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 be connected to Alibaba Cloud.

The origin site content of a CDN domain needs to 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. In any of the following cases, CDN access is not allowed.

- The CDN domain cannot be normally accessed or the content does not include any substantive information.
- The CDN domain is for a private game server.
- The CDN domain is used for a legend-type game or card game.
- 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.
- Automatic timeout rejection: Your domain name is rejected because it fails to comply with CDN access rules. Check the feedback and submit a qualified domain name for reviewing again.

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

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

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

The answer is NO. To make accelerated content delivery effective, you need to 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 you need more CDN domains, submit a ticket to apply for special support.

Restriction on the number of IP origin sites

Currently, the maximum number of IP origin sites for each CDN domain is 20 (namely 20 IP addresses). If you need more IP origin sites in special scenarios, submit a ticket to apply for special support.

Restrictions on the number of cache refresh and push operations

The restrictions on the number of cache refresh operations (including cache refresh and cache push) are as follows:

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

Introduction

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

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

This document mainly describes the basic information about the CDN Console.

Overview of CDN operation

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

- Billing method
- Key data: the number of domains in normal statuses, the total traffic for all domains this month
- Data of this month:
    - Domain peak bandwidth
    - Top 5 domains according to the accumulated downstream traffic
    - Top 5 URLs according to the number of accesses
    - 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.

You can use the left-side navigation bar to set the relevant functions and look at the data.

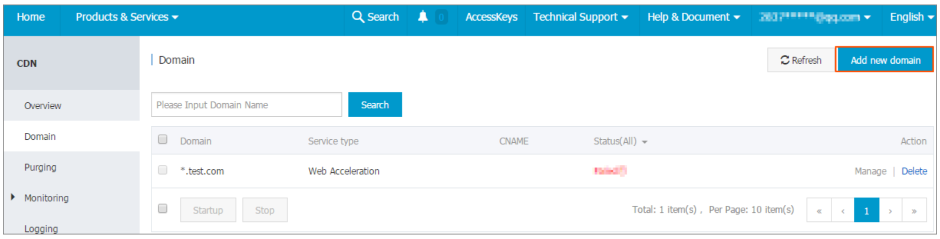
Function	Description
Add a CDN domain	You can add a new CDN domain, manage or delete an existing CDN domain, or change the basic information and configuration information of a CDN domain.
Cache refresh	The URL refresh and directory refresh modes are provided.
Resource monitoring	Resource monitoring covers traffic monitoring, user access monitoring, data analysis, and security monitoring.
Log management	Log download, log storage (coming soon), cloud report.
Diagnostic tools	Link diagnostic tools.

Add a CDN domain

Log on to the CDN Console. Click **Domain**, and click **Add new domain** in the upper-right corner. (If the source content is in OSS, select OSS Bucket acceleration.)

1. Click Domain

click **Add new domain** in the upper-right corner.



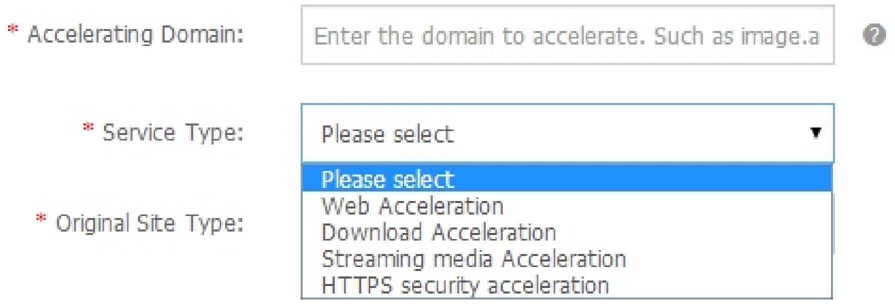
Domain	Service type	CNAME	Status(All)	Action
*.test.com	Web Acceleration		[redacted]	Manage | Delete

Total: 1 item(s) , Per Page: 10 item(s)

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

2. Enter the basic information

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



* Accelerating Domain: Enter the domain to accelerate. Such as image.a

* Service Type: Please select

* Original Site Type:

Considerations:

CDN domain

The filing for the domain you entered must be complete. If filing is still in progress, the entered domain cannot be accessed.

Domain content must comply with CDN specifications. For details, refer to CDN Service Usage Restrictions.

Service type

The descriptions of the service types are as follows.

Service Type	Description
Acceleration of images and small files	Acceleration of images and small files is recommended if the content to be

	accelerated is mostly images and Web files.
Acceleration of large file downloads	Acceleration of large file downloads is recommended if the content to be accelerated is large files (static files larger than 20 MB).
Acceleration of on-demand video/audio	In case of large video files, acceleration of live streaming media is recommended to accelerate the video on demand and live video services.
Acceleration of live streaming media (being tested)	The acceleration of live streaming media is provided. Currently, RTMP-based live streaming acceleration and HLS-based live streaming acceleration are 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.

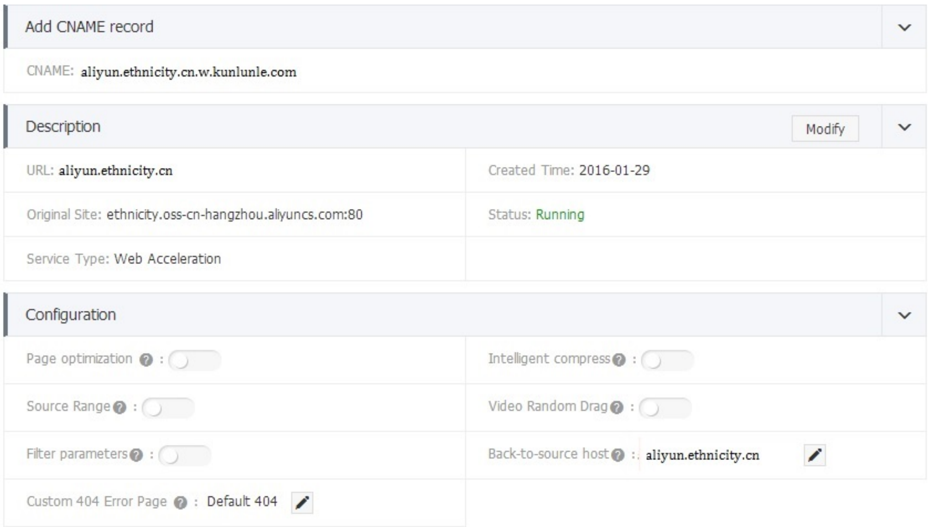
Origin site type

Origin Site Type	Description
IP address	Internet IP addresses of multiple servers can be entered. **Note:** If the IP address you entered does not belong to an Alibaba Cloud product, the domain to be added needs to be reviewed, which takes 1 or 2 working days.
Origin site domain	Enter an origin site domain. **Note:** The origin site domain you 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, you are recommended to set your origin site to src.yourcompany.com.
OSS domain	Enter an OSS bucket access address, for example, xxx.aliyuncs.com.
Central live streaming server (being tested)	This origin site type is available for **live**

	streaming media acceleration only. By default, it is set to video-center.alivecdn.com. User-defined central live streaming servers are not supported.

