

Table of Contents

| | |
|---|----|
| CDN Quick Start..... | 2 |
| Step one : Add a CDN domain..... | 2 |
| Step two : Configure CNAME record | 4 |
| Step three : CDN service effective..... | 6 |
| Domain Management..... | 6 |
| Configuration Management | 7 |
| Origin configuration..... | 7 |
| Cache configuration | 10 |
| HTTPS configuration | 14 |
| Refresh | 15 |
| Preload | 18 |
| Statistical Analysis | 20 |
| Traffic bandwidth breakdown..... | 20 |
| Status code analysis | 21 |
| Log download..... | 23 |
| SSL certificate management | 24 |

CDN Quick Start

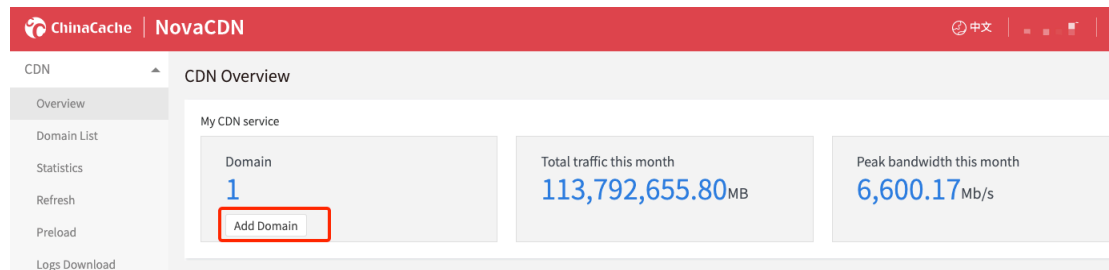
Step preview :



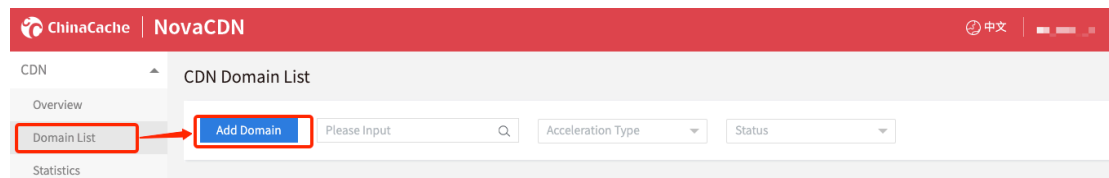
Step one : Add a CDN domain

1. You can add a CDN domain in any of the following two ways

1) Go to the console, select **【Add domain】** on Overview.



2) You can also select the **【Domain List】** in the left menu to enter the corresponding page, click **【Add domain】**



2. Fill in the basic information

The screenshot shows the 'Add Domain' form. It has a 'Basic Information' section with the following fields:

- Domain:
- Acceleration Type: ☒ Small File Acceleration, ☐ Download Acceleration, ☐ VOD Acceleration
- Protocol Type: ☐ HTTP, ☒ HTTPS
- Choose SSL certificate:

Below the form, there is a link: [Click the SSL certificate management to upload.](#)

The domain name needs to be met :

- Generally use subdomains

- Does not allow repeated additions
- The accelerated content must be legal and in line with industry regulations

According to the requirements of People's Republic of China and ChinaCache, no service will be provided to the following related websites:

- No certified ICP
- selling drugs and control cutters
- containing illegal speech and information
- Games and private service websites
- Video category, but no audiovisual license for the site
- Forum or community category, but no BBS special approval qualification website

Specify the business type :

- Acceleration of small files is recommended if the content to be accelerated is mostly images and web files.
- Acceleration of large file downloads is recommended if the content to be accelerated is large files (static files larger than 20 MB).
- Video On Demand, acceleration of live streaming media is recommended to accelerate video on demand and live streaming services

***Once the business type is confirmed, it cannot be modified. Please select it according to your business.**

Protocol type :

HTTPS protocol acceleration needs to select a certificate. For certificate upload operation, see [SSL Certificate Management](#).

3. Complete the Origin Configuration

Origin Information

*Origin Type

☐ multiple Ips

☐ Domain

*Origin address

Backup origin type

☐ IP

☐ Domain

Backup origin address

*Source HOST ?

☐ Default

☐ Customize

You can fill in the origin configuration according to the actual situation of your business, Origin server type can be IP address or origin server domain . More detailed instructions can be found in the [Origin Configuration](#) instructions.

4. Complete Cache Rules

Cache configuration

Header configuration

☐ Ignore CacheControl

?

Parameter configuration

☐ Ignore URL parameters

?

Cache Rules

Add

Adjust Priority

| Types of | Permission content | Cache Time | Operation |
|----------------|---|------------|---|
| File Extension | php;aspx;asp;jsp;do;dw;cgi;fcgi;action;ashx;axd;json | 0sec | Edit Delete |
| File Extension | js;css;aif;apk;avi;bin;bmp;cab;doc;eot;exe;flv;gif;gz;ico;ini;jpe;jpeg;jpg;m4a;mov;mp3;mp4;mpeg;mpeg;msi;pdf;png;otf;rar;svg;swf;ttf;txt;vbs;wav;wmv;woff;woff2;zip | 7days | Edit Delete |
| Directory | / | 1hours | Edit Delete |
| Directory | For all files | 0sec | Edit Delete |

A set of default cache rule have been configured based on the type of business you choose. You can modify it according to the actual business conditions. More detailed instructions can be found in the [Cache Rules](#) instructions.

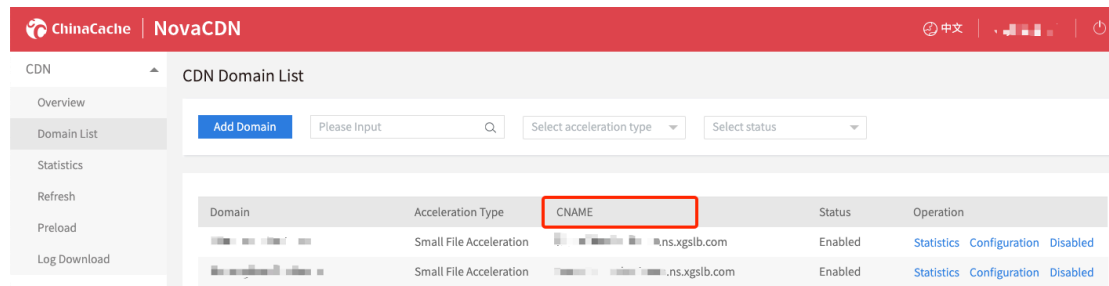
5.Domain submitted

The submitted domain will appear in the domain list, and configurations will be delivered to the entire network node within 10-30 minutes. Please wait patiently.

