

Alibaba Cloud CDN

User Guide

User Guide

Product restrictions

Restrictions on the use of CDN

Real-name authentication must be performed for accounts on the Alibaba Cloud official website.

A CDN domain must be on file with the Ministry of Industry and Information Technology (MIIT) and connected to Alibaba Cloud.

The origin site content of a CDN domain must be stored on Elastic Compute Service (ECS) or Object Storage Service (OSS). If the origin site content is not stored on Alibaba Cloud, access must be reviewed.

All domains attempting to access CDN must be reviewed. CDN access is not allowed in any of the following scenarios:

The CDN domain cannot be accessed normally or the content does not include any substantive information.

The CDN domain is for a private game server.

The CDN domain is used for role playing games or card games.

The CDN domain is for a P2P website.

The CDN domain is for a lottery website.

The CDN domain is for an illegal hospital or pharmaceutical website.

The CDN domain is for a site involving porn, gambling, drugs, etc.

An automatic timeout rejection occurs, and outputs the following: Your domain name is rejected because it failed to comply with CDN access rules. Reference the feedback and submit a qualified domain name to be reviewed again.

Domains that have accessed Alibaba Cloud CDN will be reviewed regularly. If any of the preceding violations are recorded, CDN acceleration for the associated domain will be immediately suspended and CDN services for all domains of the associated user will also be suspended.

When a CDN domain is in **Deactivated** status (including **Not Approved** status) for more than 30 days, the system will automatically delete records related to this domain name. If you need to continue CDN acceleration for this domain name, it will have to be added again.

Does accelerated content delivery take effect after a CDN domain is approved?

No. To implement accelerated content delivery, you must direct your domain to a Canonical Name (CNAME) domain generated by CDN and add a CNAME record at the Domain Name System (DNS) service provider.

Restriction on the number of CDN domains

The maximum number of CDN domains for each Alibaba Cloud account is 20. If additional CDN domains are needed, please submit a ticket requesting this service to Alibaba Cloud technical support.

Restriction on the number of IP origin sites

The maximum number of IP origin sites for each CDN domain is 20 (namely 20 IP addresses). If more IP origin sites are needed, please submit a ticket requesting this service to Alibaba Cloud technical support.

Restrictions on the number of cache refresh and push operations

- URL refresh: 2000 items/day/account
- Directory refresh: 100 items/day/account

Introduction

Alibaba Cloud CDN is a distributed network that overlays on the bearer network and is composed of edge node server clusters distributed across different regions. The CDN network replaces the traditional data transmission modes centered on web servers.

The CDN Console can help you add a CDN domain, refresh cache, and perform other configuration tasks. It also provides resource monitoring services including real-time data analysis. This document presents basic information about the CDN Console.

Overview of CDN operation

After you log on to the CDN Console, the CDN operation information for the current account is displayed on the home page as follows:

Billing method

Key data: the number of domains in normal status and the total traffic for all domains this month

This month's data:

Domain peak bandwidth

Top 5 domains according to the accumulated downstream traffic

Top 5 URLs according to access numbers

Region distribution of users who access the acceleration resources

The total number of accesses to the acceleration resources

Note: This month indicates the current calendar month.

Use the left-side navigation bar to set relevant functions and look at the data.

Function	Description
Add a CDN domain	Add a new CDN domain, manage or delete an existing CDN domain, or change the basic information and configuration of a CDN domain.

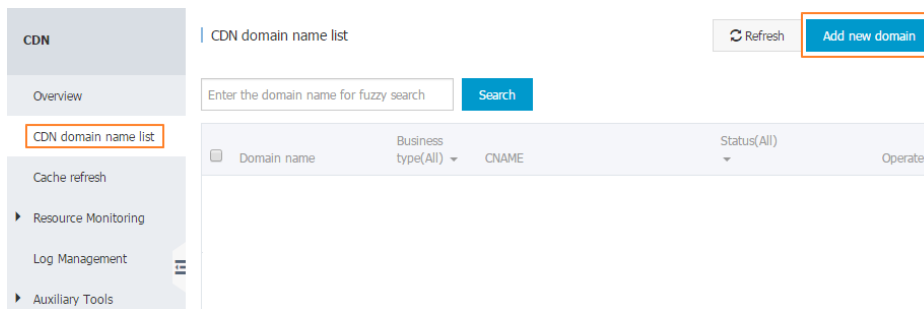
Cache refresh	URL refresh and directory refresh modes are provided.
Resource monitoring	Monitors traffic, user access, and security and displays data analysis.
Log management	Log download, log storage (coming soon), and cloud report.
Diagnostic tools	Link diagnostic tools.

Add a CDN domain

Log on to the CDN Console. Click **CDN Domain Name List** and then click **Add New Domain** in the upper-right corner. If the source content is in OSS, select OSS Bucket acceleration.

Step 1. Click CDN Domain Name List

Click **Add New Domain** in the upper-right corner.



Note: A single user can add up to 20 domain names. If you are no longer using a domain name, it is suggested that you delete its record.

Step 2. Enter basic information

Enter CDN domain, select the appropriate business type and origin site type.

CDN

Overview

Cache refresh

Resource Monitoring

Log Management

Auxiliary Tools

Add new domain

Enter basic information

Review

Complete

CDN domain name list

* CDN domain:

* Business Type:

* Origin site type:

Cancel

Next

Considerations:

CDN domain

The domain entered must have its filing completed. If filing is still in progress, the domain cannot be accessed.

Domain content must comply with CDN specifications. For details, refer to [Product restrictions](#).

Business type

The business type descriptions are as follows:

Business Type	Description
Images and small files acceleration	Recommended if the content to be accelerated is mostly images and web files.
Large file download acceleration	Recommended if the content to be accelerated is large files (static files larger than 20 MB).
Video/audio on-demand acceleration	Recommended if the content to be accelerated is video on-demand or live video services.
Live streaming media acceleration (being tested)	The acceleration of live streaming media is provided. Currently, RTMP-based and HLS-based live streaming acceleration is supported. Live streaming services do not support user-defined origin sites. Currently, the central live streaming server is provided: video-center.alivecdn.com.

Note:

- Ensure that **check url** can be accessed normally before adding a domain.

If you click **Next**, the CDN domain to be added will be verified. The rules are as follows:

- A CDN domain must be filed by the Ministry of Industry and Information Technology (MIIT).
- Duplicate CDN domains are not supported. If your CDN domain is occupied, submit a ticket for processing.
- Up to 20 CDN domains can be added under the same account.

Origin site type

Origin Site Type	Description
IP	Internet IP addresses of multiple servers can be entered. Note: If the IP address entered does not belong to an Alibaba Cloud product, the domain to be added will need to be reviewed. This can take 1 or 2 working days.
Origin site domain name	Enter an origin site domain. Note: The origin site domain entered cannot be the same as the CDN domain to be added. For example, if the CDN domain to be added is test.yourdomain.com, it is recommended to set your origin site to src.yourcompany.com.
OSS domain name	Enter an OSS bucket access address, for example, xxx.aliyuncs.com.

