “Origin-pull configuration”. By default:

- The TCP connection timeout is 5 seconds.
- The loading timeout of Origin-pull is 10 seconds.

Change Settings

You can modify the corresponding timeout as needed by clicking "Edit" on the right:

- The TCP connection timeout can be set to 5-60 seconds.
- Origin-pull load timeout can be set to 5-60 seconds.

If your accelerated domain name service region is global acceleration, the Origin-pull timeout set takes effect globally, and domestic and overseas differentiated configurations are not supported.
If you want to configure an existing certificate for your domain name, please understand the following first. If you configure a certificate from the management of Tencent Cloud and SSL Certificates Service, you can skip this step.

Upload certificate

The certificates provided by CA institutions generally include the following, among which CDN uses Nginx:

Enter the Nginx folder, open the ".crt" (certificate) file and the ".key" (private key) file using a text editor, and you can see the certificate and private key contents in PEM format.

Certificate

The certificate extension is generally ".pem", ".crt" or ".cer". Open the certificate file in a text editor and you can see the certificate contents in a format similar to the following figure.

Certificate PEM format: begins with "- BEGIN CERTIFICATE-" and ends with "- END CERTIFICATE-". The middle content is 64 characters per line, and the last line can be less than 64 characters long:

If the certificate is issued by an intermediate CA institution, the certificate file you get contains multiple certificates, and you need to artificially upload the server certificate with the intermediate certificate. The stitching rule is: the server certificate is the first, the intermediate certificate is the second, and there is no blank line in the middle. In general, the organization will have a corresponding description when issuing the certificate, please refer to the rule description.

- There can be no blank lines between certificates
• Each certificate is in PEM format

The format of the certificate chain issued by the intermediate institution is as follows:

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

**Private Key**

The private key extension is generally ".pem" or ".key". Open the private key file in a text editor and you can see the contents of the private key in a format similar to the following figure.

Private key PEM format: begins with "- BEGIN RSA PRIVATE KEY-" and ends with "- END RSA PRIVATE KEY-". The middle content is 64 characters per line, and the last line can be less than 64 characters long.

If you get a private key that starts with "- BEGIN PRIVATE KEY-" and ends with "- END PRIVATE KEY-", it is recommended that you convert it through the openssl tool, as follows:

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

**Format conversion**

Currently, CDN only supports certificates in PEM format. Certificates in other formats need to be converted to PEM format. It is recommended to convert them through openssl tool. Here are several popular ways to convert certificate format to PEM format.

**Convert DER to PEM**
The DER format generally appears on the Java platform.
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
```

Convert P7B to PEM
The P7B format generally appears in Windows Server and tomcat.
Certificate conversion:

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

Open outcertificate.cer with a text editor to view the certificate contents in PEM format.
Private key conversion: the private key is generally available in the IIS server, Export.

Convert PFX to PEM
The PFX format generally appears in 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
```

Certificate chain completion
During configuration with your own certificate, there may be The certificate chain cannot be made up. The situation.
You can complete the certificate chain by pasting the contents of the CA certificate (in PEM format) at the end of the domain name certificate (PEM format). You can also submit Ticket to contact us.

Escrow certificate
Tencent Cloud provides certificate hosting products, that is, SSL Certificate Existing certificates can be uploaded to SSL Certificates Service management platform for unified hosting and deployed to other Tencent Cloud services, and certificates can also be purchased and applied.

Tencent Cloud SSL Certificates Service provides 20 copies of DV SSL Certificates Service issued by TrustAsia for each user free of charge.
Configure the scene

Tencent Cloud CDN supports HTTPS acceleration service, which can be deployed by uploading certificates or directly deploying certificates that have been hosted to Tencent Cloud and SSL Certificates Service to the CDN platform to enable HTTPS acceleration service to achieve encrypted transmission of entire network data.

Configuration Guid

**View Settings**

Login CDN console Select "Domain name Management" in the menu bar, and click "manage" on the right side of the domain name to enter "Advanced configuration" in the last column of the domain name configuration page to view the HTTPS configuration of the specified domain name:

You can also go to the Certificate Management page in the left menu bar to view the list of all domain names configured with HTTPS acceleration under the account:

**Domain name configuration**

1. **Select a domain**

   Under the Certificate Management menu bar, click configure Certificate, and select the accelerated domain name for which you want to configure the certificate:

   - The status of accelerated domain name needs to be "deployed" or "Launch". Accelerated domain name with disabled status cannot be configured for HTTPS acceleration.
   - `.file.myqcloud.com` The suffix is Tencent Cloud Cloud Object Storage default acceleration domain name, and HTTPS acceleration can be performed directly without the need to configure a certificate.
   - `.image.myqcloud.com` The suffix domain name is the default accelerated domain name of Tencent Cloud data Vientiane, and you can perform HTTPS acceleration directly without configuring a certificate.

2. **Select a certificate**

   If you already have a certificate, you can directly paste the certificate content and private key in PEM format into the corresponding location:

   - Tencent Cloud CDN now supports ECC certificate deployment.
   - The content of the certificate needs to be in PEM format. For certificates other than this format, please refer to PEM format conversion.
   - You can choose Tencent Cloud hosting certificate to deploy directly with one click.

3. **Origin-Pull Mode**

   In addition to the Origin-pull configuration when connecting the accelerated domain name or real server configuration module, you can also adjust Origin-pull and Protocol when configuring certificates. Tencent Cloud CDN supports the following three types of Origin-pull and Protocol:
HTTP Origin-pull: all requests use HTTP Origin-pull.
HTTPS Origin-pull: all requests use HTTPS Origin-pull.
Protocol follows: according to the request Protocol to Origin-pull, HTTPS request to use HTTPS Origin-pull, HTTP request to use HTTP Origin-pull.

Batch configuration

Click batch configuration above to automatically match the appropriate domain name by uploading the certificate for batch configuration:

1. Select a certificate

If you already have a certificate, you can directly paste the certificate content and private key in PEM format into the corresponding location:

- Tencent Cloud CDN now supports ECC certificate deployment.
- The content of the certificate needs to be in PEM format. For certificates other than this format, please refer to PEM format conversion.
- You can choose Tencent Cloud hosting certificate to deploy directly with one click.

2. Select a domain

According to the uploaded / selected certificate, CDN automatically matches the list of domain names that are allowed to be configured. You can check the configuration as needed:

3. Origin-Pull Mode

In addition to the Origin-pull configuration when connecting the accelerated domain name or real server configuration module, you can also adjust the batch Origin-pull and Protocol when configuring certificates in batches. Tencent Cloud CDN supports the following three types of Origin-pull and Protocol:

- HTTP Origin-pull: all requests use HTTP Origin-pull.
- HTTPS Origin-pull: all requests use HTTPS Origin-pull.
- Protocol follows: according to the request Protocol to Origin-pull, HTTPS request to use HTTPS Origin-pull, HTTP request to use HTTP Origin-pull

After the batch configuration is submitted, the selected domain names will be deployed for certificates one by one. If an exception occurs, the list page will display the status of "update failed". At this time, the original configuration will continue to take effect.

If the update fails, click "Edit" on the right to reconfigure it.

Change certificate
Certificate modification

Click "Edit" on the right side of the certificate to specify the domain name to update the certificate, or reconfigure it in batch to overwrite the original certificate configuration.

The updated certificate entire network takes effect node by node and switches seamlessly without affecting the existing network HTTPS service. You can also click "Delete" to cancel the HTTPS acceleration service.

The certificate has expired

Tencent Cloud will send expiration reminders to user accounts in the form of text messages, e-mails and internal message 30 days, 15 days, 7 days before Expire and the day of Expire. SSL Certificates Service's custom alarm receiver is now supported. You can enter the Message subscription Configure.

Regional special configuration

If the accelerated domain name service region is global, the configured HTTPS certificate will be valid both inside and outside China, and the configuration of different certificates within and outside China is not supported for the time being.

If there is a special scenario in which the configuration of domestic and overseas certificates for a domain name is inconsistent, you can see signs within and outside China on the "Certificate Management" page, indicating that there are regional special configurations left over from the domain name:

In the domain name "Advanced configuration", you can also see two configurations:

If you have such a special configuration for your accelerated domain name and you need to change one of the certificates, please Submit a ticket Make changes.
HTTPS forced Redirect

Configure the scene

Tencent Cloud CDN supports configuring HTTPS to force Redirect. A domain name with a certificate for HTTPS acceleration can be configured. You can specify 301 CDN 302 Redirect method to forcibly jump all HTTP requests arriving at the CDN node to HTTPS.

Configuration Guid

View Settings

Login CDN console Select "Domain name Management" in the menu bar, and click "manage" on the right side of the domain name to enter "Advanced configuration" in the last column of the domain name configuration page. For the domain name that has been configured with HTTPS certificate, you can see the "Force Redirect" switch. By default, the forced jump is turned off.

Change Settings

You can click [Edit] on the right to switch between 301 and Redirect, or you can configure and close it directly through the switch.

If the service region of the domain name is global, the configured HTTPS forced jump transfer takes effect globally, and domestic and overseas configurations are not supported.
HTTP2.0 configuration

Configure the scene

If you have configured a certificate to enable HTTPS acceleration of the domain name, you can enable HTTP2.0 Protocol support by yourself.

Currently, only HTTP2.0 Access is supported, but HTTP2.0 Protocol and Origin-pull are not supported for the time being.

Configuration Guid

View Settings

Login CDN console Select Domain name Management in the menu bar, and click manage on the right side of the domain name to enter Advanced configuration in the last column of the domain name configuration page. You can see HTTP2.0 configuration, which is enabled by default.

Change Settings

You can turn the HTTP2.0 configuration on or off by clicking the switch. After the certificate configuration is deleted, the HTTP2.0 configuration will fail synchronously.

If the service region of the domain name is global, the configured HTTP2.0 will take effect globally, and domestic and overseas configurations are not supported.
OCSP binding configuration

Configure the scene

Enable the OCSP Stapling server to send cached OCSP query results to the client during the TLS handshake for user verification without having to let the client send a request to the CA itself. OCSP bookbinding greatly improves the efficiency of TLS handshake and saves user verification time.

Tencent Cloud CDN supports self-help to enable or disable OCSP Stapling configuration.

Configuration Guid

View Settings

Login CDN console Select "Domain name Management" in the menu bar, and click "manage" on the right side of the domain name to enter "Advanced configuration" in the last column of the domain name configuration page. You can see "OCSP binding configuration", which is turned off by default.

Change Settings

For a domain name configured with HTTPS acceleration, you can turn on or off the OCSP binding configuration directly by clicking the switch. After deleting the certificate configuration, the OCSP binding configuration will fail synchronously.

If the service region of the domain name is global, the configured OCSP binding will take effect globally, and domestic and overseas configurations are not supported.
Advanced Configuration
Bandwidth Limit Configuration

You can configure a bandwidth cap for a domain name. When the bandwidth consumed by the domain name exceeds the max bandwidth configured within a statistical cycle (5 minutes), all access requests will be forwarded to the origin server or the CDN service will be disabled, and a 404 error will be returned for all access requests.

Configuration Guide

1. Log in to the CDN Console, select Domain Management on the left sidebar, and click “Manage” on the right of the domain name to be edited.

2. Click the Advanced Configuration tab to see the Bandwidth Cap Configuration module. This feature is disabled by default.

3. Toggle the switch on to enable it. When enabled, the bandwidth cap is 10 Gbps by default. If the cap is reached, requests will be forwarded to the origin server. You can click the Edit icon to set the bandwidth cap and how user requests will be handled if the cap is exceeded.

- If your purpose is to prevent DDoS attacks, we recommend selecting “Return 404” to protect your origin server.
- If your purpose is to control CDN service fees, we recommend selecting “Forward to origin server” to prevent your service from being affected.
4. If the cap is exceeded, you will be notified by email, SMS or through the Message Center. You can check the domain status in the CDN Console. No matter if you select "Forward to origin server" or "Return 404", the domain will be changed to Disabled status. It takes about 5 to 15 minutes for the settings to take effect.

The domain will be closed once the bandwidth cap is reached. To continue using the CDN service, you can activate domain name acceleration again in the CDN Console. For more information, see Domain Name Operations.

Sample Case

If the domain name www.test.com is configured as follows:

CDN will periodically detect the latest bandwidth statistics of the domain name. If it finds at 12:15:00 that the bandwidth value of the domain name at the time point of 12:05:00 (representing the data generated between 12:05:00 and 12:10:00) is above 1 Kbps which exceeds the set cap, it will immediately start to deliver the configuration to forward requests to the origin server. As the configuration is delivered to all CDN nodes in batches and takes effect node by node, the bandwidth will drop gradually and the configuration will take full effect on all nodes at around 12:20:00.
Customize response header configuration

Configure the scene

When your users request business resources, you can use the returned **Response message** Add the header you configured to achieve cross-domain Access and other purposes.