Step two : Configure CNAME record

1. Obtain the CNAME address of the CDN domain

Copy the CNAME address assigned by the system from the domain name list in Domain Names in the CDN console.



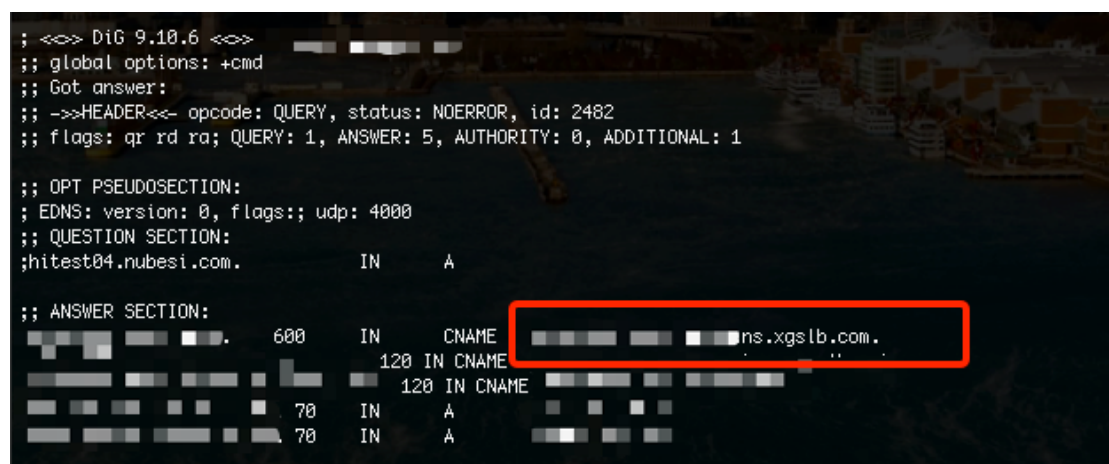
2. Configure CNAME record

Go to the DNS console of your DNS service provider and add the CNAME record.

Instructions of Configuring CNAME record

3. Verify if CNAME is enabled for the domain

After you configure the CNAME record, the CNAME record may take a variable period of time to take effect, depending on your DNS provider. You can use a ping or dig command to access your CDN domain. If the request is redirected to *.ns.xgslb.com, both the CNAME configuration and the CDN service are effective.



Step three : CDN service effective

After you have verified CNAME is enabled for the domain and the CDN service are effective。 You can check [Domain List](#), search [Statistics](#) generated by domain, and [cache refresh](#), etc.

Domain Management

1. Modify domain configuration

Log into the console. Select [Domain List] on the left menu bar, and click [Configuration] in the Action column to enter the self-configure domain page.

For detailed instructions, see Configuration Management.

Noted: The domain in the "In Configuration" state does not support modifying the configuration.

2. Enable domain acceleration

For a domain that is closed, you can enable it. Click [Domain Management] to enter the corresponding page, select the domain to enable the acceleration service, and click [Enable]

3. Disable domain acceleration

For a domain that is in normal operation, you can disable it. The disabled domain configuration will be retained (no need to configure again next time when it is turned on), but will not continue to provide you with acceleration services. To do this, click [Domain Management] to enter the corresponding page and select the domain to turn off the acceleration service, and click [Disable].

Configuration Management

Origin configuration

The origin configuration of the domain can be modified.

1) Multiple IPs

When multiple IPs are configured as the origin, the CDN sends a polling policy to randomly select an IP to return to the origin. The CDN also performs origin detection. Once an origin IP address is found to be abnormal, it will be automatically blocked for a certain period of time (default is 60s), this IP will be skipped when polling.

2) Domain origin

Supports setting the specified domain as the origin. The domain set as the origin needs to be inconsistent with the accelerated domain.

Selecting [Edit] origin information, you can configure the back origin address and back origin HOST

3) Backup origin

After getting the error when back to the primary origin (including 4XX, 5XX error code and TCP connection error), it will directly return to the hot standby origin.

Configuring a hot standby origin can effectively reduce the failure rate of returning to origin and improve the quality of service. Currently only supports IP backup origin settings.

4) Back to origin HOST settings

The origin HOST refers to the domain of the site accessed by the origin during the return process of the CDN node. The origin HOST is the accelerated domain by default. You can also configure the custom origin HOST according to your business situation.

Change origin configuration

1. View configuration

Log into the CDN console. Go to [Domain Management] and find the line of the domain you need to edit. Click [Configuration] in the operation bar. And on the "Basic Configuration" page, you can see the origin information module which you can view the current origin configuration of the domain.

Origin Information [Edit](#)

Origin Type **multiple Ips**

Origin address **2.2.2.2**

Backup origin type **IP**

Backup origin address **1.1.1.1**

Source HOST [?](#) **Default**

Origin address can be configured as multiple IP modes, or one domain

2. Modify origin information

- Click the [Edit] button on the right side of the origin information to modify the origin.
- The origin address can be configured as multiple IP modes, or one domain
- The backup origin only supports IP settings.
- By default, the source HOST is the configured acceleration domain. You can also customize the source HOST according to the service.

3. Configuration example

User access: [http:// test.nubesi.com/p1.jpg](http://test.nubesi.com/p1.jpg) and does not cache on the node.

- If the source configuration is as follows

Origin Information

Origin Type ☐ multiple Ips ☒ Domain

Origin address

Backup origin type ☐ IP ☒ Domain

Backup origin address

Source HOST [?](#) ☒ Default ☐ Customize

The source request is sent to www.origin.a.com. If 1.1.1.1 returns 200, then the node will return the successfully obtained content to the requesting client, and the client successfully obtains the image.