Note: If the origin site is a domain, the origin site domain cannot be the same as the CDN domain to be added. If related resource 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 go back to the origin site to get the content. So it is suggested that if your CDN domain is example.aliyun.com, you can use src.example.aliyun.com as the origin site for differentiation.

3. Enter the configuration information



Add CNAME record

CNAME: aliyun.ethnicity.cn.w.kunlunle.com

Description

URL: aliyun.ethnicity.cn

Created Time: 2016-01-29

Original Site: ethnicity.oss-cn-hangzhou.aliyuncs.com:80

Status: Running

Service Type: Web Acceleration

Configuration

Page optimization :

Intelligent compress :

Source Range :

Video Random Drag :

Filter parameters :

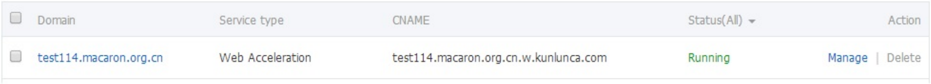
Back-to-source host : aliyun.ethnicity.cn

Custom 404 Error Page : Default 404

Domain name configurations are optional. Configurations can be performed after a CDN domain is created successfully. For details, refer to Configuration Information.

4. Confirm the information

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

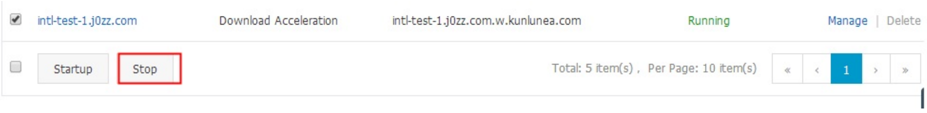


□	Domain	Service type	CNAME	Status(All)	Action
□	test114.macaron.org.cn	Web Acceleration	test114.macaron.org.cn.w.kunlunca.com	Running	Manage | Delete

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

Delete domain name configurations

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



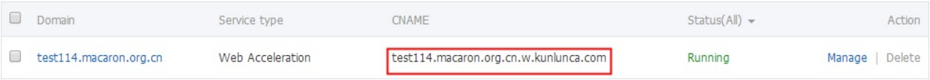
☑	intl-test-1.j0zz.com	Download Acceleration	intl-test-1.j0zz.com.w.kunlunea.com	Running	Manage | Delete

□ Startup Stop Total: 5 item(s) , Per Page: 10 item(s) « ‹ 1 › »

CNAME binding

Obtain the correct CNAME domain.

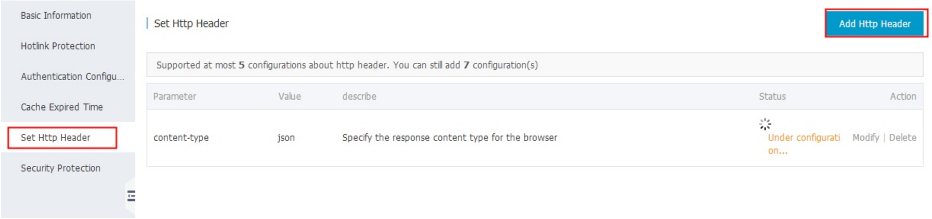
The CNAME domain is displayed in the CDN domain list, as shown in the following screenshot.



□	Domain	Service type	CNAME	Status(All)	Action
□	test114.macaron.org.cn	Web Acceleration	test114.macaron.org.cn.w.kunlunca.com	Running	Manage | Delete

Query the domain status.

Domain name configurations must be distributed to all nodes of the network, which may take 15 minutes.



Set Http Header

Supported at most **5** configurations about http header. You can still add **7** configuration(s)

Parameter	Value	describe	Status	Action
content-type	json	Specify the response content type for the browser	Under configuration...	Modify | Delete

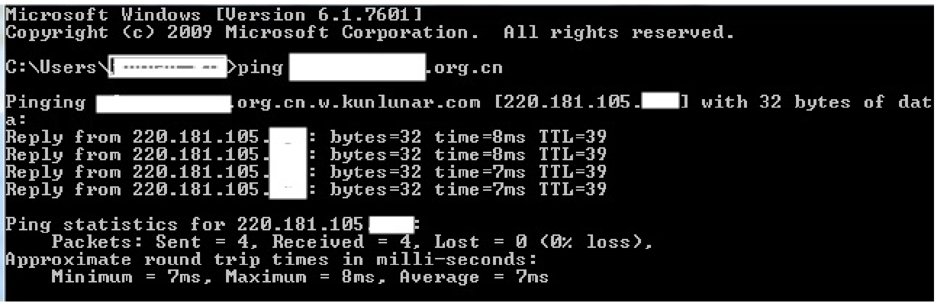
Correctly configure DNS resolution.

Go to your DNS service provider to complete the CNAME configuration. The following documents are available for your reference.

- Using HiChina CNAME for Accessing a CDN
- Using DNSPod CNAME for Accessing a CDN
- Using Xinnet CNAME for Accessing a CDN

Verify that the CNAME domain is added successfully.