Since the HTTP Header configuration is for the domain name, once the configuration takes effect, the configured header will be added to the user's response message to any resource under the domain name. Configuring HTTP Header only affects the response behavior of clients, such as browsers, and does not affect the caching behavior of CDN nodes.

Configuration Guid

**View Settings**

Login [CDN console](https://cloud.tencent.com/document/product/427) Select **Domain name Management** in the menu bar, and click **manage** on the right side of the domain name to enter the domain name configuration page. You can see the HTTP Header configuration in **Advanced configuration**, which is disabled by default:

![HTTP Header Configuration](https://cloud.tencent.com/document/product/427/12870)

**Change Settings**

1. Change Settings

Click the switch to add HTTP Header header settings. You can specify the following header configurations or custom headers:

- **Access-Control-Allow-Origin**: specifies the request source of Access resources when making cross-domain requests.
- **Access-Control-Allow-Methods**: specifies the cross-domain request method that is allowed when a cross-domain request is made.
- **Access-Control-Max-Age**: specifies the cache time for pre-requests for specific resources to return results when cross-domain requests are made.
- **Access-Control-Expose-Headers**: specifies a collection of headers visible to the client when a cross-domain request occurs.
- **Content-Disposition**: activates the client to download resources and sets the default file name.
- **Content-Language**: is used to define the language code used by the page.
- **Custom**: custom header.
Common configuration: Content-Disposition
Content-Disposition is used to activate the download of the browser, and you can set the default download file name. When the server sends a file to the client browser, if it is a file type supported by the browser, such as TXT, JPG and other types, it will be opened directly using the browser by default. If you need to prompt the user to save, you can override the browser default behavior by configuring the Content-Disposition field. Common configurations are as follows:

```
Content-Disposition: attachment; filename=FileName.txt
```

Common configuration: Content-Language
Content-Language is the language code used to define the page. Common configurations are as follows:

```
Content-Language: zh-CN
Content-Language: en-US
```

Cross-domain configuration: Access-Control-Allow-Origin
Cross-domain refers to a domain name, such as `www.abc.com`. Under a resource, to another domain name `www.def.com`. When a request is initiated by a resource under the, it appears because the domain name to which the resource belongs is different. Cross domain Different Protocol and different ports will cause the emergence of cross-domain Access. At this point, the cross-domain configuration must be added to the Response Header in order for the former to get the data successfully.

- Function introduction:

  Access-Control-Allow-Origin is used to solve the cross-domain Permission problem of resources. The domain value defines the domain that allows Access this resource. A maximum of 10 domains can be configured. If the source request Host is in the domain name configuration list, the corresponding value is directly filled in the return header. You can also set wildcards. " * Allowed to be requested by all domains

- Introduction of matching pattern
<table>
<thead>
<tr>
<th>Match Mode</th>
<th>Domain value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full match</td>
<td>*</td>
<td>When set to, the header is added in response: <code>Access-Control-Allow-Origin:</code></td>
</tr>
<tr>
<td>Second-level pan-domain name matching</td>
<td>http://*.tencent.com</td>
<td>Source <a href="http://cloud.tencent.com">http://cloud.tencent.com</a> If the list is hit, the header is added in response: <code>Access-Control-Allow-Origin: https://cloud.tencent.com</code> The source is <a href="https://cloud.qq.com">https://cloud.qq.com</a> The list has not been hit, and the response has not changed.</td>
</tr>
<tr>
<td>Port matching <a href="https://cloud.tencent.com:8080">https://cloud.tencent.com:8080</a></td>
<td>The source is <a href="https://cloud.tencent.com:8080">https://cloud.tencent.com:8080</a> If the list is hit, the header is added in response: <code>Access-Control-Allow-Origin:https://cloud.tencent.com:8080</code> The source is <a href="https://cloud.tencent.com">https://cloud.tencent.com</a> The list has not been hit, and the response has not changed.</td>
<td></td>
</tr>
</tbody>
</table>

If there is a special port, you need to have relevant information about Enter in the list. Any port matching is not supported and must be specified.

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

Access-Control-Allow-Methods is used to set cross-domain allowed HTTP request methods. Multiple methods can be set at the same time, as follows:
Access-Control-Allow-Methods: POST, GET, OPTIONS

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

Access-Control-Max-Age is used to specify the validity time of the pre-request.

For a non-simple cross-domain request, you need to add a HTTP query request, called "pre-request", before formal
communication, to find out whether the cross-domain request is secure and acceptable. The following request will be regarded as a non-simple cross-domain request:

- Initiated in a way other than GET, HEAD, or POST, or using POST, but the request data type is a data type other than application / x-www-form-urlencoded, multipart / form-data, text / plain, such as application / xml or text / xml.
- Use custom request headers.
  - Access-Control-Max-Age is in seconds. Examples of settings are as follows:
    - Access-Control-Max-Age: 1728000

Indicates that within 1728000 seconds (20 days), the cross-domain Access of the resource will not send another pre-request.

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

Access-Control-Expose-Headers is used to specify which headers can be given to the client as part of the response, Open. By default, only 6 headers can be given to the client by Open:

- Cache-Control
- Content-Language
- Content-Type
- Expires
- Last-Modified
-Pragma

If you want the client Access to have other header information, you can set it as follows. When you enter multiple headers, you need to separate them with ",".

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

Indicates that the client can get the header information from Access to Content-Length and X-My-Header.

**Custom header**

You can add custom Header, custom key-value settings:
The following Header additions are not supported:

- Date
- Expires
- Content-Type
- Content-Encoding
- Content-Length
- Transfer-Encoding
- Cache-Control
- If-Modified-Since
- Last-Modified
- Connection
- Content-Range
- ETag
- Accept-Ranges
- Age
- Authentication-Info
When multiple Header are added repeatedly, the bottom priority is higher than the top priority, which is directly covered by the bottom configuration.

2. Turn off configuration

You can configure the switch through HTTP Header and close the configuration with one button. When the switch is off, even if there is an existing configuration below, it will not take effect on the current network:

If the accelerated domain name service region is global, response header configuration will take effect globally, and inconsistent configurations between domestic and overseas configurations are not supported.
SEO optimized configuration

Configure the scene

The optimized configuration of SEO is a function to solve the problem that the weight of search results of a domain name is affected by frequent changes in IP by CDN after the domain name is connected to CDN. By identifying whether Access IP belongs to a search engine, users can choose direct Origin-pull Access resources to ensure the stability of search engine weights.

- As the search engine IP updates more frequently, Tencent Cloud CDN can only ensure that it can identify the vast majority of search engine IP.
- The optimized configuration function of SEO is only when the domain name access method is **Own source** Can be used when. When the SEO optimized configuration feature is enabled, if the domain name has multiple real server addresses, the default Origin-pull address is the first real server address added.

Configuration Guid

**View Settings**

Login [CDN console](#) Select “Domain name Management” in the menu bar, and click "manage" on the right side of the domain name to enter the domain name configuration page. You can see the optimized configuration of SEO in "Advanced configuration". It is disabled by default.

**Change Settings**

You can use the SEO optimized configuration switch to turn the service on or off by yourself.

If the acceleration region of the domain name is global, the optimized configuration of SEO will take effect globally, and inconsistent configurations between domestic and overseas configurations are not supported.
Intelligent compression configuration

Configure the scene

Through intelligent compression configuration, CDN will compress resources with GZIP and Brotil according to the set rules when returning content, effectively reducing the size of transmitted content and saving overhead.

- When a new resource is requested for the first time, because the CDN node does not have this resource, Origin-pull will be requested. The uncompressed version will be returned (real server is not compressed), and the node compressed version will be returned for subsequent requests.
- At present, intelligent compression only supports static acceleration and download acceleration.

Configuration Guid

View Settings

Login CDN console Select "Domain name Management" in the menu bar, and click "manage" on the right side of the domain name to enter the domain name configuration page. You can see the intelligent compression configuration in "Advanced configuration":

- When an accelerated domain name is connected, it defaults to the suffixes .js, .html, .css, .xml, .json, .shtml, .htm, and enables Gzip compression for resources within the 256Byte-2048KB range.

Change Settings

You can click "Edit" on the right to specify the compressed file suffix and file range.

Instruction

- GZIP supports compression in the range of 0MB-30MB.
- The Brotil compression feature is being upgraded and cannot be enabled for the time being.

If the acceleration region of the domain name is global, the intelligent compression configuration will take effect globally when enabled, and inconsistent configurations between domestic and overseas configurations are not supported.
HTTPS Configuration

Last updated : 2020-02-24 10:48:22

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 a certificate for the domain name and deploy it on all CDN nodes to implement encrypted data transfer across the network.

- After CDN acceleration is enabled for COS Or Cloud Image, default domain names .file.myqcloud.com And .image.myqcloud.com Directly support HTTPS with no need to configure the certificate.
- Tencent Cloud CDN's support for HTTP 2.0 protocol is in beta test and can be used directly once enabled.

Configuration Guide

Tencent Cloud CDN supports two certificate deployment methods:

- Self-owned certificate: Upload your own certificate and private key to CDN for deployment. Transfer is encrypted throughout the process to ensure the security of your certificate.
- Tencent Cloud-hosted certificate: You can go to Certificate Management To host your existing certificate in Tencent Cloud for use by multiple Tencent Cloud products. You can also apply for a third-party certificate provided by TrustAsia free of charge through this platform and deploy it directly to CDN.

1. Log in to the CDN Console And click Domain Name Management On the left sidebar to enter the management page. Find the domain name you want to edit and click Manage In the "Operation" column.

2. Click Advanced Configuration And find HTTPS Configuration . Click Configure Now To enter the Certificate Management Page where you can configure a certificate. For the configuration process, please see Certificate Management.

3. After the certificate is Successfully configured , the Forced HTTPS Redirect Switch will appear, which is disabled by default.
4. After enabling **Forced HTTPS Redirect**, even if the user initiates an HTTP request, it will be redirected to HTTPS for access. The redirect method is 302 redirect by default.

You can click **Edit** to modify the redirect method:

![Edit button](image)

### HTTP2.0 Configuration
After successfully configuring the HTTPS certificate for the domain name, you can enable HTTP 2.0.

OCSP stapling configuration

Feature Description
OCSP stapling is a TLS certificate status query extension. An OCSP stapling server can send the cached OCSP query result to the client during TLS handshake for verification by the user without having the client send the request to the CA. OCSP stapling greatly improves the efficiency of TLS handshake and reduces user verification time.

After successfully configuring the HTTPS certificate for the domain name, you can enable OCSP stapling.

Algorithms supported by HTTPS origin-pull

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

<table>
<thead>
<tr>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDHE-RSA-AES256-SHA</td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-SHA384</td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-GCM-SHA384</td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-SHA</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES256-SHA</td>
</tr>
<tr>
<td>SRP-AES-256-CBC-SHA</td>
</tr>
<tr>
<td>DH-RSA-AES256-SHA</td>
</tr>
<tr>
<td>DH-DSS-AES256-SHA</td>
</tr>
<tr>
<td>DHE-RSA-AES256-SHA</td>
</tr>
<tr>
<td>DHE-DSS-AES256-SHA</td>
</tr>
<tr>
<td>CAMELLIA256-SHA</td>
</tr>
<tr>
<td>PSK-3DES-EDE-CBC-SHA</td>
</tr>
<tr>
<td>ECDH-RSA-AES256-SHA</td>
</tr>
<tr>
<td>ECDH-ECDSA-AES256-SHA</td>
</tr>
<tr>
<td>AES256-SHA</td>
</tr>
<tr>
<td>ECDHE-RSA-AES128-SHA</td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES128-SHA</td>
</tr>
<tr>
<td>SRP-AES-128-CBC-SHA</td>
</tr>
<tr>
<td>DH-RSA-AES128-SHA</td>
</tr>
<tr>
<td>DH-DSS-AES128-SHA</td>
</tr>
<tr>
<td>DHE-RSA-AES128-SHA</td>
</tr>
<tr>
<td>DHE-DSS-AES128-SHA</td>
</tr>
<tr>
<td>Key Exchange Algorithm</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-SHA</td>
</tr>
<tr>
<td>ECDH-RSA-AES128-SHA</td>
</tr>
<tr>
<td>ECDH-ECDSA-AES128-SHA</td>
</tr>
<tr>
<td>CAMELLIA128-SHA</td>
</tr>
<tr>
<td>PSK-RC4-SHA</td>
</tr>
<tr>
<td>AES128-SHA</td>
</tr>
<tr>
<td>SEED-SHA</td>
</tr>
<tr>
<td>DES-CBC3-SHA</td>
</tr>
<tr>
<td>IDEA-CBC-SHA</td>
</tr>
<tr>
<td>EDH-RSA-DES-CBC3-SHA</td>
</tr>
<tr>
<td>EDH-DSS-DES-CBC3-SHA</td>
</tr>
<tr>
<td>RC4-SHA</td>
</tr>
<tr>
<td>RC4-MD5</td>
</tr>
<tr>
<td>SRP-3DES-EDE-CBC-SHA</td>
</tr>
<tr>
<td>DH-DSS-DES-CBC3-SHA</td>
</tr>
</tbody>
</table>
SEO Optimization

Last updated : 2020-01-19 16:34:36

SEO optimization configuration is a feature that solves the problem with incorrect weights of domain name search results 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 weight.