The source HOST defaults to the accelerated domain. The corresponding A record is 1.1.1.1. for test.nubesi.com. The actual request is sent to 1.1.1.1 when back to origin and the resources obtained are: Http://test.nubesi.com/p1.jpg.

- If the source configuration is as follows

Origin Information

Origin Type ☐ multiple Ips ☒ Domain

Origin address

Backup origin type ☐ IP ☒ Domain

Backup origin address

Source HOST ☐ Default ☒ Customize

The source HOST is set to test.a.com, and the actual request is sent to 1.1.1.1 when back to origin and the resources obtained are: Http://test.a.com/p1.jpg.

Cache configuration

What is the cache configuration

Cache configuration refers to the user's customized cache expiration time (TTL) rule for the specified resource content.

NovaCDN has following default cache policies:

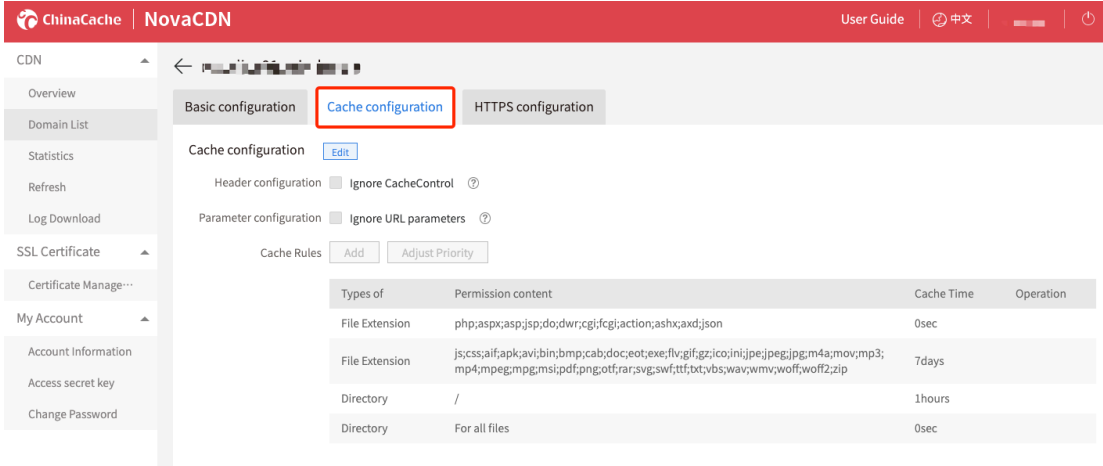
- Honor origin cache headers, this can be disabled by ticking the “ignore CacheControl” option.
- Include query parameter in cache key, this can be disabled by ticking the “ignore URL parameters” .
- If “ignore CacheControl” is ticked, or if origin response header does not contain cache-control/expires/pragma header, the following cache rules take effect.
 - No cache for “php;aspx;asp;jsp;do;dwr;cgi;fcgi;action;ashx;axd;json” , this can be changed or removed by user.
 - Cache 7 days for
 “js;css;aif;apk;avi;bin;bmp;cab;doc;eot;exe;flv;gif;gz;ico;ini;jpe;jpeg;jpg;m4a;mov;mp3;mp4;mpeg;mpg;msi;pdf;png;otf;rar;svg;swf;ttf;txt;vbs;wav;wmv;woff;woff2;zip” , this can be changed or removed by user.
 - Cache root URL and contents for 1 hour, this can be changed or removed by user.
 - No Cache for all other contents, this default rule is always having lowest priority, it can be changed but can NOT be removed by user.
- Regular expression: “/” means the directory and the files under that direct directory (does not include sub-folders). “/.*” means the directory and sub-folder and the files under that direct directory and sub-folders.

- Priority of caching rules: priority is determined based on the order of the cache rules in the list; the rule on the top has highest priority and one in the bottom has lowest priority.

Edit Cache Configuration

1. View configuration

Log into the CDN console, go to [Domain Management], find the line of the domain you need to edit, click [Configuration] in the action bar, and you can see the cache configuration information on the "Cache Configuration" page.



The screenshot shows the ChinaCache NovaCDN console interface. The left sidebar contains navigation links: Overview, Domain List, Statistics, Refresh, Log Download, SSL Certificate, Certificate Manage..., My Account, Account Information, Access secret key, and Change Password. The main content area has three tabs: Basic configuration, Cache configuration (highlighted with a red box), and HTTPS configuration. Under the Cache configuration tab, there are sections for Header configuration (Ignore CacheControl), Parameter configuration (Ignore URL parameters), and Cache Rules. The Cache Rules section includes an 'Add' button and an 'Adjust Priority' button. Below these are four rows of configuration data:

| Types of | Permission content | Cache Time | Operation |
|----------------|--|------------|-----------|
| File Extension | php;asp;aspx;jsp;do;dw;cgi;fcgi;action;ashx;axd;json | 0sec | |
| File Extension | js;css;ai;f;apk;avi;bin;bmp;cab;doc;eot;exe;flv;gif;gz;ico;ini;jpeg;jpg;m4a;mov;mp3;mp4;mpeg;mpeg;msi;pdf;png;otf;rar;svg;swf;tif;txt;vbs;wav;wmv;woff;woff2;zip | 7days | |
| Directory | / | 1hours | |
| Directory | For all files | 0sec | |

2. Modify the cache configuration

Click [Edit]. You can add cache time configuration to the default configuration according to your business needs. CDN supports three types of cache expiration time settings.

1) Set the cache expiration time by file extension

New cache rule

Cache Type

☒ File Extension ☐ Directory

Cache Content

Input the file extension with a semicolon,e.g.js;css;png

Cache Time

sec

Confirm

Cancel

The file extension can be filled by setting the cache time based on the file type.

The cached content can be filled in at the same time, each item is separated by

“English semicolon” . The content is case-sensitive, and must be a file suffix starting with “English period” . When the cache time is set to 0, it means that the file is not cached, and all requests are forwarded to the user origin.