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



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

C:\Users\[redacted]>ping [redacted].org.cn

Pinging [redacted].org.cn.w.kunlunar.com [220.181.105.[redacted]] with 32 bytes of dat
a:
Reply from 220.181.105.[redacted]: 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[redacted]:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 8ms, Average = 7ms
```

Function overview

Item	Description	Default
Page optimization	Compresses and removes useless blank lines and carriage return characters from a page to effectively reduce the page size.	Disabled
Smart compression	Supports smart compression for content in multiple formats to effectively reduce the size of content transmitted by users.	Disabled
Filter parameter	If this item is selected, parameters after ? in a URL request will be removed in the back-to-source process.	Disabled
Source host	Specifies the domain name of a host that a CDN node accesses in the back-to-source process. Three options are available: CDN domain, origin site domain, and user-defined domain.	CDN domain
Customizing the 404 page	Three options are available: default 404 page, public welfare 404 page and user-defined 404 page.	Default 404 page
Range source	The range source function allows a user to notify an origin site server to return	Disabled

	partial content within a specified range. This function is of great help for the accelerated delivery of large files.	
Drag/drop playback	Enables random drag/drop playback in a video/audio on demand scenario.	Disabled
Anti-leech	You can configure a referrer black list or white list to identify and filter visitors.	Disabled
Authentication configuration	Uses URL authentication methods to protect resources on an origin site.	Disabled
Cache policy configuration	You can customize cache expiration rules for specified resources.	Disabled
Setting HTTP Request Header	You can set an HTTP request header. Eight HTTP request header parameters are currently available for your customization.	Disabled
Security protection	Includes WAF protection and CC protection.	Enabled
SettinghttpDNS	httpDNS is a DNS service. It uses the HTTP protocol to directly access the server of Alibaba Cloud CDN.	Disabled

HTTPS Delivery

Setting Back-to-source

Back-to-source with the same protocol

Function introduction

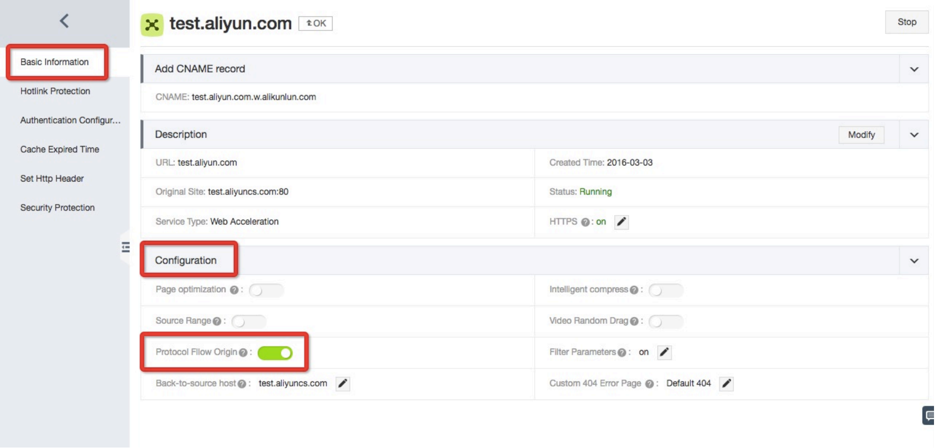
When this feature is enabled, back-to-source requests for resources will use exactly the same protocol as used by the client to request the resources. That is to say, if the client makes an HTTPS request for the resources, but the resources are not cached on the node, a back-to-source HTTPS request will be made for the resources. The same is true with HTTP requests.

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

Configuration instructions

In the CDN Domain List page, select an appropriate domain name to access the management page.

In the **Basic Infomation** module, enable or disable the Back-to-source with Same Protocol feature.



test.aliyun.com ↑OK

CNAME: test.aliyun.com.w.alikunlun.com

URL: test.aliyun.com

Created Time: 2016-03-03

Original Site: test.aliyuncs.com:80

Status: Running

Service Type: Web Acceleration

HTTPS : on

Page optimization :

Intelligent compress :

Source Range :

Video Random Drag :

Protocol Fllow Origin :

Filter Parameters : on

Back-to-source host : test.aliyuncs.com

Custom 404 Error Page : Default 404

Back-to-source host

Function introduction

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

Considerations

Because an origin site is a CDN domain in the OSS space, the **Back-to-source host** must be set to the CDN domain so as to get back to the source for data.

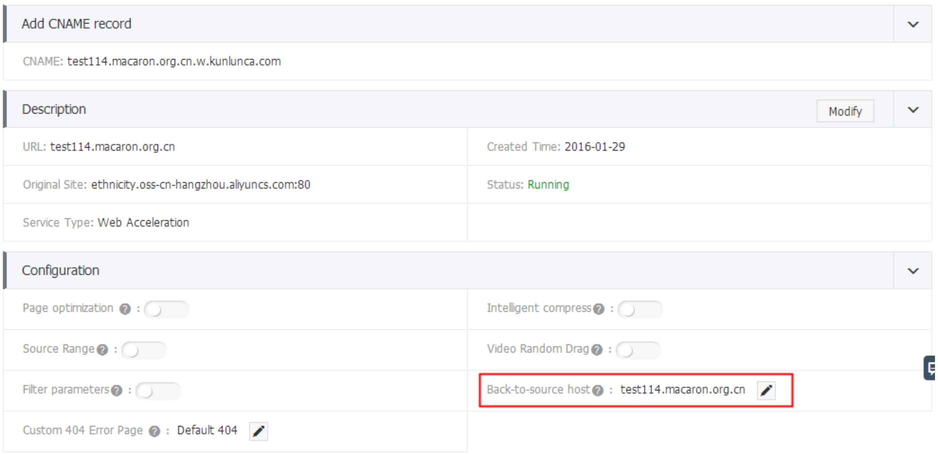
Configuration guide

The **Back-to-source host** configuration is optional and its default value is CDN domain.

The value options include CDN domain, origin site domain, and user-defined domain.

Change the configuration

Enter the CDN Domain Overview page > Select a domain to enter the management page > Basic information > Enter the basic configuration to set **Back-to-source host**



CNAME: test114.macaron.org.cn.w.kunlunca.com

URL: test114.macaron.org.cn

Created Time: 2016-01-29

Original Site: ethnicity.oss-cn-hangzhou.aliyuncs.com:80

Status: Running

Service Type: Web Acceleration

Page optimization : ○

Intelligent compress : ○

Source Range : ○