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.

Configuration Guide

1. Log in to the CDN Console and click Domain Management on the left sidebar to enter the management page. Find the desired domain name and click Manage in the “Operation” column.

2. Click Advanced Configuration and you can see the SEO Optimization module. Automatic origin-pull for search engine is disabled by default.

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.
### Advanced Configuration

#### 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 mins) exceeds the set limit.

<table>
<thead>
<tr>
<th>Bandwidth Cap</th>
<th>Max Bandwidth and overlimit process: 10Gbps</th>
<th>Return 404</th>
</tr>
</thead>
</table>

#### 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>
</tr>
</thead>
<tbody>
<tr>
<td>Tencent Cloud Certificate</td>
<td>2020-10-22</td>
<td>HTTPOrigin-Pull</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>HTTP2.0</th>
<th></th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>OCSP Stapling</th>
<th></th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>Pull Source for Search Engine</th>
<th></th>
</tr>
</thead>
</table>
Feature Overview

Contents distributed by CDN are public resources by default. To prevent malicious users from stealing your contents for profits, CDN supports the configuration of URL authentication.

Algorithm Description

**Type A**

- 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 to 100 uppercase or lowercase letters and digits.
  - uid: 0.
  - md5hash: MD5 (file path-timestamp-rand-uid-custom key).

If the original request URL is `http://www.test.com/test/1.jpg`, then the file path used for MD5 calculation will be `/test/1.jpg`.

**Type B**

- 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).

If the original request URL is `http://www.test.com/test/1.jpg`, then the file path used for MD5 calculation will be `/test/1.jpg`.

**Type C**

- Access URL format: `http://DomainName/md5hash/timestamp/FileName`
- Algorithm Description:
  - timestamp: A hex timestamp in UNIX format.
  - md5hash: MD5 (custom key + file path + timestamp).

If the original request URL is `http://www.test.com/test/1.jpg`, then the file path used for MD5 calculation will be `/test/1.jpg`.
**TypeDef**

- 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).

If the original request URL is `http://www.test.com/test/1.jpg`, then the file path used for MD5 calculation will be `/test/1.jpg`.

**Configuration Guide**

1. Log in to the CDN Console and click **Domain Management** on the left sidebar to enter the management page. Find the desired domain name and click **Manage** in the "Operation" column.

2. Click **Security Configuration** and you can see the **Authentication Configuration** module, which is disabled by default.

3. In the **Authentication Configuration** module, click **Configuration** to enable authentication. Currently, three types can be configured:

   Currently, TypeB cannot be selected due to feature upgrade.
4. After selecting the type, you can configure authentication parameters. The following takes **TypeA** as an example:

- **Authentication Key**: Select a specified string as the authentication key based on your business conditions.
- **Signature Parameter**: Set a parameter name with a signature string. The value is **sign** by default and can be customized.
- **Effective Time**: The server compares the **timestamp** (obtained by parsing the signature) plus the effective time with the current time to determine whether the signature is effective.
5. After parameter configuration is completed, specify the authentication range and object.

![Authentication Configuration](image)

**Authentication Calculator**

You can use the authentication calculator to check whether the request path and signature are correct.

In the **Authentication Configuration** module, click *Configuration.* Currently, three types can be configured. Select the type, configure the authentication parameters, and then determine the authentication URL. The following takes
TypeA as an example:

Currently, TypeB cannot be selected due to feature upgrade.
If the access path has a URL with Chinese characters, you need to decode the URL first before performing the authentication configuration.
Configure HTTP Header

Tencent Cloud provides HTTP Header Configuration which allows such features as cross-domain access by adding configured header field in the returned Response message When your user requests for service resource.

If resource is not hit at a node, the request will go back to origin. In this case, the header information returned from origin server will be returned to user altogether; If resource is hit in the cache at a node, CDN will return cached Access-Control-Allow-Origin, Timing-Allow-Origin, Content-Disposition and Accept-Ranges header information of the origin server to the user by default. If you wish to cache all of headers from origin, please submit a ticket and request for manual configuration support;

Since the HTTP Header configuration is for the domain name, once the configuration takes effect, the configured header will be added to the user's response message to any resource under the domain name. Configuring HTTP Header only affects the response behavior of clients, such as browsers, and does not affect the caching behavior of CDN nodes.

Configuration Guide

1. Log in to the CDN Console And click Domain Name Management On the left sidebar to enter the management page. Find the domain name you want to edit and click Manage In the "Operation" column.

2. Find it in [Advanced configuration] HTTP Header configuration Module. By default, HTTP Header configuration is closed.

3. Click to open HTTP Header Switch to add headers:

   CDN provides the following six common types of header settings, as well as custom header settings:

   Access-Control-Allow-Origin: Specify the request origins allowed to access the resource for a cross-domain request;
   - Access-Control-Allow-Methods: specifies the cross-domain request method that is allowed when a cross-domain request is made.
   - Access-Control-Max-Age: Specify the maximum time span during which the returned result of pre-request for a particular resource is cached for a cross-domain request.
   - Access-Control-Expose-Headers: Specify the header information allowed for access for a cross-domain request;
   - Content-Disposition: activates the client to download resources and sets the default file name.
   - Content-Language: is used to define the language code used by the page.
   - Custom: custom header.

4. Suppose the configuration content is: Access-Control-Allow-Origin, sets wildcards *. After confirming the submission, the switch is on, and the configuration information that is in effect is displayed below. Click "modify" to change the configuration information. Click "Delete" to delete the configuration.

5. Close HTTP Header After the switch, the configuration information below is invalid, that is, the HTTP Header configuration is not enabled. It can be opened manually again.

General Configurations

Content-Disposition

Content-Disposition is used to activate the download of the browser, and you can set the default download file name. When the server sends a file to the client browser, if it is a file type supported by the browser, such as TXT, JPG and other types, it will be opened directly using the browser by default. If you need to prompt the user to save, you can override the browser default behavior by configuring the Content-Disposition field. Common configurations are as
follows:
'Content-Disposition': 'attachment; filename=' filename.jpg',

**Content-Language**

Content-Language is used to define the language code used in the page. Common configurations are shown below:

'Content-Language': 'zh-cn',

*Content-Language*: en-US

**Cross-domain Configurations**

Cross-domain refers to a domain name, such as www.abc.com Under a resource, to another domain name www.def.com When a request is initiated by a resource under the, it appears because the domain name to which the resource belongs is different. Cross domain Different Protocol and different ports will cause the emergence of cross-domain Access. At this point, the cross-domain configuration must be added to the Response Header in order for the former to get the data successfully.

**Access-Control-Allow-Origin**

**Features**

Access-Control-Allow-Origin is used to solve the cross-domain Permission problem of resources. The domain value defines the domain that allows Access for the resource. If the source request Host is in the domain name configuration list, the corresponding value is directly filled in the return header. You can also set wildcards * Allowed to be requested by all domains

Support up to 10 domain name configurations, one line, each separated by carriage return.

- Introduction of matching pattern

<table>
<thead>
<tr>
<th>Match Mode</th>
<th>Domain value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full match</td>
<td>*</td>
<td>Set to * Then return to response-header to add the header: Access-Control-Allow-Origins, and the value is: * .</td>
</tr>
</tbody>
</table>
| Fixed matching           | http://www.test.com  
                          | https://www.test.com  
                          | http://www.b.com        | If the source is https://www.test.com If it is hit in the list, the header “Access-Control-Allow-Origins,” is added to the response-header and the value is: https://www.test.com .  
If the source is https://www.b.com , which is not hit in the list, so there is no need to add the header: Access-Control-Allow-Origins to the return response-header. |
| Second-level pan-domain name matching | http://*.test.com | If the source is http://www.test.com If the match is made, the header: Access-Control-Allow-Origins, will be added to the response-header and the value is: http://www.test.com  .  
If the source is https://www.test.com Does not match, so there is no need to add the header: Access-Control-Allow-Origins to the returned response-header. |
<table>
<thead>
<tr>
<th>Match Mode</th>
<th>Domain value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port matching</td>
<td><a href="https://www.test.com:8080">https://www.test.com:8080</a></td>
<td>If the source is <a href="https://www.test.com:8080">https://www.test.com:8080</a>. If the match is made, the header: Access-Control-Allow-Origins, will be added to the response-header and the value is: <a href="https://www.test.com:8080">https://www.test.com:8080</a>. If the source is <a href="https://www.test.com">https://www.test.com</a>. Does not match, so there is no need to add the header: Access-Control-Allow-Origins to the returned response-header.</td>
</tr>
</tbody>
</table>

If there is a special port, you need to have relevant information about Enter in the list. Any port matching is not supported and must be specified.

**Access-Control-Allow-Methods**
Access-Control-Allow-Methods is used to set cross-domain allowed HTTP request methods. Multiple methods can be set at the same time, as follows:

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

**Access-Control-Max-Age**
Access-Control-Max-Age specifies the valid time of pre-request.
For a non-simple cross-domain request, you need to add a HTTP query request, called "pre-request", before formal communication, to find out whether the cross-domain request is secure and acceptable. The following request will be regarded as a non-simple cross-domain request:

- The request is initiated using a method other than GET, HEAD or POST or it is initiated 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 second. Here is a configuration example:

Access-Control-Max-Age
This indicates no more pre-request will be sent for the cross-domain access to this resource within 1728000 seconds (20 days).

**Access-Control-Expose-Headers**
Access-Control-Expose-Headers is used to specify which headers can be given to the client as part of the response, Open. By default, only 6 headers can be given to the client by Open:

- Cache-Control
- Content-Language
- Content-Type
- Expires
- Last-Modified
- Pragma
If you want the client Access to get other header information, you can set it as follows. When you enter multiple headers, you need to use the , Separate.

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

Indicates that the client can get the header information from Access to Content-Length and X-My-Header.

**Custom header**

1. Support to add custom Header, users can select "Custom" in the parameter list.
2. Enter customizes the key-value value.

The following Header additions are not supported:

- Expires
- Content-Type
- Content-Encoding
- Content-Length:
- Transfer-Encoding
- Cache-Control
- If-Modified-Since

**Connection**
- Content-Range
- ETag
- Accept-Ranges
- Age
- Authentication-Info
- Proxy-Authenticate
- Retry-After
- Set-Cookie
- Vary
- WWW-Authenticate
- Content-Location
- Content-MD5
- Content-Range
- Meter
- Allow
- <Error>

When multiple Header are added repeatedly, the bottom priority is higher than the top priority, which is directly covered by the bottom configuration.
Permission Management
Permission's explanation on the console
Last updated : 2020-03-19 17:57:05

After specifying that Action and Resource create a custom policy, you can directly call API to operate on related resources. The mapping relationship between the console function point and Action is described below.

Tencent Cloud CDN authorized resource dimension is a domain name, which does not support Permission Assign within and outside the same domain name.

