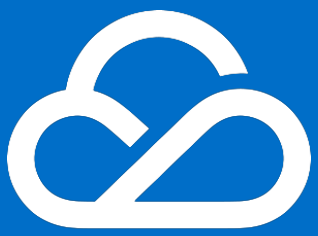
Content Delivery Network

Configuration Management

Product Introduction



Tencent Cloud

Copyright Notice

Trademark Notice

Tencent Cloud

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

Configuration Management

Configuration Overview

CDN supports various custom configurations which allow you to optimize your CDN acceleration according to your business needs.

Basic Configuration

Configuration	Description
Basic Info	Change the project to which a domain belongs, domain's content type
Origin server info	Configure hot slave origin and modify origin server to ensure the success of back-to-origin requests
Hosting Source	Specify the site domain accessed by the CDN node at the origin server

Access Control

Configuration	Description
Filter Parameter Configuration	Specify whether a node will ignore the parameters following the "?" in user request URLs
Hotlink Protection Configuration	Configure HTTP referer blacklist & whitelist
IP Blacklist & Whitelist	Configure IP blacklist & whitelist for access control
IP Access Frequency Limit	Configure access frequency limit of an IP to a single node
Video Drag Configurations	Support to open video drag configuration

Cache Configuration

Configuration	Description
Cache Validity Period Configuration	Configure cache expiration rules for specified resource contents

Origin Configuration

Configuration	Description
Intermediate Node Configuration	Specify whether to use an intermediate node
Range GETs Configuration	Enable/disable Range back-to-origin transmission in slices
Follow 302 Configuration	Configure whether a request should be redirected when the origin server returns the status code 302

Advanced Configuration

Configuration	Description
HTTPS Configuration	Configure HTTPS to achieve a secure acceleration. HTTPS forced redirection is supported
SEO Optimization	Enable SEO optimization configuration to ensure a consistent domain authority on search engines
HTTP Header	Add HTTP header configurations
Capped Bandwidth Configuration	Configure bandwidth cap for domains. When the cap is reached, the CDN service will be disabled and the access request is forwarded to the origin server

Oversea CDN Configuration

Configuration	Description
International Private Line (Beta)	Enable international private line during the use of oversea CDN acceleration service to improve back-to-origin connections

Basic Configurations

Basic Information

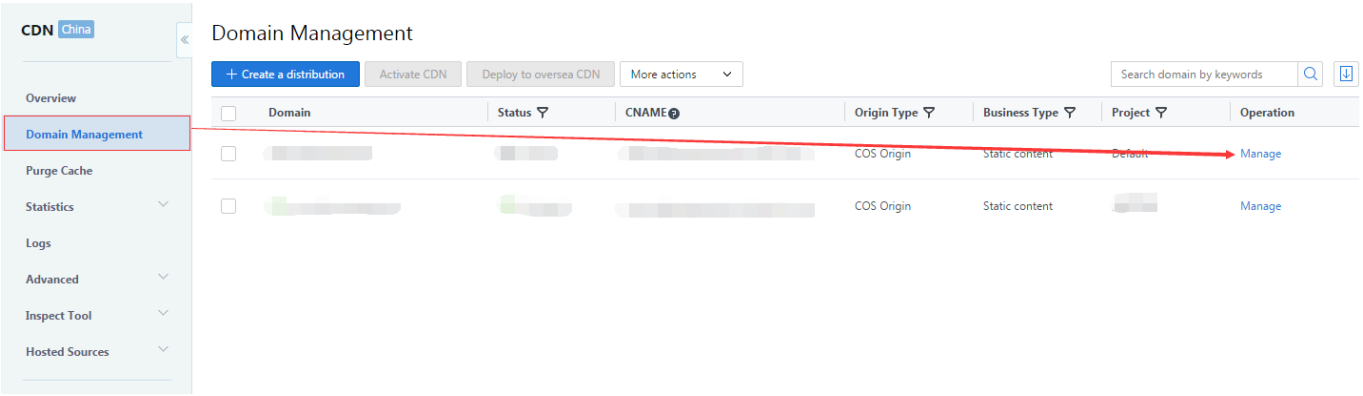
The basic information of a domain includes its accelerated domain, CNAME, time of creation, the project to which it belongs, and its content type.

You can modify a domain's project and content type as necessary.

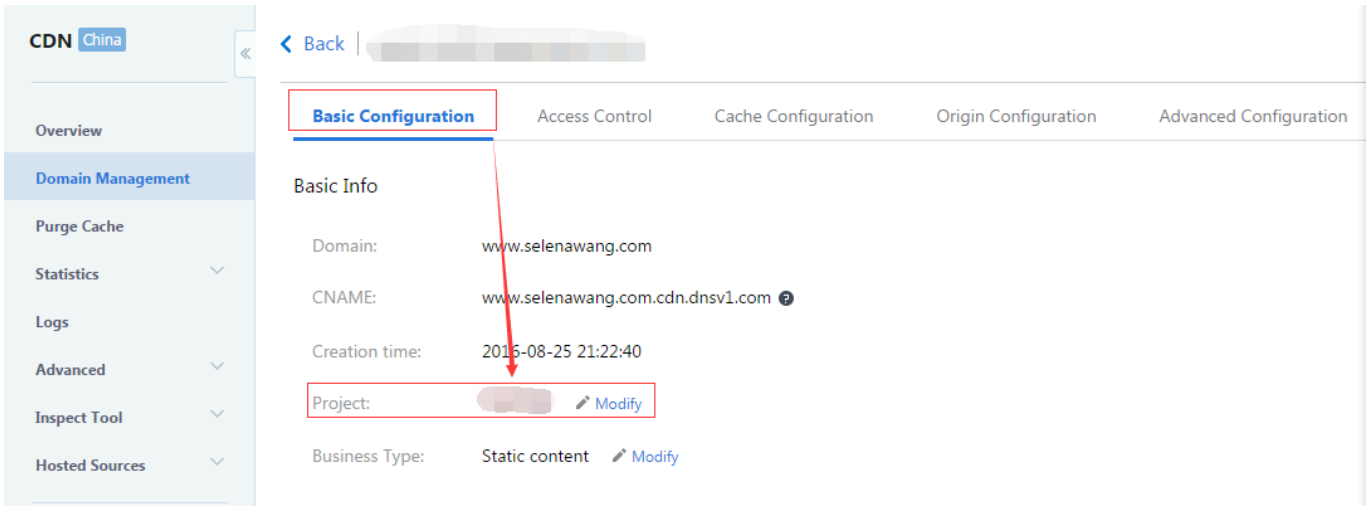
Project

If there are a large number of domains, you can group them into projects for classified management. Click Project Management to view the existing projects.

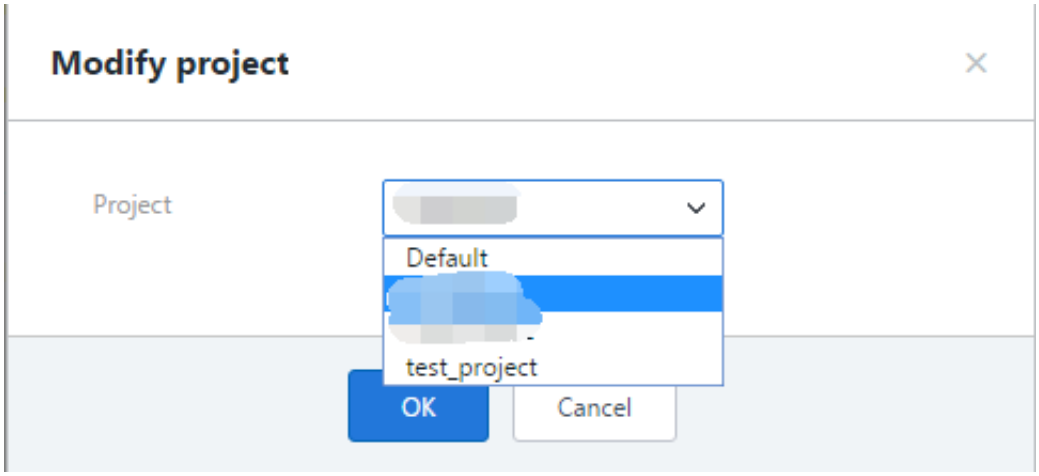
Log in to CDN Console and go to "Domain Management" page. Then click Manage button to the right of the domain name to enter the management page:



You can check the current project to which a domain belongs from Basic info in "Basic Configuration":



Click "Modify" to the right of Project to change the project:



Users who use the CDN permission system should proceed with caution, since this operation may cause changes to the permissions of sub-users.

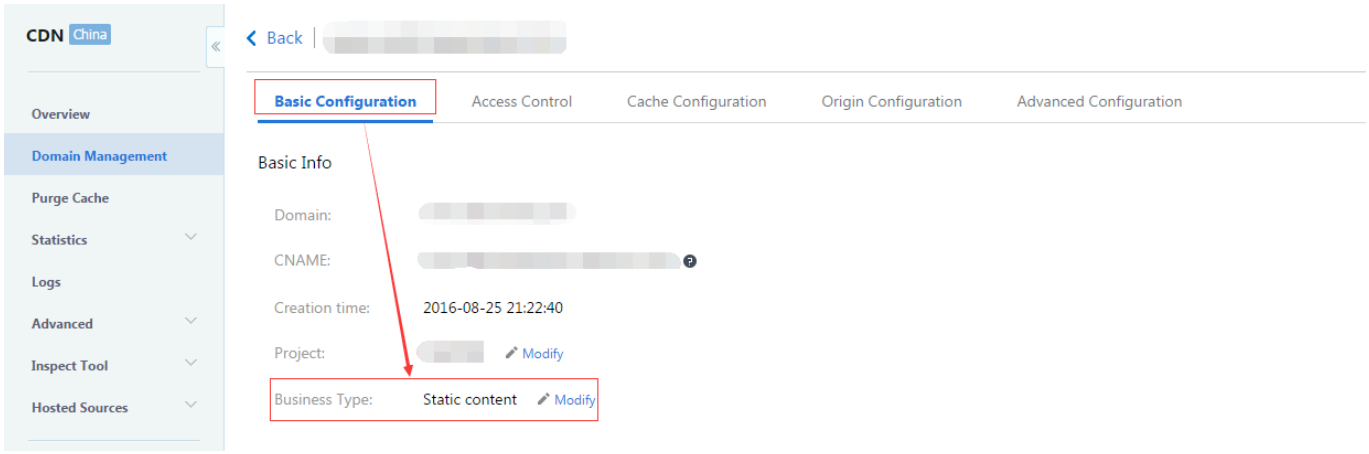
Content Type

The selected content type determines which resource platform will be used by the domain. Acceleration configurations vary with resource platforms. Please choose the content type that matches your business:

- Static content: Suitable for acceleration scenarios for static resources such as e-commerce, websites, game images;
- Media streaming: Suitable for application scenarios such as LVB, ILVB downstream acceleration and VOD acceleration;

- Downloading: Suitable for scenarios such as audio & video source file download, mobile phone firmware delivery.

You can check the current content type of a domain from Basic info in "Basic Configuration":



Click the "Modify" link to the right of Content type to change the content type.

Origin Configurations

You may modify the origin server configuration for your domain:

- Switching between own origin and COS origin is supported;
- You can configure hot slave origin servers for a domain whose connection method is own origin. When a back-to-origin request towards the master origin encounters an error (including 4XX or 5XX error codes and TCP connection error), the request will be forwarded to the slave origin server;
- The switching between master and slave origin configurations is supported.

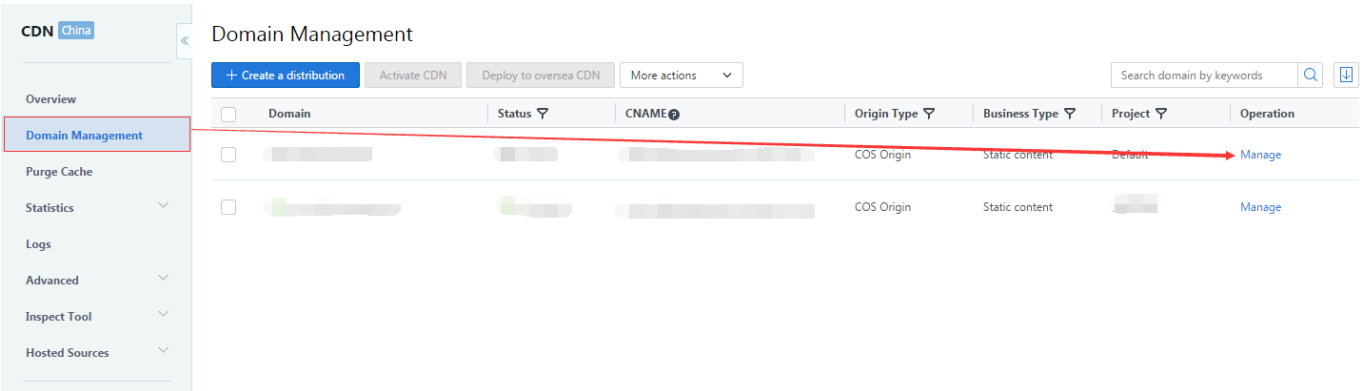
Configuring hot slave origin server can effectively reduce failure rate of back-to-origin requests and improve your business.

HTTPS back-to-origin method is currently not supported by slave origin servers. Please do not choose HTTPS back-to-origin method when configuring certificates for domains with hot slave origin servers.

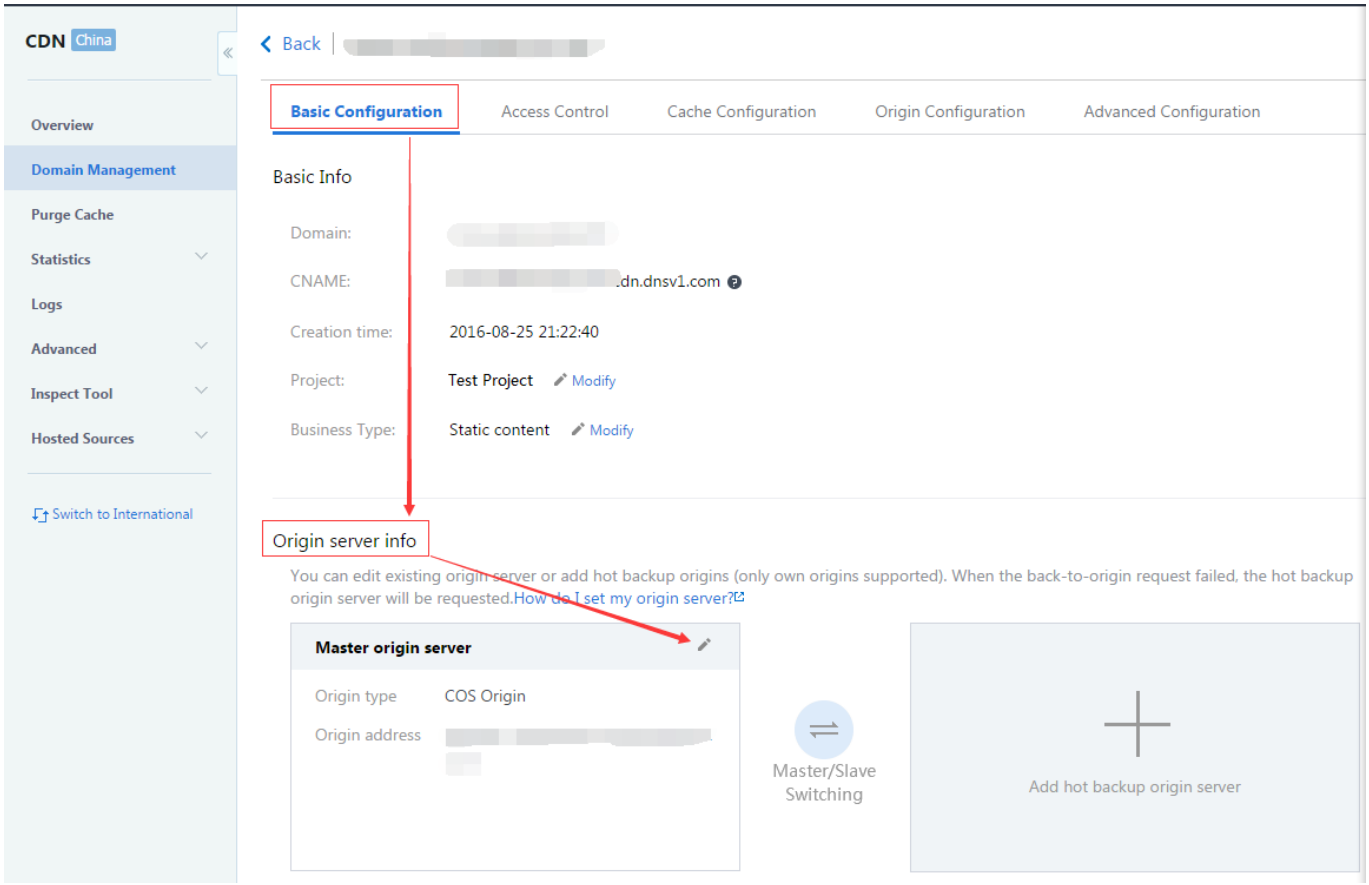
Modifying Origin Server

Switching between own origin and COS origin is supported to provide a higher flexibility.