Video Random Drag : ○

Filter parameters : ○

Back-to-source host : test114.macaron.org.cn

Custom 404 Error Page : Default 404

Setting Cache Policy

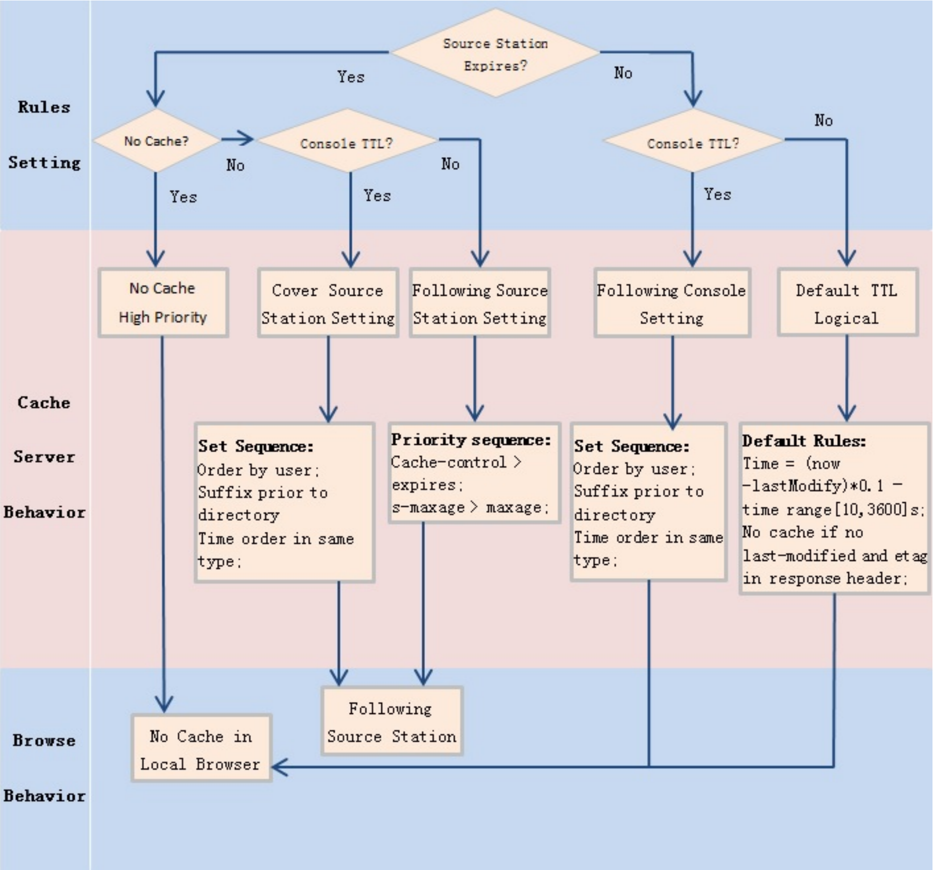
Cache policy configuration

Function introduction

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

You can customize a cache policy priority.

Default cache policies.


Rules Setting
Source Station Expires?
Yes
No
No Cache?
No
Yes
Console TTL?
Yes
No
Console TTL?
Yes
No
Cache Server Behavior
No Cache High Priority
Cover Source Station Setting
Following Source Station Setting
Following Console Setting
Default TTL Logical
Set Sequence: Order by user; Suffix prior to directory Time order in same type;
Priority sequence: Cache-control > expires; s-maxage > maxage;
Set Sequence: Order by user; Suffix prior to directory Time order in same type;
Default Rules: Time = (now -lastModify)*0.1 - time range[10,3600]s; No cache if no last-modified and etag in response header;
Browse Behavior
No Cache in Local Browser
Following Source Station

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).

Considerations

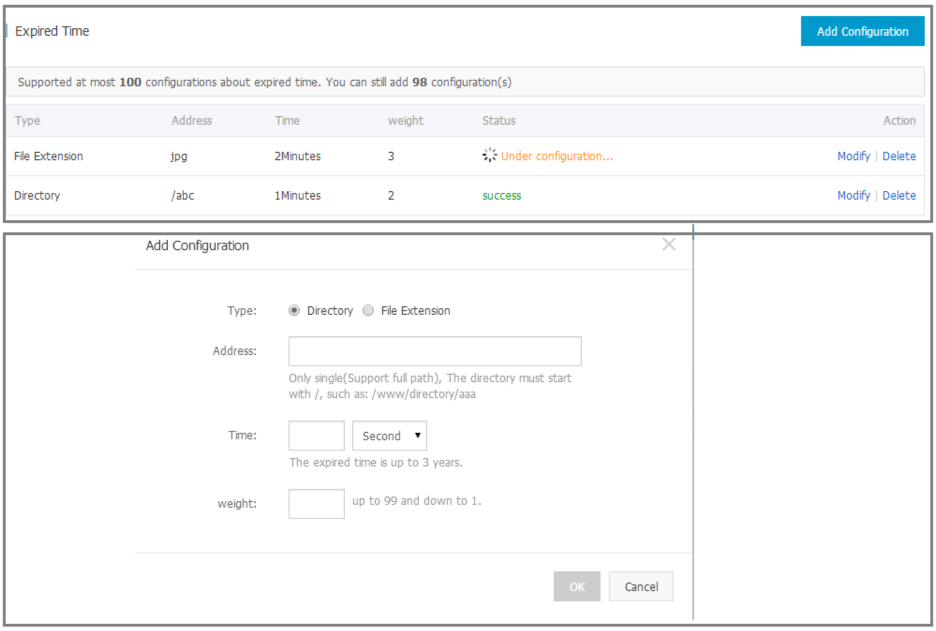
- For static files that are not updated frequently (for example, image files and application download files), it is suggested that the cache duration be set to one month longer.
- For static files that need to be updated frequently (for example, JS files and CSS files), you can shorten the cache duration 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 0 s, meaning 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 suggested that the content on an origin site should not be updated using the same name but using different version numbers, for example, img-v1.0.jpg and img-v2.1.jpg.

Configuration guide

Enter the CDN Domain Overview page > Select a domain to enter the management page > Perform Cache Policy Configuration



Expired Time

Supported at most **100** configurations about expired time. You can still add **98** configuration(s)

Type	Address	Time	weight	Status	Action
File Extension	jpg	2Minutes	3	Under configuration...	Modify | Delete
Directory	/abc	1Minutes	2	success	Modify | Delete

Add Configuration

Type: ● Directory ○ File Extension

Address:

Only single(Support full path), The directory must start with /, such as: /www/directory/aaa

Time: Second ▾

The expired time is up to 3 years.

weight: up to 99 and down to 1.

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.
- Cache policy 2: The cache duration for files in the /www/dir/aaa directory is one hour.
- Cache policy 3: The cache duration for the full path /www/dir/aaa/example.php is 0 s (No cache action will be done).
- The priority is Policy 3 > Policy 1 > 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 weight randomly.

Customizing the 404 page

Function introduction

You can customize the page that is displayed when a 404 status code is returned to optimize user experience. Three options are available: default 404 page, public welfare 404 page and user-defined 404 page.

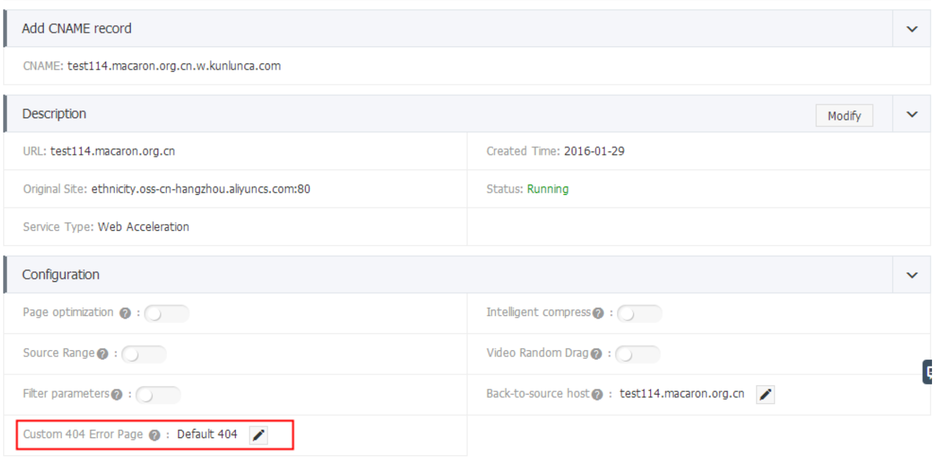
- Default 404 page: When an HTTP 404 error is returned, the server returns the default 404 Not Found page.
- Public welfare 404 page: When an HTTP 404 error is returned, the server redirects it to the real-time updated public welfare 404 page. For more details, refer to Public Welfare 404 Page.
- User-defined 404 page: When an HTTP 404 error is returned, the server redirects it to the user-defined 404 page you designed and edited. In this case, you need to predefine a complete URL for the page.

Considerations

- The public welfare 404 page is a public welfare resource of Alibaba Cloud. It is completely free and generates no traffic fees.
- User-defined 404 pages are personal resources which should be billed based on normal delivery.

Configuration guide

Enter the CDN Domain Overview page > Select a domain to enter the management page > Basic information > Enter the basic configuration to set the Customizing the 404 Page function



Add CNAME record

CNAME: test114.macaron.org.cn.w.kunlunca.com

Description

URL: test114.macaron.org.cn
Created Time: 2016-01-29
Original Site: ethnicity.oss-cn-hangzhou.aliyuncs.com:80
Status: Running
Service Type: Web Acceleration

Configuration

Page optimization :
Intelligent compress :
Source Range :
Video Random Drag :
Filter parameters :
Back-to-source host : test114.macaron.org.cn
Custom 404 Error Page : Default 404