Service Overview

The service overview is divided into four modules according to the content displayed:

<table>
<thead>
<tr>
<th>Function module</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service usage display</td>
<td>DescribeCdnData</td>
<td>If only part of the domain name is authorized, you can only query the usage of each domain name independently.</td>
</tr>
<tr>
<td></td>
<td>DescribeBillingData</td>
<td></td>
</tr>
<tr>
<td>Domain name situation</td>
<td>DescribeDomains</td>
<td>Returns the total number of authorized domain names</td>
</tr>
<tr>
<td>Billing Details</td>
<td>DescribePayType</td>
<td>Changing the billing method of authorized sub-accounts is not supported for the time being.</td>
</tr>
<tr>
<td>Traffic's bag situation</td>
<td>DescribeTrafficPackages</td>
<td>Traffic's package is account-level data, and Associate can query any resources.</td>
</tr>
</tbody>
</table>

Domain Name Management

<table>
<thead>
<tr>
<th>Function module</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain name list and query</td>
<td>DescribeDomains</td>
<td>Query / display / download basic configuration of domain name Full detailed configuration requires authorized DescribeDomainsConfig</td>
</tr>
<tr>
<td>Add Domain Name</td>
<td>DescribeDomains</td>
<td>Domain names that can be added to any acceleration service area</td>
</tr>
<tr>
<td>Function module</td>
<td>Authorized Action</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Close the domain name</td>
<td>StopCdnDomain</td>
<td>-</td>
</tr>
<tr>
<td>Launch domain name</td>
<td>StartCdnDomain</td>
<td>-</td>
</tr>
<tr>
<td>Delete domain name</td>
<td>DeleteCdnDomain</td>
<td>-</td>
</tr>
<tr>
<td>Modify the project to which the domain name belongs</td>
<td>UpdateDomainConfig</td>
<td>The project to which the domain name belongs is part of the domain name configuration. All configurations of the domain name can be modified after authorization</td>
</tr>
<tr>
<td>Domain name configuration management</td>
<td>UpdateDomainConfig</td>
<td>After authorization, you can view / modify all configurations of the domain name.</td>
</tr>
</tbody>
</table>

**Certificate Management**

<table>
<thead>
<tr>
<th>Function module</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query the list of certificates</td>
<td>DescribeDomainsConfig</td>
<td>After authorization, you can view all the configurations of the domain name.</td>
</tr>
<tr>
<td>Configure a Certificate</td>
<td>UpdateDomainConfig</td>
<td>All configurations of the domain name can be modified after authorization</td>
</tr>
<tr>
<td>Batch configuration certificate</td>
<td>UpdateDomainsHttps</td>
<td>Used to configure certificates in bulk</td>
</tr>
</tbody>
</table>

**Statistical Analysis**
<table>
<thead>
<tr>
<th>Function module</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access data details query</td>
<td>DescribeCdnData</td>
<td>After authorization, you can query all Access data of the domain name Metric</td>
</tr>
<tr>
<td>Origin-pull data details query</td>
<td>DescribeOriginData</td>
<td>After authorization, you can query all Origin-pull data of the domain name Metric</td>
</tr>
<tr>
<td>Traffic / number of requests Top query</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain name Top ranking query</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain name status code ranking query</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inquiry on the ranking of consumption in domestic provinces</td>
<td>ListTopData</td>
<td>After authorization, you can query all kinds of data / dimension ranking.</td>
</tr>
<tr>
<td>Ranking of ISP consumption in China</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ranking of overseas regional usage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Independent IP number query</td>
<td>DescribeIpVisit</td>
<td>-</td>
</tr>
</tbody>
</table>

**Purge and Prefetch**

<table>
<thead>
<tr>
<th>Function module</th>
<th>Authorized Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Refresh submission</td>
<td>PurgeUrlsCache</td>
</tr>
<tr>
<td>Directory refresh submission</td>
<td>PurgePathCache</td>
</tr>
<tr>
<td>Query refresh record</td>
<td>DescribePurgeTasks</td>
</tr>
</tbody>
</table>
### Function module

<table>
<thead>
<tr>
<th>Function module</th>
<th>Authorized Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submitted by prefetch job</td>
<td>PushUrlsCache</td>
</tr>
<tr>
<td>Query prefetch's records</td>
<td>DescribePushTasks</td>
</tr>
</tbody>
</table>

### Cloud Log Service

<table>
<thead>
<tr>
<th>Function module</th>
<th>Authorized Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query log download link</td>
<td>DescribeCdnDomainLogs</td>
</tr>
</tbody>
</table>

### Entire network status monitoring

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

### Operation report

<table>
<thead>
<tr>
<th>Function module</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access data details query</td>
<td>DescribeCdnData</td>
<td>After authorization, you can query all Access data of the domain name Metric</td>
</tr>
<tr>
<td>Origin-pull data details query</td>
<td>DescribeOriginData</td>
<td>After authorization, you can query all Origin-pull data of the domain name Metric</td>
</tr>
</tbody>
</table>
### Traffic / number of requests Top query

<table>
<thead>
<tr>
<th>Function module</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic / number of requests Top query</td>
<td>ListTopData</td>
<td>After authorization, you can query all kinds of data / dimension ranking.</td>
</tr>
<tr>
<td>Domain name Top ranking query</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain name status code ranking query</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inquiry on the ranking of consumption in domestic provinces</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ranking of ISP consumption in China</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ranking of overseas regional usage</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Independent IP number query

<table>
<thead>
<tr>
<th>Function module</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independent IP number query</td>
<td>DescribelpVisit</td>
<td>-</td>
</tr>
</tbody>
</table>

### Traffic bag management

<table>
<thead>
<tr>
<th>Function module</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query the list of Traffic's bags.</td>
<td>DescribeTrafficPackages</td>
<td>The returned content of the API has nothing to do with Resource, and any resource authorized can be queried.</td>
</tr>
</tbody>
</table>

Traffic package renewal / stop renewal logic, authorization is not supported for the time being.

### IP attribution query
<table>
<thead>
<tr>
<th>Function module</th>
<th>Authorized Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query whether IP belongs to Tencent Cloud CDN</td>
<td>DescribeCdnIp</td>
<td>The returned content of the API has nothing to do with Resource, and any resource authorized can be queried.</td>
</tr>
</tbody>
</table>

**Self-diagnose tools**

Self-diagnose tool does not hold sub-accounts for authorization for the time being.
Policy creation

Last updated : 2020-03-19 17:57:05

To facilitate users to query and manage Permission with a more fine-grained configuration domain name, the CDN Permission strategy has been fully upgraded. Users can implement Permission and Assign at the domain name level through custom policy statements.

1. Login Access Management console Click the "Policy" menu to enter the policy management page, and click "Create Custom Policy":
2. Select [create by Policy Builder]:
3. Select "content Distribution Network" in the product check box, and select the set of features that need to be authorized. If Permission is authorized to read and write all of them, check "All" to select all services. The mapping relationship between features and console can be viewed. Action mapping table.
4. Fill in the domain name that needs to be authorized at the resource. * On behalf of all domain names, click add statement and click next to create a policy that can be authorized by Associate's existing users / user groups.
Project-level Permission explanation

Last updated: 2020-03-19 17:57:05

Policy creation

If you need to refine the authorization operations at the project level, such as data query, Purge and Prefetch, and domain name management operations to different sub-accounts, you can use the following steps to create a policy:

1. Login Access Management console Click the Policy of Directory on the left.

2. Click [Create Custom Policy], and then select [create by Features or project Permission]

3. Fill in the policy name as required, and check "content Distribution Network" in the service type below.

4. Open the action set that needs to be authorized and the Associate project (the default project cannot be authorized), and then associate with sub-users.

Resource level & project level

Currently, the operation sets are classified and the corresponding OPEN API2.0 and OPEN API3.0 APIs are shown below. Sub-users with the operation set Permission can call the 2.0 and 3.0 APIs in the list for any domain name in the Permission project:

<table>
<thead>
<tr>
<th>Permission assemble</th>
<th>API2.0</th>
<th>API3.0</th>
<th>Whether authorization is required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query consumption data and statistics</td>
<td>DescribeCdnHostInfo DescribeCdnHostDetailedInfo GetCdnStatusCode GetCdnStatTop GetCdnProvIspDetailStat</td>
<td>DescribeCdnData DescribeOriginData ListTopData DescribeIpVisit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Query domain name information</td>
<td>GetHostInfoById GetHostInfoByHost</td>
<td>DescribeDomains DescribeDomainsConfig</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Query CDN log download link</td>
<td>GenerateLogList GetCdnLogList</td>
<td>DescribeCdnDomainLogs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Add Domain Name</td>
<td>AddCdnHost</td>
<td>AddCdnDomain</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Permission assemble</td>
<td>API2.0</td>
<td>API3.0</td>
<td>Whether authorization is required</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------</td>
<td>--------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Activate / deactivate domain name</td>
<td>OnlineHost OfflineHost</td>
<td>StartCdnDomain StopCdnDomain</td>
<td>Yes</td>
</tr>
<tr>
<td>Delete 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>Service query</td>
<td>QueryCdnIp (no authorization required)</td>
<td>DescribeCdnIp</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Console Permission**

- View consumption data and statistics: if the policy enables "View consumption data and Statistics" and Associate project, you can view the following module information on the console:
  - Overview page: data display module only
  - Statistical analysis: real-time monitoring
  - Statistical analysis: data analysis
  - Entire network data monitoring
- Query domain name information: if the policy enables "query Domain name Information" and Associate project, view the list of domain names and detailed configuration information in Permission's project on the "Domain name Management" page of the console.
- Query CDN log download link: if the policy enables [query CDN Log download Link] and Associate project, you can query the Access log download link on the Log Service page in the console.
- Add domain name: if the policy enables "add Domain name" and Associate project, you can add a domain name to the specified project.
- Activate / deactivate domain name: if the strategy enables the [Activate / deactivate domain name] and Associate project, you can specify the accelerated domain name in the project by Activate / deactivate.
- Delete domain name: if the policy enables "Delete Domain name" and Associate project, you can delete the accelerated domain name in the specified project. The domain name must be deactivate. Therefore, if you need to delete a domain name with Activate status, you need to have [Activate / deactivate domain name] Permission.
- Modify domain name configuration: if the policy enables "modify Domain name configuration" and Associate project, you can modify the accelerated domain name configuration in the specified project.
- Purge and Prefetch: if the strategy opens the [Purge and Prefetch] and Associate project, you can submit the corresponding refresh, prefetch (whitelist) job on the "Refresh Cache" page, and query the execution status of Purge and Prefetch and job.
CDN Permissions

Tencent Cloud CDN has been integrated with Cloud Access Management (CAM), so that you can manage user groups, users, roles, and polices in the CAM Console.

As the permission control system of CDN is currently being upgraded, you can assign management permissions of CDN to your sub-users and roles in the following ways.

Default Policies

Default policies applicable to CDN include:

- AdministratorAccess: A sub-user associated with this policy can manage the assets, financial information, users, and permissions of all Tencent Cloud services (including CDN) under their account.
- QCloudResourceFullAccess: A sub-user associated with this policy can manage the assets of all Tencent Cloud services (including CDN) under their account.

Project Permissions

Project Management Authorization

CDN supports assigning permissions by project, i.e., configuring project admins. By creating a project management policy in the following steps and assigning a project, you can grant a sub-user permissions to manage all CDN resources of the project.

1. Click Create by Product Feature or Project Permission.
2. Name the policy and click Project Management in Service Type.
3. Enable Manage CDN Resources in the Project.
4. Associate the specified project.

After the policy above is created and associated with a sub-user, the sub-user can manipulate all resources of Tencent Cloud services (including CDN) within the project.

Feature-specific Project Authorization

CDN supports project-level authorization by preset feature set. By creating a CDN service policy in the following steps, you can grant a sub-user permissions to use specified features in the project:

1. Click Authorize by Product Feature or Project Permission.
2. Name the policy and click CDN in Service Type.
3. Enable the desired feature set, such as View usage data and statistics.
4. Associate the specified project.

After the policy above is created and associated with a sub-user, the sub-user can query the statistics of the resources (domain names) in the project through the following APIs.

Notes on APIs
Sub-users that have resource-specific permissions at the project level can only call the following APIs for related operations.

<table>
<thead>
<tr>
<th>Permission Set</th>
<th>API 3.0</th>
<th>Authorization Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query usage data and statistics</td>
<td>DescribeCdnData DescribeOriginData ListTopData DescribeIpVisit</td>
<td>Yes</td>
</tr>
<tr>
<td>Query domain name information</td>
<td>Not available yet</td>
<td>Yes</td>
</tr>
<tr>
<td>Query a CDN log download link</td>
<td>Not available yet</td>
<td>Yes</td>
</tr>
<tr>
<td>Add a domain name</td>
<td>Not available yet</td>
<td>Yes</td>
</tr>
<tr>
<td>Launch/deactivate a domain name</td>
<td>Not available yet</td>
<td>Yes</td>
</tr>
<tr>
<td>Delete a domain name</td>
<td>Not available yet</td>
<td>Yes</td>
</tr>
<tr>
<td>Modify domain name configuration</td>
<td>Not available yet</td>
<td>Yes</td>
</tr>
<tr>
<td>Purge and prefetch</td>
<td>Not available yet</td>
<td>Yes</td>
</tr>
<tr>
<td>Query a service</td>
<td>Not available yet</td>
<td>No</td>
</tr>
</tbody>
</table>

**Notes on the Console**

- 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
  - Statistical analysis: Real-time monitoring
  - Statistical analysis: Data analysis
  - Internet-wide data monitoring

- 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 Management** 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 accelerated 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 accelerated 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.