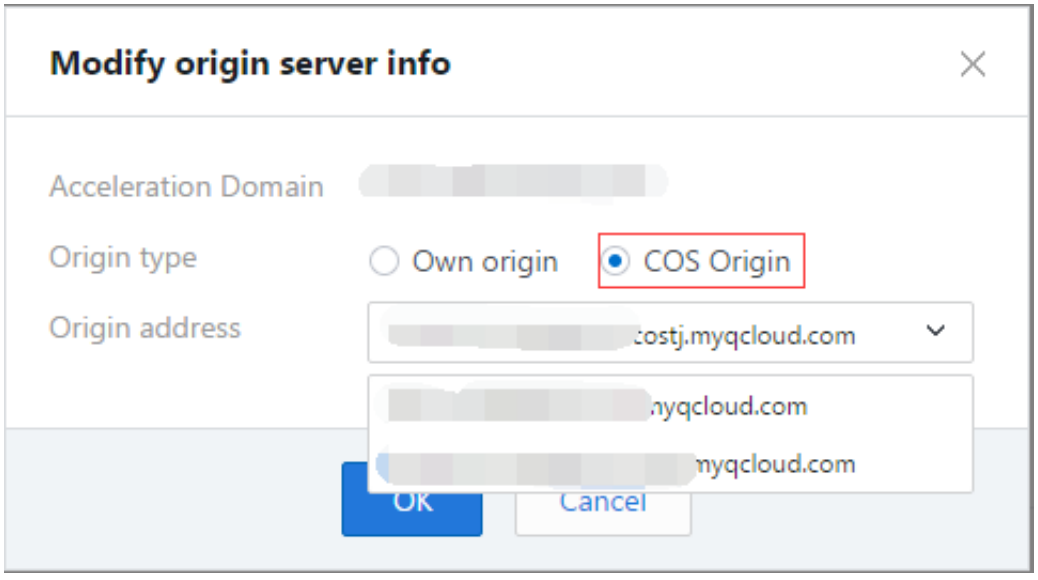
Log in to CDN Console and go to "Domain Management" page. Then click Manage button to the right of the domain name to enter the management page:



Go to Origin Server Info under "Basic Configuration" to view the current origin server configuration of the domain:

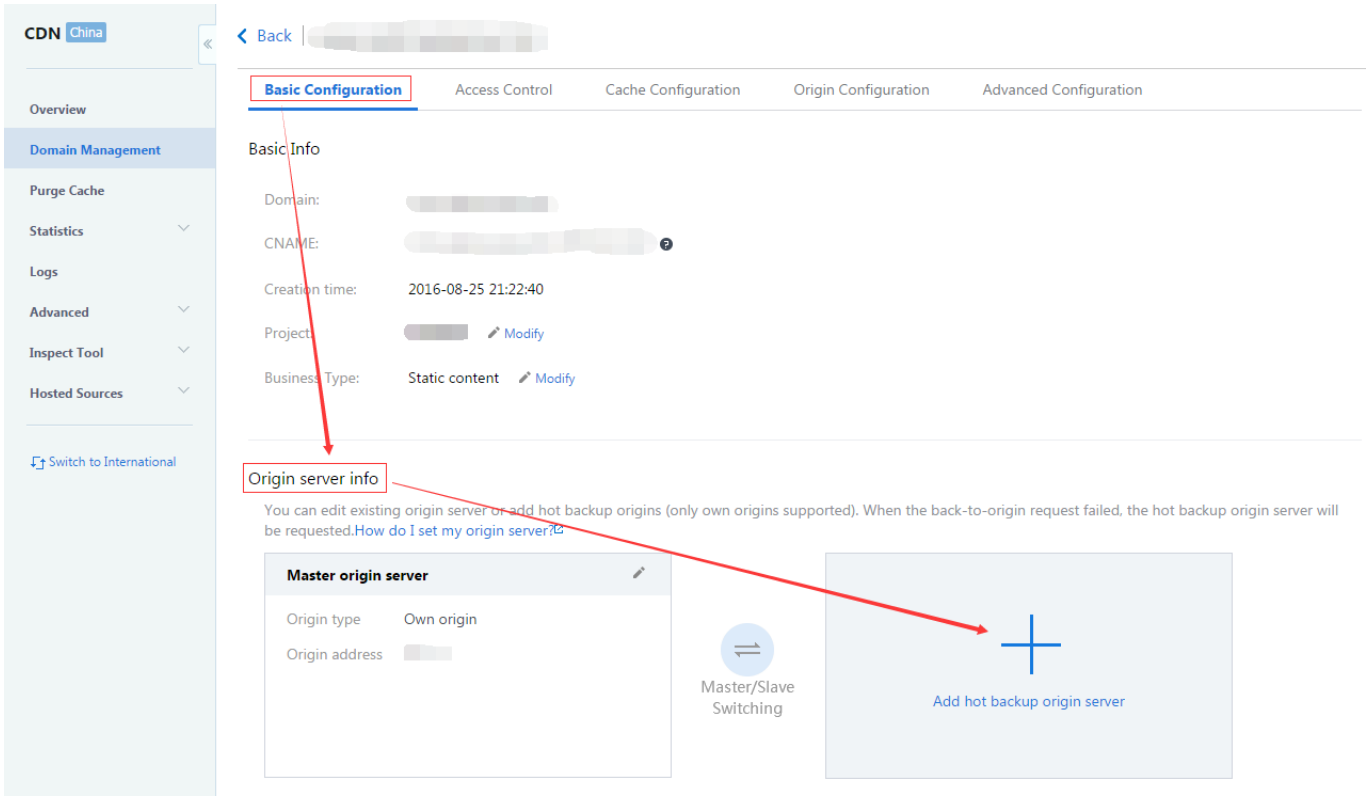


Click the modify button at the top-right corner of the origin server configuration to make changes. Switching between COS origin and own origin is supported:

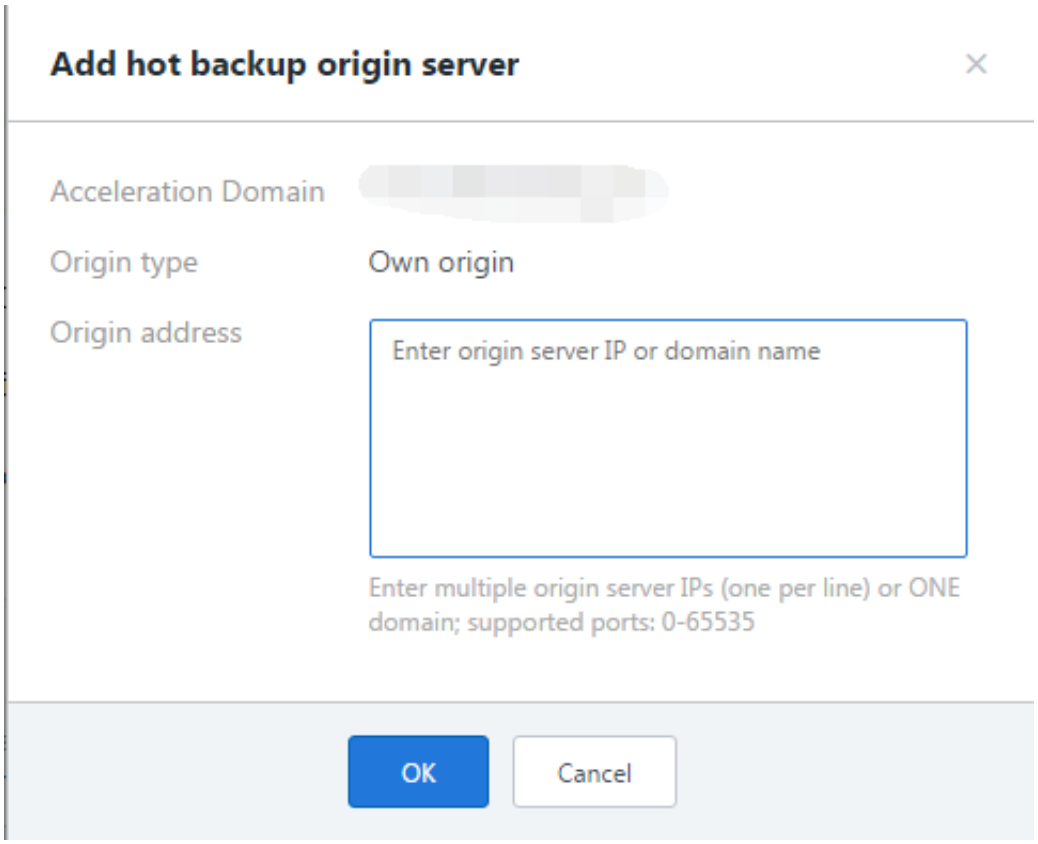


Adding Hot Slave Origin Server

You can add hot slave origin servers for a domain whose connection method is own origin. When a back-to-origin request towards the master origin encounters an error (including 4XX or 5XX error codes and TCP connection error), the request will be forwarded to the slave origin server.

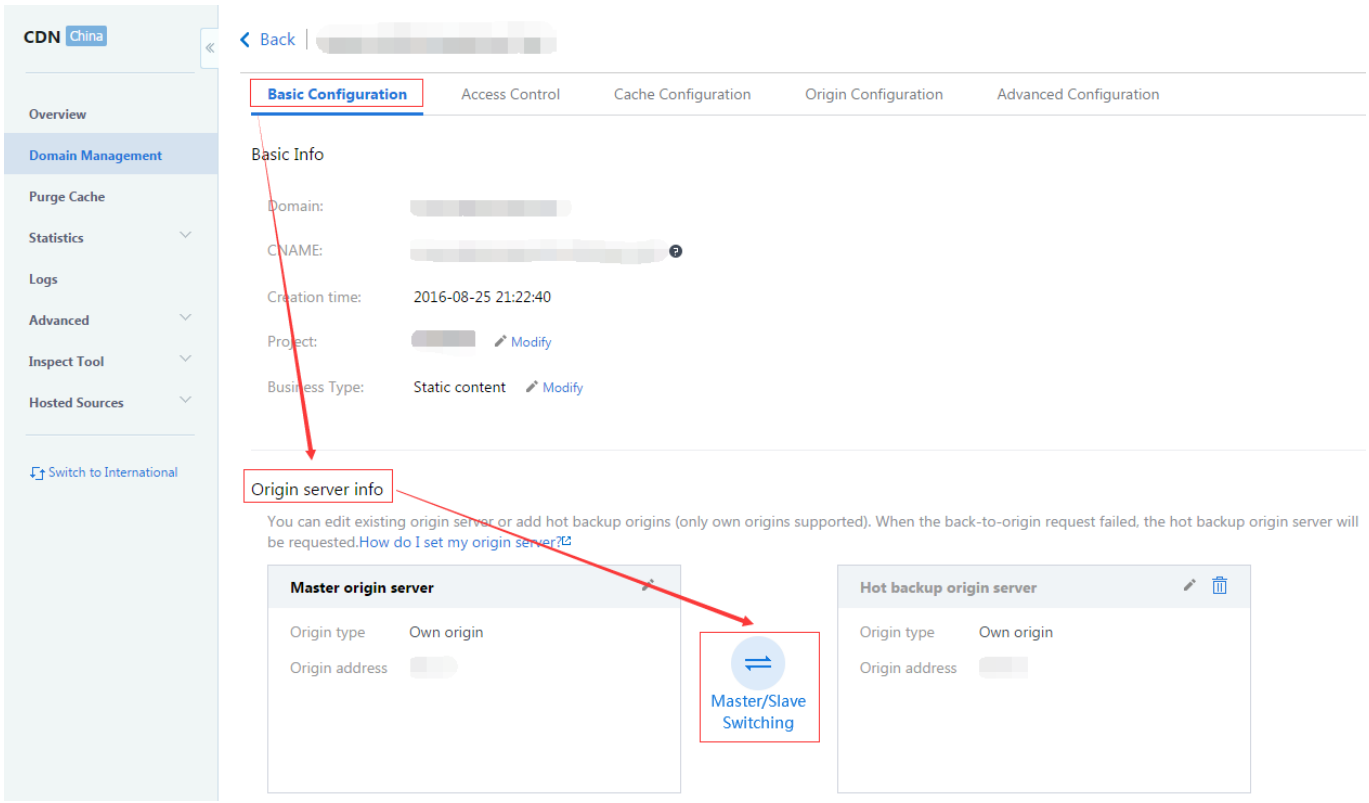


Hot slave origin servers can only be configured as own origins:



Switching between master and slave origin configurations

Once slave origin server is configured, you can witch between the master and slave origin server configurations with one click:


CDN China
Overview
Domain Management
Purge Cache
Statistics
Logs
Advanced
Inspect Tool
Hosted Sources
Switch to International
Back
Basic Configuration
Access Control
Cache Configuration
Origin Configuration
Advanced Configuration
Basic Info
Domain:
CNAME:
Creation time:
2016-08-25 21:22:40
Project:
Modify
Business Type:
Static content
Modify
Origin server info
You can edit existing origin server or add hot backup origins (only own origins supported). When the back-to-origin request failed, the hot backup origin server will be requested.How do I set my origin server?
Master origin server
Origin type
Own origin
Origin address
Master/Slave Switching
Hot backup origin server
Origin type
Own origin
Origin address

Origin HOST Header Configurations

Overview

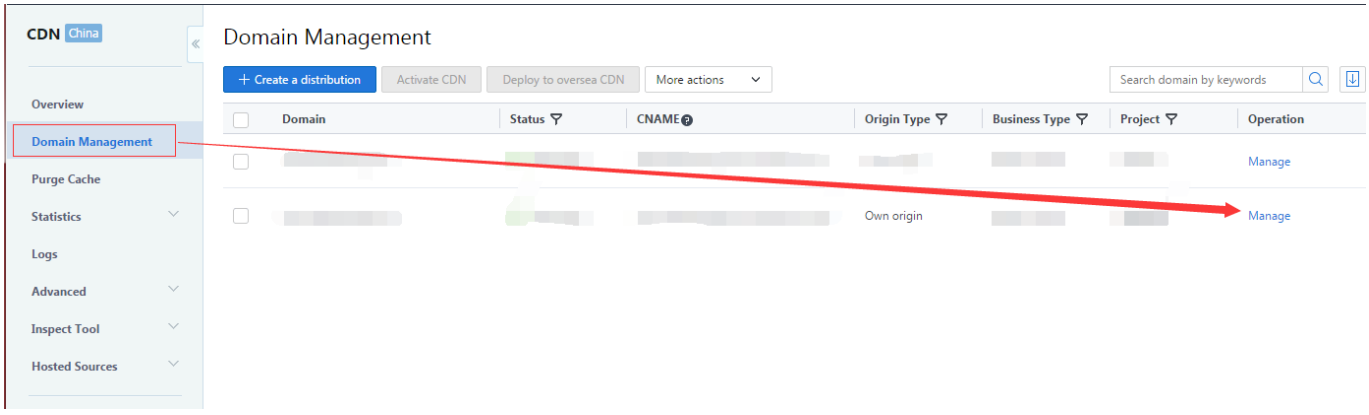
Origin Host Header refers to the site domain accessed by the CDN node at the origin server.

Note:

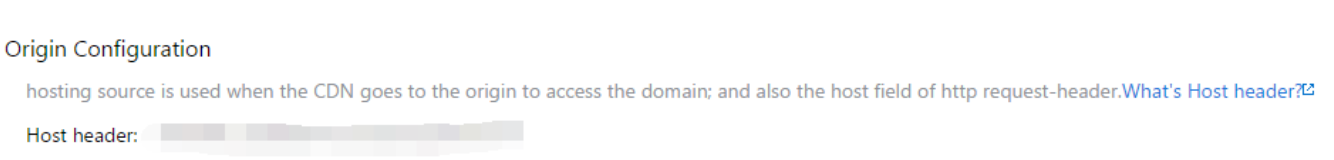
- Origin server and origin host header: The IP/domain configured at the origin server allows the CDN node to find the origin server when it attempts to access the origin. There can be multiple WEB sites on the server, and the hosting source indicates on which site the resource resides.

Configuration Instructions

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

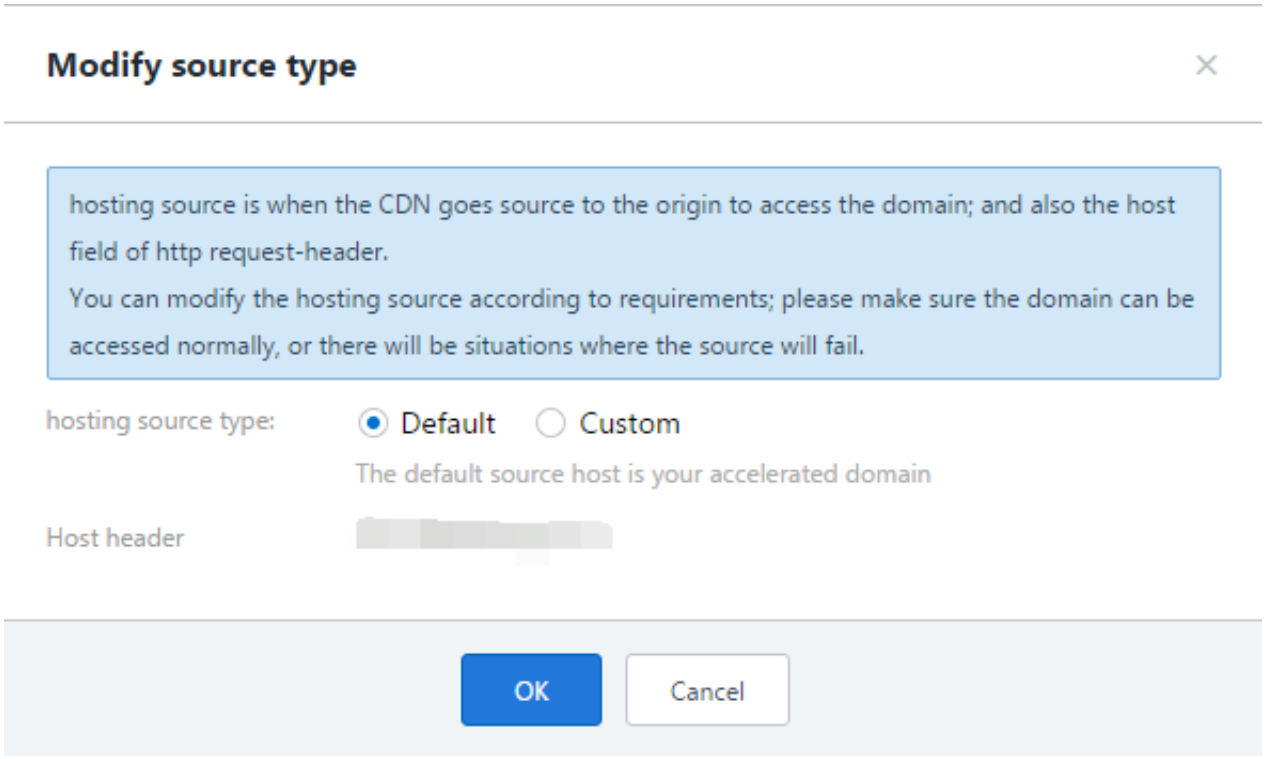


Go to Origin Configuration in "Basic Configuration" to configure hosting source:



Default Configuration

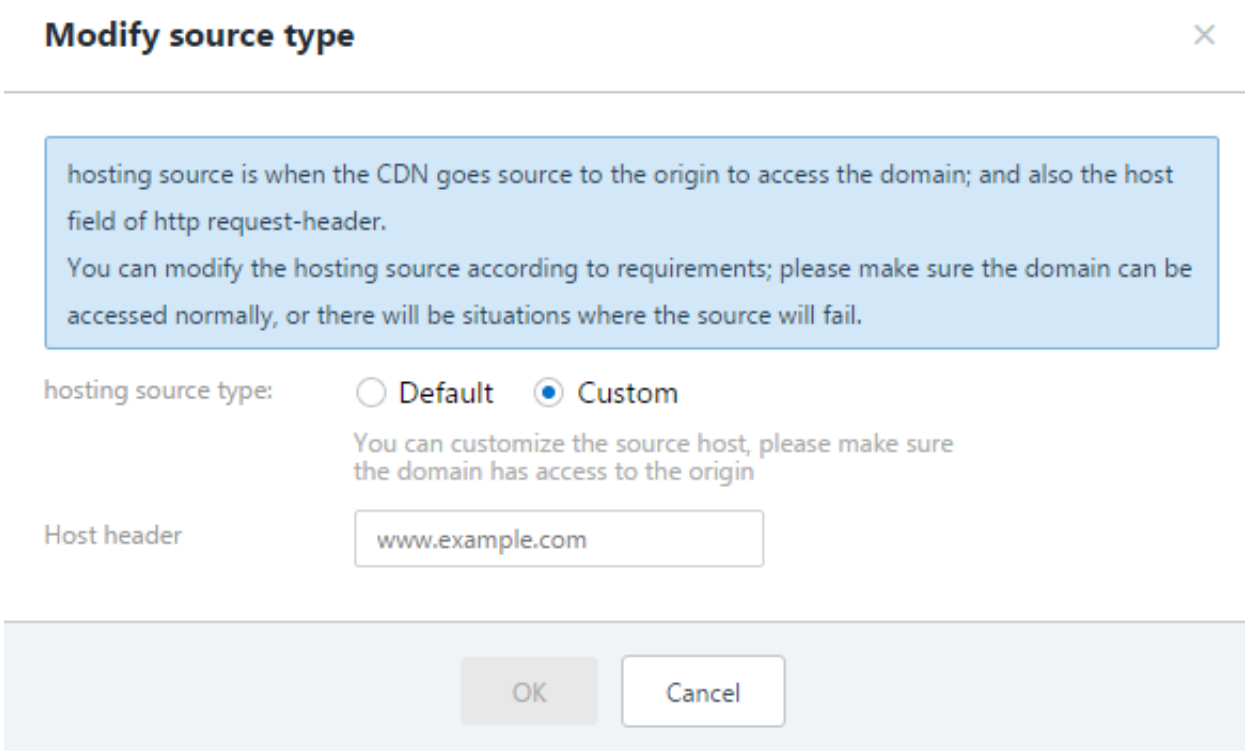
By default, the origin host header of a sub-domain is the configured accelerated domain; The origin host header of a wildcard domain is the access domain:



- If the accelerated domain connected is www.test.com, when the node sends an access request to origin server for the resource under this domain, the host field in the Request HTTP Header will be "www.test.com";
- If the accelerated domain connected is a wildcard domain such as *.test.com, and the access domain is abc.test.com, then the origin host header will be abc.test.com.