2) Set the cache expiration time by directory

New cache rule

Cache Type

☐ File Extension ☒ Directory

Cache Content

The directory must be a directory beginning with “/” , such as /abc, the path to the entire site is /*

Cache Time

sec

Confirm

Cancel

The directory path can be populated by setting the cache time based on the directory. Multiple cache contents are separated by “;” the content is case sensitive and must be a directory beginning with “/” , the path to the entire site is /*

3. Cache priority

Click [Adjust Priority] to customize the cache expiration configuration order that has been added.

Use the up and down arrows on the right to adjust the order of cache expiration time configuration and click [Confirm] to complete the adjustment.

Cache Rules

| Types of | Permission content | Cache Time | Operation |
|-----------|---|------------|-----------|
| file | php;aspx;asp;jsp;do;dwr;cgi;fcgi;action;ashx;axd;json | 0sec | ▼ ▲ |
| file | shtml;html;htm;js | 12hours | ▼ ▲ |
| directory | / | 1day | ▼ ▲ |

Priority is determined based on the order of the cache roles in the list, the role on the top has higher priority.

HTTPS configuration

What is HTTPS?

HTTPS is a security protocol for transmission encryption based on the HTTP protocol, which can effectively guarantee data transmission security. When you configure HTTPS, you need to provide a certificate corresponding to the domain name and deploy it on the CDN node of the entire network to implement data encryption and transmission on the entire network.

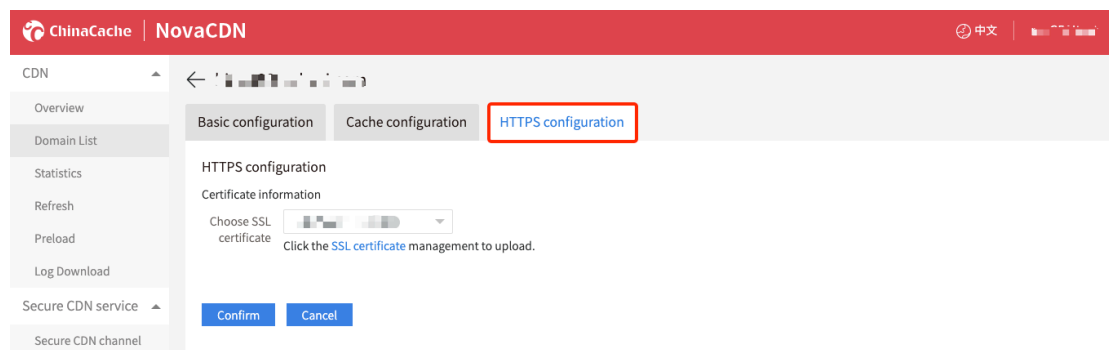
Configuration Guide

1. View HTTPS configuration

Log in to the CDN console, go to [Domain Name Management], find the line of the domain name you need to edit, click [Configuration] in the action bar, and you can see the configuration information on the HTTPS Configuration page.

2. Enable HTTPS configuration

To upgrade the HTTPS protocol acceleration from HTTP, click the [Edit] button and select the certificate to be used. If the certificate status is "Normal", it will appear in the certificate list. If there is no certificate, you need to enter the [SSL certificate management](#) upload.



Refresh

What is refresh?

Refresh means force to clear out cached content of the CDN node. There are two ways to do this:

File refresh: Forces the refreshed URL to be deleted on the CDN node. When there is a new request, it will return to the source to grab the content.

Directory refresh: All files in the directory are expired on the CDN node. When there is a new request, the source is checked back and processed according to the mechanism of file expiration processing.

Why do I need to refresh?

When the resource cached to the CDN node expires, the node will mark the content as expired, but will not delete it and will not actively return the source.

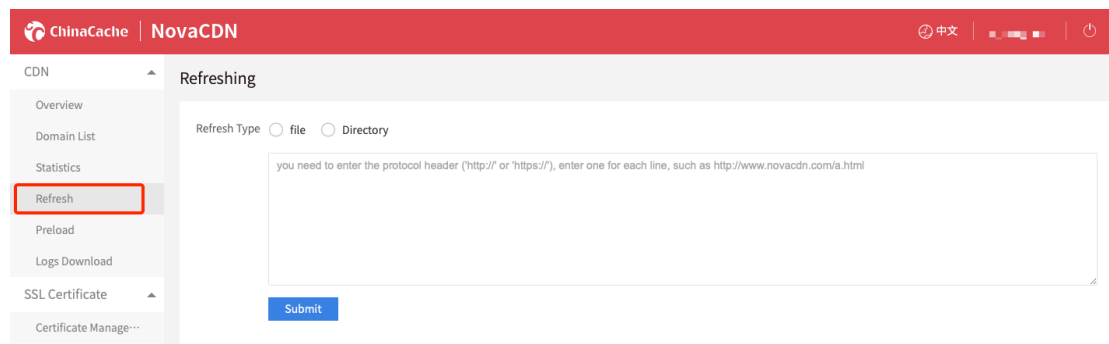
When a user requests an expired content, the node will return the last-modified (last change time) of the source check file. If the content on the node is consistent with the last-modified content of the source station, the file of the source station is not updated, and the node returns the previously cached file directly to the user; if the last-modified of the source file is inconsistent with the node, it is considered The source station file has been updated, and the node will recapture a content at the source station and return it to the user and cache it on the CDN node to delete the previous expired content.

Therefore, when the content of the source station needs to be updated by the user as soon as possible, the content needs to be expired by manually submitting the refresh, so that the user can access the latest content.

Operational guidance

1. Submit refresh task

Log in to the console and click [Refresh] on the left navigation bar to enter the refresh page.



- 1) Select the refresh type
- 2) Enter the URL you want to refresh in the text box (you need to enter the protocol header "http://" or "https://"), enter one for each line, such as

File refresh : http://www.example.com/test

Directory refresh : https://www.example.com /image/
- 3) Click [Submit] when finished.