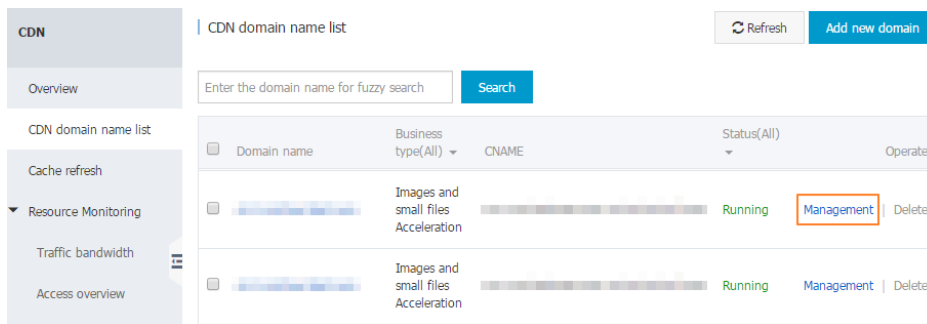
Note: If the origin site is a domain, it cannot be the same as the CDN domain to be added. If related resources requested by a user has not been cached on the CDN node, the CDN node will get it from the origin site and return it to the user. If the CDN domain and the origin site domain are the same, request parsing will be repeated on the CDN node, and the CDN node cannot return to the origin site to retrieve the content. If your CDN domain is example.aliyun.com, it is recommended that you use src.example.aliyun.com as the origin site for differentiation.

Step 3. (Optional) Enter the configuration information

Domain configurations can be performed after a CDN domain is created successfully. This procedure is optional.

Step 4. Confirm the information

After confirming the basic information and domain name configurations, click **Complete**. The new domain name is displayed in the list. Click **Management** or the domain name to modify the configurations.



Note: When the domain name status is **Running**, the configuration is taking effect.

Delete domain name configurations

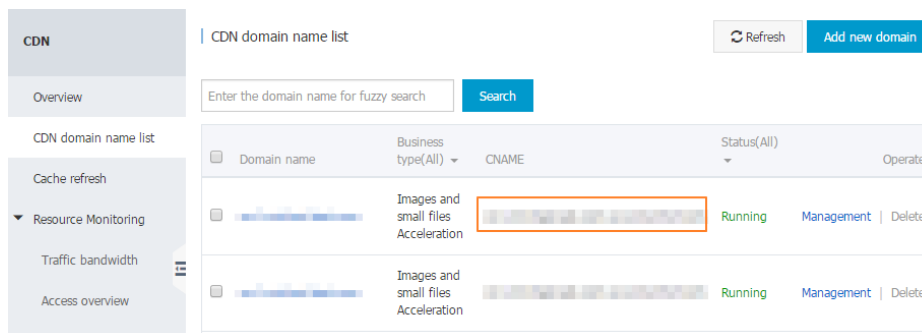
To delete a domain name, you must **Stop** it if it is in **Running** status. After the status changes to **Stopped**, the **Delete** button becomes available and the domain name can be deleted.



CNAME binding

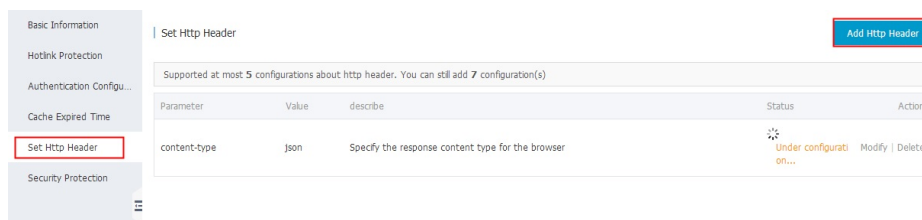
Obtain the correct CNAME domain.

The CNAME domain is displayed in the CDN domain list, as shown in the following screenshot:



Query the domain status.

Domain name configurations must be distributed to all nodes in the network; this can take up to 15 minutes.



Correctly configure DNS resolution.

Go to your DNS service provider to complete the CNAME configuration.

Verify that the CNAME domain has been added successfully.

Ping the added CDN domain. If you are directed to the `*.kunlun.com` domain, the CDN is serving your website.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\>ping .org.cn

Pinging .org.cn.w.kunlun.com [220.181.105.] with 32 bytes of data:
Reply from 220.181.105.: bytes=32 time=8ms TTL=39
Reply from 220.181.105.: bytes=32 time=8ms TTL=39
Reply from 220.181.105.: bytes=32 time=7ms TTL=39
Reply from 220.181.105.: bytes=32 time=7ms TTL=39