Custom Configuration

You can set custom origin host header according to your business needs.



Note

- Currently, the configuration of origin host header is only available for domains with a connection method of Own Origin;
- Please make sure the origin host header domain you set is available for access, otherwise it will cause the failure of back-to-origin request, making your business affected.

Access Control

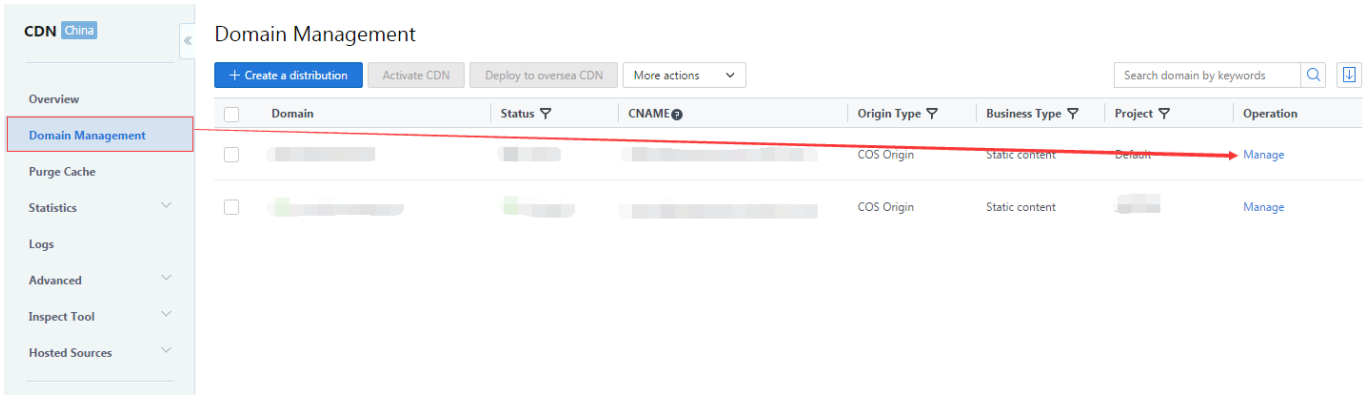
Parameter Filtering

Overview

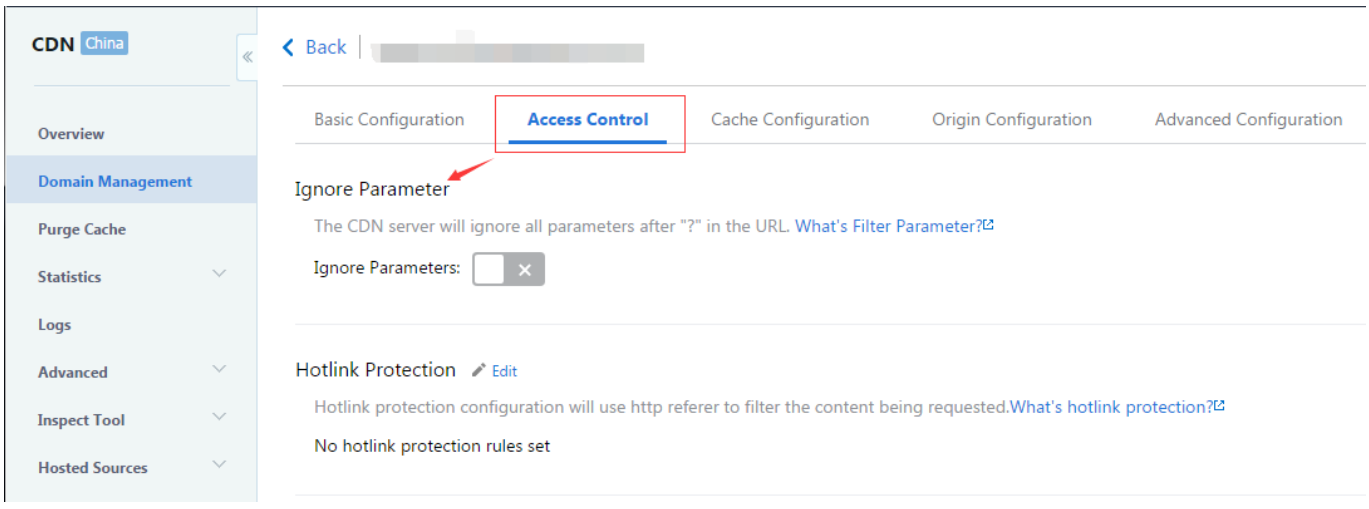
CDN's parameter filtering switch allows you to control whether to filter out parameters following the question mark in the user request URLs based on your business needs. You can use this feature to achieve versioning with flexibility, or to perform Token-based authentication against resources.

Configuration Instructions

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



You can find Ignore Parameter in "Access Control" to set parameter filtering:



Default Configuration

The switch is disabled by default. In this case, parameters following the "?" in user request URLs will not be ignored.

1. For example, if the URL of resource requested by a user is

   http://www.test.com/1.jpg?version=1.1

   , and the requested content is not cached on the node which receives this request, the resource will be acquired from the origin server and then cached to the node;
2. If the user requests for resource with URL:

   http://www.test.com/1.jpg?version=1.1

   again, and the resource has been already cached on the node, the resource will be hit and directly returned to the user;
3. If the user then requests for resource with

   http://www.test.com/1.jpg?version=1.2

   , which does not match the full path of resource because parameter filtering is disabled, thus the resource will be pulled from the origin server again.

Enabling Parameter Filtering

When the parameter filtering configuration is enabled, parameters following the "?" in user request URLs will be ignored.

1. For example, if the URL of resource requested by a user is

   http://www.test.com/1.jpg?version=1.1

   and the content is not cached on the node which receives this request, the resource will be

acquired from the origin server and then cached to the node. With parameter filtering enabled, the resource URL stored by the node will be

http://www.test.com/1.jpg

;

2. If the user requests for resource with URL:

   http://www.test.com/1.jpg?version=1.1

   again, the actual resource that be looked up on the node will be

   http://www.test.com/1.jpg

   , which has already been cached, thus the resource is hit and directly returned to the user;
3. If the user then requests for resource with URL:

   http://www.test.com/1.jpg?version=1.2

   , the actual resource that be looked up on the node will be

   http://www.test.com/1.jpg

   , which has already been cached, thus the resource is hit and directly returned to the user.

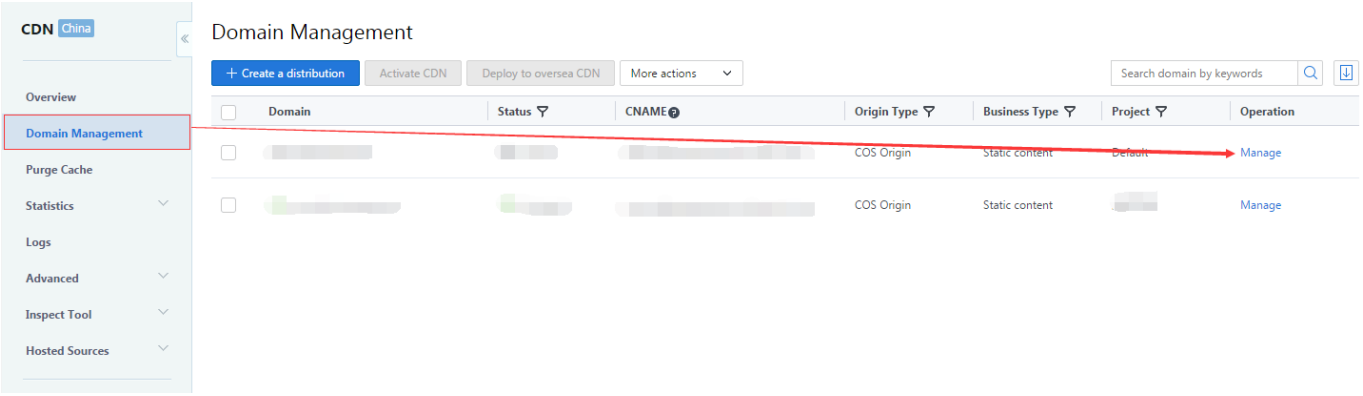
referer Hotink Protection

Overview

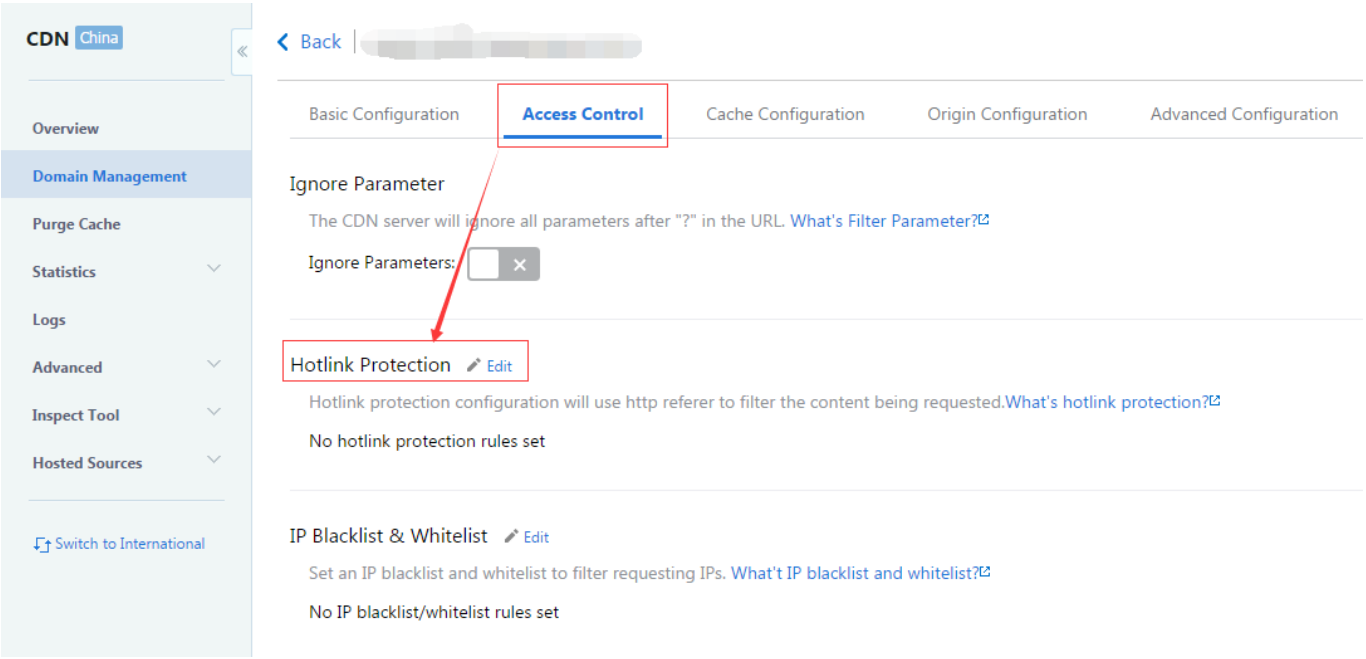
You can use the referer hotlink protection configuration feature provided by CDN to restrict the sources of access requests to your service resources. By setting a filtering policy for referer field value in user's HTTP Request Header, you can restrict the sources of access requests.

Configuration Instructions

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



You can find referer Hotlink Protection in "Access Control":



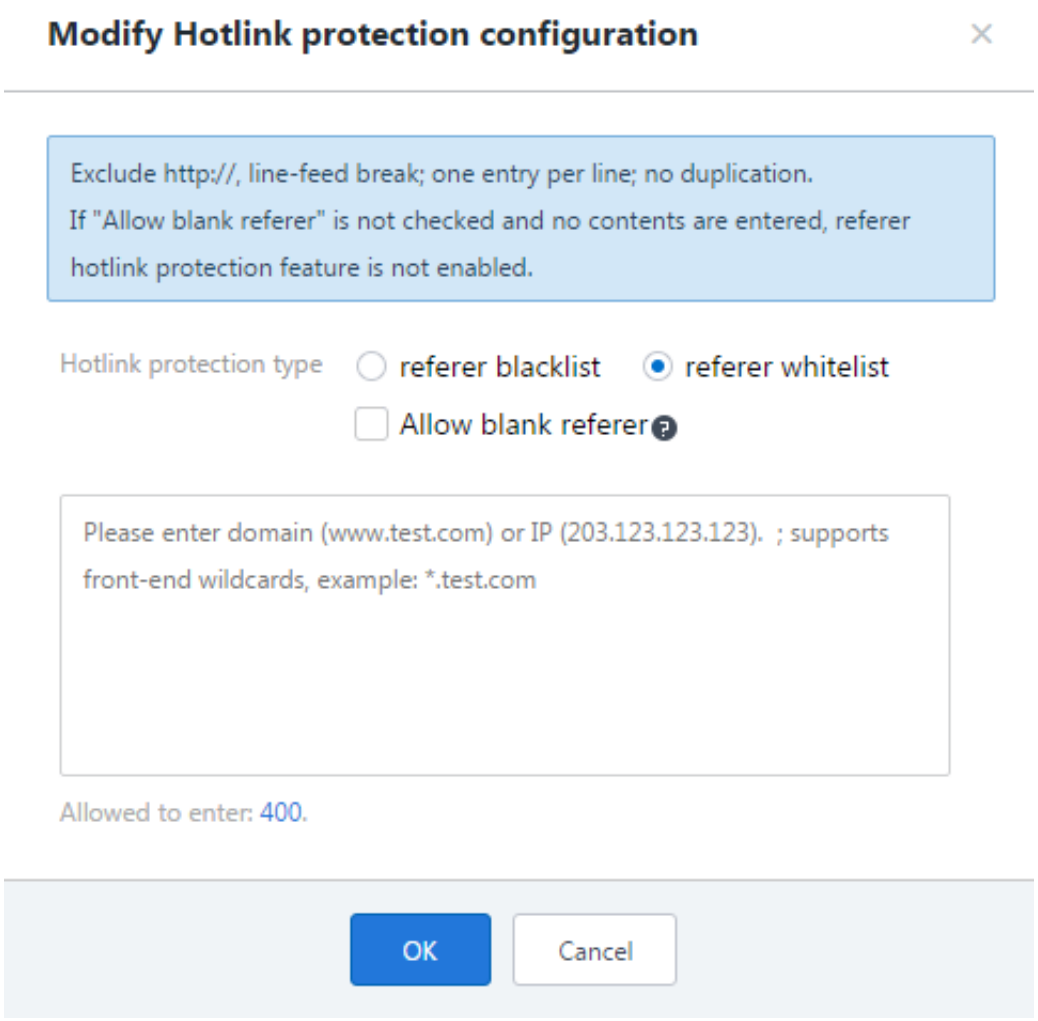
Default Configuration

By default, hotlink protection is disabled and no blacklist and whitelist exist.

Custom Configuration

Configuring referer whitelist

Click Edit near the hotlink protection configuration section and select referer whitelist to configure the whitelist:



If a user has configured a referer whitelist for domain "www.abc.com" with the following content:

www.test.com

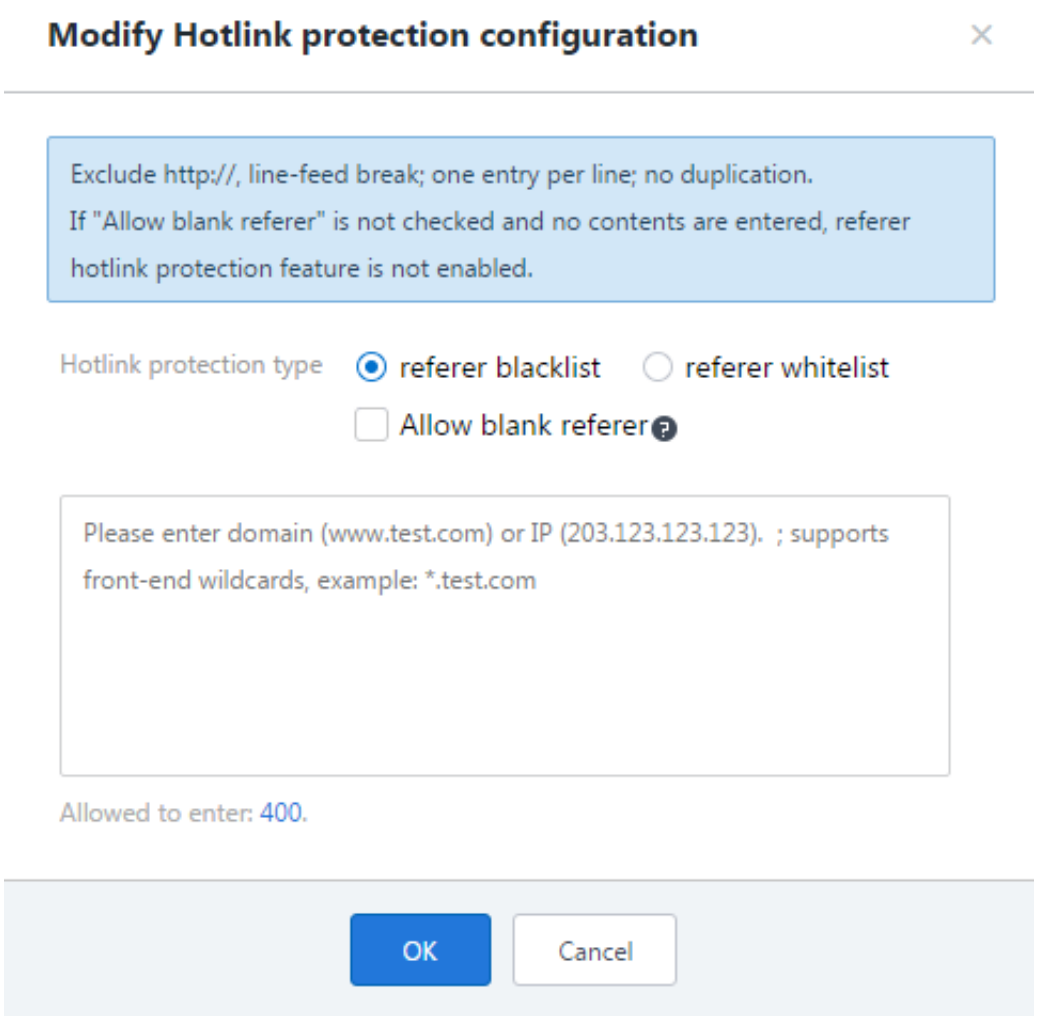
and Includes blank referer is unchecked, only the requests with a referer value of "www.test.com" are allowed to access the resource. For any other requests, a 403 error will be returned.