Note :

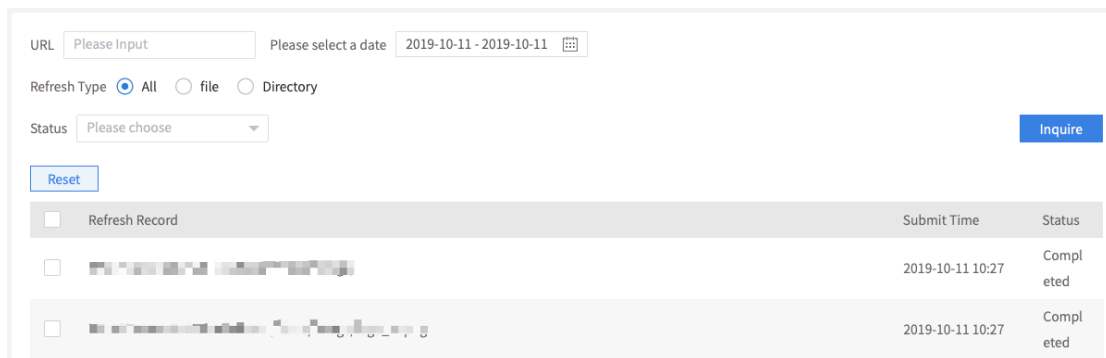
The maximum number of file refreshes submitted in a single time is no more than 20, and the maximum number of files per day is less than 500;

The maximum number of catalog refreshes submitted in a single submission is no more than 20, and no more than 500 per day;

The refresh task usually takes effect in 10 minutes.

2. View refresh record

You can view the refresh record for a period of time on the page. Fill out information like the refresh the URL, time, operation type, status and fill in and select, click [Query] to view.



The screenshot shows a web interface for querying refresh records. It includes a form with the following fields and controls:

- URL:** A text input field with the placeholder "Please Input".
- Please select a date:** A date range selector showing "2019-10-11 - 2019-10-11" with a calendar icon.
- Refresh Type:** Radio buttons for "All" (selected), "file", and "Directory".
- Status:** A dropdown menu with the placeholder "Please choose".
- Buttons:** A blue "Reset" button and a blue "Inquire" button.

Below the form is a table displaying the refresh records:

| <input type="checkbox"/> | Refresh Record | Submit Time | Status |
|--------------------------|----------------|------------------|-----------|
| <input type="checkbox"/> | [Redacted] | 2019-10-11 10:27 | Completed |
| <input type="checkbox"/> | [Redacted] | 2019-10-11 10:27 | Completed |

For a task that fails to refresh, it supports a refresh reset. Note that after the reset, a new refresh task will be displayed in the list.

Preload

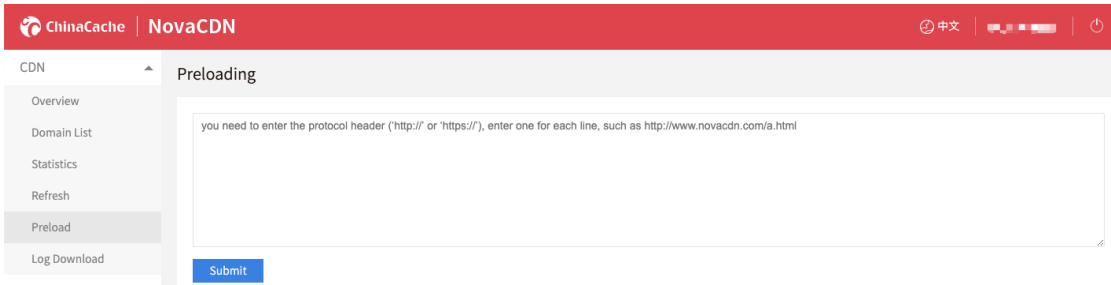
What is preload?

Preloading simulates the user's first request on all CDN nodes, allowing specific content to be cached in each node. In this way, the user's first request will not return to the source because there is no content on the node, and the CDN node directly returns the resource requested by the user.

Operational guidance

1. Submit a preload task

Log in to the console and click [Preload] on the left navigation bar to enter the preload page.



- 1) Enter the URL of the object to be preloaded in the text box (note that you need to add the protocol header "http://" or "https://"), enter one for each line, such as
http://www.example.com/test.html
https://www.example.com/test.jpg

- 2) Click [Submit] when finished.

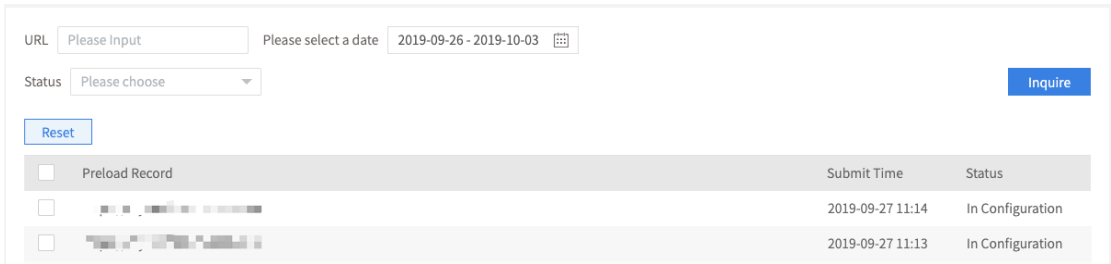
Note:

The maximum number of pre-loaded URLs submitted in a single time is no more than 30, and no more than 1000 in a day.

The preloading task usually takes effect in 10 minutes.

2. View preload record

You can view the preloading records for a period of time on the page. Complete the filling and selection of URLs, time, and status, and click [Query] to view.