**Note:**
On the Certificate Management page in the console, the sub-user can modify the corresponding HTTPS configuration (API 2.0 is not supported at this time).

• 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 tasks and query their execution status on the Cache Purge page.

**Note:**
The prefetch feature is in trial period and only open to whitelist users.

### Domain Name Permissions

To make it easier for you to configure domain name queries and manage permissions in a more refined manner, the CDN system is currently upgrading the permission policy section and will gradually support policy syntax, so that you can grant permissions at the domain name level through custom policy statements.

The new v3.0 APIs and statistical analysis-enabled console fully support policy syntax with the corresponding actions as below:

- **DescribeCdnData:** It queries the domain name access monitoring data, including real-time metrics such as bandwidth, traffic, traffic hit rate, requests, status codes, and response time, which supports a granularity of 1 minute. This corresponds to the data on the real-time monitoring page and access monitoring page in Statistical Analysis in the console.

- **DescribeOriginData:** It queries domain name origin-pull monitoring data, including real-time metrics such as origin-pull bandwidth, origin-pull traffic, origin-pull requests, origin-pull failure rate, and origin-pull status codes, which support a granularity of 1 minute. This corresponds to the data on the real-time monitoring page and origin-pull monitoring page in Statistical Analysis in the console.

- **ListTopData:** It supports queries where results can be sorted by multiple criteria, such as sorting traffic data entries by domain name or by URL in the specified time period in descending order, which corresponds to the related list section in Statistical Analysis in the console.
DescribeIpVisit: It queries active IPs with a granularity of 5 minutes and daily active users data, which corresponds to the related module in **Statistical Analysis** in the console.

**Policy Syntax**

The following policy syntax can be used to grant domain name-level permissions:

```json
{
    "version": "2.0",
    "statement": [
        {
            "action": ["*"]
        },
        {
            "resource": ["qcs::cdn::uin/987654321:domain/www.test.com"]
        },
        "effect": "allow"
    ]
}
```

**Syntax description**

- **action**: It indicates the action that needs to be authorized. Only four actions are supported, i.e., DescribeCdnData, DescribeOriginData, ListTopData, and DescribeIpVisit. For more information, see [Domain Name Permissions](#).
- **resource**: It indicates the object that needs to be authorized. For the CDN service, only domain name-level authorization is supported, and the format in the example must be used.
- **effect**: It can be configured as "allow" to allow calling "action" for "resource" or "deny" to prohibit calling "action" for "resource".
- Multiple statements can be configured. If both "deny" and "allow" are configured for a domain name, "deny" takes precedence.

**Note:**

- The policy syntax only supports authorizing the 4 actions as describes above, i.e., DescribeCdnData, DescribeOriginData, ListTopData, and DescribeIpVisit. For more information, see [Domain Name Permissions](#). If `action` is set to "*", all those actions are authorized.
- Domain name-level permissions can be granted by project and through policy syntax at the same time. If a sub-user is granted the data access permission in project A, but denied the data query permission for domain name a in project A by the policy syntax, then the sub-user has no permissions for project A.
Certificate Management

Last updated : 2020-02-24 12:22:51

You can configure CDN certificates for domain names that have been connected to HTTPS. CDN supports the configuration of your existing certificate, or Tencent Cloud SSL Certificates Service management A certificate hosted or issued in the console.

Tencent Cloud will send expiration reminders to user accounts in the form of text messages, e-mails and internal message 30 days, 15 days, 7 days before Expire and the day of Expire. SSL Certificates Service's custom alarm receiver is now supported. You can enter the Message subscription Configure.

Certificates and Private Keys

If you want to configure an existing certificate for your domain name, please know the following first.

If you configure Tencent Cloud SSL Certificates Service management For the certificate hosted or issued in the console, you can skip this section and refer to the following article directly. Configure a Certificate Process.

The certificates provided by CAs include the following types, of which Nginx Is used by CDN.

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

Certificates

Common certificate extensions include "*.pem", "*.crt", and "*.cer". Open a certificate file in a text editor and you can see a certificate similar to the content as shown in the figure below.
A "*.pem" certificate begins with "- BEGIN CERTIFICATE-" and ends with "- END CERTIFICATE-". Every line in between contains 64 characters, while the last line may have less than 64 characters.
If your certificate is issued by an intermediate CA, your certificate file will consist of multiple certificates. In this case, you need to splice the server certificates and intermediate certificates manually for upload by putting the server certificate content before the intermediate certificate content without any blank lines in between. Please refer to the rules or instructions that came with the certificate.

- 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-----
MIIEbTCCAg+gAwIBAgIQQABQJ/2h4hH4AKAYzZ2kVZQDA4GBsGqYBQH6IzyNQwB
-----END CERTIFICATE-----
```

### Private Key

Common private key extensions include ".pem" and ".key". Open a private key file in a text editor and you will see a certificate similar to the content as shown in the figure 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 converting the format using OpenSSL with the following command:

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

Configure Certificate

1. Log in to the CDN Console and click Certificate on the left sidebar to go to the certificate management page.
2. Click Configure Certificate to go to the certificate configuration page.

Select a Domain Name
Select the domain that you want to configure the certificate for from the **Domain** Drop-down list.

---

**Configure Certificate**

Please make sure the domain has already connected with Tencent Cloud CDN and the status is "Deploying" or "Activated".

**Select the domain you want to configure certificate**

- The domain name should already have CDN service enabled, and the domain name status should be **Deploying** or **Activated**. Certificates cannot be configured for **Closed** Domain names.
- After CDN acceleration is enabled through **COS** or **Cloud Image**, certificates cannot be configured for the default domain names `.file.myqcloud.com` and `.image.myqcloud.com`.

---

**Selecting a Certificate**

You can choose to use your own certificate or Tencent Cloud escrow certificate.

**Proprietary Certificate**

select **Self-owned Certificate** and paste the certificate and private key into the text box. You can add remarks for certificate identification.
Configure Certificate

Please make sure the domain has already connected with Tencent Cloud CDN and the status is "Deploying" or "Activated".

Select the domain you want to configure certificate

Domain: dsafdf.dannychen.cn

Select a certificate

Certificate source
- Own certificate
- Tencent Cloud Hosting Certificate

Certificate Content
- PEM code

Private key contents
- PEM code

Remark (optional)
- Please enter remark contents

The certificate must be in PEM format; if not, see Converting Other Formats to PEM.
If your certificate has a certificate chain, please convert it to PEM format and merge it with the certificate content for upload. In case of incomplete certificate chain, see Completing a Certificate Chain.

Tencent Cloud Hosting Certificate
You can log in SSL Certificates Service management Console, apply for a third-party certificate provided free of charge by Asia Integrity, or trust the existing certificate to Tencent Cloud.
Select "Tencent Cloud hosted Certificate" to see the list of certificates available for this domain name. Select the
certificate you want to use from the certificate list, which is displayed in the format "Certificate ID".

Select the origin-pull method

<table>
<thead>
<tr>
<th>Origin-Pull method</th>
<th>HTTP</th>
<th>Follow protocol</th>
<th>HTTPS</th>
</tr>
</thead>
</table>

Origin-pull Methods

After the certificate is configured, you can select the origin-pull method that the CDN node used to obtain resources from the origin server. CDN supports three origin-pull methods: HTTP, HTTPS, and Protocol.

- After HTTP Origin-pull is successfully configured, requests from users to CDN nodes support HTTPS/HTTP, while origin-pull requests from CDN nodes are all HTTP requests.
- If Protocol Origin-pull is selected, a valid certificate needs to be deployed on your origin server; otherwise, origin-pull will fail. After successful configuration, if requests from users to CDN nodes are HTTP requests, origin-pull requests from CDN nodes will also be HTTP requests. The same is true for HTTPS.
- If the HTTPS port on the origin server is not 443, the configuration will fail.
- COS and FTP origin server domain names only support HTTP origin-pull.

Configuration Success

Click Trending To complete the configuration. The successfully configured domain name and certificate information will be displayed on the Certificate Management Page.

Batch Configuration of Certificate

If you have a multi-domain certificate or wildcard certificate that is applicable to multiple CDN accelerated domain names, you can configure it for multiple domain names in batches using batch configuration.

1. Log in to the CDN Console And click Certificate On the left sidebar to go to the certificate management page.
2. Click **Batch Configuration** to go to the batch management page.

### Uploading a Certificate
Paste the PEM-encoded certificate and private key to the corresponding text boxes. You can modify the remarks to identify the configured certificate and then click **Next**.

**Associating a Domain Name and Selecting an Origin-pull Method**
CDN can identify the accelerated domain names that can use the certificate you uploaded (the domain names should be in **Deploying** or **Activated** Status). You can select the domain names to be associated and the origin-pull method.
Select the origin-pull method

- **Origin-Pull method**: HTTP  Circle Follow protocol

- **Submit**

**Submitting Configuration**

Click **Trending** And CDN will configure the certificate for the selected domain name. It takes about 5 minutes for the configuration to take effect for each domain name. You can check the certificate configuration status on the **Certificate Management** Page.

- If the configuration failed, you can click **Edit** On the right of the domain name to configure the certificate again.
- If there is any domain name already configured with a certificate among the domain names configured in batches, the original certificate of that domain name will be overwritten; if the overwrite fails, the certificate status of that domain name will change to **Update failed**. In this case, the original certificate remains valid.

You can click **Edit** On the right of the domain name to overwrite it again.

**Edit Certificate**

You can click **Edit** On the right of the domain name to update a successfully configured certificate.
You can switch between your own certificate and Tencent Cloud hosted certificate, and re-select Origin-pull method. Click “submit” to complete the deployment. The deployment process is seamless and will not affect your business usage.

Deleting a Certificate

Click `.setRegion(region)` On the right of the domain name to delete the deployed certificate from CDN.

Completing a Certificate Chain

When configuring a self-owned certificate, you may encounter an issue where the Certificate chain cannot be completed.

In this case, you can paste the CA-issued certificate (in PEM format) after the domain name certificate (in PEM format) to
complete the certificate chain, or you can submit a ticket.

Converting Other Formats to PEM

Currently, CDN only supports certificates in PEM format. Certificates in other formats need to be converted to PEM format first. We recommend using OpenSSL to perform the conversion. Below shows how to convert several common formats to PEM.

**DER to PEM**
The 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**
The P7B format is generally used on Windows Server and Tomcat.
Certificate conversion:

```
openssl pkcs7 -print_certs -in incertificate.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**
The 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
```
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.
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.
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 ≤ 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 
  \[
  \text{hit rate} = \frac{\text{total downstream traffic} - \text{origin-pull traffic}}{\text{total downstream traffic}}
  \]
  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.
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.
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.
You can also switch to another metric by selecting it from the drop-down list on the top-left corner of the details page.

Granularity Description

Granularity on the overview page

The monitoring page provides options to display data curves at a 1-minute, 5-minute, 1-hour, or 1-day granularity. The minimum time granularity can be displayed varies by the selected time period.

- Time period \( \leq 6 \) hours: The minimum time granularity is 1 minute. The latency for displaying the 1-minute curve is about 3 minutes.
- \( 6 \) hours \(<\) time period \( \leq 24 \) hours: The minimum time granularity is 5 minutes. The latency for displaying 5-minute curve is about 5-10 minutes.
- \( 24 \) hours \(<\) time period \( \leq 31 \) days: The minimum time granularity is 1 hour.
- Time period \( > 31 \) days: The minimum time granularity is 1 day.

Granularity on the details page

The time granularity options on the metric details page are as follows:

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

- The data collected at a 1-minute granularity can be queried only in the new version of the console. For historical data, the minimum granularity for query is 5 minutes.
- The maximum time period for query is 90 days.

Aggregation Description

The method for aggregating 1-minute data into 5-minute, 1-hour, or 1-day data varies by data metric.

- Origin-pull bandwidth: The smallest granularity provided by CDN for monitoring bandwidth data is 1 minute. Based on industry standard, fees are generally billed by 5-minute granularity, which is calculated by taking the average of 1-minute data values. Therefore, the bandwidth data at a 1-hour or 1-day granularity can be calculated based on the maximum 5-minute bandwidth value.
• Origin-pull traffic: The traffic data at a 5-minute, 1-hour, or 1-day granularity is obtained by aggregating 1-minute traffic data.
• Origin-pull requests: The request count at a 5-minute, 1-hour, or 1-day granularity is obtained by aggregating 1-minute request counts.
• Origin-pull failure rate: Calculated by dividing the total number of origin-pull failures by the total number of origin-pull requests based on the selected time granularity.
• Origin-pull status codes: The status code data at a 5-minute, 1-hour, or 1-day granularity is obtained by aggregating 1-minute status code data.
### Status codes description

Last updated: 2020-01-14 12:17:31

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</td>
<td>The server cannot parse the request</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Check whether the request syntax is correct.</td>
</tr>
<tr>
<td>403</td>
<td>Request is rejected</td>
<td></td>
</tr>
<tr>
<td></td>
<td></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></td>
</tr>
<tr>
<td></td>
<td></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></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The maximum URL size is 2 KB by default.</td>
</tr>
<tr>
<td>423</td>
<td>Looping request</td>
<td></td>
</tr>
<tr>
<td></td>
<td></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></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Check the client status and timeout configuration.</td>
</tr>
<tr>
<td>502</td>
<td>Gateway Error</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Check whether the business origin server is normal.</td>
</tr>
<tr>
<td>503</td>
<td>COS frequency control is triggered</td>
<td></td>
</tr>
<tr>
<td></td>
<td></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></td>
</tr>
<tr>
<td></td>
<td></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></td>
</tr>
<tr>
<td></td>
<td></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></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Check the domain name resolution configuration of the origin server.</td>
</tr>
<tr>
<td>532</td>
<td>Failed to establish a connection with the origin server in the HTTPS request</td>
<td></td>
</tr>
<tr>
<td></td>
<td></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></td>
</tr>
<tr>
<td></td>
<td></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></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Check the stability of the business 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>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.</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

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.
Purge and Prefetch
Cache Purge

Feature Overview

CDN is capable of configuring basic cache. Cache expiration time can be configured according to rules such as specified business 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: Delete the cache of corresponding resources on all CDN nodes.
- Purge directory: if you select the “Purge Changed Resources” mode, when an end user accesses a resource under the corresponding directory, the Last-Modify information of the resource will be obtained from the origin-pull. If it is the same as that of the currently cached resource, the cached resource will be directly returned; otherwise, the changed resource will be pulled from the origin server and cached again. If you select the “Purge All Resources” mode, 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 does 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 again. 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

After a resource is overwritten by a new one with the same name on the origin server, to prevent users on the entire network from accessing the legacy version of the resource cached on the node, you can submit a request to purge the URL/directory for the resource and clear all caches so users can directly access the latest version of the resource.

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 for timely cleanup.

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** section, you can query tasks by specified time period, keyword, and purge task type. With regard to
keyword, you can only query tasks by specifying 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 users who have activated GCD, up to 10,000 global URLs can be purged per day, which are independent of URL purge quotas in China.
- 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 users who have activated GCD, up to 100 global directories can be purged per day, which are independent of directory quotas in China.
- 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:**

- The operations of directory purge, URL purge, and purge history query must have already been connected to the latest permission system and support permission configuration at the resource (domain name) level.
- For permission assignment method, please see [Permission Configuration](#).

**Use Cases**

**Directory purge - purge changed 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:
```
[root@M_0_14_centos ~]# curl https://examplebucket1-1259222427.file.myqcloud.com/filetest1.txt -sv
* About to connect() to examplebucket1-1259222427.file.myqcloud.com port 443 (#0)
* Trying 161.69.121.120...
* Connected to examplebucket1-1259222427.file.myqcloud.com (161.69.121.120) port 443 (#0)
* Initializing NSS with certpath: /etc/pki/nssdb
* CAfile: /etc/pki/tls/certs/ca-bundle.crt
* CApath: none
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* Server certificate:
  subject: CN=*.weixin.qq.com,O=Shenzhen Tencent Computer Systems Company Limited,L=shenzhen,ST=guangdong,C=CN
  start date: May 13 08:45:20 2019 GMT
  expire date: May 13 08:45:29 2020 GMT
  common name: *.weixin.qq.com
  issuer: CN=GlobalSign Organization Validation CA - SHA256 - G2,O=GlobalSign nv-sa,C=BE
> GET /fileTest1.txt HTTP/1.1
> User-Agent: curl/7.29.0
> Host: examplebucket1-1259222427.file.myqcloud.com
> Accept: */*
>
HTTP/1.1 200 OK
Date: Wed, 11 Dec 2019 09:28:53 GMT
Content-Type: text/plain
Content-Length: 258
Connection: keep-alive
Server: wms_ocmidHy
Cache-Control: max-age=600
Last-Modified: Wed, 11 Dec 2019 09:12:12 GMT
X-NWS-UUID-VERIFY: b45f12ce9711b2e257b1a7b35904ac403
X-NWS-LOG-UUID: d4f587fc-3ab5-ad35-bb50-cbf239c72855
X-Cache-Lookup: Hit From DiskRank3
X-Cache-Lookup: Hit From Inner Cluster
X-Cache-Lookup: Hit From Upstream
X-Cache-Lookup: Hit From Inner Cluster

* Connection #0 to host examplebucket1-1259222427.file.myqcloud.com left intact
```
2. On the origin server, replace 1.txt with a file that has the same name, and the file's last modified time changes, while 2.txt stays the same:
3. Initiate requests again. As the cache has not expired, the legacy content of the `1.txt` resource will be accessed:

```
[root@VM_0_14_centos ~]# curl https://examplebucket1-1259222427.file.myqcloud.com/fileTest/1.txt -sv
* About to connect() to examplebucket1-1259222427.file.myqcloud.com port 443 (ssl) #0
* Trying 101.69.121.89...)
* Connected to examplebucket1-1259222427.file.myqcloud.com (101.69.121.89) port 443 (ssl)
* Initializing NSS with certpath: /etc/pki/tls/certs/ca-bundle.crt
* CAfile: /etc/pki/tls/certs/ca-bundle.crt
  CPath: none
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* Server certificate:
  subject: CN=root.wx.baidu.com,O=Shenzhen Tencent Computer Systems Company Limited,C=CN
  start date: May 13 08:45:29 2019 GMT
  expire date: May 13 08:45:29 2020 GMT
  common name: root.wx.baidu.com
* issuer: CN=GlobalSign Organization Validation CA - SHA256 - G2,O=GlobalSign nv-sa,C=BE
> GET /fileTest/1.txt HTTP/1.1
> User-Agent: curl/7.29.0
> Host: examplebucket1-1259222427.file.myqcloud.com
> Accept: */*
> < HTTP/1.1 200 OK
> Date: Wed, 11 Dec 2019 09:32:36 GMT
> Content-Type: text/plain
> Content-Length: 258
> Connection: keep-alive
> Server: NMS TCloud S1
> Cache-Control: max-age=600
> Expires: Wed, 11 Dec 2019 09:42:36 GMT
> Last-Modified: Wed, 11 Dec 2019 09:32:12 GMT
> X-Cache-Lookup: Hit From Disktank3
> Accept-Ranges: bytes
<
> Connection #0 to host examplebucket1-1259222427.file.myqcloud.com left intact
```
4. Submit a directory purge task, select **Purge Changed Resources**, and wait for the purge to complete:

![Purge and Prefetch](image)

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 hit by nodes and returned:
```
[root@M_0_14_centos ~]# curl https://examplebucket1-1259222427.file.myqcloud.com/fileTest/1.txt -sv
* About to connect() to examplebucket1-1259222427.file.myqcloud.com port 443 (0)
* Trying 101.71.72.212...
* Connected to examplebucket1-1259222427.file.myqcloud.com (101.71.72.212) port 443 (0)
* Initializing NSS with certpath: /etc/ssl/certs/ca-bundle.crt
* CApath: none
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* Server certificate:
*   subject: CN=*.weixin.qq.com,O=Shenzhen Tencent Computer Systems Company Limited,L=shenzhen,ST=guangdong,C=CN
*   start date: May 13 08:45:29 2019 GMT
*   expire date: May 13 08:45:29 2020 GMT
*   common name: *.weixin.qq.com
*   issuer: CN=GlobalSign Organization Validation CA - SHA256 - G2,O=GlobalSign nv-sa,C=BE
> GET /fileTest/1.txt HTTP/1.1
> User-Agent: curl/7.29.0
> Host: examplebucket1-1259222427.file.myqcloud.com
> Accept: */*
> HTTP/1.1 200 OK
> Date: Wed, 11 Dec 2019 09:43:10 GMT
> Content-Type: text/plain
> Content-Length: 254
> Connection: keep-alive
> Last-Modified: Wed, 11 Dec 2019 09:43:37 GMT
> X-NAS-UUID-VERIFY: 905fe357269927d4fde8be5011335643
> Accept-Ranges: bytes
> ETag: "ba79267656855b3bba4e0ff642c5a7"  
> x-cos-request-id: NAaMVu9WvXwX0rj1hj1ANsRd21INFS35n8Q1RDA=
> x-dsa-tunnel: hop_count=4
> X-NAS-LOG-UUID: e1318191-923d-4544-b759-b282b1eef8887
> X-Cache-Lookup: Hit From Upstream
> X-Cache-Lookup: Hit From Inner Cluster
> X-Cache-Lookup: Hit From Upstream
> X-Cache-Lookup: Hit From Inner Cluster

* Connection #0 to host examplebucket1-1259222427.file.myqcloud.com left intact
```
```bash
[root@OM_0_14.centos ~]# curl https://examplebucket1-1259222427.file.myqcloud.com/fileTest/2.txt -sv
* About to connect() to examplebucket1-1259222427.file.myqcloud.com port 443 (#0)
* Trying 101.69.121.120...
* Connected to examplebucket1-1259222427.file.myqcloud.com (101.69.121.120) port 443 (#0)
* Initializing NSS with certpath: /etc/pki/tls/certs/ca-bundle.crt
* CApath: none
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* Server certificate:
  * subject: C=CN,ST=guangdong,L=shenzhen,O=shenzhen Tencent Computer Systems Company Limited,CN=shenzhen Tencent Computer Systems Company Limited
  * start date: May 13 08:45:29 2019 GMT
  * expire date: May 13 08:45:29 2020 GMT
  * common name: *.weixin.qq.com
  * issuer: CN=GlobalSign Organization Validation CA - SHA256 - G2,O=GlobalSign nv-sa,C=BE
* GET /fileTest/2.txt HTTP/1.1
* User-Agent: curl/7.29.0
* Host: examplebucket1-1259222427.file.myqcloud.com
* Accept: */*
>
HTTP/1.1 200 OK
Date: Wed, 11 Dec 2019 09:44:24 GMT
Content-Type: text/plain
Content-Length: 135
Connection: keep-alive
Server: wns_ocmids Hil
Cache-Control: max-age=600
Last-Modified: Wed, 11 Dec 2019 09:54:24 GMT
X-NWS-UID-VERIFY: 77063780ee0075a84c8d6d555c4ff03f
X-NWS-LOG-UID-TOD: b69c4f26f1c69c08-9978-18c91e70e494
X-Cache-Lookup: Hit from disklank
Accept-Ranges: bytes
X-Daa-Tunnel: hop_count=3
X-Cache-Lookup: Hit From Inner Cluster
X-Cache-Lookup: Hit From Upstream
X-Cache-Lookup: Hit From Inner Cluster