Ping statistics for 220.181.105.:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 8ms, Average = 7ms
```

Function overview

Back-to-source settings

Item	Description	Default
Source host	Specifies the host domain name that a CDN node will access in the back-to-source process. Three options are available: CDN domain, original site domain name, and custom domain name.	CDN domain
Back-to-source with the same protocol	Back-to-source requests for resources use exactly the	Disabled

	same protocol as used by the client to request the resources.	
--	---	--

Cache settings

Item	Description	Default
Cache policy configuration	Customizes cache expiration rules for specified resources.	Disabled
Setting the HTTP Request Header	Sets an HTTP request header. Eight parameters are currently available for HTTP request header customization.	Disabled
Customizing the 404 page	Customizes the 404 page. Three options are available: default 404 page, public welfare 404 page, and custom 404 page.	Default 404 page

Access control

Item	Description	Default
Anti-leech	Configures a referer blacklist or whitelist to identify and filter visitors.	Disabled
URL authentication	Uses URL authentication methods to protect resources on an origin site.	Disabled
IP blacklist	Configures the access IP blacklist to identify and filter visitors.	Disabled

Performance optimization

Item	Description	Default
Page optimization	Compresses and removes useless blank lines and carriage return characters to effectively reduce the page size.	Disabled
Smart compression	Supports smart compression for content in multiple formats to effectively reduce	Disabled

	the size of user transmitted content.	
Filter parameter	Removes parameters after ? in a URL request during the back-to-source process.	Disabled

Video-related settings

Item	Description	Default
Back-to-source of range	Allows a user to notify an origin site server to return partial content within a specified range. This function helps with accelerated delivery of large files.	Disabled
Drag/drop playback	Enables random drag or drop playback in a video or audio on-demand scenario.	Disabled

Other settings

Item	Description	Default
SettinghttpDNS	Provides a DNS service by using the HTTP protocol to directly access the server of Alibaba Cloud CDN.	Disabled

Setting Back-to-source

Back-to-source with the same protocol

Introduction

When the back-to-source with the same protocol feature is enabled, back-to-source requests for resources will use the same protocol used by the client in order to request resources. If the client makes an HTTPS request for resources, but the resources are not cached on the node, a back-to-

source HTTPS request will be made for resources. This protocol is also applicable for HTTP requests.

Note: The origin site must support both the port 80 and port 443; otherwise, the back-to-source may fail.

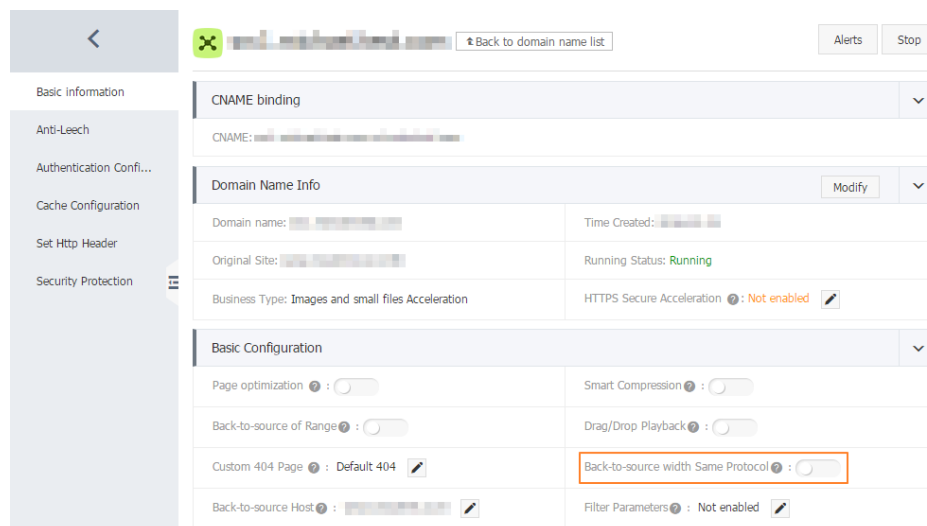
Operation procedure

Log on to the CDN console.

On the left navigation bar, click **CDN domain name list**.

Select a domain to enter the management page.

Enable or disable the **Back-to-source with the Same Protocol** feature.



The screenshot shows the CDN console interface. On the left is a navigation menu with options: Basic Information, Anti-Leech, Authentication Confi..., Cache Configuration, Set Http Header, and Security Protection. The main content area has a top bar with a back arrow, a domain name, and a 'Back to domain name list' link. Below this are sections for 'CNAME binding', 'Domain Name Info' (with fields for Domain name, Time Created, Original Site, Running Status, Business Type, and HTTPS Secure Acceleration), and 'Basic Configuration'. The 'Basic Configuration' section contains several toggle switches: Page optimization, Smart Compression, Back-to-source of Range, Drag/Drop Playback, Custom 404 Page (set to Default 404), Back-to-source with Same Protocol (highlighted with a red box), Back-to-source Host, and Filter Parameters (set to Not enabled).

Back-to-source host

Introduction

You can customize a Web server domain name that a CDN node accesses in the back-to-source process.

Notice: The **Back-to-source host** must be set to the CDN domain for data to return to the source because an origin site is a CDN domain in the OSS space.

Operation procedure

Log on to the CDN console.

On the left navigation bar, click **CDN domain name list**.

Select a domain to enter the management page.

Set **Back-to-source Host**.

The **Back-to-source Host** configuration is optional and its default value is **CDN Domain**.

The value options include CDN Domain, original site domain name, and Custom domain name.

The screenshot shows the CDN console interface. On the left is a navigation menu with options: Basic Information, Anti-Leech, Authentication Confi..., Cache Configuration, Set Http Header, and Security Protection. The main content area is titled 'CDN domain name list' and contains several sections: 'CNAME binding', 'Domain Name Info', and 'Basic Configuration'. The 'Domain Name Info' section shows details like Domain name, Original Site, Business Type, and Time Created. The 'Basic Configuration' section contains various toggle switches and input fields. The 'Back-to-source Host' field is highlighted with a red box, indicating it is the field to be configured.

Setting Cache Policy

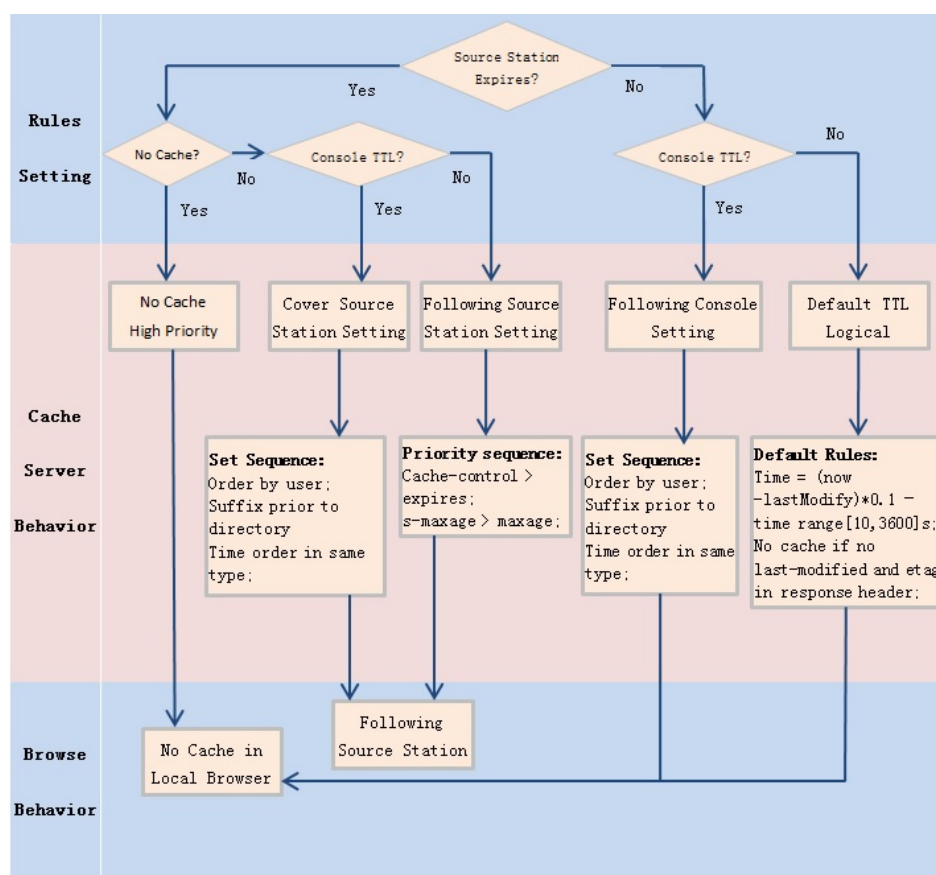
Cache policy configuration

Introduction

This function can be used to set the actions of a cache server against resources in different directory paths, or resources with different filename suffixes. You can customize cache expiration rules for specified resources.

You can customize a cache policy priority.

The following figure shows the default cache policies.



Note:

This function is used to set file expiration time. The priority specified here is higher than that configured on the origin site. If no cache policy is configured on the origin site, you can set a cache policy by directory and filename suffix (the full path mode is supported).

For static files that are not updated frequently (for example, image files and application download files), it is suggested that the cache duration be set to one month or longer.

For static files that need to be updated frequently (for example, JS files and CSS files), you can reduce the cache duration based on service conditions.

For dynamic files (for example, PHP files, JSP files, and ASP files), it is suggested that the cache duration be set to 0s, indicating that the files will not be cached. If dynamic files such as PHP files are not updated frequently, it is suggested that the cache duration be set to a small value.

It is recommended that the content on an origin site is updated with the same file name, but tagged with different version numbers; for example, img-v1.0.jpg and img-v2.1.jpg.

Operation procedure

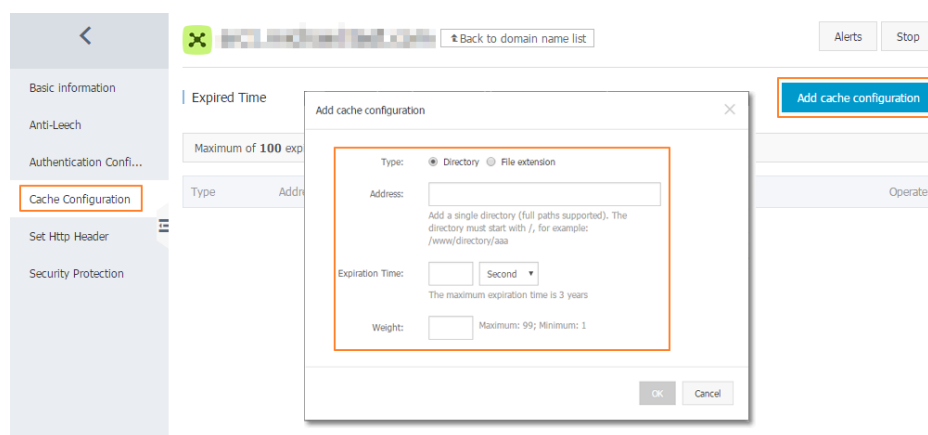
Log on to the CDN console.

On the left navigation bar, click **CDN domain name list**.

Select a domain to enter the management page.

On the left navigation bar, click **Cache Configuration**.

Click **Add cache configuration**.



For example, set three cache policies for the CDN domain example.aliyun.com.

- Cache policy 1: the cache duration for all files suffixed with .jpg and .png is one month, and the weight is 90.
- Cache policy 2: the cache duration for files in the /www/dir/aaa directory is one hour, and the weight is 70.
- Cache policy 3: the cache duration for the full path /www/dir/aaa/example.php is 0 s (No cache action will be performed), and the weight is 80.

The priority is Policy 1 > Policy 3 > Policy 2.

Note:

The range of weight is from 1 to 99. The larger the number, the higher the priority.

It is recommended that you do not set the same weights for different cache policies. Cache policies with the same weight will be assigned a random weight value.

Customizing the 404 page

Introduction

You can customize the page that is displayed when a 404 status code is returned. The following three options are available:

Default 404 page: when an HTTP 404 error is returned, the server returns the default 404 Not Found page.