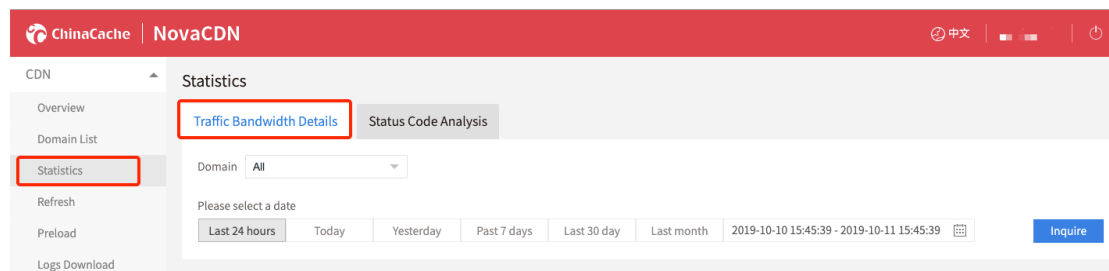
| <input type="checkbox"/> | Preload Record | Submit Time | Status |
|--------------------------|----------------|------------------|------------------|
| <input type="checkbox"/> | [REDACTED] | 2019-09-27 11:14 | In Configuration |
| <input type="checkbox"/> | [REDACTED] | 2019-09-27 11:13 | In Configuration |

For failed task support reset, note that a new preload task will be displayed in the list after reset.

Statistical Analysis

Traffic bandwidth breakdown

Log in to the console, click [Statistics] on the left navigation bar, and click [Traffic Bandwidth Details] to enter the page.

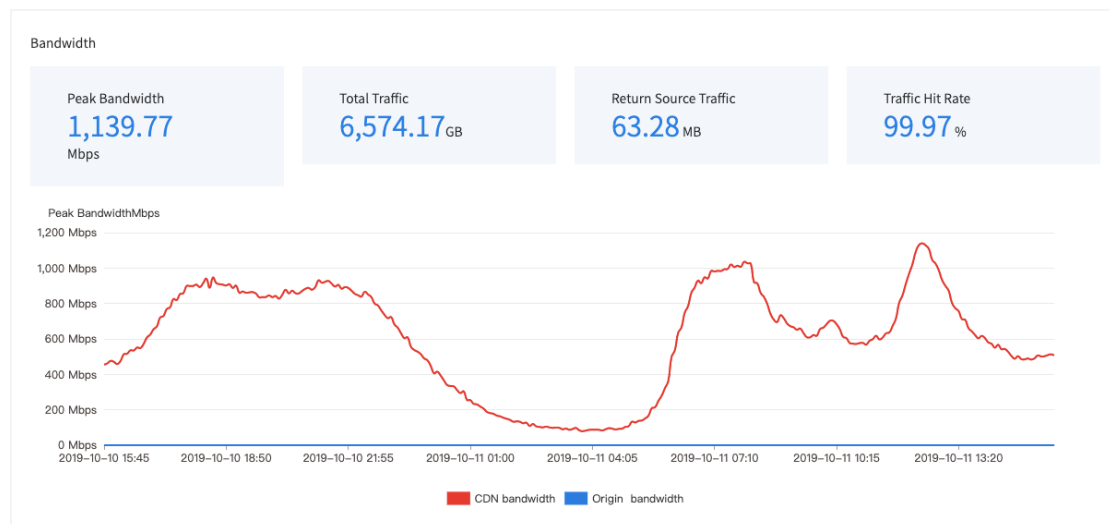


Query conditions

- 1) Accelerate domain name: support specified domain name query
- 2) Time interval: The time span of a single query is up to 31 days

Result data

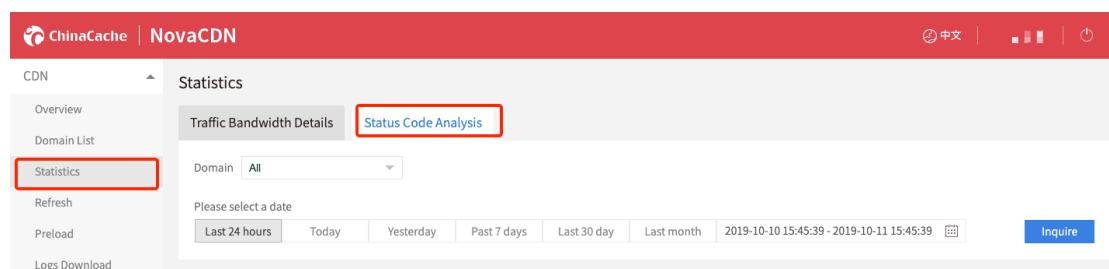
After selecting the query conditions, click [Search], you can view the total traffic, return source traffic, total requests, number of return requests, and CDN bandwidth and return bandwidth curves in the selected time interval. Support for downloading reports for you to view detailed bandwidth data.



1. The minimum granularity of traffic and bandwidth statistics is 5 minutes.
2. In the specified time zone, you cannot query the traffic bandwidth details that have not been connected to the CDN service or have accessed and deleted the domain name.

Status code analysis

Log in to the console, click [Statistics] on the left navigation bar, and click [Status Code Analysis] to enter the page.

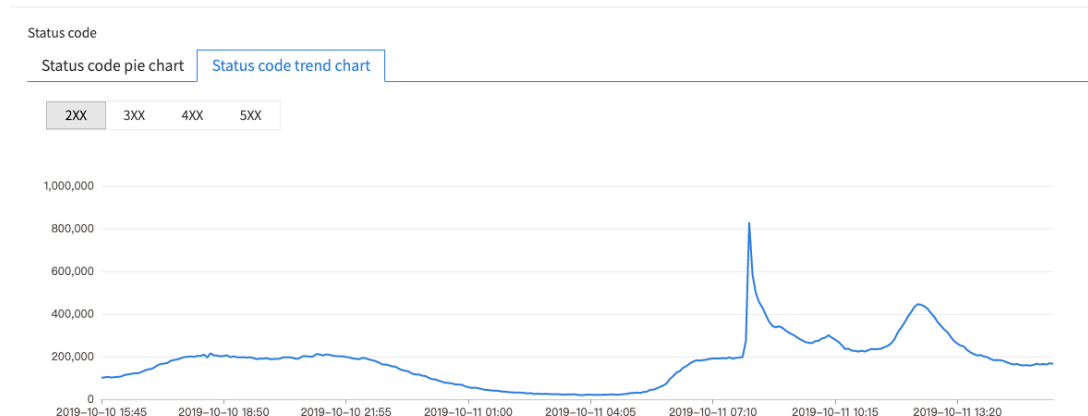
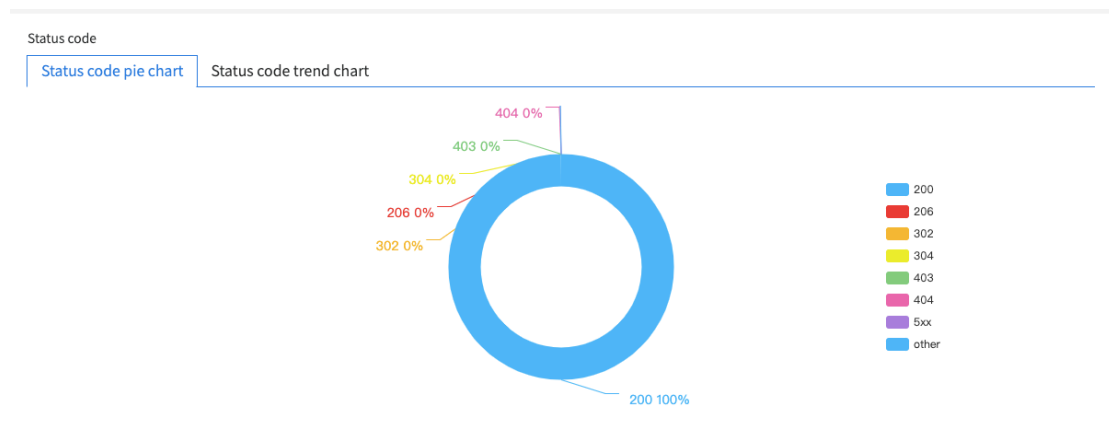