Must-Know Facts About Whitelist

- If the referer field of a request matches the string set for the whitelist, the CDN node will return the requested information normally;
- If the referer field of a request does not match the string set for the whitelist, the CDN node will reject returning requested information and return the 403 status code;
- Once the whitelist is configured, the CDN node will only return the requested information for the requests that match the string in the whitelist;
- When "Includes blank referer" is checked, CDN will return requested information normally if the referer field is blank or does not exist for a request (such as browser request).

Configuring the Referer Blacklist

Click Edit near the hotlink protection configuration section and select referer blacklist to configure the blacklist:



If a user has configured referer blacklist for domain "www.abc.com" with the following content:

```
www.test.com
```

and Includes blank referer is unchecked, a 403 error will returned for any request with a referer value of "www.test.com". For any other requests, the requested information will be returned normally.

Must-Know Facts About Blacklist

- If the referer field of a request matches the string set for the blacklist, the CDN node will reject returning the requested information and return the 403 status code.
- If the referer field of a request does not match the string set for the blacklist, the CDN node

will return the requested information normally;

- When "Includes blank referer" is checked, the CDN will reject returning the requested information and return the 403 status code if the referer field is blank or does not exist for a request (such as browser request).

Note

- Referer blacklist and whitelist are not compatible with each other. You can only enable either of them at the same time;
- You can add a maximum of 400 entries for the hotlink protection feature, separated by line breaks (one entry per line).
- Hotlink protection supports the "domain name/IP" rule (prefix match). For example, if "www.abc.com" is set in the list, "www.abc.com/123" and "www.abc.com.cn" will be considered to match the list; if "127.0.0.1" is set in the list, "127.0.0.1/123" will be considered to match the list;
- Hotlink protection supports the use of wildcard. If "*.qq.com" is set in the list, "www.qq.com" and "a.qq.com" will be considered to match the list..

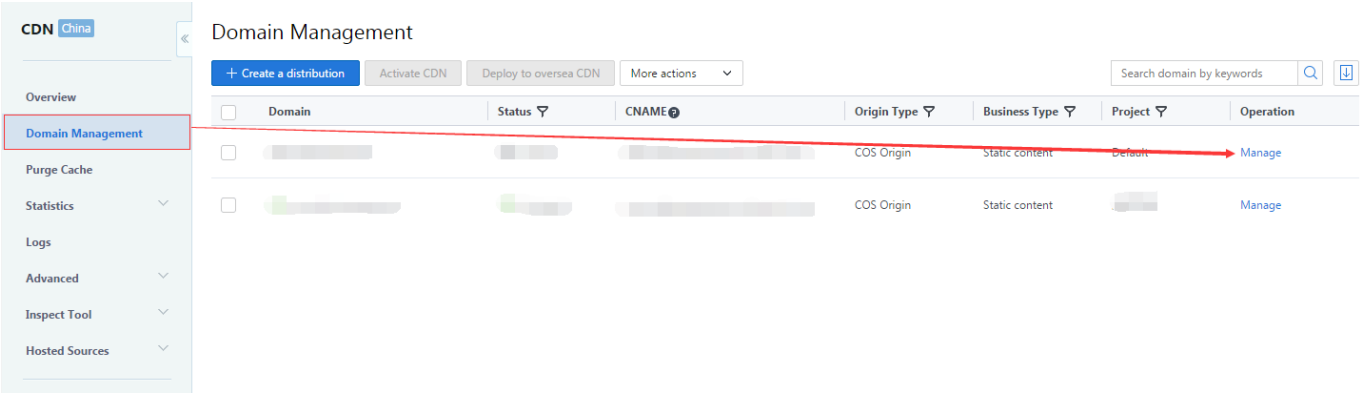
IP Blacklist/Whiltelist

Overview

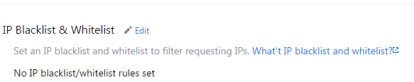
CDN provides IP Blacklist&Whitelist Configuration feature which allows you to set up filtering policies for the source IPs of user requests based on your business needs to prevent various problems such as cheating and attacks from malicious IPs.

Configuration Instructions

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



You can find IP Blacklist & Whitelist configuration in "Access control":



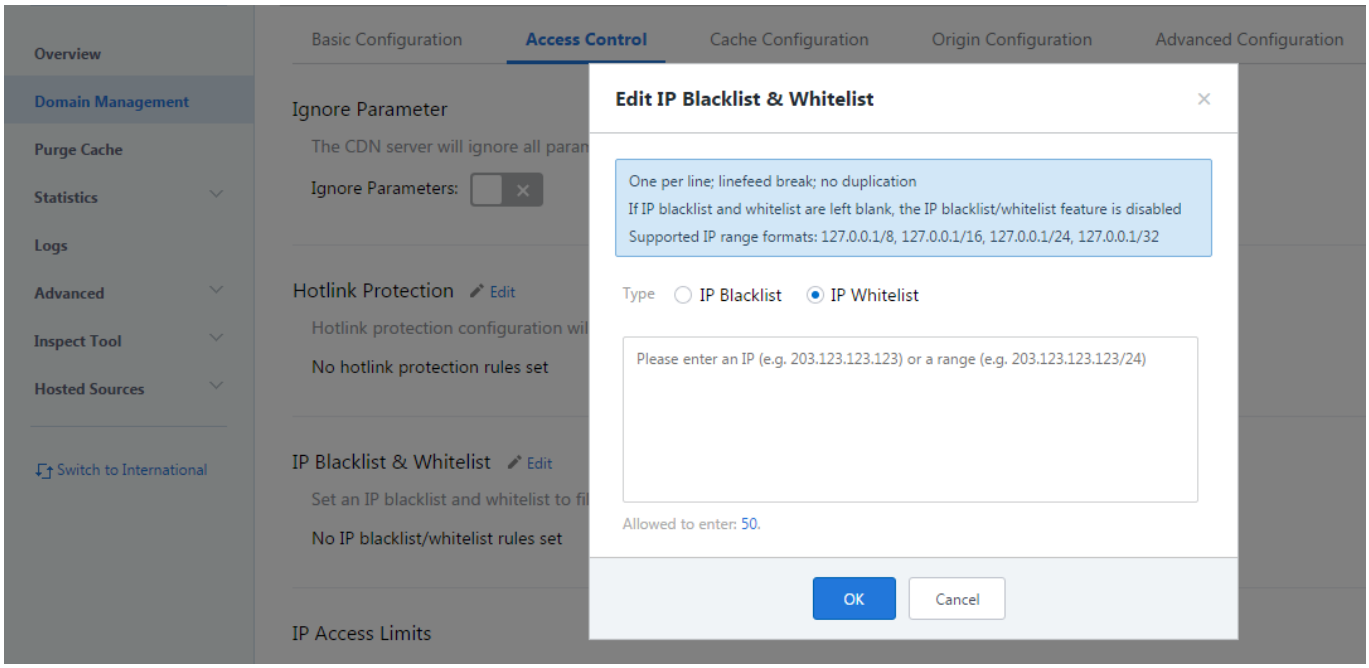
Default Configuration

By default, IP blacklist & whitelist feature is disabled and no blacklist and whitelist exist.

Custom Configuration

Configuring IP Whitelist

Click Edit button and select Whitelist to configure whitelist:



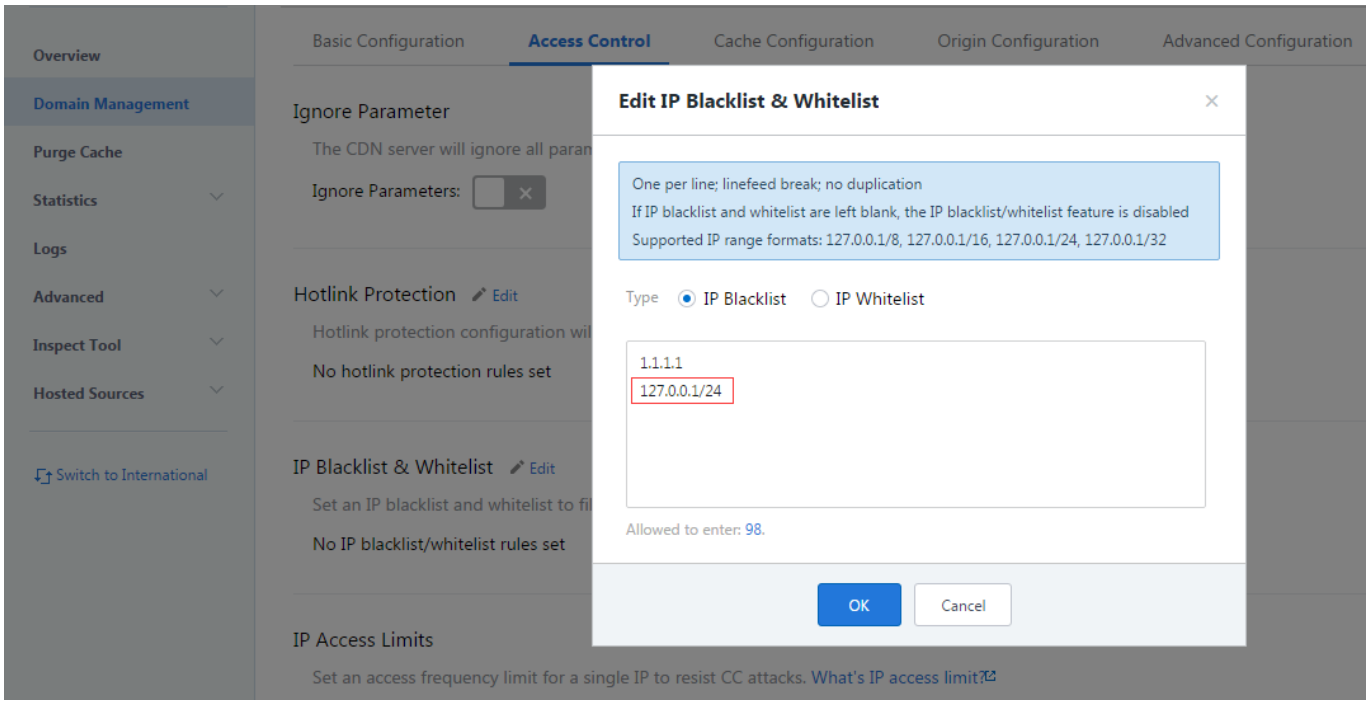
Assume that a user has configured IP whitelist for domain "www.abc.com" with the following content:

1.1.1.1
2.2.2.2/24

This indicates that the requested content can be returned successfully only if the source IP of the request is 1.1.1.1 or matches the network segment 2.2.2.2/24. A 403 error will be returned for any request that does not meet the condition.

Configuring IP Blacklist

Click Edit button and select Blacklist to configure blacklist:



Assume that a user has configured IP blacklist for domain "www.abc.com" with the following content:

```
3.3.3.3
4.4.4.4/16
```

This indicates a 403 error will be returned only if the source IP of the request is 3.3.3.3 or matches the network segment 4.4.4.4/16. For any other requests, the requested content will be returned.

Note

- IP blacklist and whitelist are not compatible with each other. You can only enable either of them at the same time;
- You can add a maximum of 100 entries, separated by line breaks (one entry per line);
- Currently, only network segments of the following formats are supported: /8, /16, /24, /32. Any other segment formats are not supported;
- When both lists are empty, it means that IP blacklist & whitelist feature is currently disabled.

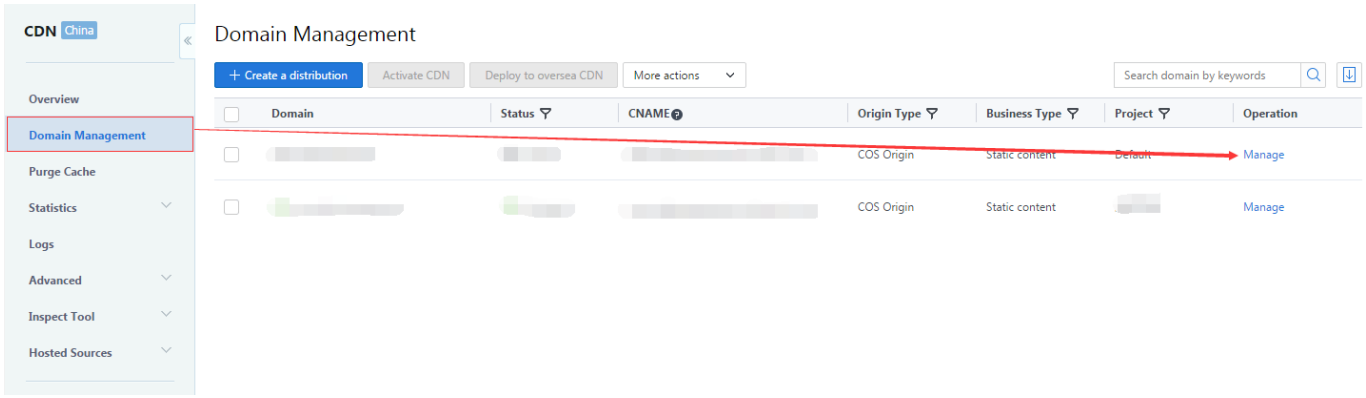
Set IP Access Control

Overview

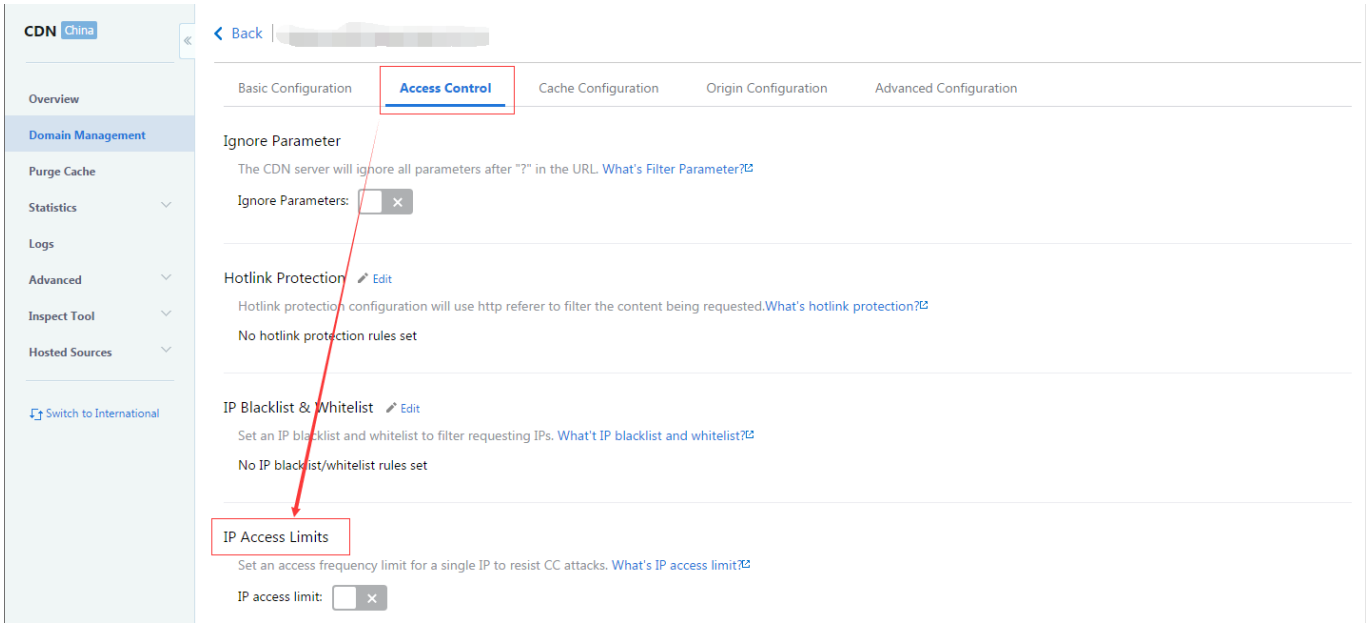
CDN provides IP access frequency limit configuration which restricts how many times an IP is allowed to access a node within one second to prevent CC attacks.

Configuration Instructions

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



You can see IP Access Frequency Limit in "Access Control":

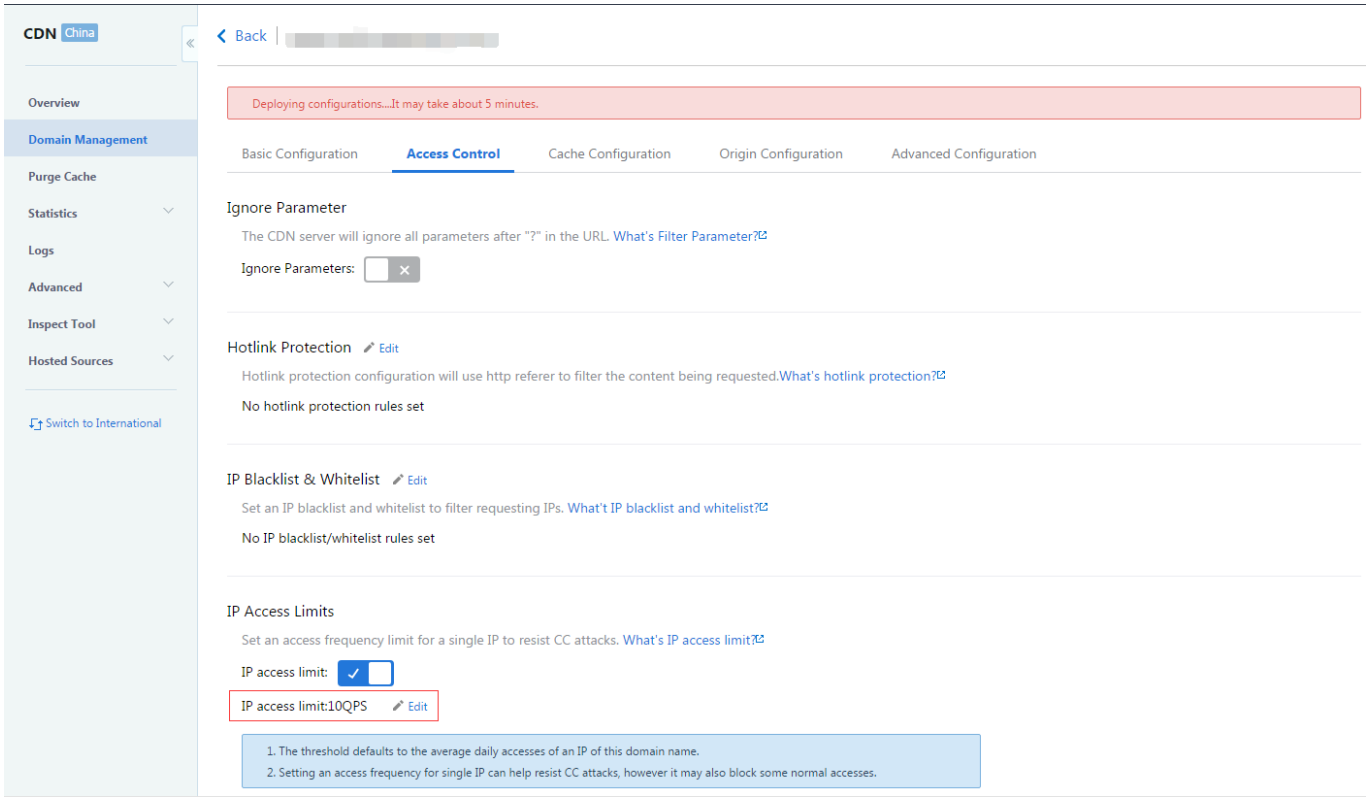


Default Configuration

By default, IP Access Frequency Limit configuration is disabled.