Public welfare 404 page: when an HTTP 404 error is returned, the server redirects it to the real-time updated public welfare 404 page.

Custom 404 page: when an HTTP 404 error is returned, the server redirects it to the customized 404 page you designed and edited. In this case, you need to predefine a complete URL for the page.

Note:

The public welfare 404 page is a public welfare resource of Alibaba Cloud. It is free and generates no traffic fees.

Custom 404 pages are personal resources which are billed based on normal delivery.

Operation procedure

Log on to the CDN console.

On the left navigation bar, click **CDN domain name list**.

Select a domain to enter the management page.

Customize the 404 page.

The screenshot shows the Alibaba Cloud CDN console interface. On the left is a sidebar with navigation options: Basic Information, Anti-Leech, Authentication Confi..., Cache Configuration, Set Http Header, and Security Protection. The main content area is divided into two sections: 'Domain Name Info' and 'Basic Configuration'. The 'Domain Name Info' section includes fields for CNAME binding, Domain name, Original Site, Business Type (Images and small files Acceleration), Time Created, Running Status (Running), and HTTPS Secure Acceleration (Not enabled). The 'Basic Configuration' section includes toggle switches for Page optimization, Smart Compression, Back-to-source of Range, Drag/Drop Playback, Custom 404 Page (set to Default 404), Back-to-source width Same Protocol, Back-to-source Host, and Filter Parameters (Not enabled). The 'Custom 404 Page' option is highlighted with a red box.

If you select the **Custom 404** option, you need to store the page resources, like other static files, under the origin site domain. You can access the page through a CDN domain by entering the complete URL (including http://) of the CDN domain.

For example, if the CDN domain is exp.aliyun.com and the 404 page is error404.html, you can store the error404.html page to the origin site. Select the **Custom 404** option, and enter http://exp.aliyun.com/error404.html.

Set the HTTP request header

Introduction

You can set an HTTP request header. Eight HTTP request header parameters are available for customization. The parameters are as follows:

Parameter	Description
Content-Type	Specifies a content type for the response returned to a client program.
Cache-Control	Specifies a cache mechanism that is typically following the request/response process of a client program.
Content-Disposition	Specifies a default filename for activating the file download setting when a response is returned to a client program.

Content-Language	Specifies a language in which a response is returned to a client program.
Expires	Specifies expiration time for the response returned to a client program.
Access-Control-Allow-Origin	Specifies an origin that is allowed to send cross-domain requests.
Access-Control-Allow-Methods	Specifies the allowed cross-domain request method.
Access-Control-Max-Age	Specifies the cache duration of the returned result for a pre-fetch request initiated by a client program for a particular resource.

Note:

The HTTP request header setting will affect responses to client programs (for example, browser) for all resources under the CDN domain, but will not affect the behavior of the cache server.

Only the preceding HTTP header parameters are supported currently. If additional requirements for HTTP header settings are required, please submit a ticket to Alibaba Cloud technical support.

The Access-Control-Allow-Origin parameter can be set to * (indicating all domains) or to a complete domain name such as www.aliyun.com. Wildcard domain setting is not supported currently.

Operation procedure

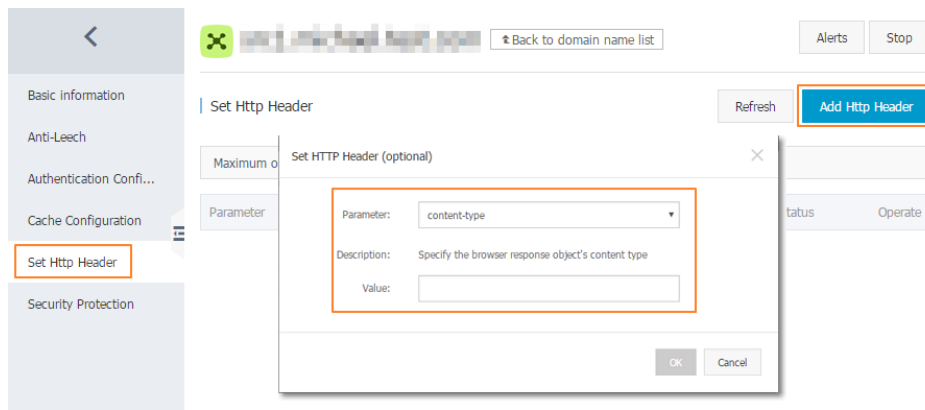
Log on to the CDN console.

On the left navigation bar, click **CDN domain name list**.

Select a domain to enter the management page.

On the left navigation bar, click **Set Http Header**.

Click **Add Http Header**.



Resource Access Control

Anti-leech

Introduction

The anti-leech function is based on the HTTP referer mechanism where the referer, namely an HTTP header field, is used for source tracking, source recognition and processing. You can configure a referer black list or white list to identify and filter visitors in order to limit access to your CDN resources.

Currently, the anti-leech function supports the black list or white list mechanism. After a visitor initiates a request for a resource, and the request arrives at a CDN node, the CDN node filters the identity of the visitor based on the presets of the anti-leech black list or white list. If the identity complies with the rules, the visitor can access the requested resource; if the identity does not comply with the rules, the request is forbidden and a 403 response code is returned.

Note:

This function is optional and is disabled by default.

To enable this function, you can select **Refer Blacklist** or **Refer Whitelist** to edit. You can only select one of these options to edit.

A null Referer field can be used to access resources on a CDN node (that is, whether a web browser can use its URL to directly access resources on a target URL).

Operation procedure

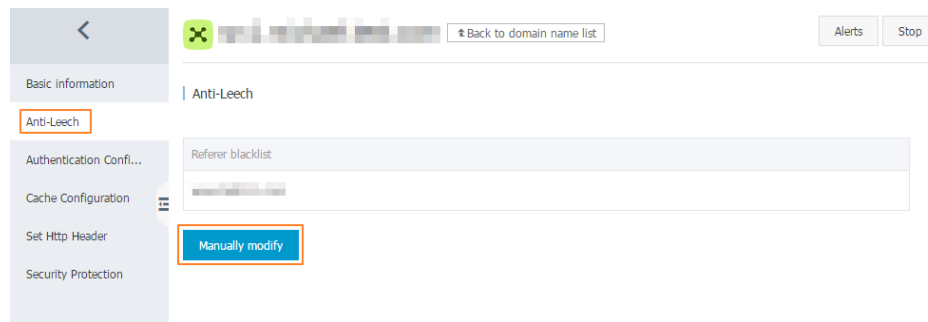
Log on to the CDN console.

On the left navigation bar, click **CDN domain name list**.

Select a domain to enter the management page.

On the left navigation bar, click **Anti-Leech**.

Click **Manually modify** to set the referer black list or white list.



URL authentication

Introduction

The URL authentication function protects user' s site resources from illegal download and misuse. Leeching issues are only partially solved by adding the referer blacklist or whitelist. Because the referer content may be forged, this method cannot protect site resources completely. Applying URL authentication is recommended to protect the security of origin site resources.

Concept

The URL authentication function uses Alibaba Cloud CDN nodes in combination with client resource sites to provide a more secure anti-theft protection for origin site resources. The CDN client site

provides a user with an encrypted URL (including permission verification information) and the user uses it to initiate a request to the CDN node. The CDN node verifies the permission information in the encrypted URL to determine the legality of the request. Legal requests will receive a normal response and illegal requests will be rejected. This protects CDN client site resources.

URL authentication methods

Alibaba Cloud CDN supports authentication Method A, Method B and Method C. You can select an appropriate method to protect origin site resources based on your business requirements.

Authentication method A

Concept

Structure of users' encrypted URLs

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

Authentication field descriptions

The PrivateKey field can be set by the user.

Field	Description
timestamp	The expiration time. It is a positive integer with a fixed length of 10 and a time in seconds from January 1, 1970. This 10-digit integer is used to control the expiration time.
rand	Random number. It is typically set to 0.
uid	Temporarily unused (set to 0).
md5hash	The verification string is calculated using the MD5 algorithm. It is comprised of digits and lowercase English letters (0-9, a-z) with a fixed length of 32.

After the CDN server receives the request, it first determines whether the request timestamp is less than the current time. If so, it determines that the request has expired and returns an HTTP 403 error. If the timestamp is greater than the current time, it constructs an equivalent string (see the following string construction method). Then, it uses the MD5 algorithm to calculate the HashValue and compares it with the md5hash contained in the request. If they are consistent, the request passes the authentication and the file is returned. Otherwise, the request authentication fails and an HTTP 403 error is returned.

The HashValue is calculated according to the following method:

```
sstring = "URI-Timestamp-rand-uid-PrivateKey" (URI is the relative address of a user's request object. It does not contain parameters such as "/Filename")
HashValue = md5sum(sstring)
```

Example

Request an object through req_auth.

```
http://cdn.example.com/video/standard/1K.html
```

Set the access key to aliyuncdnexp1234 (set by the user).

3. The expiration date of the authentication configuration file is 2015-10-10 00:00:00, and the calculated number of seconds is 1,444,435,200.

The CDN server constructs a signature string used to calculate the HashValue.

```
/video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234"
```

The CDN server calculates the HashValue according to the signature string.

```
HashValue = md5sum("/video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234") =
80cd3862d699b7118eed99103f2a3a4f
```

The request URL is as follows.

```
http://cdn.example.com/video/standard/1K.html?auth_key=1444435200-0-0-
80cd3862d699b7118eed99103f2a3a4f
```

The calculated HashValue is the same as the md5hash = 80cd3862d699b7118eed99103f2a3a4f value in the user request, so the request passes the authentication.

Authentication method B

Concept

Format of users' encrypted URLs

The user access URL is as follows.

```
http://DomainName/timestamp/md5hash/FileName
```

Encrypted URL structure: domain name/URL generation time (accurate to minutes) (timestamp)/md5 value (md5hash)/real path of the source server (FileName). The URL validity period is 1,800 s.

When the request passes the authentication, the back-to-source URL is as follows.

```
http://DomainName/FileName
```

Authentication field descriptions

Note:

The PrivateKey field can be set by the CDN user.

The validity period 1,800 s indicates that the authentication fails when the user fails to access the client source server 1,800 s after the preset access time. For example, if the preset access time is 2020-08-15 15:00:00, the actual link expiration time is 2020-08-15 15:30:00.

Field	Description
DomainName	The domain name of the CDN client site.
timestamp	The time designated for when the user accesses the client source server. This is part of the URL as well as a factor used to calculate the md5hash. The format is YYYYMMDDHHMM and the validity period is 1,800 s.
md5hash	The timestamp, FileName, and preset PrivateKey are used in the MD5 algorithm to get this string, namely md5 (PrivateKey + timestamp + FileName).
FileName	The actual back-to-source access URL (Note: during authentication, the FileName begins with /).

Example

Back-to-source request object.

```
http://cdn.example.com/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
```

Set the access key to aliyuncdnexp1234 (set by the user).

The time format for when the user accesses the client source server is 201508150800 (the format is YYYYMMDDHHMM).

The CDN server constructs a signature string used to calculate the md5hash.

```
aliyuncdnexp1234201508150800/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
```

The CDN server calculates the md5hash according to the signature string.

```
md5hash = md5sum("aliyuncdnexp1234201508150800/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3") =  
9044548ef1527deadafa49a890a377f0
```

The request URL is as follows.

```
http://cdn.example.com/201508150800/9044548ef1527deadafa49a890a377f0/4/44/44c0909bcfc20a01a  
faf256ca99a8b8b.mp3
```

The calculated md5hash is the same as the md5hash = 9044548ef1527deadafa49a890a377f0 value in the user request, so the request passes the authentication.

Authentication method C

Principle

Format of users' encrypted URLs

Format 1:

`http://DomainName/{<md5hash>/<timestamp>}/FileName`

Format 2:

`http://DomainName/FileName{&KEY1= <md5hash>&KEY2= <timestamp>}`

Where:

Content in brackets indicates the encryption information added to the standard URL.

<md5hash> is the authentication information string after MD5 encryption.

<timestamp> is a non-encrypted string expressed in plaintext. It is a hexadecimal value with a fixed length of 10, indicating the time in seconds from January 1, 1970.

Format 1 is used to encrypt the URL, as shown below.

```
http://cdn.example.com/a37fa50a5fb8f71214b1e7c95ec7a1bd/55CE8100/test.flv
```

The <md5hash> value is a37fa50a5fb8f71214b1e7c95ec7a1bd. The <timestamp> value is 55CE8100.

Authentication field descriptions

<md5hash> field descriptions:

Field	Description
PrivateKey	An interference string. Different users use different interference strings.
FileName	The back-to-source access URL (Note: during authentication, the path begins with /).
time	The time when the user accesses the source server. It is UNIX time expressed as a hexadecimal value.

- PrivateKey is set to aliyuncdnexp1234.
- FileName is set to /test.flv.
- time is set to 55CE8100.

So the md5hash value is as follows.

```
md5hash = md5sum(aliyuncdnexp1234/test.flv55CE8100) = a37fa50a5fb8f71214b1e7c95ec7a1bd
```

Plaintext: timestamp = 55CE8100.

The URL is generated as so:

Format 1:

```
http://cdn.example.com/a37fa50a5fb8f71214b1e7c95ec7a1bd/55CE8100/test.flv
```

Format 2:

```
http://cdn.example.com/test.flv&KEY1=a37fa50a5fb8f71214b1e7c95ec7a1bd&KEY2=55CE8100
```

Example

When the user uses an encrypted URL to access a CDN node, the CDN server extracts encrypted string 1 and obtains the <FileName> of the original URL. After this process, the CDN server authenticates the URL.

The CDN server uses the <FileName> of the original URL and the request time and PrivateKey to perform MD5 encryption and obtain encrypted string 2.

The CDN server compares encrypted string 2 with encrypted string 1. If the strings are not the same, the request is rejected.

The current time on the CDN server is used to subtract the plaintext time in the access URL to determine whether the preset time limit t expires (the time limit t is set to 1,800 s by default).

The validity period 1,800 s means that the authentication fails when the user fails to access the client source server 1,800 s after the preset access time. For example, if the preset access time is 2020-08-15 15:00:00, the actual link expiration time is 2020-08-15 15:30:00.

The request is valid if the time difference is less than the preset time limit. The CDN server will send a normal response. Any aberration from this means the request is rejected and an HTTP 403 error is returned.

Sample authentication code

Refer to the Sample Authentication Code document in [CDN Utilities](#).

Operation procedure

Log on to the CDN console.

On the left navigation bar, click **CDN domain name list**.

Select a domain to enter the management page.

On the left navigation bar, click **Authentication Configuration**.

Enable authentication function.

Select an authentication type and set the authentication key in the authentication configuration module.

The screenshot shows the 'Authentication Configuration' page in the Alibaba Cloud CDN console. On the left, a navigation menu lists 'Basic information', 'Anti-Leech', 'Authentication Configuration' (highlighted), 'Cache Configuration', 'Set Http Header', and 'Security Protection'. The main content area is titled 'Authentication Configuration'. It features a toggle switch for 'Enable authentication function' which is turned on, with a 'View authentication description' link next to it. Below this, the 'Authentication type' is set to 'Type A' (radio buttons for Type A, Type B, and Type C). The 'Authentication KEY' section includes a 'Master Key' field (marked with a red asterisk) and a 'Backup Key' field. A red note at the bottom states: 'Note: The authentication key must be 6 to 32 characters long and supports uppercase/lowercase letters and numbers'. At the bottom of the form are 'OK' and 'Cancel' buttons.

IP blacklist

Introduction

CDN supports the blacklist rules. An IP address that is listed on the blacklist cannot access the corresponding domain.

Considerations

You can use an IP network segment to add IP addresses to the blacklist, for example, 127.0.0.1/24.

24 indicates that the first 24 bits in the subnet mask are used as effective bits, for example, 32-24=8 bits are used to express host numbers.

In this way, the subnet can accommodate $2^8 - 2 = 254$ hosts, and the IP network segment scope of 127.0.0.1/24 is 127.0.0.1~127.0.0.255.

Performance Optimization

Smart compression

Introduction

The Smart Compression function can be used to compress majority of static files in order to reduce the size of content transmitted by users, accelerating content delivery.

Contents in the following formats can be compressed: content-type:text/xml, text/plain, text/css, application/javascript, application/x-javascript, application/rss+xml, text/javascript, image/tiff, image/svg+xml, and application/json.

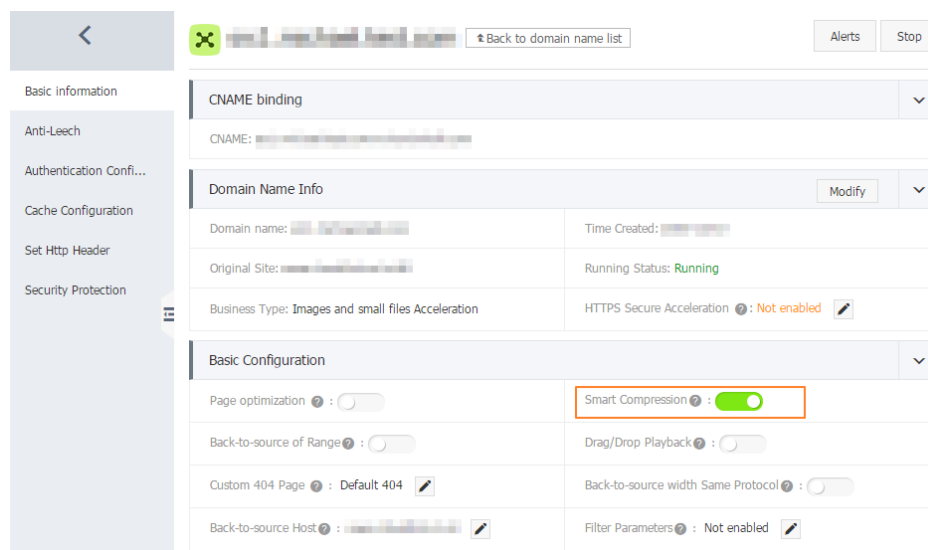
Operation procedure

Log on to the CDN console.

On the left navigation bar, click **CDN domain name list**.

Select a domain to enter the management page.

Enable or disable the smart compression function.



Page optimization

Introduction

The page optimization function can be used to delete comments and repeated whitespaces embedded in HTML, JavaScript, and CSS, in order to remove redundant page content, reduce file size, and improve the efficiency of delivery.

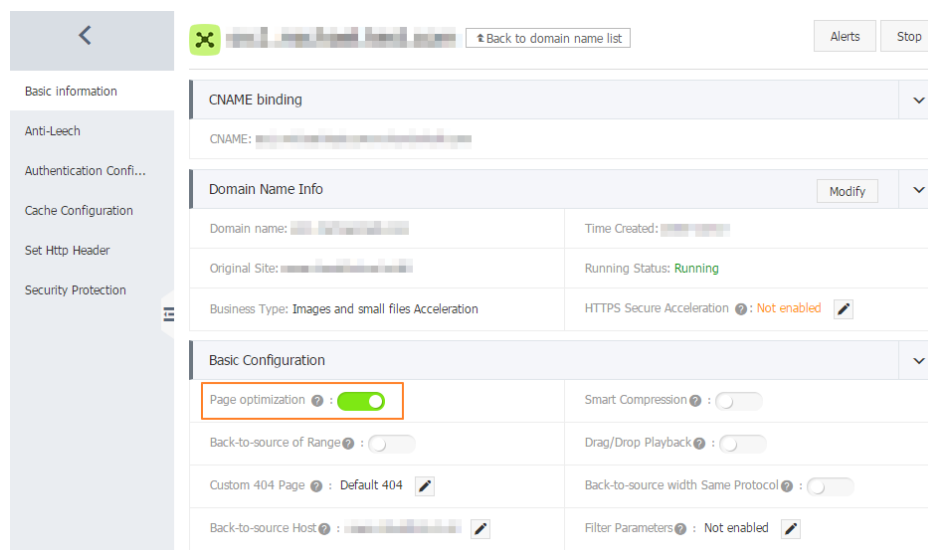
Operation procedure

Log on to the CDN console.

On the left navigation bar, click **CDN domain name list**.

Select a domain to enter the management page.

Enable or disable the page optimization function.



Filter parameter

Introduction

When a URL request carrying ? and request parameters is sent to a CDN node, the CDN node determines whether to send the request to the origin site. If the Filter Parameter function is enabled, after the request arrives at the CDN node, the URL without parameters will be intercepted and requested against the origin site. Additionally, the CDN node retains only one copy. If the Filter Parameter function is disabled, different copies will be cached on the CDN node for different URLs.

An HTTP request typically contains the requisite parameters. If the content of a parameter has a low priority and the parameter overview file can be ignored, it is recommended to enable the Filter Parameter function. This improves the file cache hit rate and the delivery efficiency.

If a parameter has important indicators (for example, if it contains file version information), it is recommended that you disable this function.

Example of use

The `http://www.abc.com/a.jpg?x=1` URL request is sent to a CDN node.

If the Filter Parameter function is enabled, the CDN node initiates the `http://www.abc.com/a.jpg` request (ignore the parameter `x=1`) to the origin site. After the origin site returns a response, the CDN node retains a copy. Then, the origin site continues to respond to `http://www.abc.com/a.jpg` to the terminal. For all requests similar to `http://www.abc.com/a.jpg?parameters`, the origin site responds to the CDN copy content `http://www.abc.com/a.jpg`.

If the Filter Parameter function is disabled, different copies are cached on the CDN node for different URLs. For example, different content are returned from the origin site in case of `http://www.abc.com/a.jpg?x=1` and `http://www.abc.com/a.jpg?x=2`.

Considerations

URL authentication has a higher priority than the Filter Parameter function. Because type A authentication information is contained in the parameter section of an HTTP request, the system first performs the authentication and then caches a copy on the CDN node after the authentication succeeds.