Query conditions

- 1) Accelerate domain name: support specified domain name query
- 2) Time interval: The time span of a single query is up to 31 days

Results data

You can view the percentage analysis and distribution pie chart 、trend chart of the return status code.



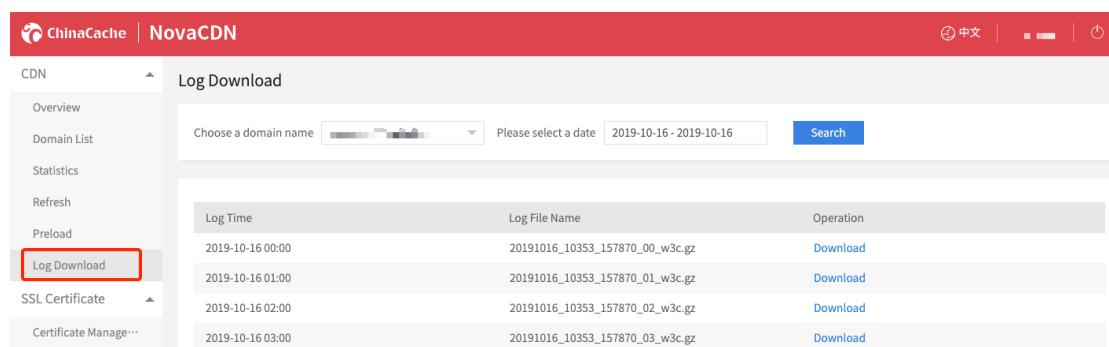
- 1) Support 2xx, 3xx, 4xx, 5xx status code statistics, other status code will be generalized as 'other'
- 2) Status code distribution: view status code, request details and request percentages.
- 3) The shortest interval for status code statistics is 5 minutes.

4) In the specified time zone, status code statistics cannot be queried for the domains that have not been configured for CDN service or the ones are already offline.

Log download

Log download

Login to portal, click on [Log download] on the left navigation bar, enter log download page.



| Log Time | Log File Name | Operation |
|------------------|---------------------------------|--------------------------|
| 2019-10-16 00:00 | 20191016_10353_157870_00_w3c.gz | Download |
| 2019-10-16 01:00 | 20191016_10353_157870_01_w3c.gz | Download |
| 2019-10-16 02:00 | 20191016_10353_157870_02_w3c.gz | Download |
| 2019-10-16 03:00 | 20191016_10353_157870_03_w3c.gz | Download |

Select the domain name and date, click on [Search] to get logs download link.

1. Support logs download in last 30 days.
2. Provide daily logs download.
3. The logs for the day will be available the next day.

Log field description

The corresponding field order and meaning in the logs are shown in the following table:

| Order | Log content |
|-------|--|
| 1 | Time stamp |
| 2 | Response time (in millisecond) |
| 3 | Client IP |
| 4 | Edge server status/response client HTTP status code |
| 5 | Response bytes sent to client (in bytes) |
| 6 | Request method |
| 7 | File request path |
| 8 | The username of client authentication request, usually is '-' |
| 9 | Back to origin info, back to origin is 'DIRECT/{origin IP or domain}' not back to origin is 'NONE/-' |
| 10 | Response data type |
| 11 | Refer information |
| 12 | User-Agent information |
| 13 | Cookie information |

SSL certificate management

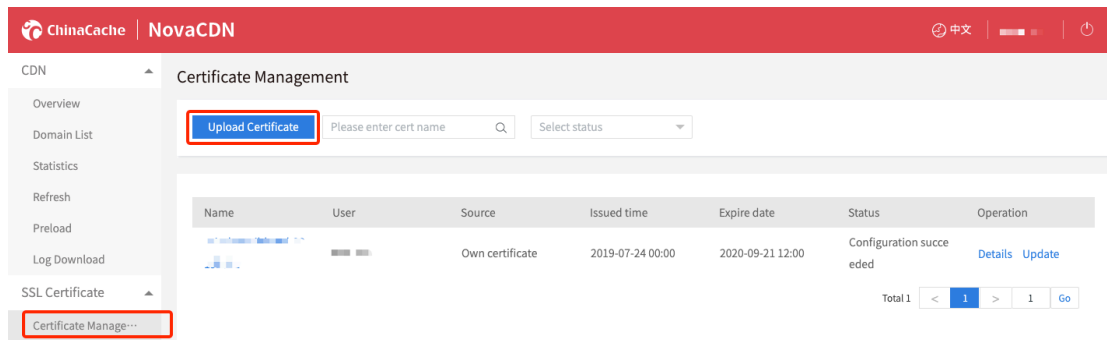
You can upload your own certificate through the SSL Certificate Services

Console and view the certificate details through the certificate list. The certificate you uploaded will be pushed to the CDN service.