Custom Configuration

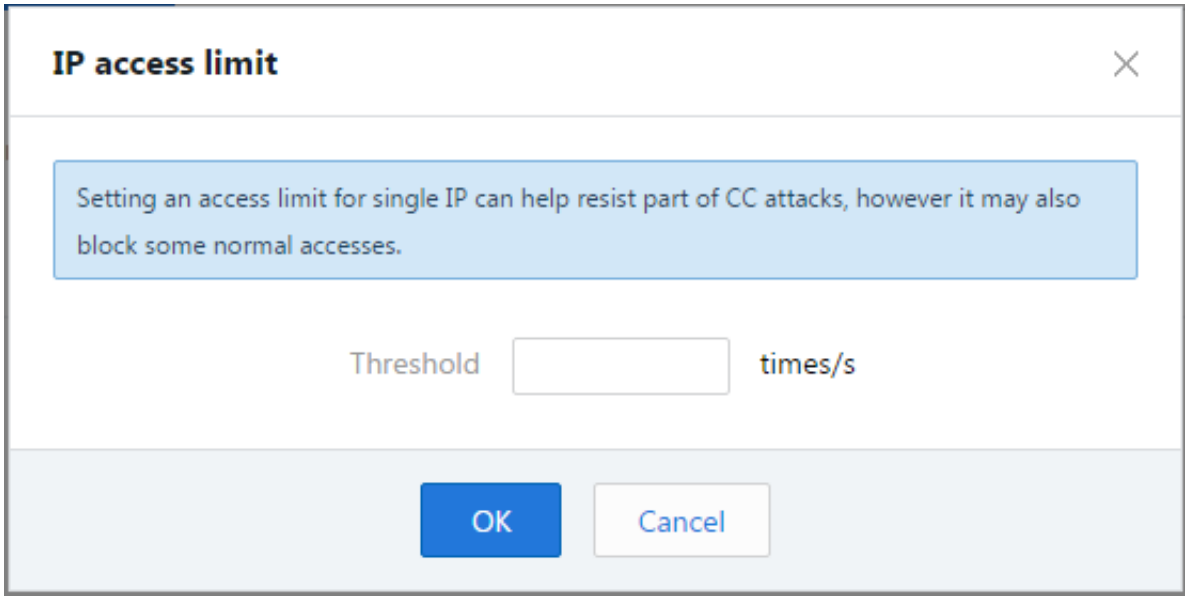
Click "On" button to enable IP Access Frequency Limit configuration. The system will suggest a threshold according to the average daily accesses of a single IP in the recent 30 days. You can see the given default threshold in the Current IP access limit field:



Note:

- Default threshold is calculated as follows: Count the average access frequency of an IP at each of the 288 statical points for each day (one point per 5 minutes) and take the largest value among the values for all the statical points for each day. Then get the default threshold by dividing the sum of largest value for each day by 30 (the recent 30 days);
- Minimum default threshold is 10QPS (for reference only). It is recommended to configure the threshold based on your business changes.

Click Edit button to customize the threshold:



Note:

- IP access frequency limit is designed to restrict how many times an IP is allowed to access a node within one second. If the limit is exceeded, a 514 error will be returned;
- Setting a reasonable threshold is recommended since a low frequency limit may affect the use by users who have a high access frequency.

Video Drag Configurations

Overview

The action of video dragging mainly occurs in VOD scenarios. When a user drags the video progress bar, a request (similar to the one shown below) will be sent to the server end:

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 at various CDN nodes, thus the nodes can directly respond to such requests once this configuration is enabled.

Configuration Instructions

Note About Configuration

Note

- The origin server is required to support Range requests
- Currently supported file types are: mp4, flv, ts
- You need to enable parameter filtering feature before enabling video dragging.

Parameter Description

File Type	meta Info	start Parameter Description	Request Example
MP4	For videos on the origin server, the meta info must be located at the file header. Videos with their meta info located at the file tail are not	The start parameter specifies a time (in seconds) and uses decimal to specify millisecond (for example, start=1.01 means the	http://www.test.com/demo.mp4?start=10 means the video will be played from the 10th second

File Type	meta Info	start Parameter Description	Request Example
	supported	starting time is 1.01s). CDN will locate the last key frame before the time specified by the start parameter (if the specified time is not a key frame)	
FLV	Videos on the origin server must include meta info	The start parameter specifies a byte. CDN will automatically locate the last key frame before the byte specified by the start parameter (if the specified byte is not a key frame)	http://www.test.com/demo.flv?start=10 means the video will be played from the 10th byte
TS	No special requirements	The start parameter specifies a time (in seconds) and uses decimal to specify millisecond (for example start=1.01 means the starting time is 1.01s). CDN will locate the last key frame before the time specified by the start parameter (if the specified time is not a key frame)	http://www.test.com/demo.ts?start=10 means the video will be played from the 10th second

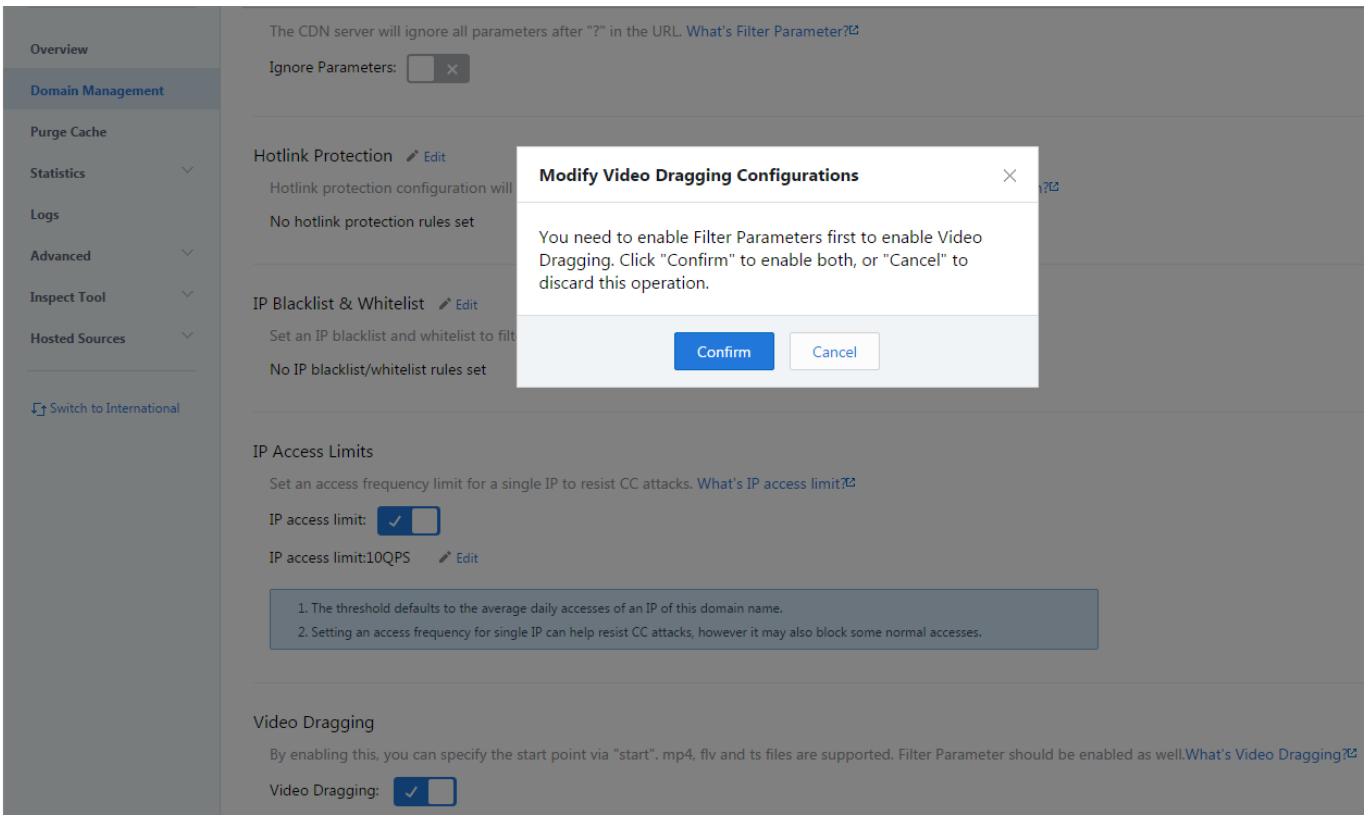
Default Configuration

By default, video dragging configuration is disabled.

Enabling Video Dragging

Video dragging configuration is located in Access Control in domain management.

If parameter filtering is disabled, it will be automatically enabled when video dragging has been enabled.



Cache Expiration

Overview

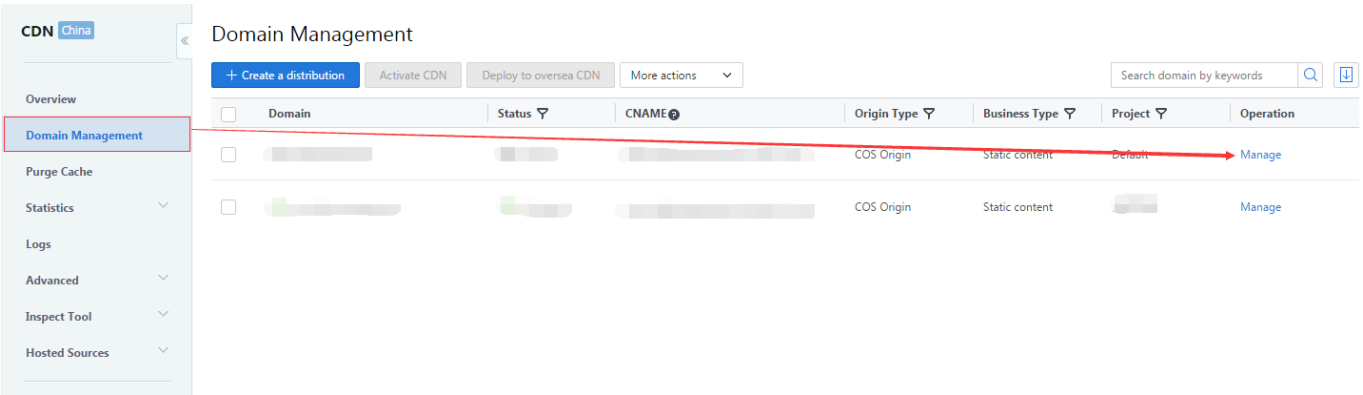
Cache expiration configuration refers to a set of expiration policies the CDN acceleration nodes should follow when caching your business contents.

User resources cached on CDN nodes all have a "Expiration Time". If a resource cached on a node is not expired, when a user request for the resource reaches the node, the node will directly return the cached resource to the user to speed up the resource acquisition; If a resource is beyond the set validity period and thus becomes expired, the node will forward the user request for the resource to the origin server, reacquire and cache the resource, then return it to the user.

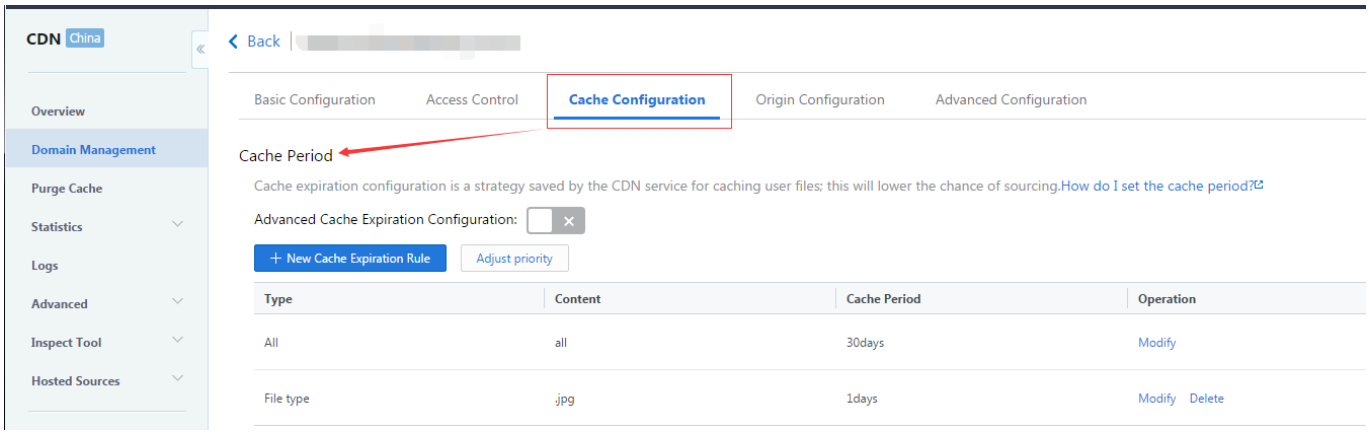
A reasonable cache validity period can effectively improve the resource hit rate and reduce back-to-origin rate, achieving a saving in bandwidth. Tencent Cloud CDN supports cache validity period settings at various dimensions, custom priority adjustment and cache inheritance policies (advanced cache configuration).

Configuration Instructions

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



You can find Cache Expiration Configuration in "Cache Configuration":



Default Configuration

Default configuration is as follows when a domain is connected:

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

You may modify the default settings mentioned above.

Custom Configuration

You can make cache validity period settings in addition to the default settings base on your business needs. CDN supports three settings:

Setting cache validity period by file types

You can set cache validity period by file types by entering the filename extensions, as shown below:

.jpg .png 300 seconds

In this case, all picture resources matching .jpg and .png under the domain will be cached for 5 minutes on the node.

Setting cache validity period by folders

You can set cache validity period by folders by entering the folder path, as shown below:

/test;/test2 1000 seconds

In this case, if the domain is "www.test.com", all resources under "www.test.com\test\" and "www.test.com\test2\" will be cached for 1000 seconds on the node.

Setting cache validity period based on full path of file

You can set cache validity period for a certain file, as shown below:

/test/1.jpg 2000 seconds

In this case, if the domain is "www.test.com", the resource "www.test.com\test\1.jpg" will be cached for 2000 seconds.

You can also set cache validity period for a certain type of files, as shown below:

/test/*.jpg 3000 seconds

In this case, if the domain is "www.test.com", all resources with a jpg format under "www.test.com\test\" will be cached for 3000 seconds.

Note:

- You can set multiple cache validity periods at a time, with the entries separated by ";". The entries are case-sensitive;
- File types must be specified as extensions starting with ".", such as ".jpg"; Folder types must begin with "/", such as "/12345/test", instead of ending with "/";
- A maximum of 10 custom entries can be added, each of which can only contain 150 characters;
- Cache validity period can be set to any number of seconds in the form of an integer, "0" means resource will not be cached;
- When you are setting caching policies based on full path of file, "*" can only be used to match a certain type of files. Other regular expression matching methods are not supported currently;
- The home page type ending with "/" is not supported in the setting of caching policies based on full path of file.

Priority

Matching Sequence

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

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

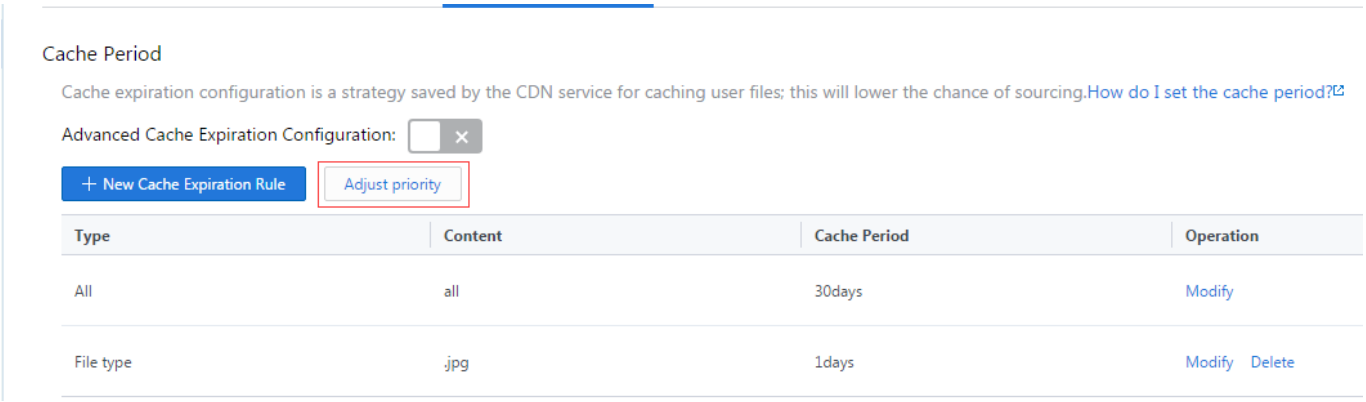
If the domain is "www.test.com", and the resource is "www.test.com/test/abc.jpg", the matching rule will be as follows:

1. Match with the first entry. It is hit, so the cache validity period is 30 days;
2. Match with the second entry. It is not hit;
3. Match with the third entry. It is hit, so the cache validity period is 300 seconds;
4. Match with the fourth entry. It is hit, so the cache validity period is 400 seconds;
5. Match with the fourth entry. It is hit, so the cache validity period is 200 seconds;

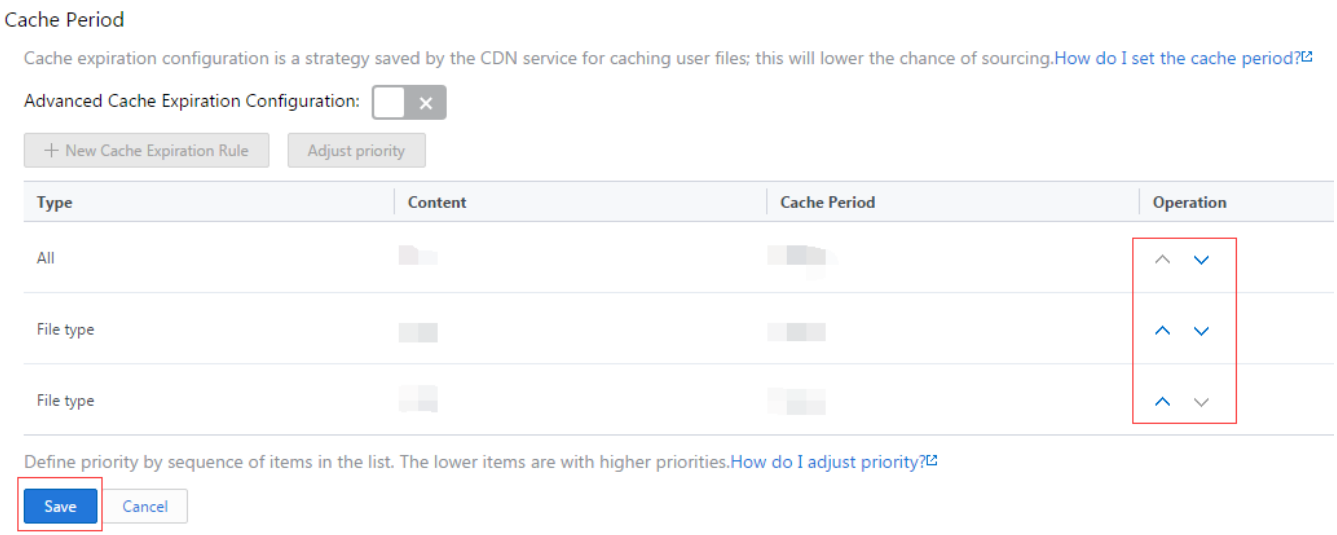
The final cache validity period is subject to the last matching result, 200 seconds.