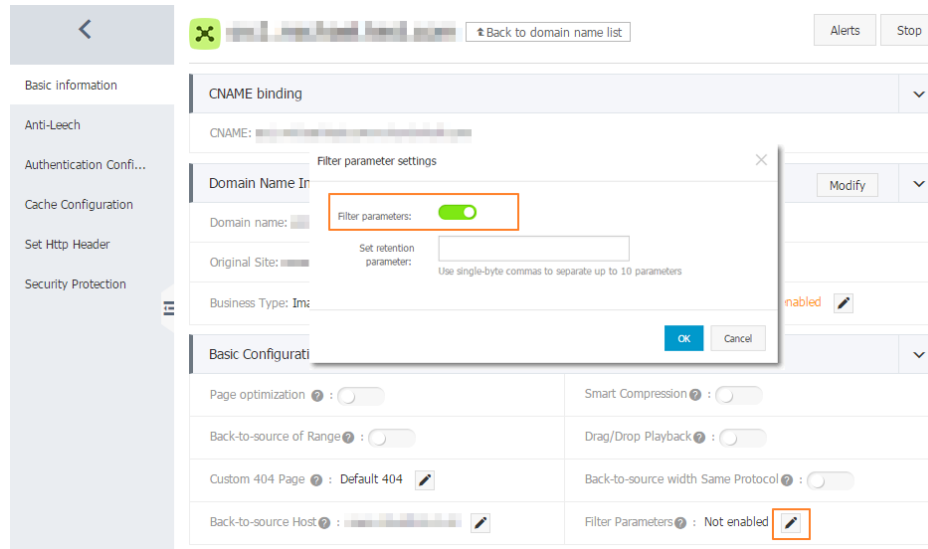
Operation procedure

Log on to the CDN console.

On the left navigation bar, click **CDN domain name list**.

Select a domain to enter the management page.

Enable or disable the filter parameter function.



Video-related Settings

Drag/Drop playback

Introduction

In a video on demand scenario, when the playback progress bar is dragged, the client will send a URL request similar to `http://www.aliyun.com/test.flv?start=10` to the server. The server will return the data starting from the 10th second to the client. This is called Drag/Drop Playback.

After receiving such a request from a client and the Drag/Drop Playback function is enabled, a CDN node can directly return the data to the client starting from the specified second.

Considerations

To use the Drag/Drop Playback function, an origin site must support Range requests. The origin site must be able to return correct 206 Partial Content for an HTTP request header containing a Range field.

The supported file formats are MP4 and FLV.

File Format	Meta Information	start Parameter	Example
MP4	Meta information of an origin site video must be contained in the file header. A video with its meta information contained in the file tail is not supported.	The start parameter specifies the time in seconds. Decimals are supported to indicate milliseconds. For example, start=1.01 indicates that the start time is 1.01s. If the current start is not a key frame, the CDN locates the key frame prior to the time specified by the start parameter.	The http://domain/video.mp4?start=10 requests playing a video from the 10th second.
FLV	An origin site video must contain meta information.	The start parameter specifies a byte. If the current start is not a key frame, the CDN automatically locates the key frame prior to the frame specified by the start parameter.	The http://domain/video.flv?start=10 requests playing a video from the 10th byte.

Operation procedure

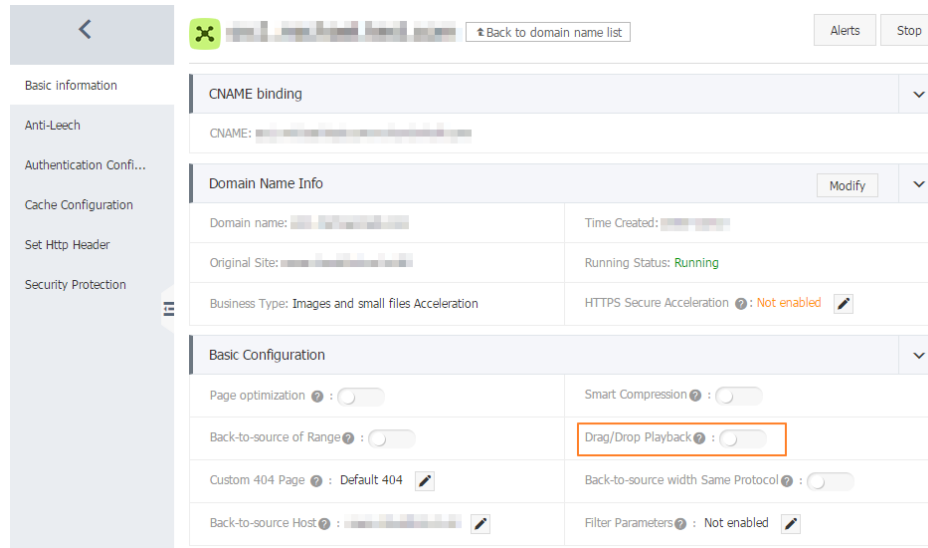
This function is optional and is disabled by default.

Log on to the CDN console.

On the left navigation bar, click **CDN domain name list**.

Select a domain to enter the management page.

Enable or disable the drag/drop playback function.



The screenshot shows the management console for a CDN domain. On the left is a navigation bar with options: Basic Information, Anti-Leech, Authentication Confi..., Cache Configuration, Set Http Header, and Security Protection. The main content area has a header with a back arrow, a domain name, a 'Back to domain name list' link, and 'Alerts' and 'Stop' buttons. Below the header, there are sections for 'CNAME binding', 'Domain Name Info', and 'Basic Configuration'. The 'Domain Name Info' section shows details like Domain name, Time Created, Original Site, Running Status (Running), Business Type (Images and small files Acceleration), and HTTPS Secure Acceleration (Not enabled). The 'Basic Configuration' section contains several toggle switches: Page optimization, Smart Compression, Back-to-source of Range, Drag/Drop Playback (highlighted with a red box), Custom 404 Page (Default 404), Back-to-source width Same Protocol, Back-to-source Host, and Filter Parameters (Not enabled).

Back-to-source of range

Introduction

The Back-to-source of Range function allows a client to notify an origin site server to return partial content within a specified range. It accelerates delivery of large files by reducing the consumption of back-to-source traffic and improving the resource response speed.

When the Back-to-source of Range function is enabled, a parameter request can be returned to an origin site. In this case, the origin site returns the file byte range according to the Range parameter and the CDN node returns the content in the byte range to the client.

For example, if a request sent from a client to a CDN node contains range:0-100, the range:0-100 parameter will also be contained in the request received on the origin site. When the origin site returns the parameter content to the CDN node, the node returns the content in 101 bytes ranging from 0 to 100 to the client.

When the Back-to-source of Range function is disabled, a CDN higher-level node will request an origin site for all files. However, the requested files will not be cached on the CDN node because a client will automatically disconnect HTTP links after receiving bytes specified by Range. This causes a low cache hit rate and large back-to-source traffic.

For example, if a request sent from a client to a CDN node contains range:0-100, the range:0-100 parameter will not be contained in the request received on the server. The origin site will return a complete file to the CDN node and the CDN node will return only 101 bytes to the client. However, the file cannot be cached on the CDN node because the link is disconnected.

Considerations

To use the Back-to-source of Range function, an origin site must support Range requests, meaning that the origin site must be able to return correct 206 Partial Content for an HTTP request header containing a Range field.

Operation procedure

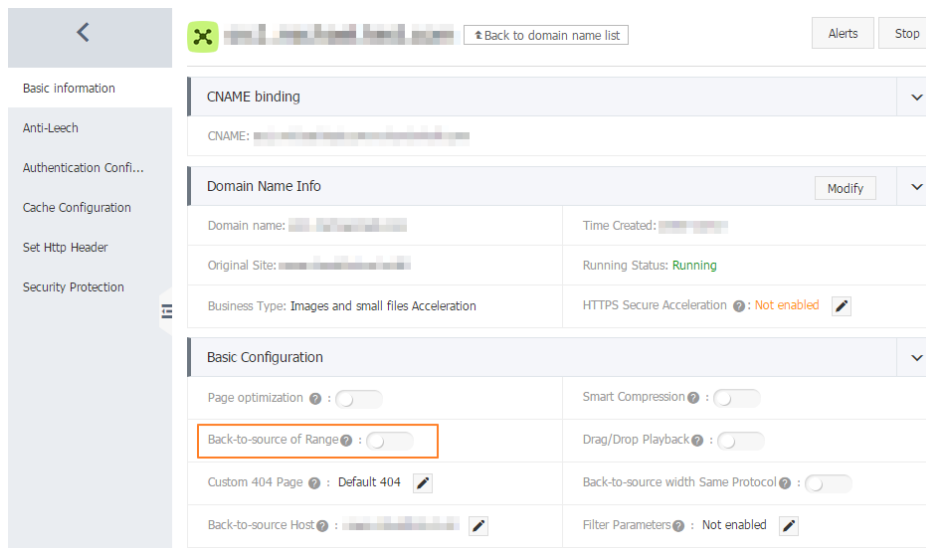
This function is optional and is disabled by default.

Log on to the **CDN console**.

On the left navigation bar, click **CDN domain name list**.

Select a domain to enter the management page.

Enable or disable the Back-to-source of Range function.



Set httpDNS

Introduction

A traditional DNS resolution is implemented by accessing the local DNS of a carrier in order to obtain the resolution result. However, this action can easily allow for DNS hijacking, DNS errors, and inter-network traffics and lead to slowed, or failed, website access.

httpDNS is a DNS service that uses HTTP protocol to directly access the Alibaba Cloud CDN server. Because it bypasses the carrier's local DNS, it can avoid DNS hijacking and obtain real-time accurate DNS resolution results.

Principle: initiate a request to access a designated Alibaba Cloud CDN httpDNS server through HTTP protocol. The httpDNS server performs domain resolution based on second-level DNS nodes distributed everywhere, obtains the domain name resolution result, and returns the result.

httpDNS interface

Direct access through an HTTP interface is supported. The access method is as follows.

Service URL