If you select the **user-defined 404 page** option, you need to store the page resources, like other static files, under the origin site domain and 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 **user-defined 404 page** option, and enter http://exp.aliyun.com/error404.html.

Set the HTTP request header

Function introduction

You can set an HTTP request header. Eight HTTP request header parameters are currently available for your customization. The parameters are described 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 should be followed in 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 prefetch request initiated by a client program for a particular resource.

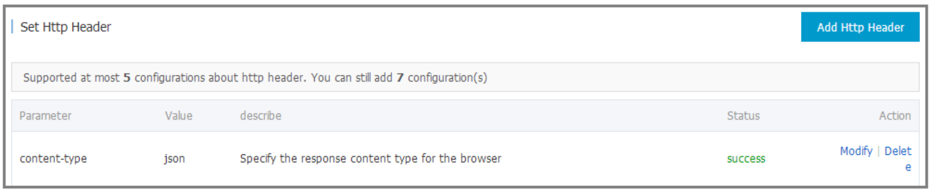
Considerations

- 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 above HTTP header parameters are supported currently. If you have more requirements for HTTP header settings, submit a ticket for feedback.
- The Access-Control-Allow-Origin parameter can be set to * (indicating all domains) or a

complete domain name such as www.aliyun.com. Wildcard domain setting is not supported currently.

Configuration guide

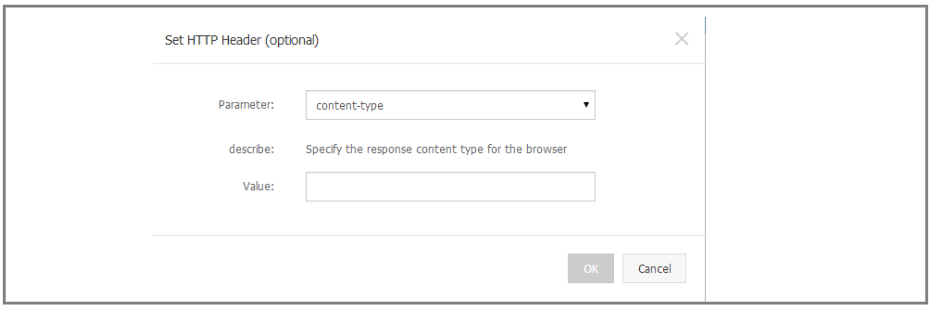
Enter the CDN Domain Overview page > Select a domain to enter the management page > Set the HTTP request header



Set Http Header

Supported at most **5** configurations about http header. You can still add **7** configuration(s)

Parameter	Value	describe	Status	Action
content-type	json	Specify the response content type for the browser	success	Modify | Delete



Set HTTP Header (optional)

Parameter: content-type

describe: Specify the response content type for the browser

Value:

Resource Access Control

Anti-leech

Function 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, recognition and judgement. You can configure a referer black list or white list to identify and filter visitors to limit CDN resources to be accessed.
- 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 preset 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

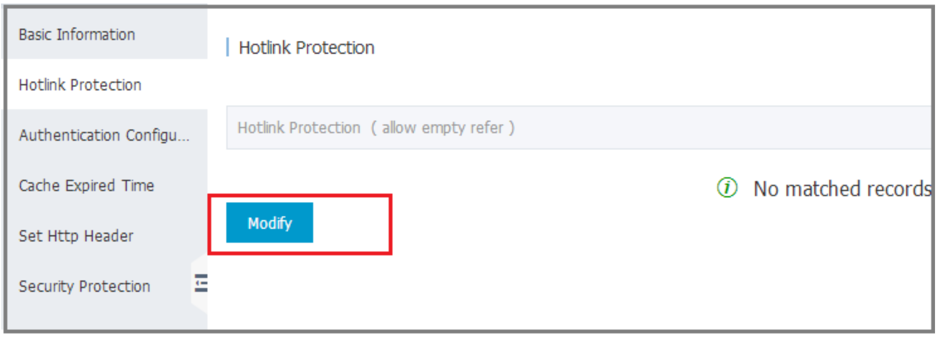
returned.

Considerations

- This function is optional and is disabled by default.
- To enable this function, you can select **Refer Blacklist** or **Refer Whitelist** to edit. The **Refer Blacklist** and **Refer Whitelist** are mutually excluded, so you can select only one of them.
- You can set whether 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).

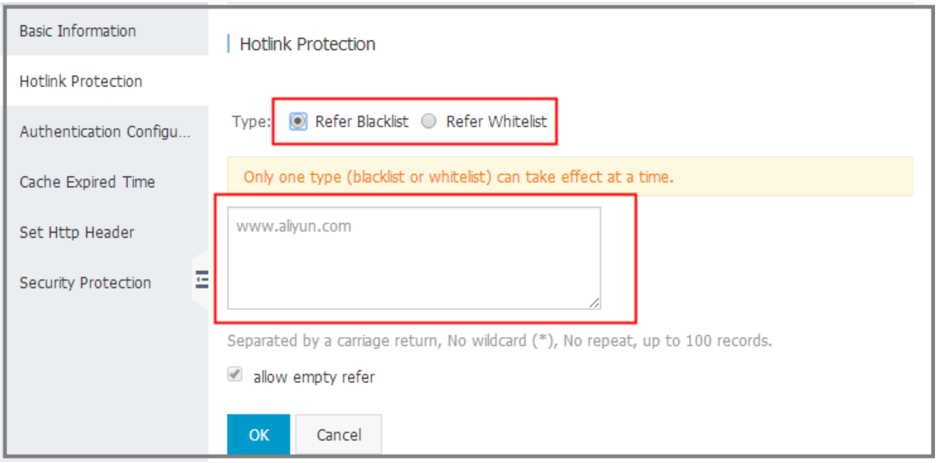
Configuration guide

Enter the CDN Domain Overview page > Select a domain to enter the management page > Set Anti-Leech



Hotlink Protection (allow empty refer)

No matched records



Type: ● Refer Blacklist ○ Refer Whitelist

Only one type (blacklist or whitelist) can take effect at a time.

www.aliyun.com

Separated by a carriage return, No wildcard (*), No repeat, up to 100 records.

☑ allow empty refer

URL authentication

Overview

The URL authentication function protects user’ s site resources from illegal download and misappropriation. Adopting the anti-leeching method by adding the referer black list/white list solves some leeching issues. However, because the referer content may be forged, the referer anti-leeching method cannot completely protect site resources. Therefore, using URL authentication more effectively protects the security of origin site resources.

Principle

The URL authentication function uses Alibaba Cloud CDN nodes together with client resource sites to provide more secure and reliable 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 effectively protects CDN client site resources.

URL authentication methods

Alibaba Cloud CDN is compatible with and supports authentication Method A, Method B and Method C. You can select an appropriate method based on their business needs to effectively protect their origin site resources.

Authentication method A

Principle

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 generally set to 0.
uid	Temporarily unused (set to 0).
md5hash	The verification string calculated using the MD5 algorithm. It is a mix of numbers 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 judges that the request is expired and returns an HTTP 403 error. If the timestamp is greater than the current time, it constructs an equivalent string (see the sstring construction method below). 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 method below:

```
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

Principle

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 actual 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 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.

Field	Description
DomainName	The domain name of the CDN client site.
timestamp	Time when the user accesses the client source server. This is part of the URL and also 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).

3. Time 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 braces 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 actual back-to-source access URL (Note: during authentication, the path begins with /).
time	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 that, the CDN server authenticates the URL according to the predefined service logic.

1. 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.
2. The CDN server compares encrypted string 2 with encrypted string 1. If the strings are not the same, the request is rejected.
3. 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).
4. 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.
5. If the time difference is less than the preset time limit, the request is legal. Then, the CDN server will send a normal response. Otherwise, the request is rejected and an HTTP 403 error is returned.

Sample authentication code

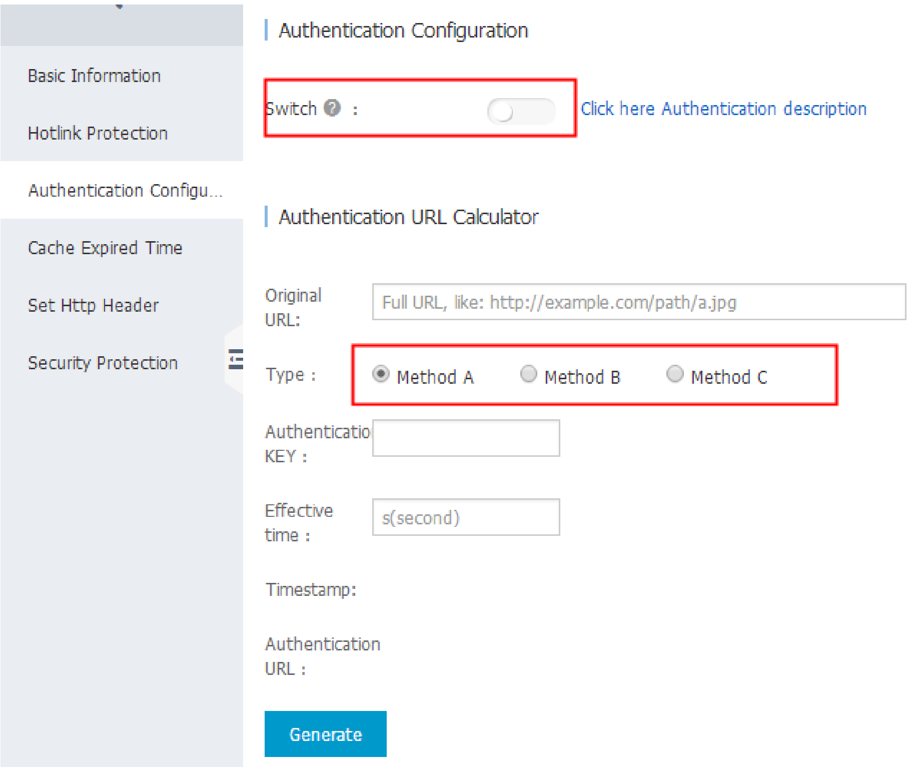
Refer to the Sample Authentication Code document in **CDN Utilities**.