Changing Priority

You can customize the order of existing cache validity period entries according to your business needs. Click Adjust priority above the cache validity period entries:



Use the up and down arrows on the right to change the order of cache validity period entries, then click Save:



Cache Inheritance

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

- If the cache-control field is max-age, the cache validity period for this resource is subject to the one set for the resource, instead of inheriting the value specified by max-age;
- If the cache-control field is no-cache or no-store, the CDN node will not cache the resource.

Advanced Cache Configuration

The Advanced cache expiration Configuration switch above the cache expiration configuration list can provide the following features when enabled.

When a user requests for a certain resource from the origin server and the Response HTTP Header includes the cache-control field with a value of max-age=xxxx, the cache validity period for the resource on the node will be subject to the smaller one between the set validity period and max-age:

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

seconds;

When advanced cache configuration is enabled, if Cache-Control field does not exist in the Response Header of your origin server, CDN will add the "Cache-Control:max-age=600" header by default.

Caching based on status codes

In addition to the cache policies mentioned above, CDN nodes will also use the following default cache policies based on status codes when requesting for resources from the origin server:

- 2XX: Use normal cache policies;
- 3XX: Resources are not cached by default;
- 4XX: Resources are cached for 10 seconds in case of status code 404. In other cases, they're not cached by default;
- 5XX: Resources are not cached by default.

Back-to-origin Configurations

Set Intermediate Server

Overview

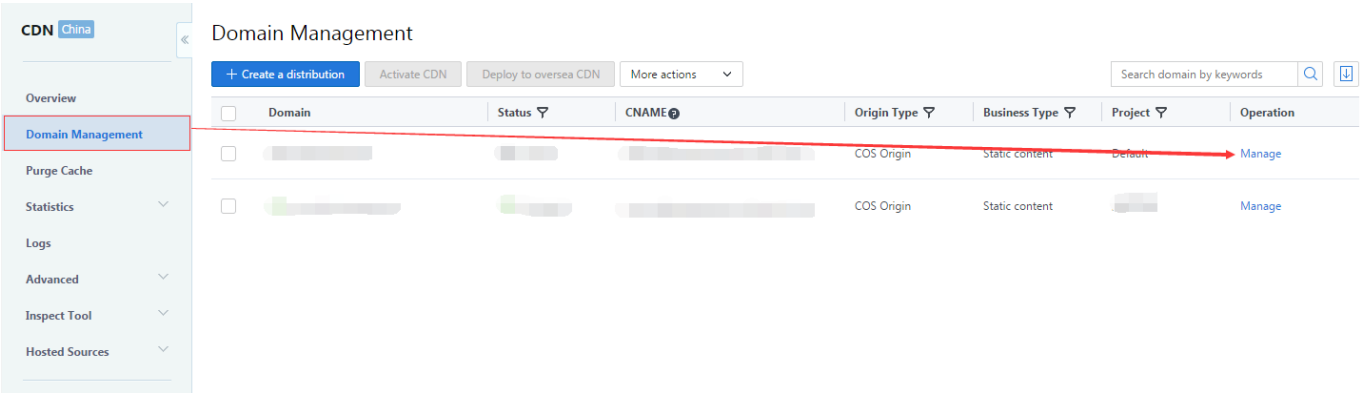
An intermediate node can be considered as a secondary cache node. When a user sends a request, it will first reach the edge node. If this node doesn't have the requested resource, it will send request to the intermediate node, which will then send the request to the origin server if it still does not have the requested resource.

Once intermediate node is enabled, access requests to origin from users will be converged at this node. The node will then acquire the requested data from the origin in a centralized manner, reducing the pressure on the origin server.

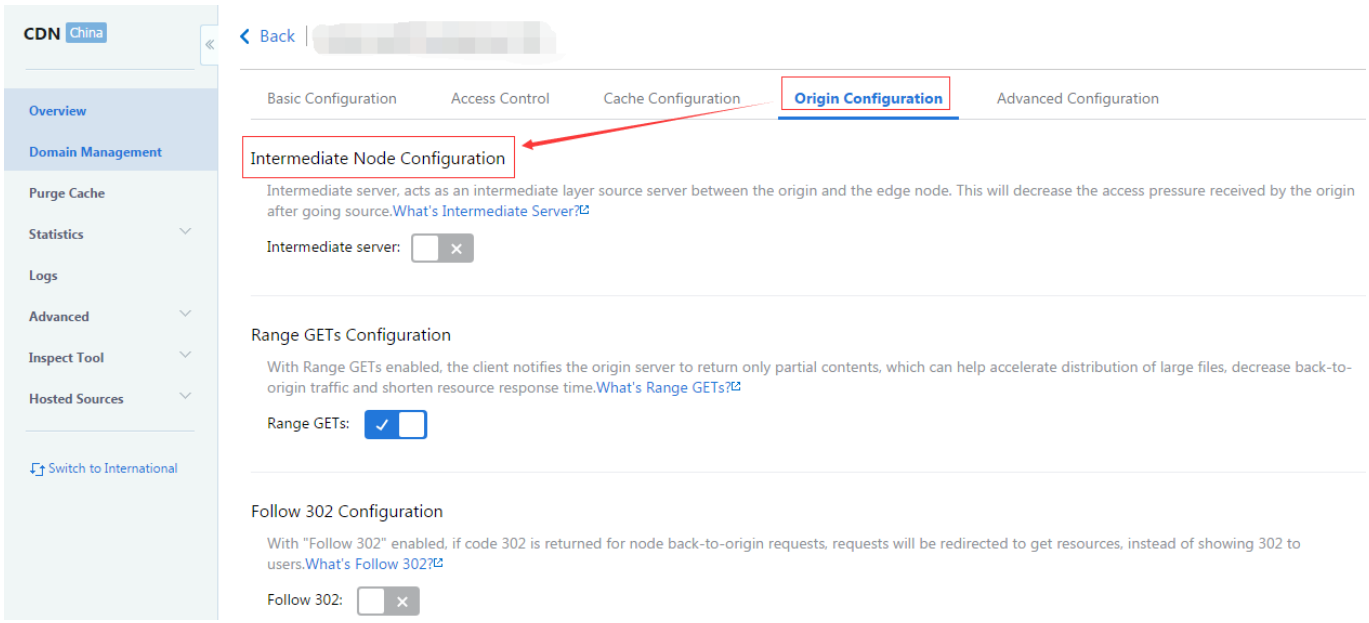
It is recommended to enable intermediate node in order to improve your CDN acceleration and reduce back-to-origin bandwidth.

Configuration Instructions

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



Go to Intermediate Node Configuration under "Origin Configuration" to enable intermediate node:



The intermediate node configuration is disabled by default.

Configure Range GETs

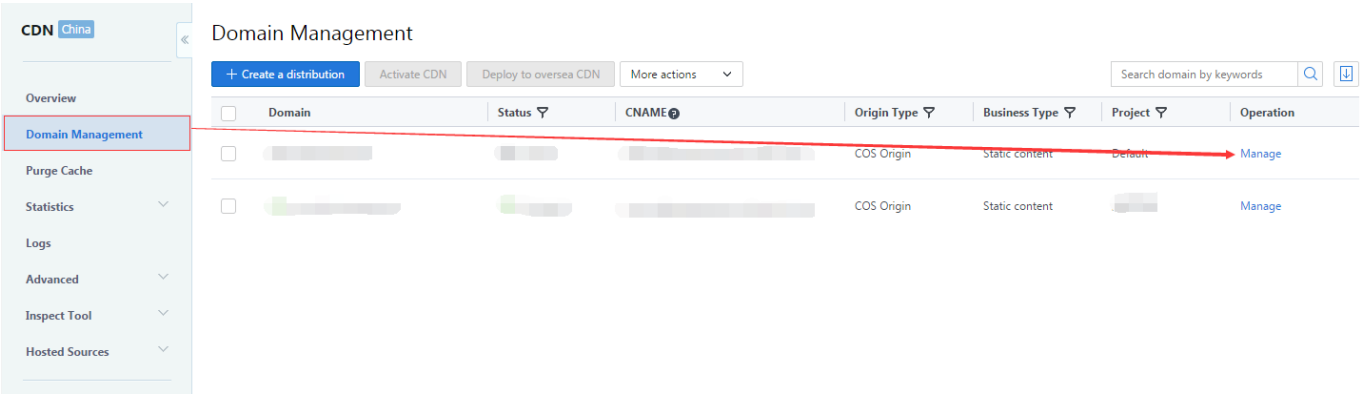
Overview

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

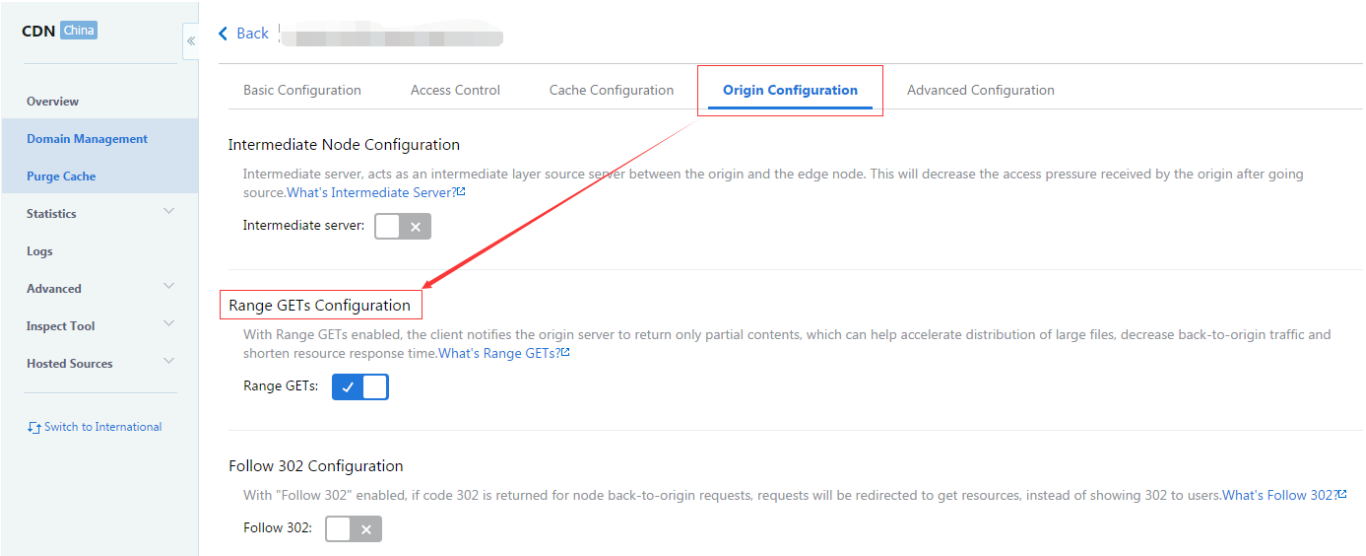
The origin server is required to support Range requests

Configuration Instructions

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



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



Default Configuration

By default, Range GETs Configuration is Enabled.

Result of Configuration

If a user makes a request for resource:

http://www.test.com/test.apk

when the node receives the request and finds out that the cached test.apk has expired, it will send a back-to-origin request.

When Range GETs Configuration is enabled:

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

When Range GETs Configuration is disabled:

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

Note:

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

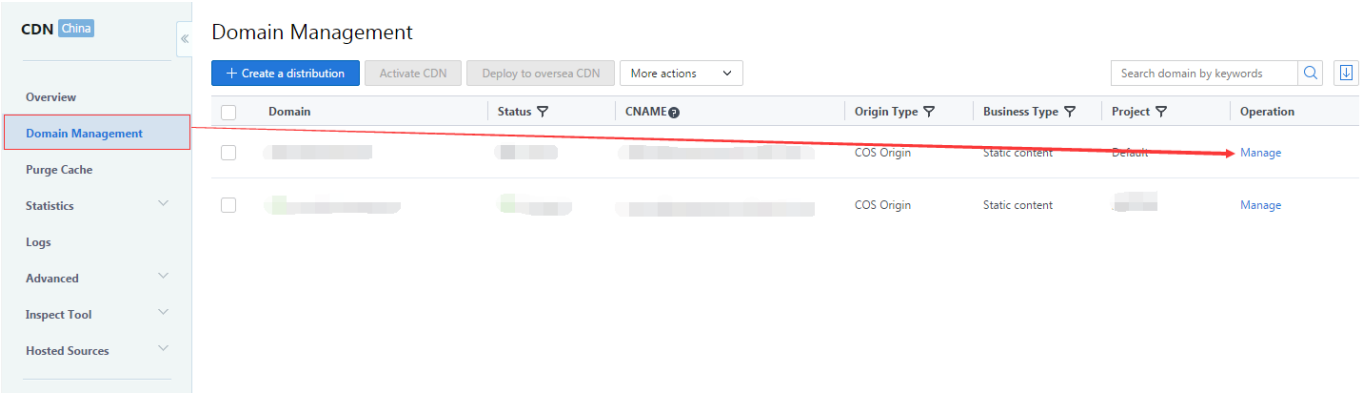
Configure Follow 302

Overview

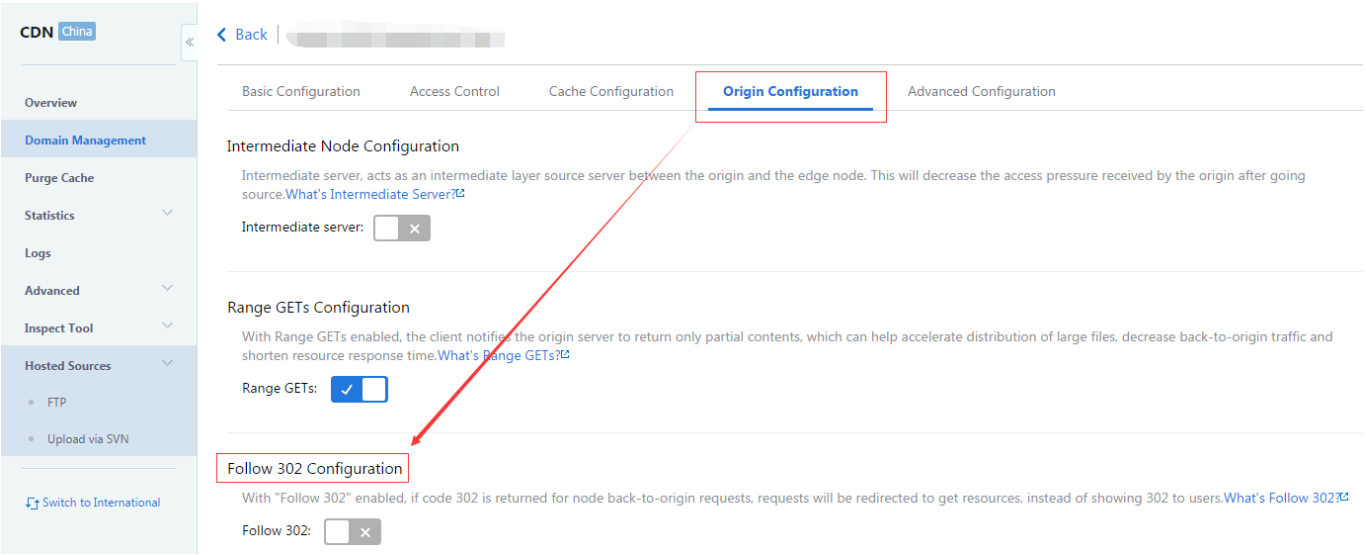
CDN provides "Follow 302 Configuration" feature.

Configuration Instructions

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



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



Default Configuration

By default, Follow 302 Configuration is disabled.

Result of Configuration

For example, if a user requests for resource

http://www.test1.com/1.jpg

and the resource isn't cached on the node, the node will request to acquire the resource from the origin server. If the HTTP Response status code sent from the origin server is 302, the request will be redirected to

http://www.test2.com/2.jpg

.

When Follow 302 Configuration is disabled:

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

  http://www.test2.com/2.jpg

  , there will be no acceleration if this domain is not connected to CDN.
- If another user sends a request to

  http://www.test1.com/1.jpg

  at this point, the above process will be repeated.

When Follow 302 Configuration is enabled:

- When Follow 302 Configuration is enabled, the node will directly request for the resource if it

receives the status code 302 as HTTP Response.

- The resource will be acquired, cached to the node and then returned to the user.
- If another user also sends a request for

  http://www.test2.com/1.jpg

  , the resource will be hit on this node.

Note:

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

Configure Bandwidth Cap

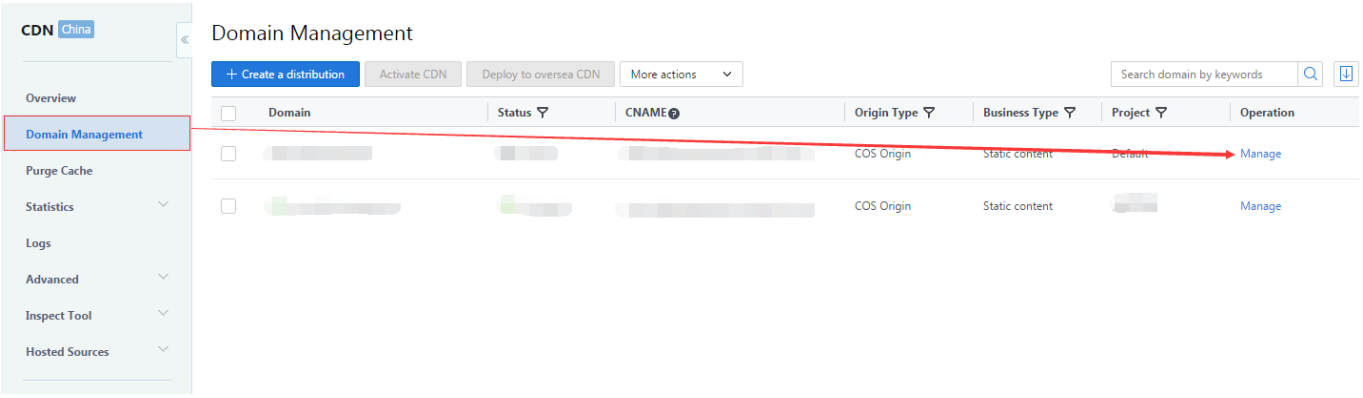
Overview

You can configure a bandwidth cap for the domain. When the bandwidth of the domain exceeds this cap within a statistical point (5 minutes), all access requests will be forwarded back to the origin server or the CDN service will be disabled, depending on your configuration (in either of the cases, a 404 error will be returned for all access requests).