```
http://umc.danuoyi.alicdn.com/multi_dns_resolve
```

Request method

POST

Supported parameter

client_ip=x.x.x.x

This parameter can be ignored if the IP address of the client initiating the httpDNS request is used.

Request example

Multiple domains to be resolved are placed in the body of a POST request and are separated by whitespaces (blank spaces, TABs, newline characters).

```
#curl 'http://umc.danuoyi.alicdn.com/multi_dns_resolve?client_ip=182.92.253.16'  
'-d 'd.tv.taobao.com'
```

Returned format

JSON data is returned. After resolution, domain IP addresses are extracted and polling can be performed among them. TTL cache and expiration rules must be followed.

```
{"dns":[{"host":"d.tv.taobao.com","ips":[{"ip":"115.238.23.240","spdy":0},{"ip":"115.238.23.250","spdy":0}],"ttl":300,"port":80}],"port":80}
```

Request example with multiple domains

Request example:

```
#curl 'http://umc.danuoyi.alicdn.com/multi_dns_resolve?client_ip=182.92.253.16'  
'-d 'd.tv.taobao.com vmtstvcn.alicdn.com'
```

Return example:

```
{"dns":[{"host":"vmtstvcn.alicdn.com","ips":[{"ip":"115.238.23.250","spdy":0},{"ip":"115.238.23.240","spdy":0}],"ttl":300,"port":80},{"host":"d.tv.taobao.com","ips":[{"ip":"115.238.23.240","spdy":0},{"ip":"115.238.23.250","spdy":0}],"ttl":300,"port":80}],"port":80}
```

Cache refresh

You can purge URLs and directories, as shown in the following screenshot.

URL refresh

Concept: Forces specified files on the CDN Cache node to expire in order to update back-to-source again.

Time to Take Effect: 5 to 10 minutes

Considerations:

Entered URL must contain http://.

Up to 2,000 URLs with the same ID can be refreshed and warmed up each day.

Directory refresh

Concept: Forces files in the specified directory on the CDN Cache node to expire in order to update back-to-source again. Can be used in scenarios with large amounts of content.

Time to Take Effect: Within 30 minutes

Considerations:

Entered content must begin with `http://` and end with `/`.

Up to 100 refresh requests can be submitted each day.

URL push

Concept: Actively pushes content from the origin site to the L2 Cache node. Upon first access, you can directly hit cache to relieve pressure on the origin site.

Time to Take Effect: 5 to 10 minutes

Considerations:

Entered URL must contain `http://`.

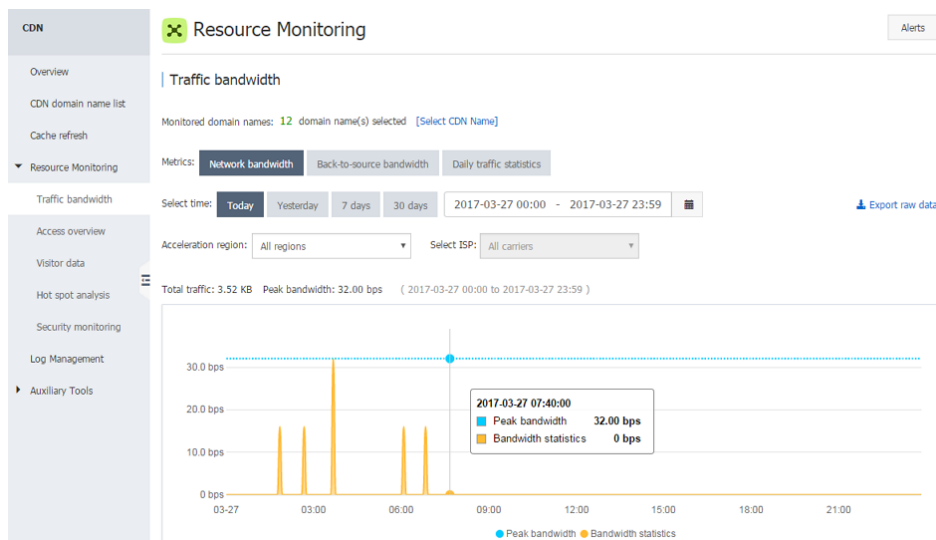
Up to 2,000 URLs with the same ID can be refreshed and warmed up each day.

Resource monitoring

Resource monitoring provides data analysis and monitors traffic, user access, and security.

You can specify domains and time spans to export original data of traffic monitoring.

Note: The precision of original data collection varies according to time spans, which are 300s, 3600s, and 14400s for daily export, weekly export, and monthly export, respectively.



Item	Metric	Time Span
Traffic bandwidth	Network bandwidth, back-	Today, yesterday, within 7

	to-source bandwidth, daily traffic statistics	days, 30 days, and user-defined 90 days
Access overview	Hit rate, access QPS, HTTP code	Today, yesterday, within 7 days, 30 days, and user-defined 90 days
Visitor data	PV, UV, regional user distribution, operator proportions	Today, yesterday, within 7 days, 30 days, and user-defined 90 days
Hot spot analysis	Popular domain names, popular URLs, popular referers, file response proportions	The recent 30 days
Security monitoring	CC monitoring	Today, yesterday, within 7 days, 30 days, and user-defined 90 days

Diagnostic tools

An IP address detection tool is provided in order to verify whether a specified IP address is an Alibaba Cloud CDN node IP address or an IP address from a third-party node.