Operation guide

1. Upload SSL certificate

Login to portal, click [SSL Certificate]->[Certificate Management] to enter the certificate management list. click [Upload Certificate] to enter the certificate information.



Fill in the certificate name, and paste the contents of certificate and private key into the text box. You can add a comment to distinguish the certificate.

Fill in the contact email and we will send you a notification before the certificate expires based on the reminder time you set.

Click [Submit] and the CDN will send the certificate to the edge node. You can view the certificate configuration status on the [Certificate Management] page.

← Upload Certificate

• Name

• Certificate

• Private Key

Remarks

• Contact email

Expiration reminder

Note:

- Please upload certificate that will not expire in 30 days

- Certificate should be in PEM format, other format please convert on https://myssl.com/cert_convert.html
- When your certificate has a certificate chain, please paste the contents of the CA certificate (PEM format) at the end of the domain name certificate (PEM format) to complete the certificate chain.

2. View certificate details

Login to portal, click [SSL Certificate]->[Certificate Management] to enter the certificate management list. Click [Details] to check the certificate information and associated CDN service.

The screenshot shows a web interface for managing SSL certificates. At the top, there is a breadcrumb trail: < Certificate Management > Details. Below this, the 'Certificate information' section displays the following details: Name (redacted), Source (Self-uploaded Certificate), Creation time (2019-10-18 00:00), Expire date (2020-10-17 12:00), Status (Configuration succeeded), Contact email (redacted), and Remarks (redacted). Below the certificate information, the 'CDN Services' section contains a table with two columns: 'Associated CDN service' and 'Status'. The table shows one entry with a redacted service name and a status of 'Enabled'.

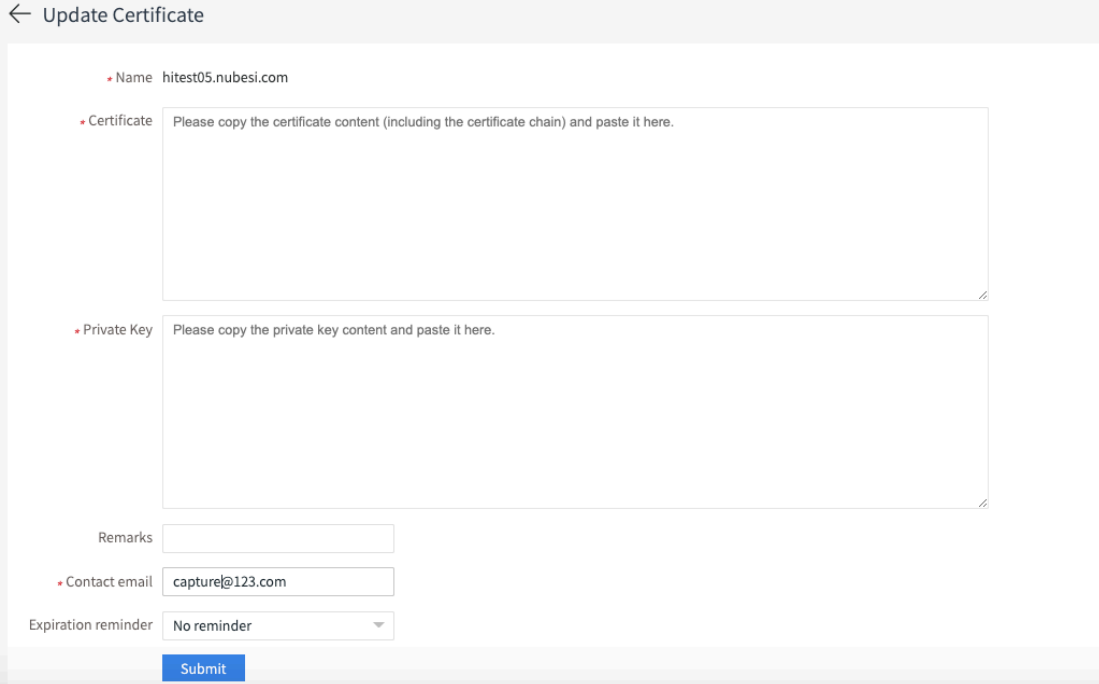
| Certificate information | |
|-------------------------|---------------------------|
| Name | [Redacted] |
| Source | Self-uploaded Certificate |
| Creation time | 2019-10-18 00:00 |
| Expire date | 2020-10-17 12:00 |
| Status | Configuration succeeded |
| Contact email | [Redacted] |
| Remarks | [Redacted] |

| CDN Services | |
|------------------------|---------|
| Associated CDN service | Status |
| [Redacted] | Enabled |

3. Update certificate

When your certificate is about to expire, please update the certificate in time in order not to affect the normal use of the business.

Login to portal, click [SSL Certificate]->[Certificate Management] to enter the certificate management list. Click [Update] to enter the update certificate page. Paste the new certificate content and private key content into the text box, you can optionally modify the note information and expiration reminder settings. Click [Submit], the CDN will send the certificate to the edge node, and modify the certificate configuration of the CDN service associated with the certificate. You can view the certificate configuration status on the [Certificate Management] page.



The screenshot shows a web form titled "Update Certificate" with a back arrow icon. The form contains the following fields and controls:

- Name:** A text field containing "hitest05.nubesi.com".
- Certificate:** A large text area with the placeholder text "Please copy the certificate content (including the certificate chain) and paste it here." and a small icon in the bottom right corner.
- Private Key:** A large text area with the placeholder text "Please copy the private key content and paste it here." and a small icon in the bottom right corner.
- Remarks:** A text field.
- Contact email:** A text field containing "capture@123.com".
- Expiration reminder:** A dropdown menu currently showing "No reminder".
- Submit:** A blue button at the bottom of the form.

Note:

- Please upload certificate that will not expire in 30 days
- Certificate should be in PEM format, other format please convert on

https://myssl.com/cert_convert.html

- When your certificate has a certificate chain, please paste the contents of the CA certificate (PEM format) at the end of the domain name certificate (PEM format) to complete the certificate chain.