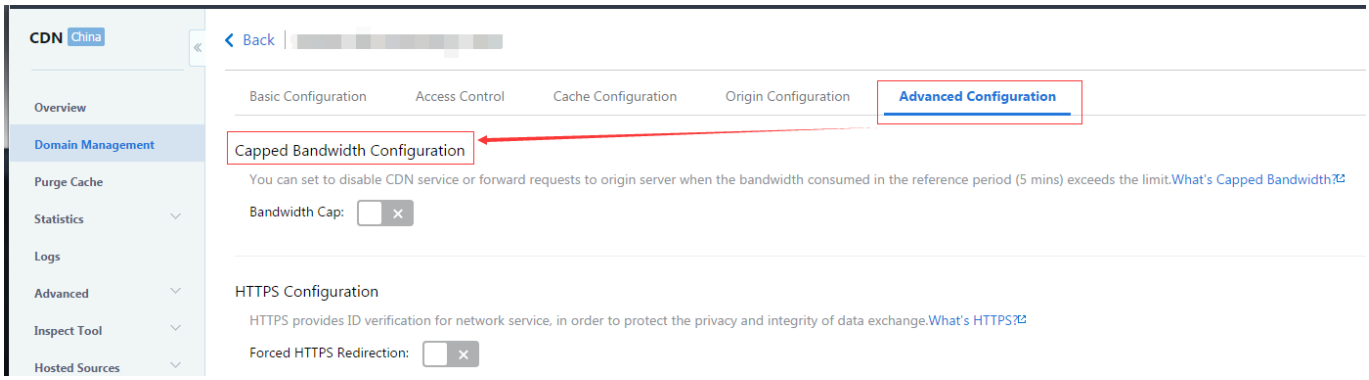
When the bandwidth cap is reached, the domain will go into Disabled status whether it is set to forward the access request back to origin server or to return the 404 status code. It takes about 5 to 15 minutes for the behavior of back-to-origin/returning 404 to take effect.

Configuration Instructions

Log in to CDN Console and go to Domain Management page. Then click the Manage button to the right of the domain name whose configuration is to be modified:



You can find Capped Bandwidth Configuration in Advanced Configuration:

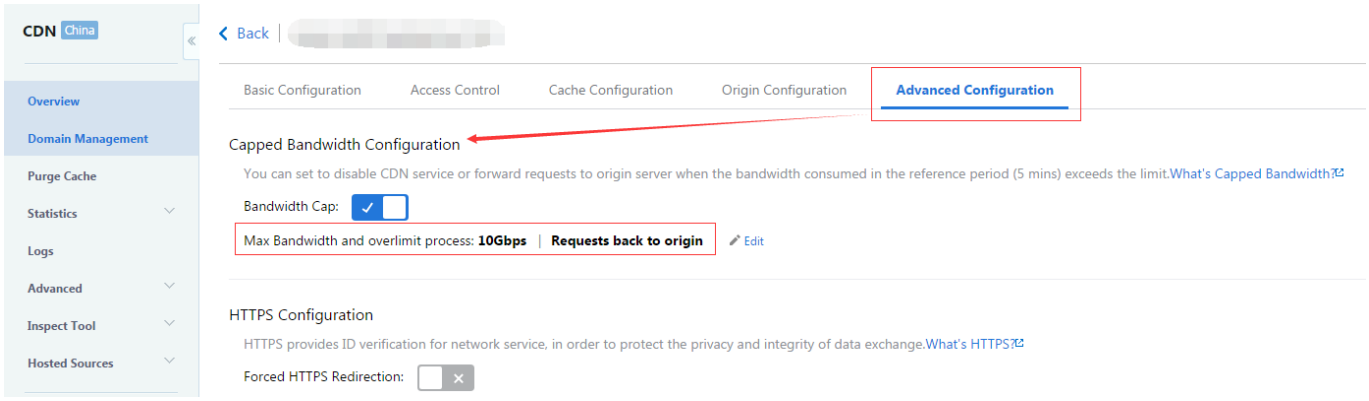


Default Configuration

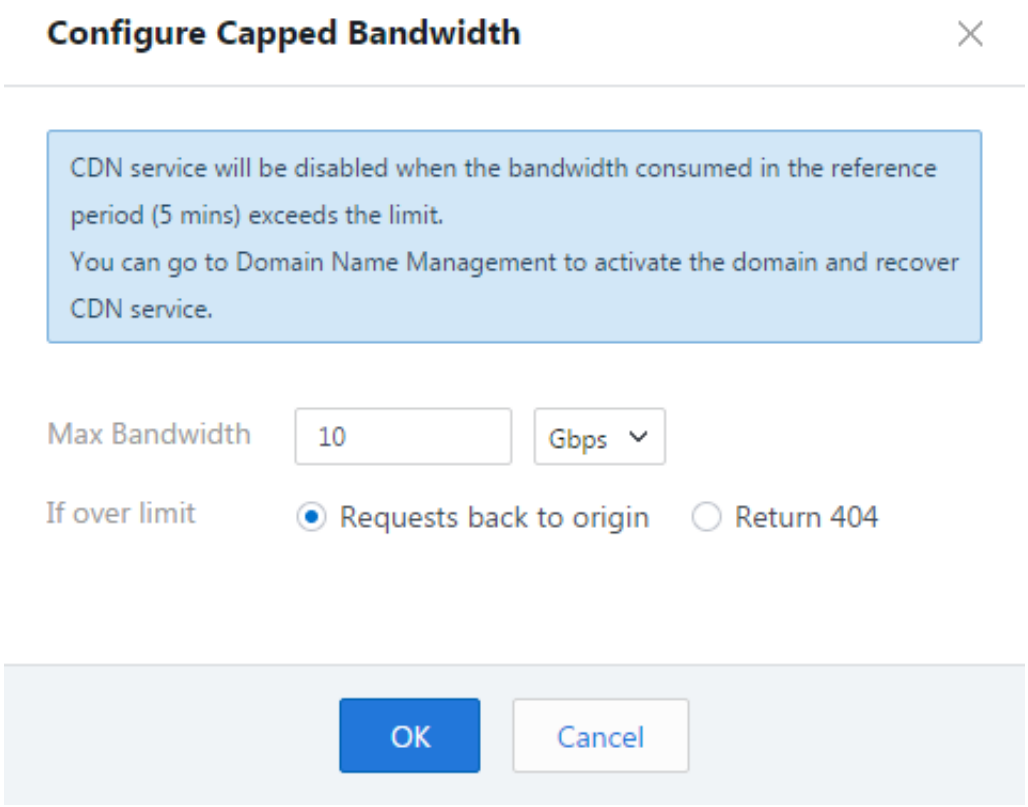
By default, capped bandwidth configuration is disabled.

Configuring the Threshold

When capped bandwidth configuration is enabled, by default, the bandwidth cap is 10Gbps and when the cap is reached, "access request is forwarded to origin server":



You can modify the cap as well as how to process user requests when it is reached:



Note

- If the domain is disabled because the bandwidth cap is reached and you wish to continue using CDN service, you can manually activate the domain in the Domain Management page of the CDN console;
- If your purpose is to prevent strong DDoS attacks, it is recommended to set to "return 404 for access request" to protect your origin server;
- If your purpose is to control CDN service cost, it is recommended to set to "forward access request to origin server" to prevent your service from being affected.

Configure HTTPS

Overview

HTTPS (Hypertext Transfer Protocol Secure) is a security protocol built on HTTP protocol to be used for encrypted communication and can effectively ensure data transmission security. When configuring HTTPS, you need to provide the certificate for your domain and deploy it across all CDN nodes on the entire network to achieve encrypted data transmission across the network.

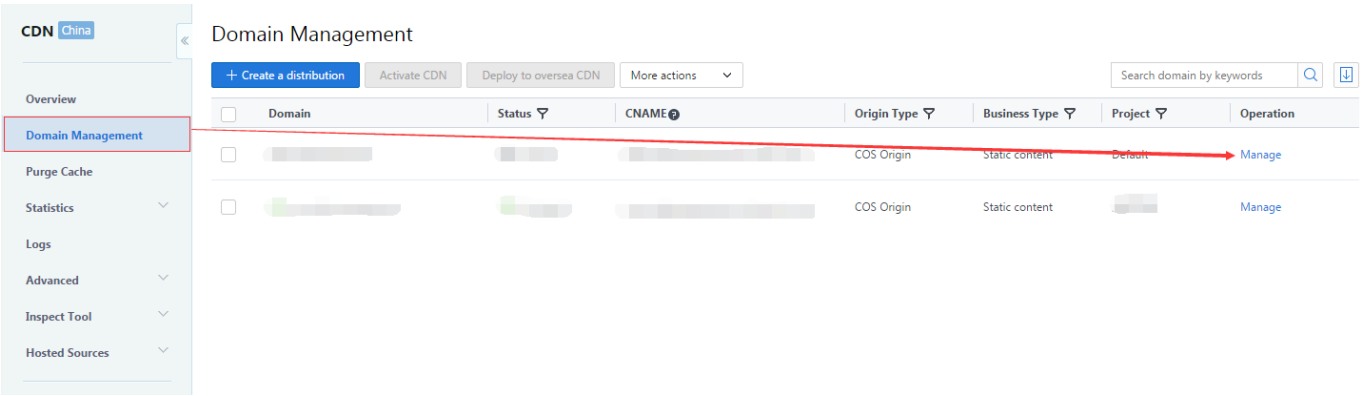
HTTPS configuration is now completely available for you.

Configuration Instructions

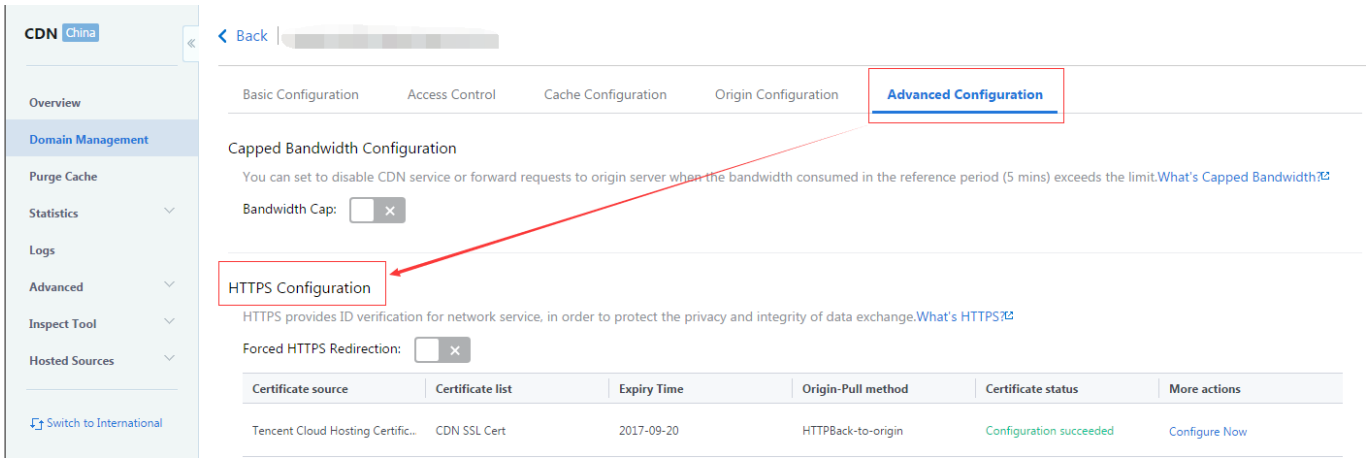
HTTPS configuration is only available to domains which meet the following conditions:

- Domain status is Deploying or Activated in "Domain Management" page;
- It is not a COS-synchronized domain with ".file.myqcloud.com" as suffix;
- Domain's connection method is Self-owned origin, COS origin or FTP origin;

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



Go to "Advanced Configuration" and find "HTTPS Configuration"



Certificate Types

Tencent Cloud currently supports two certificate deployment methods:

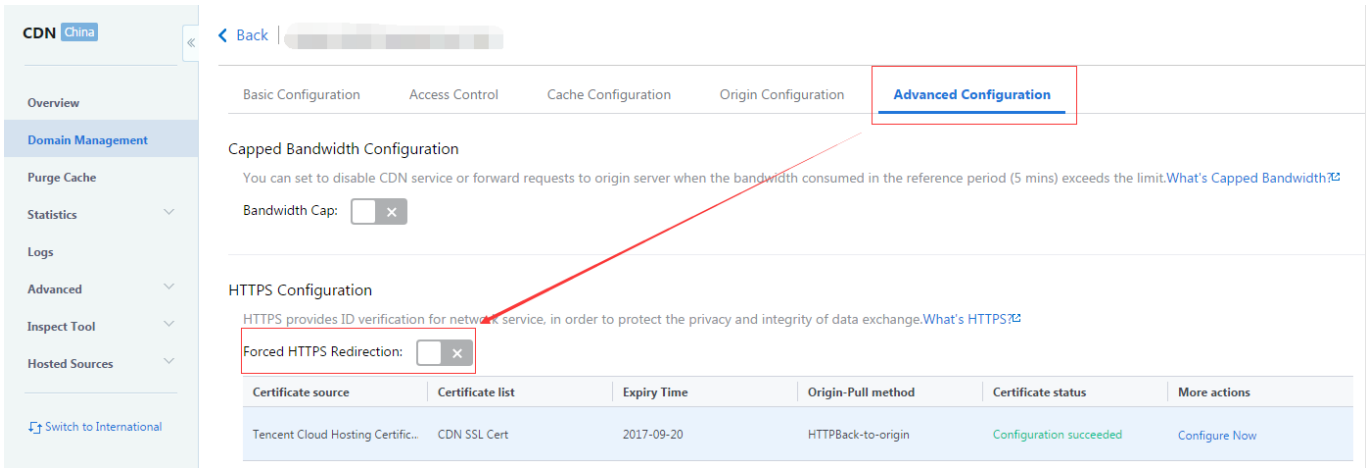
- Self-owned certificate: Upload self-owned certificate and private key to CDN for deployment. Transmission is encrypted throughout the process to ensure security of your certificate;
- Tencent Cloud-hosted certificate: You can go to SSL Certificate Management and trust your certificate to Tencent Cloud to use it for multiple cloud products. You can also apply for a Free Certificate provided by TrustAsia through this platform and deploy it directly to CDN;
- Tencent Cloud certificate: The original ".qcloudcdn.com" domain suffix belongs to Tencent Cloud and uses Tencent Cloud certificate. The entrance for adding this certificate has been closed.

Certificate Management

Go to Certificate Management page to add, modify or delete certificates. For more information, refer to Certificate Management Instructions.

Forced HTTPS

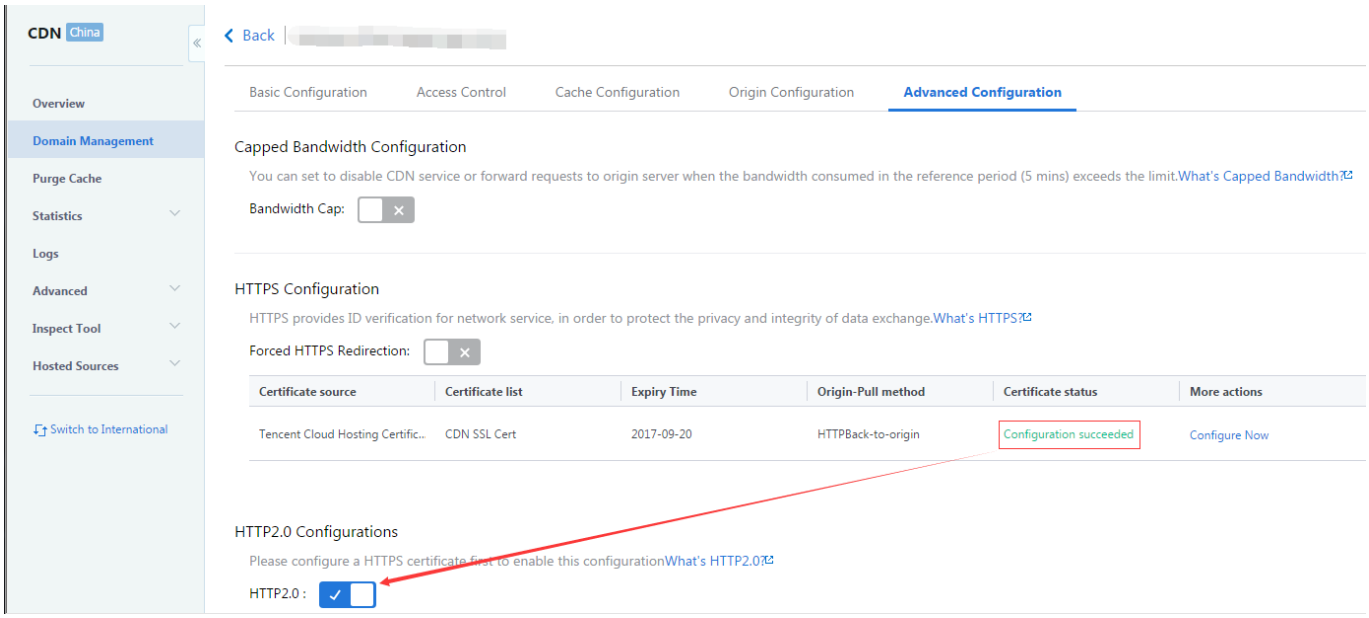
The Forced Redirect button will appear when the certificate is successfully configured. When it is enabled, any HTTP request made by the user will be redirected to HTTPS for access:



The feature is only available after HTTPS certificate is successfully configured

HTTP2.0

If you already obtained the qualifications of HTTP 2.0 closed beta, you can open HTTP2.0 after finish the configuration of HTTPS certificate:



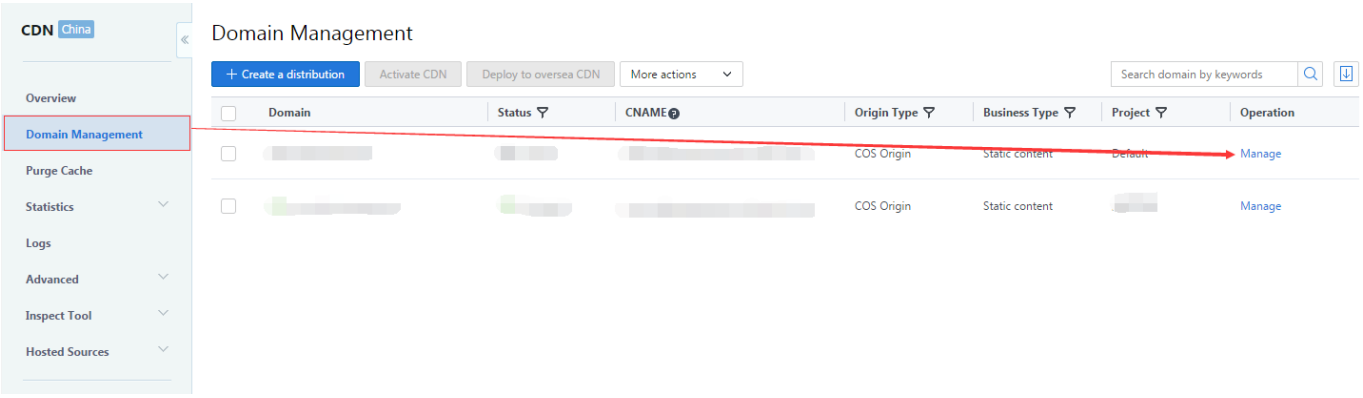
SEO Optimization

Overview

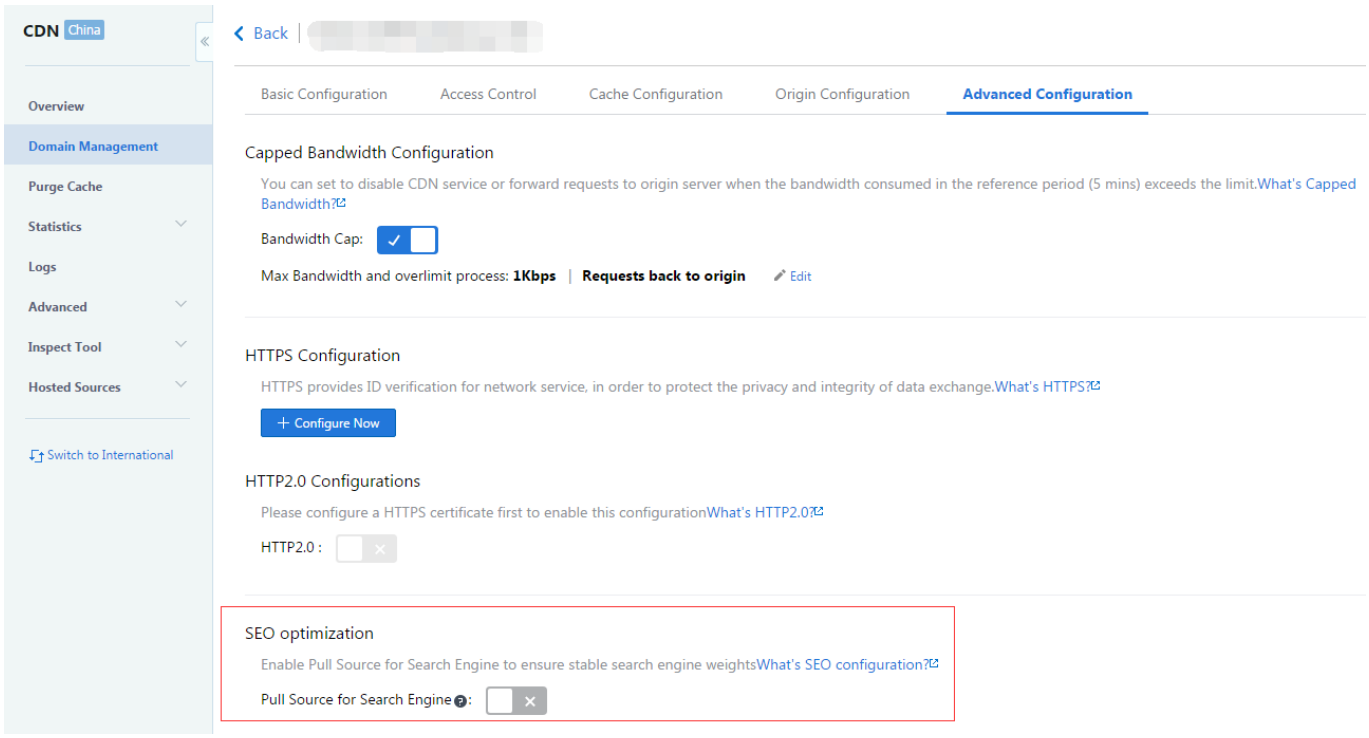
SEO optimization configuration is designed to deal with the problem that the domain authority on search engines will be affected by the frequent changes of IP address made by CDN following the connection of domain to CDN. By identifying whether the accessing IP belongs to a search engine and allowing users to choose to access resources directly from origin server, the feature can ensure a consistent domain authority on search engines.
Once SEO optimization configuration feature is enabled, requests from search engines will be directed to the origin server while other requests will access the CDN node normally.