Configuration guide

Enter the CDN Domain Overview page > Select a domain to enter the management page > Perform Authentication Configuration

- You can select an authentication method and set the authentication key in the authentication configuration module.

  The authentication calculator supports the authentication link calculation for any URLs. It helps to test whether the authentication function is effective.



Authentication Configuration

Switch ? :

Authentication URL Calculator

Original URL: Full URL, like: http://example.com/path/a.jpg

Type : ● Method A ○ Method B ○ Method C

Authenticatio KEY :

Effective time : s(second)

Timestamp:

Authentication URL :

IP black list

Function introduction

CDN supports the black list rules. An IP address on the black list cannot access the corresponding domain.

Considerations

You can use an IP network segment to add IP addresses to the black list or white list, for example, 127.0.0.1/24.

Where, 24 indicates that the first 24 bits in the subnet mask are used as effective bits, namely 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

Function introduction

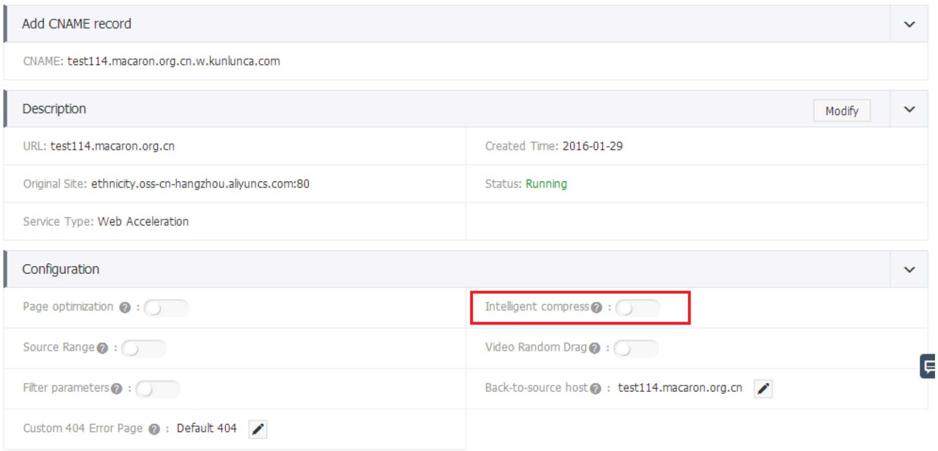
- The Smart Compression function can be used to compress most of the static files to effectively reduce the size of the contents transmitted by users and accelerate delivery.
- Currently, contents in the following formats can be compressed: content-type:text/xml, text/plain, text/css, application/javascript, application/x-javascript, application/rss+xml, text/javascript, image/tiff, image/svg+xml, and application/json.

Configuration guide

- Applicable service types: All

Change the configuration

Enter the CDN Domain Overview page > Select a domain to enter the management page > Basic information > Enter the basic configuration to enable or disable the Smart Compression function



Add CNAME record

CNAME: test114.macaron.org.cn.w.kunlunca.com

Description

URL: test114.macaron.org.cn

Created Time: 2016-01-29

Original Site: ethnicity.oss-cn-hangzhou.aliyuncs.com:80

Status: Running

Service Type: Web Acceleration

Configuration

Page optimization :

Intelligent compress :

Source Range :

Video Random Drag :

Filter parameters :

Back-to-source host : test114.macaron.org.cn

Custom 404 Error Page : Default 404

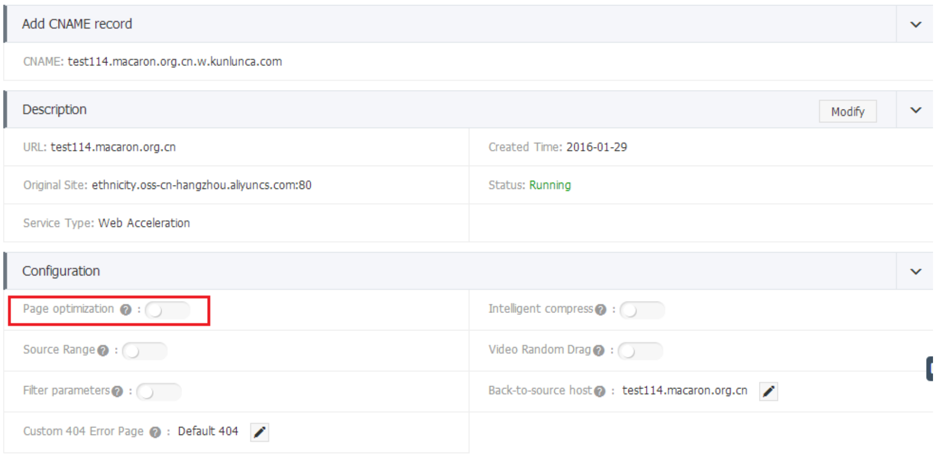
Page optimization

Function introduction

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

Configuration guide

Enter the CDN Domain Overview page > Select a domain to enter the management page > Basic information > Enter the basic configuration to enable or disable the Page Optimization function



CNAME: test114.macaron.org.cn.w.kunlunca.com

URL: test114.macaron.org.cn

Created Time: 2016-01-29

Original Site: ethnicity.oss-cn-hangzhou.aliyuncs.com:80

Status: Running

Service Type: Web Acceleration

Page optimization : ○

Intelligent compress : ○

Source Range : ○

Video Random Drag : ○

Filter parameters : ○

Back-to-source host : test114.macaron.org.cn

Custom 404 Error Page : Default 404

Filter parameter

Function 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. In addition, the CDN node keeps 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 most commonly contains parameters. If the content of a parameter has a low priority and the parameter overview file can be ignored, it is suitable to enable the Filter Parameter function. This effectively improves the file cache hit rate and the delivery efficiency.
- If a parameter has important meanings, for example, it contains file version information, you are recommended to disable this function.