* Connection #0 to host examplebucket1-1259222427.file.myqcloud.com left intact
```
Log Management

Feature Overview

After the domain name is connected to the content distribution network (CDN), all user-side resource requests will be dispatched to the CDN node to respond. If the node has cached the resource, it will directly return the content. If the CDN node does not cache the resource, it will send the request pass through to real server of the domain name configuration to pull the required resources.

Because the CDN node responds to most user requests, in order to facilitate customers to analyze user Access, CDN packages entire network and Access logs with an hourly granularity, which is stored for 30 days by default and provides download service.

For now, only node Access log is provided, but Origin-pull log is not provided.

Scenario

Analysis of Access's behavior

Customers can download Access log, according to their own needs for hot resource analysis, active user analysis and so on.

Service quality monitoring
By downloading Access's log, you can grasp the overall service status of CDN nodes and calculate the average response time, average download speed and so on Metric.

Operation Instructions

How to use

Login CDN console Click the **Log Service** of Directory on the left. You can select the domain name and time to query the Access log. You can check multiple log packages and download them locally in batches:
Access logs are packed on an hourly basis by default. If there is no request for the domain name within a certain hour, no log packet will be generated in this time range.

The overseas Access log of the same domain name is packaged separately from the domestic Access log, and the naming format of the log packet is “time-domain name-acceleration area”.

Access logs are collected from each CDN cache node, so there are differences in delay. In general, log packages can be queried and downloaded with a delay of about 30 minutes. Log packages are constantly appended and tend to be stable after 2-3 hours.

The domain name history Access log only retains the log package within 30 days. You can use the SCF function to transfer the log package to Cloud Object Storage COS, for permanent storage according to the following guidelines.

**Field description**

The order and meaning of fields in the log are shown in the following table:

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Log Content</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>The number of bytes of Access this time, including the size of the file itself and the size of the request header header</td>
</tr>
<tr>
<td>6</td>
<td>The domestic log represents the province number, and the overseas log represents the area number (see below for the mapping table)</td>
</tr>
<tr>
<td>7</td>
<td>The domestic log represents ISP's serial number, and the overseas log is unified as -1 (see below for mapping table)</td>
</tr>
<tr>
<td>8</td>
<td>HTTP status code</td>
</tr>
<tr>
<td>9</td>
<td>Referer information</td>
</tr>
</tbody>
</table>
Sequence | Log Content
--- | ---
10 | Response time (milliseconds), which refers to the time it takes for a node to respond to all return packets and then to the client after receiving the request
11 | User-Agent information
12 | Range parameter
13 | HTTP Method
14 | HTTP Protocol logo
15 | Cache HIT/MISS, is marked as HIT when CDN Edge server hits and parent node hits

Region / ISP mapping table

Mapping of provinces in the territory

<table>
<thead>
<tr>
<th>Regional ID</th>
<th>Region</th>
<th>Regional ID</th>
<th>Region</th>
<th>Regional ID</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>twenty-two</td>
<td>Beijing</td>
<td>eighty-six</td>
<td>Inner Mongolia</td>
<td>one hundred and two</td>
<td>Brazil</td>
</tr>
<tr>
<td>1069</td>
<td>Hebei</td>
<td>1177</td>
<td>Tianjin</td>
<td>one hundred and two</td>
<td>Ningxia</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Brazil</td>
<td>1208</td>
<td>Gansu</td>
<td>1467</td>
<td>Qinghai</td>
</tr>
<tr>
<td>1468</td>
<td>Xinjiang</td>
<td>one hundred and two</td>
<td>Heilongjiang province</td>
<td>1445</td>
<td>Bahrain</td>
</tr>
<tr>
<td>1464</td>
<td>Benin</td>
<td>2</td>
<td>Fujian province</td>
<td>one hundred and two</td>
<td>Jiangsu province</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Anhui</td>
<td>one hundred and two</td>
<td>Shandong</td>
<td>1050</td>
<td>Shanghai</td>
</tr>
<tr>
<td>1442</td>
<td>Zhejiang province</td>
<td>one hundred and two</td>
<td>Vietnam</td>
<td>1135</td>
<td>Hubei</td>
</tr>
<tr>
<td>1465</td>
<td>Brazil</td>
<td>1466</td>
<td>Vietnam</td>
<td>one hundred and two</td>
<td>Guizhou province</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Vietnam</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>one hundred and two</td>
<td>Brazil</td>
</tr>
<tr>
<td>1441</td>
<td>Vietnam</td>
<td>* 2018-5-4</td>
<td>Others</td>
<td>1</td>
<td>Hong Kong/Macao/Taiwan</td>
</tr>
<tr>
<td>-1</td>
<td>Overseas</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### ISP mapping in China

<table>
<thead>
<tr>
<th>ISP ID</th>
<th>Carrier</th>
<th>ISP ID</th>
<th>Carrier</th>
<th>ISP ID</th>
<th>Carrier</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>China Telecom</td>
<td>twenty-six</td>
<td>China Unicom</td>
<td>thirty-eight</td>
<td>CERNET</td>
</tr>
<tr>
<td>forty-three</td>
<td>Great Wall Broadband</td>
<td>1046</td>
<td>China Mobile</td>
<td>3947</td>
<td>China Tietong</td>
</tr>
<tr>
<td>-1</td>
<td>Overseas ISP</td>
<td>* 2018-5-4</td>
<td>Other ISP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Mapping of overseas areas

<table>
<thead>
<tr>
<th>Regional ID</th>
<th>Region</th>
<th>Regional ID</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000000001</td>
<td>Asia Pacific region 1 (Service area)</td>
<td>one hundred and two</td>
<td>Slovakia</td>
</tr>
<tr>
<td>2000000002</td>
<td>Asia-Pacific region 2 (Service area)</td>
<td>one hundred and two</td>
<td>Serbia</td>
</tr>
<tr>
<td>2000000003</td>
<td>Asia-Pacific region 3 (Service area)</td>
<td>one hundred and two</td>
<td>Finland</td>
</tr>
<tr>
<td>2000000004</td>
<td>Middle East (service area)</td>
<td>one hundred and two</td>
<td>Belgium</td>
</tr>
<tr>
<td>2000000005</td>
<td>North America (service area)</td>
<td>one hundred and two</td>
<td>Bulgaria</td>
</tr>
<tr>
<td>2000000006</td>
<td>Europe (service area)</td>
<td>one hundred and two</td>
<td>Slovenia</td>
</tr>
<tr>
<td>2000000007</td>
<td>South America (service area)</td>
<td>one hundred and two</td>
<td>Moldova</td>
</tr>
<tr>
<td>2000000008</td>
<td>Africa (service area)</td>
<td>one hundred and two</td>
<td>Macedonia</td>
</tr>
<tr>
<td>-20</td>
<td>Asia (client region)</td>
<td>one hundred and two</td>
<td>Estonia</td>
</tr>
<tr>
<td>-21</td>
<td>South America (client area)</td>
<td>one hundred and two</td>
<td>Croatia</td>
</tr>
</tbody>
</table>

* Confirm to submit the request

©2013-2019 Tencent Cloud. All rights reserved.
<table>
<thead>
<tr>
<th>Regional ID</th>
<th>Region</th>
<th>Regional ID</th>
<th>Region</th>
<th>Regional ID</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>-22</td>
<td>North America (client area)</td>
<td>100</td>
<td>Poland</td>
<td>1916</td>
<td>Greenland</td>
</tr>
<tr>
<td>-23</td>
<td>Europe (client region)</td>
<td>100</td>
<td><img src="docfile/CVM/OM08.png" alt="docfile/CVM/OM08.png" /></td>
<td>2026</td>
<td>Taiwan (China)</td>
</tr>
<tr>
<td>24</td>
<td>Africa (client region)</td>
<td>100</td>
<td>10.0.0.0/16</td>
<td>2083</td>
<td>Myanmar</td>
</tr>
<tr>
<td>twenty-five</td>
<td>Oceania (client area)</td>
<td>100</td>
<td>(Traffic hit rate: %)</td>
<td>2087</td>
<td>Brunei</td>
</tr>
<tr>
<td>thirty-five</td>
<td>ConfigDesc</td>
<td>100</td>
<td>MasterNodeDiskType</td>
<td>2094</td>
<td>Sri Lanka</td>
</tr>
<tr>
<td>fifty-seven</td>
<td>Thailand</td>
<td>100</td>
<td>Libya</td>
<td>2150</td>
<td>Panama</td>
</tr>
<tr>
<td>seventy-three</td>
<td>India</td>
<td>100</td>
<td>Armenia</td>
<td>2175</td>
<td>Colombia</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Vietnam</td>
<td>100</td>
<td>Yemen</td>
<td>2273</td>
<td>Monaco</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>SucceedCount</td>
<td>100</td>
<td>Belarus</td>
<td>2343</td>
<td>Andorra</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>United Kingdom</td>
<td>100</td>
<td>Luxembourg</td>
<td>2421</td>
<td>Turkmenistan</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Sweden</td>
<td>1036</td>
<td>Singapore</td>
<td>2435</td>
<td>Laos</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Germany</td>
<td>1044</td>
<td>XCosSecurityToken: credentials.sessionToken</td>
<td>2488</td>
<td>East Timor</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Italy</td>
<td>1066</td>
<td>Pakistan</td>
<td>2490</td>
<td>Tonga</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Spain</td>
<td>1070</td>
<td>Malta</td>
<td>2588</td>
<td>Philippines</td>
</tr>
<tr>
<td>Regional ID</td>
<td>Region</td>
<td>Regional ID</td>
<td>Region</td>
<td>Regional ID</td>
<td>Region</td>
</tr>
<tr>
<td>------------</td>
<td>--------</td>
<td>------------</td>
<td>--------</td>
<td>------------</td>
<td>--------</td>
</tr>
<tr>
<td>one hundred and two Starter</td>
<td>1091</td>
<td>Bahamas</td>
<td>2609</td>
<td>Venezuela</td>
<td></td>
</tr>
<tr>
<td>one hundred and two Israel</td>
<td>1129</td>
<td>Argentina</td>
<td>2612</td>
<td>Bolivia</td>
<td></td>
</tr>
<tr>
<td>one hundred and two Ukraine</td>
<td>1134</td>
<td>Bangladesh</td>
<td>2613</td>
<td>Brazil</td>
<td></td>
</tr>
<tr>
<td>one hundred and two Russia</td>
<td>1158</td>
<td>Cambodia</td>
<td>2623</td>
<td>Costa Rica</td>
<td></td>
</tr>
<tr>
<td>one hundred and two Kazakhstan</td>
<td>1159</td>
<td>Macao (China)</td>
<td>2626</td>
<td>Mexico</td>
<td></td>
</tr>
<tr>
<td>one hundred and two Portugal</td>
<td>1176</td>
<td>Singapore</td>
<td>2639</td>
<td>Honduras</td>
<td></td>
</tr>
<tr>
<td>one hundred and two Greece</td>
<td>1179</td>
<td>Maldives</td>
<td>2645</td>
<td>El Salvador</td>
<td></td>
</tr>
<tr>
<td>one hundred and two Saudi Arabia</td>
<td>1180</td>
<td>Afghanistan</td>
<td>2647</td>
<td>Paraguay</td>
<td></td>
</tr>
<tr>
<td>one hundred and two Denmark</td>
<td>1185</td>
<td>Fiji</td>
<td>2661</td>
<td>Peru</td>
<td></td>
</tr>
<tr>
<td>one hundred and two Iran</td>
<td>1186</td>
<td>Mongolia</td>
<td>2728</td>
<td>Nicaragua</td>
<td></td>
</tr>
<tr>
<td>one hundred and two Norway</td>
<td>1195</td>
<td>Indonesia</td>
<td>2734</td>
<td>Ecuador</td>
<td></td>
</tr>
<tr>
<td>one hundred and two South Korea</td>
<td>1200</td>
<td>Hong Kong (China)</td>
<td>2768</td>
<td>100-8000kbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`-- tcaplus</td>
<td>1233</td>
<td>Qatar</td>
<td>2999</td>
<td>Aruba</td>
</tr>
<tr>
<td>one hundred and two Cyprus</td>
<td>1255</td>
<td>Iceland</td>
<td>3058</td>
<td>100-8000kbps</td>
<td></td>
</tr>
<tr>
<td>one hundred and two Czech</td>
<td>1289</td>
<td>Albania</td>
<td>3144</td>
<td>Poland</td>
<td></td>
</tr>
<tr>
<td>one hundred and two Switzerland</td>
<td>1353</td>
<td>Uzbekistan</td>
<td>3216</td>
<td>Dominican</td>
<td></td>
</tr>
<tr>
<td>one hundred and two Iraq</td>
<td>1407</td>
<td>San Marino</td>
<td>3379</td>
<td>South Korea</td>
<td></td>
</tr>
<tr>
<td>Regional ID</td>
<td>Region</td>
<td>Regional ID</td>
<td>Region</td>
<td>Regional ID</td>
<td>Region</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------</td>
<td>-------------</td>
<td>----------------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Netherlands</td>
<td>1416</td>
<td>Kuwait</td>
<td>3701</td>
<td>Malaysia</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Romania</td>
<td>1417</td>
<td>Montenegro</td>
<td>3839</td>
<td>Canada</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>TotalSize: [</td>
<td>1493</td>
<td>Tajikistan</td>
<td>4450</td>
<td>Australia</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Hungary</td>
<td>1501</td>
<td>Bahrain</td>
<td>4460</td>
<td>Mainland China-North China</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Georgia</td>
<td>1543</td>
<td>print result2</td>
<td>-15</td>
<td>Other Asian countries</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>SecurityGroupName:CDB</td>
<td>1559</td>
<td>South Africa</td>
<td>-14</td>
<td>Eastern South America</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Austria</td>
<td>1567</td>
<td>Egypt</td>
<td>-13</td>
<td>Other North American countries</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Palestine</td>
<td>1590</td>
<td>Kenya</td>
<td>-12</td>
<td>The rest of Europe</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Turkey</td>
<td>1592</td>
<td>Nigeria</td>
<td>-11</td>
<td>Other African countries</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Lithuania</td>
<td>1598</td>
<td>Tanzania</td>
<td>-10</td>
<td>The rest of Oceania</td>
</tr>
<tr>
<td>one hundred and two</td>
<td>Oman</td>
<td>1611</td>
<td>SecondsBehindMaster</td>
<td>-2</td>
<td>Other oversea ISPs</td>
</tr>
</tbody>
</table>

**Overseas ISP mapping**

<table>
<thead>
<tr>
<th>ISP ID</th>
<th>Carrier</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>Overseas ISP</td>
</tr>
</tbody>
</table>

**Notes**

According to the number of bytes recorded in the fifth field of Access log, the statistically calculated Traffic / bandwidth data is inconsistent with the CDN billing Traffic / bandwidth data. Because:

- Only application layer data can be recorded in Access's log. In actual network transmission, the network Traffic generated is 5-15% more than that of pure application layer Traffic. It consists of two parts:
  - Consumption by TCP/IP headers: In TCP/IP-based HTTP requests, each packet has a maximum size of 1500 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.

Use Cases

Example of Access log in China

Overseas Access log example
Real-time log

Last updated: 2020-03-30 19:37:02

Function introduction

Through the real-time collection and push of the CDN Access log, the content distribution network (CDN) can quickly retrieve and analyze the log data. You can quickly access through the CDN console and enjoy a full range of stable and reliable log services from log collection, log storage to log retrieval.

CDN Real-time Log Service is currently under internal testing. You can submit an application form for trial. If you have already submitted your application, we will review your application within seven business day.

Application Scenarios

View/analyze the situation of user Access in real time.

Basic Concepts

Log set