Configuration Instructions

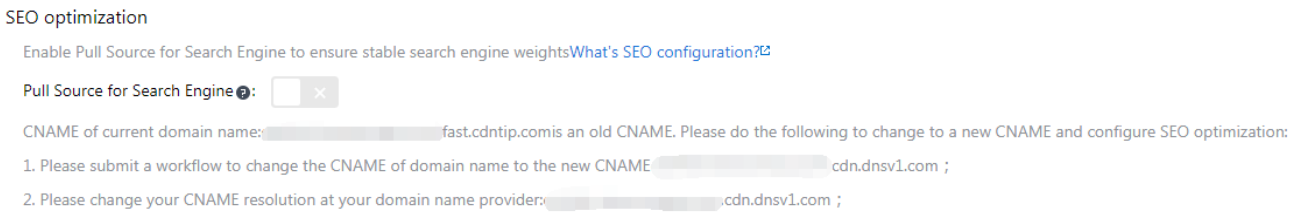
Log in to CDN Console and go to "Domain Management" page. Then click Manage button to the right of the domain name to enter the management page:



You can find SEO Optimization in "Advanced Configuration":



- SEO optimization is only available when connection method is "Own origin". Once SEO optimization is enabled, if the domain has multiple origin server addresses, the default origin address for back-to-origin requests will be the first one added;
- If the CNAME of the current domain is an old CNAME (as shown below), you need to update it to a new CNAME to use SEO optimization configuration feature.



How to update CNAME:

- Submit a ticket to request to change the CNAME of the domain to a new one;
- Go to your domain resolution service provider and switch the CNAME resolution of the domain to a new CNAME;

Note: Due to the frequent updating of IP addresses for search engines, Tencent Cloud CDN can only ensure to identify the majority of search engine IP addresses.

Configure HTTP Header

Overview

Generally, there are two types of HTTP messages:

- Request message sent from client to server
- Response message sent from server to client

Both types of the messages consist of a start line, one or more header fields, a blank line indicating the end of header field, and optionally, a message body. There are four types of HTTP header fields: general header, request header, response header and entity header. Each header field consists of a name (Key), colon (:) and a Value.

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.

Note:

- 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;
- HTTP Header configuration is specific to a domain. Once the configuration takes effect, the configured header field will be added to user's response messages to any of the resources under this domain;
- Configuring HTTP Header will only affect the response behaviors of the client (such as browser), and will not affect caching behaviors of CDN nodes;
- By default, CDN will inherit Access-Control-Allow-Origin and Content-Disposition header fields from the origin server, please avoid configuring origin server and CDN at the same time.

Configuration Instructions

CDN provides the following five header field configurations:

- Content-Disposition: Enable customized resource downloading configuration and default file name upon downloading;
- Content-Language: Specify resource response language at the client (such as browser);
- Access-Control-Allow-Origin: Specify the request origins allowed to access the resource for a cross-domain request;
- Access-Control-Allow-Methods: Specify the request methods allowed for a cross-domain request;
- 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.

General Configurations

Content-Disposition

Content-Disposition is used to enable the downloading of browser and set the default name for the downloaded file. If the type of the file sent from server to client browser is supported by the browser (such as txt, jpg), the file will be directly opened in the browser by default. If you want the user to be prompted to save the file, you can configure Content-Disposition field to override browser's default behavior. Common configurations are shown below:

Content-Disposition：attachment;filename=FileName.txt

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 means that the resource from one domain (for example, www.abc.com) makes a request for a resource under another domain (for example, www.def.com). Since the resources belong to different domains, this is considered cross-domain. Moreover, different protocols or different ports will also cause cross-domain access. When this happens, cross-domain related configurations need to be added in the Response Header, so that the resource making the request can get the data it wants.

Access-Control-Allow-Origin

Access-Control-Allow-Origin is used to solve cross-domain permission issues for resources. The field value defines which domains are allowed to reference this resource. You can also set wildcard "*" to allow all domains to reference the resource. Common configurations are shown below:

Access-Control-Allow-Origin: *
Access-Control-Allow-Origin:

http://www.test.com

Note:

- Wildcard domain names are not supported (such as *.qq.com)
- Either use "*" or specify a URI

- Please add http:// or https:// as prefix when configure specified domain name;

Access-Control-Allow-Methods

You can configure multiple allowed cross-domain request methods using Access-Control-Allow-Methods:

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

Access-Control-Max-Age

Access-Control-Max-Age specifies the valid time of pre-request.

For non-simple cross-domain requests, an additional HTTPS query request ("pre-request") is needed before the formal communication to check whether the cross-domain request is secure and acceptable. In any of the following situations, the request will be considered as a pre-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.

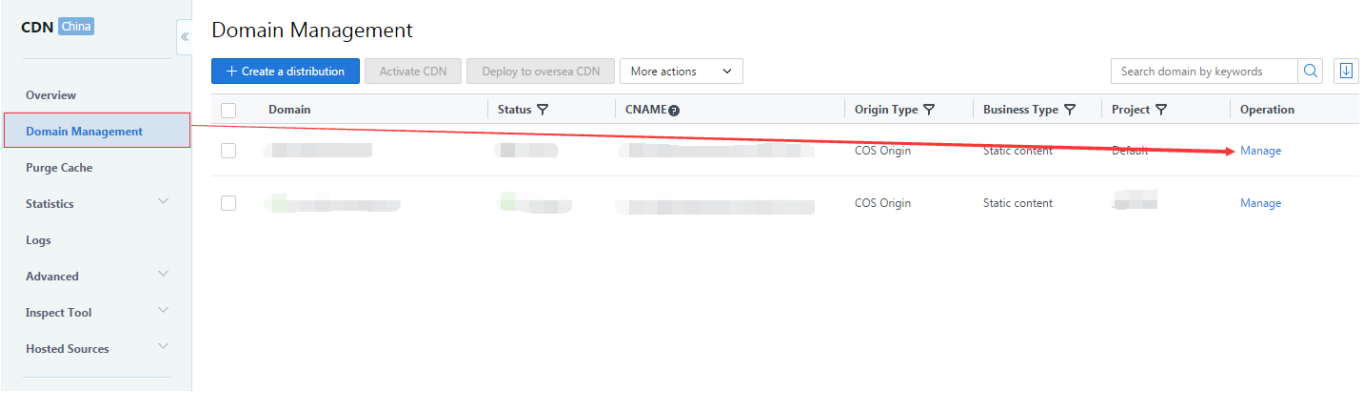
Access-Control-Max-Age is measured in second. Here is a configuration example:

```
Access-Control-Max-Age: 1728000
```

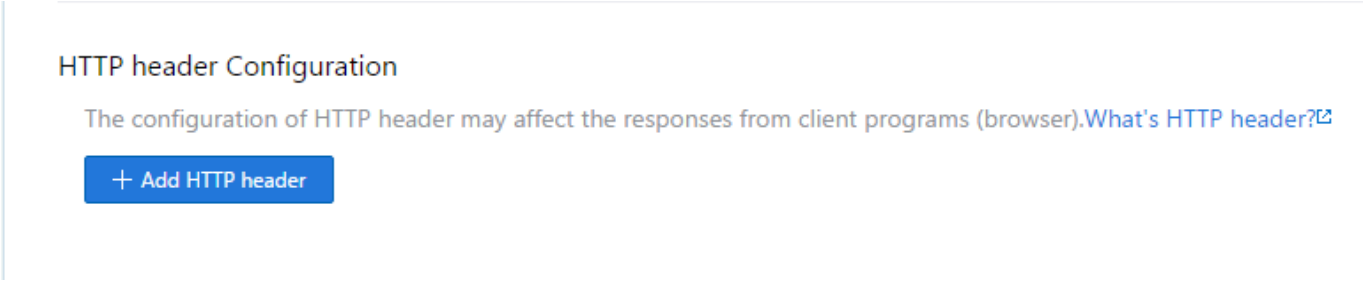
This indicates no more pre-request will be sent for the cross-domain access to this resource within 1,728,000 seconds (20 days).

Configuration Process

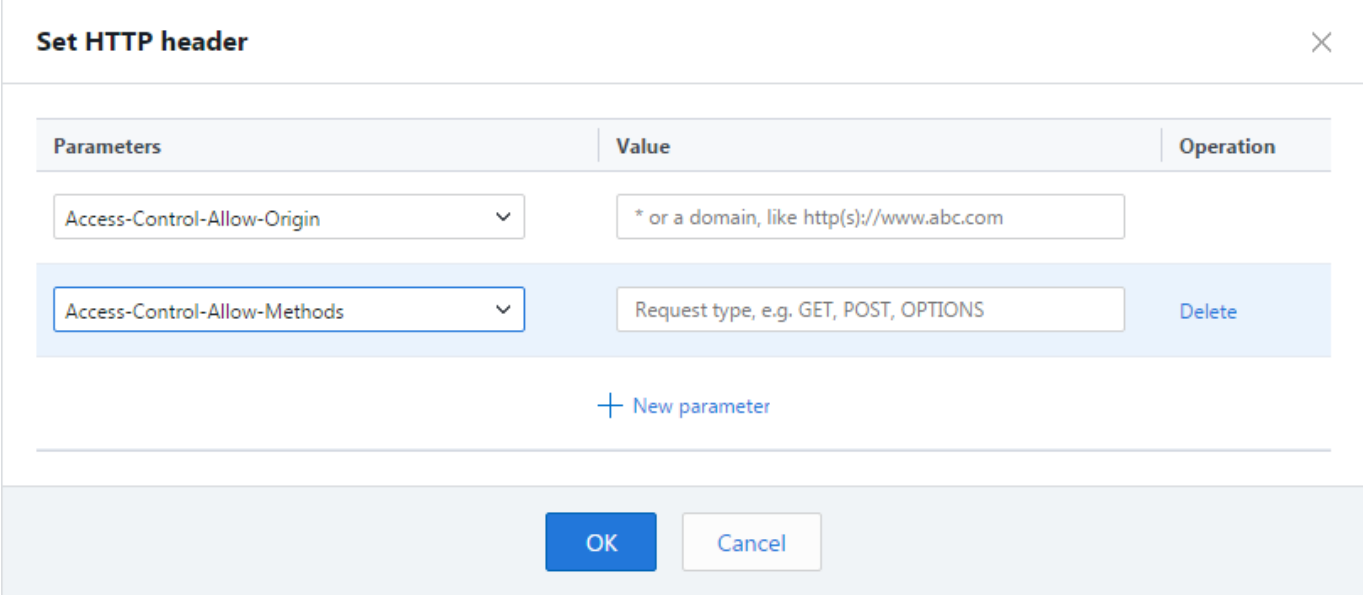
Log in to CDN Console and go to "Domain Management" page. Then click Manage button to the right of the domain name to enter the management page:



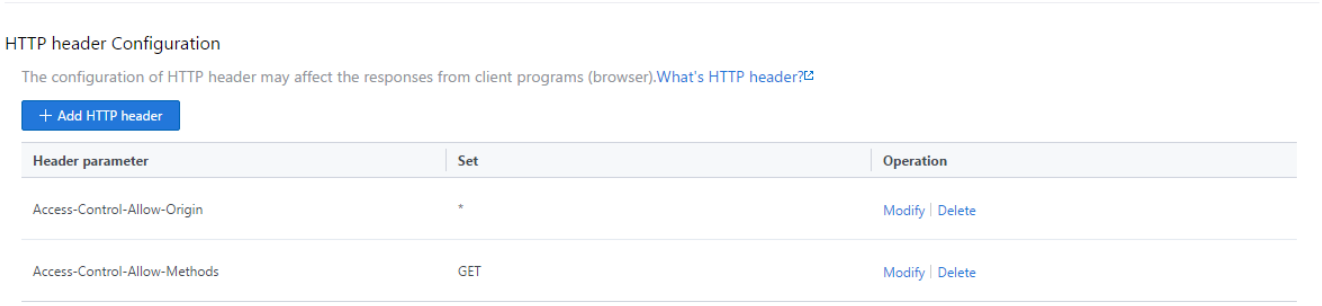
Go to "Advanced Configuration" and find "HTTP header Configuration", then click "Add HTTP header":



Select the header to add and complete the configuration for it. You can add multiple headers at a time, but the same header can only be added once:



Click OK to complete configuration. It will take about 5 minutes for the configuration to take effect:



You can also modify or delete existing headers.

International Direct Connect

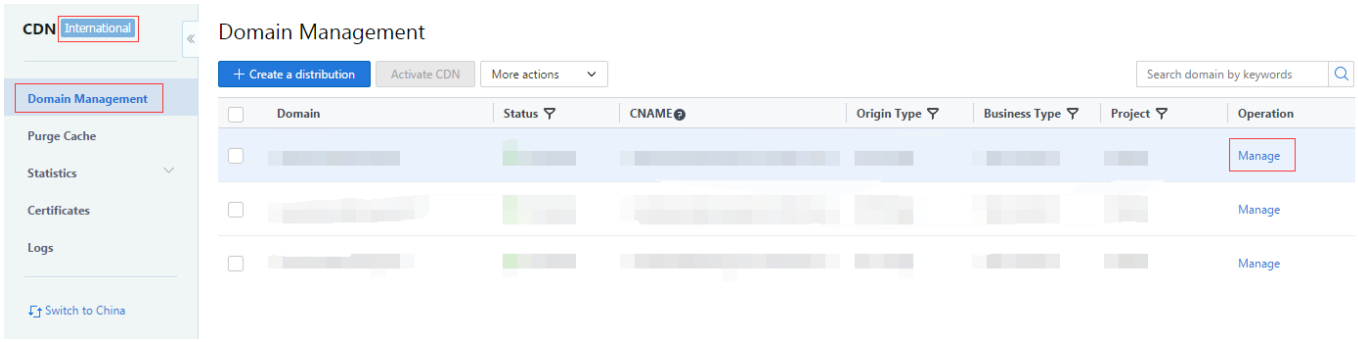
Overview

If your origin server is located at home, an overseas acceleration often suffers unstable or slow back-to-origin connection. You can greatly improve cross-border access by using an overseas intermediate node in combination with international private line service. When a user sends a request, it will first reach the edge node. If this node does not have the requested resource, it will send a request to the oversea intermediate node. And if the requested resource is not available at the oversea intermediate node, the intermediate node will need to send a request to a level-three node at home. This cross-border request will be sent via Tencent's private network instead of the public network. If the level-three node at home still does not have the requested resource, the request will go to the origin server. Activating the international private line configuration will significantly improve your international access.

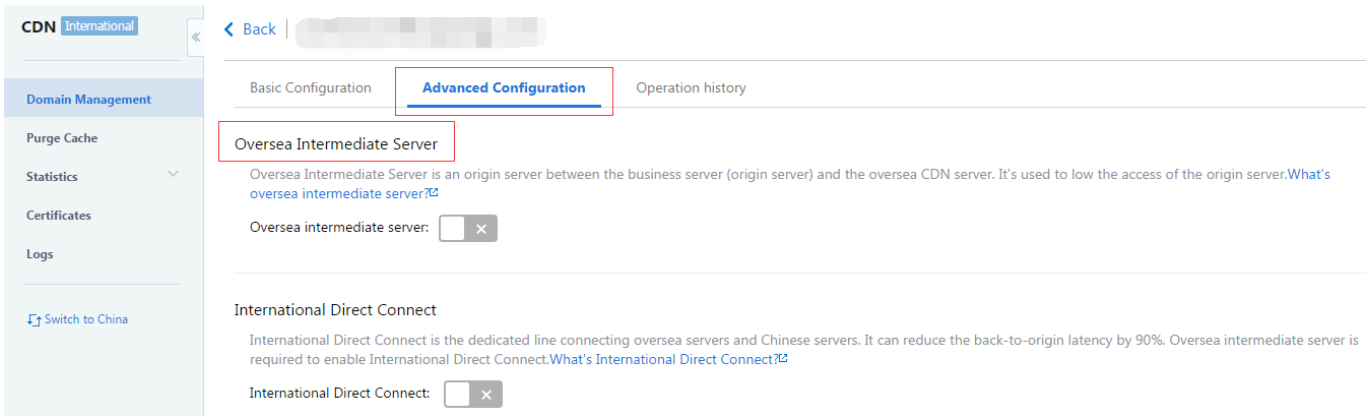
Note: You need to enable overseas intermediate node to activate international private line service. Currently, international private line service is only available for users who have activated overseas CDN acceleration. Oversea CDN acceleration service is under beta test. It will become fully available in the future.

Configuration Instructions

Log in to CDN Console, switch to international acceleration and go to Domain Management page. Then click the Manage button to the right of the domain to be configured



You can find International Private Line in "Advanced Configuration"



Default configuration: The intermediate node configuration is disabled by default