Logset (Logset) is the project management unit of the log service, which is used to distinguish the logs of different projects. A Logset corresponds to a project or application. CDN Logset has the following basic attribute information:

- Logset name: cdn_logset
- Area: Logset belongs Region
- Save time: the current saving time period of the data in Logset
- Creation time: Logset creation time

Log topic

Log topic (Topic) is the basic management unit of the log service. A Logset can contain multiple logs topic. A log topic corresponds to a class of applications or services. It is recommended to collect similar logs on different machines into the same log topic. For example, a business project has three kinds of logs: operation log, application log, Access log, each type can create a log topic.

Log service system takes log topic as a unit to distinguish and manage different log data of users. Each log topic can be configured with different data sources, different index rules and shipping rule. Therefore, log topic is the basic unit of log service configuration and management of log data. After creating log topic, it is necessary to configure relevant rules in order to effectively collect logs as scheduled, and use functions such as retrieval analysis and shipping.

From the point of view of the function of the scene, the log topic mainly provides:

- Collect logs to logs topic.
- Use the log topic as the unit to store the management log.
The log topic is used as a unit to retrieve the analysis log.
Take the log topic as the unit shipping log to other platforms.
Download and consume logs from topic.

Operations Guide

Login CDN console Click Log Service of Directory on the left, and select Real-time Log to enter the real-time log page and start creating real-time log shipping.

Create log topic

Click [Create] to create a log, topic.

One Logset can create at most 10 topic.

Configuration log topic

Enter added the log topic name and bound the domain name to the log topic.

- The name of topic in Create's log cannot be the same as that of topic in the existing log.
- A domain name can only be bound to one log topic, not multiple logs topic.
- After the configuration information is saved, the configuration takes effect for about 15 minutes.

Management log topic

After successfully configuring the log topic, you can manage the log topic: stop / Launch log shipping to the log topic, retrieve the log with the log topic as a unit, manage the log topic and delete the log topic.

Stop / Launch log shipping

You can manually stop / Launch log shipping to log topic.

- After stopping, all logs bound to the topic domain name of the log will no longer continue from shipping to the topic, and the log of shipping will continue to be retained. The effective time is about 5-15 minutes.
- After Launch, all logs bound to the log topic domain name will continue from shipping to the topic. The effective time is about 5-15 minutes.

Search

The log topic is used as the unit for log retrieval. Select the log topic you want to retrieve, and click "search" to enter the log retrieval page.

- Time interval selection: support to retrieve log data for today, 24 hours (one of the nearly 7 days), and nearly 7 days.
- Arrangement display: supports sorting in descending / ascending order according to log time.
- Retrieval: support full-text retrieval, health value retrieval and fuzzy keyword retrieval. For more information, please see Retrieval grammar .
## 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, is marked as HIT in CDN Edge server hit and parent node hit.</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>Carrier</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>Parameters carried by URL</td>
</tr>
<tr>
<td>Proto</td>
<td>String</td>
<td>Text</td>
<td>HTTP Protocol logo</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, HTTP source address</td>
</tr>
<tr>
<td>Request_range</td>
<td>String</td>
<td>Text</td>
<td>Range parameter, request scope</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>Request_time</td>
<td>Integer</td>
<td>Long</td>
<td>Response time (milliseconds), which refers to the time it takes for a node to respond to all return packets and then to the client after receiving the request.</td>
</tr>
<tr>
<td>Rsp_size</td>
<td>Integer</td>
<td>Long</td>
<td>Returns the number of bytes.</td>
</tr>
<tr>
<td>Time</td>
<td>Integer</td>
<td>Long</td>
<td>Request time, UNIX timestamp.</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 identification of the request.</td>
</tr>
</tbody>
</table>

**Manage**

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

The effective time of the new configuration is about 5-15 minutes.

**Delete**

You can delete the log topic manually.

After deletion, all logs bound to the domain name under the log topic will no longer continue from shipping to the topic, and all the logs of shipping will be emptied. The effective time is about 5-15 minutes.
You can check the status of ISPs across the entire network in the CDN Console. CDN sends continuous requests to monitoring files at detection points across regions and collects their response data to obtain corresponding information about latency and availability of ISPs across regions.

Real-time network status overview

1. Log in to the CDN Console.
2. Go to Query Service > Global Status on the left sidebar to enter the monitoring page.
3. You can view the real-time status overview of the entire network to check the latency and availability of each region.

- Hover over the regions 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.
- In the figure, refresh time for real-time data is one minute.
Status overview of the entire network

In Network Monitoring, you can query the historical latency and availability charts of the specified region or ISP for a specified time period.

1. Click *Select Regions and Carriers* to create a query.

Time range: You can query the access statistics for the last 30 days with a maximum time span of 30 days.
2. After selecting the query conditions, click **Confirm** to view the latency and availability charts.
Monthly Operations Report

Last updated: 2019-12-02 15:40:22

CDN provides monthly reports on your monthly business status to facilitate your business operations.

1. Log in to the CDN Console.
2. Click Query Service > Monthly Report on the left sidebar to enter the management page.
3. You can view the report of any month in the past year.

4. A monthly operations report contains the following:
   - **Overall trend**: This displays the details of traffic/bandwidth consumption for the specified month as compared to the previous month.
   - **Top 5 traffic usage**: This analyzes the top 5 projects/domain names in terms of traffic consumption and displays their specific percentages.
   - **Top 10 usage**: This analyzes the top 10 projects/domain names in terms of usage as compared to the previous month.
   - **Hit rate**: This analyzes the average hit rate in the current month as compared to the previous month, and displays the 3 domain names with the lowest hit rate.
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 Troubleshooting Tool

Overview

CDN provides a self-diagnose tool that helps you perform self-inspection when you find that there is a problem while accessing a resource URL. The process of self-diagnose includes a series of inspection items such as checking the DNS resolution of connected domain, connection quality, the availability of sites and the consistency of data access, to help you locate the problem and provide solutions.

Note: The resource URL to be diagnosed must be an "Activated" domain under your account. The bandwidth generated during the diagnosis process will be calculated as billing bandwidth. It is suggested that the target resources to be diagnosed do not exceed 200MBytes.

Instructions

Current Device Access Diagnosis

You can initiate diagnosis through "Current device access diagnosis" when you find that there is a problem while accessing a resource. The procedure for current device access diagnosis is as follows:

1. From the console, go to Inspect Tool >> Self-diagnose page and select "Current device access diagnosis" tab;
2. Enter the resource URL to be diagnosed. Currently only URLs with the prefix “http://” are supported. Cannot diagnose URLs which start with "https" at this moment. Once the correct URL is entered, click "Get test URL", and a test address will be generated in the page;
3. Click the test address generated in step 2 to open the diagnosis page and start collecting diagnosis information. Please do not close the diagnosis page during the process, the page will close on its own when the process is completed;
4. After the diagnosis, you can go to "Diagnosis report" tab to review the results.
User Access Diagnosis

When a user reports that there is a problem while accessing resource, you can locate the problem using "User access diagnosis", and solve the problem through actions suggested by Tencent Cloud. The procedure for user access diagnosis is as follows:

1. From the console, go to Inspect Tool >> Self-diagnose page and select "User access diagnosis" tab;

2. Enter the resource URL to be diagnosed. Currently only URLs with the prefix "http://" are supported. Cannot diagnose URLs which start with "https" at this moment. Once the correct URL is entered, click "Get test URL", and a test address will be generated in the page;

3. Send this test address to your user. Diagnosis information will be collected when your user opens the test URL. Please do not close the page during the process.

4. After the diagnosis, you can go to "Diagnosis report" tab to review the results that have been collected from the user.
Reviewing the Diagnosis Report

From the console, go to Inspect Tool >> Self-diagnose page and select “Diagnosis report” tab to see a list of diagnosis reports. Diagnosis reports that have been generated will be presented in the page, sorted by time of creation.
You can click "Check" to view the details of the report.

The Report Details page is divided into two sections, "Diagnosis object" and "Diagnosis report":

**Diagnosis object**: Contains Diagnosis ID, abnormal URL, abnormal domain name, origin type information.

**Diagnosis report**: Contains diagnosis results about CNAME, DNS resolution, site availability, link quality, and data access consistency.

**Item 1: CNAME**

1. Normal: If the CNAME that is actually resolved from the diagnosis domain is consistent with the CNAME that should be deployed and resolved, the result will be "normal".
2. Abnormal CNAME Configuration: If the CNAME that is actually resolved from the diagnosis domain is not consistent with the CNAME that should be deployed and resolved, the result will be "abnormal". You can click "Check details" to review the CNAME that is actually resolved and the one that should be deployed and resolved as well as its CDN provider. Only one CNAME is presented in the details if multiple CNAMEs are actually resolved from the diagnosis domain. In this case, it is suggested that you change the CNAME configuration at the DNS service provider. If the CNAME configuration is abnormal, other diagnosis items will not be commenced.

**Item 2: DNS Resolution**

1. Normal: If the actual node accessed by the diagnosis domain is consistent with the optimal node, the result will be "normal". You can click "Check details" to review Client IP, Local DNS, IPs of the actual node and the optimal node, regions and ISP information.
2. Non-optimal path: If the actual node accessed by the diagnosis domain is different from the optimal node, the result will be "non-optimal path". It is suggested that you contact Tencent Cloud technicians.

3. Failed to obtain node IP: Under circumstances such as when the IP of the diagnosis domain is hijacked, or the connection to the node failed, the diagnosis result will be "failed to obtain node IP". It is suggested that you contact Tencent Cloud technicians.

**Item 3: Site availability**

1. Normal: If the connections to the node and the origin server are normal, the diagnosis result will be "normal connections to node and origin server"
2. Abnormal: If the connections to the node or the origin server are abnormal, the diagnosis result will be "abnormal connection to node" or "abnormal connection to origin server" or "abnormal connection to both node and origin server". It is suggested that you contact Tencent Cloud technicians.

**Item 4: Link quality**

1. Normal: If the access to the diagnosis domain is normal, the diagnosis result will be "normal", and the total resource access latency will be presented. You can also click "Check details" to review details about the time spent within every part of the link.
2. Abnormal: If the access to the diagnosis domain failed, the diagnosis result will be "abnormal". It is suggested that you contact Tencent Cloud technicians. If link quality is diagnosed as abnormal, data access consistency diagnosis will not be commenced.

**Item 5: Data Access Consistency**

1. Normal: If diagnosed resources can be normally accessed at the origin and the node plus they have the same MD5, the diagnosis result will be "normal". You can click "Check details" to review the information about the resources at origin server and node.
2. Abnormal origin server resource: If a status code such as 4XX, 5XX occurred when accessing resources at the origin server, or the MD5 values of resources on different origin servers are inconsistent, the diagnosis result will be "abnormal origin server resource". It is suggested to check the resources at the origin server. You can also click "Check details" to review more details about the resources at origin server and node.
3. Abnormal CDN resource: If resources at origin server are normal, but a status code of 4XX or 5XX was returned when accessing resources at the node, or the MD5 values of resources at origin and node are inconsistent, the diagnosis result will be "abnormal CDN resource". It is suggested that you contact Tencent Cloud technicians. You can also click "Check details" to review more details about the resources at origin server and node.

If you're not able to solve the problem using the diagnosis report, we suggest that you submit a ticket, or contact Tencent Cloud technicians for troubleshooting.
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.

![Suspicious Images module]

2. **Manual Management**
   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.

   ![Screenshot of Tencent Cloud console with appeal feature]

**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.