Example of use:

For example, 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 keeps 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

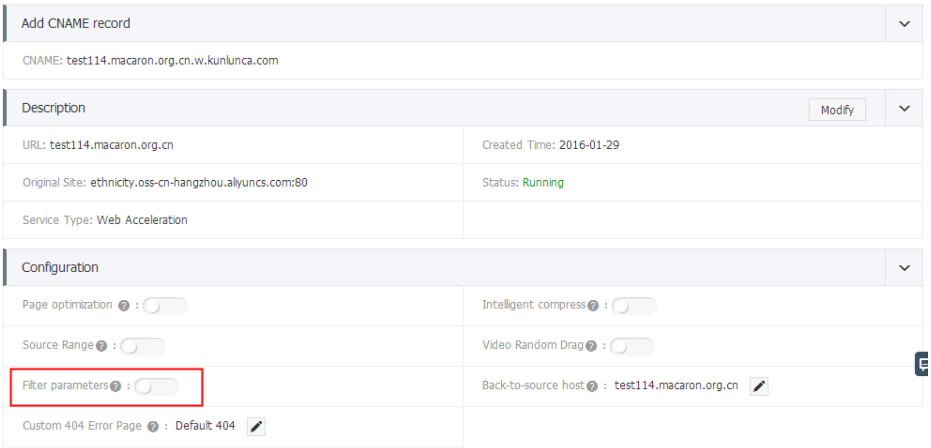
URL authentication has a higher priority than the Filter Parameter function. Because type A authentication information is contained in the parameter section of an HTTP request, the system first performs the authentication and then caches a copy on the CDN node after the authentication succeeds.

Configuration guide

Applicable service types: All

Change the configuration

Enter the CDN Domain Overview page > Select a domain to enter the management page > Basic information > Enter the basic configuration to enable or disable the Filter Parameter function



Add CNAME record

CNAME: test114.macaron.org.cn.w.kunlunca.com

Description

URL: test114.macaron.org.cn

Created Time: 2016-01-29

Original Site: ethnicity.oss-cn-hangzhou.aliyuncs.com:80

Status: Running

Service Type: Web Acceleration

Configuration

Page optimization ? : ○

Intelligent compress ? : ○

Source Range ? : ○

Video Random Drag ? : ○

Filter parameters ? : ○

Back-to-source host ? : test114.macaron.org.cn

Custom 404 Error Page ? : Default 404

Video-related Settings

Drag/Drop playback

Function introduction

- In a video on demand scenario, when you drag the playback progress bar, the client will send to the server a URL request like http://www.aliyun.com/test.flv?start=10. The server will return to the client the data starting from the 10th second. This is called Drag/Drop Playback.
- When the Drag/Drop Playback function is enabled, a CDN node, after receiving such a request from a client, can directly return to the client the data starting from the specified second.

Considerations

- To use the Drag/Drop Playback 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.
- Currently, the supported file formats include 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	The start parameter specifies the time in seconds. Decimals are supported to indicate milliseconds	The http: //domain/video.mp4 ?start=10 request means playing a video from the 10th

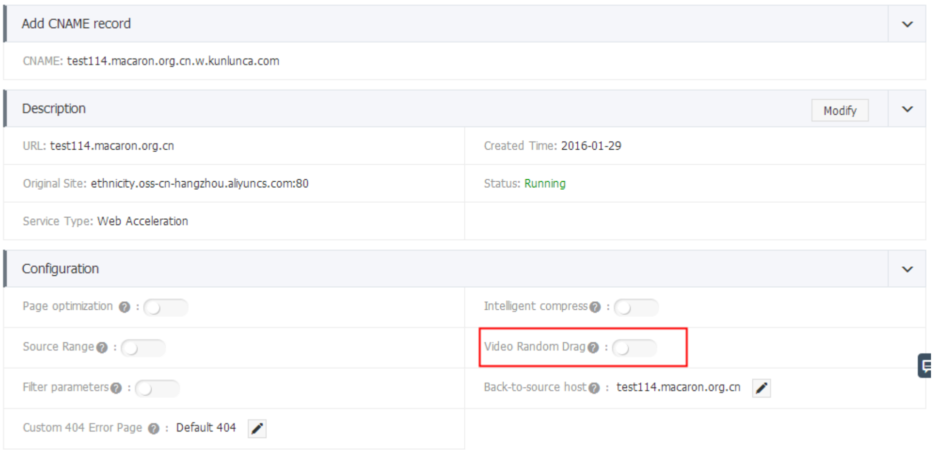
	meta information contained in the file tail is not supported.	(for example, start=1.01 indicates that the start time is 1.01 s). The CDN locates the key frame prior to the time specified by the start parameter (if the current start is not a key frame).	second.
FLV	An origin site video must contain meta information.	The start parameter specifies a byte. The CDN automatically locates the key frame prior to the frame specified by the start parameter (if the current start is not a key frame).	The http://domain/video.flv, the http://domain/video.flv?start=10 request means playing a video from the 10th byte.

Configuration guide

This function is optional and is disabled by default.

Change the configuration

Enter the CDN Domain Overview page > Select a domain to enter the management page > Basic information > Enter the basic configuration to enable or disable the Drag/Drop Playback function



Add CNAME record

CNAME: test114.macaron.org.cn.w.kunlunca.com

Description

URL: test114.macaron.org.cn

Created Time: 2016-01-29

Original Site: ethnicity.oss-cn-hangzhou.aliyuncs.com:80

Status: Running

Service Type: Web Acceleration

Configuration

Page optimization : ○

Intelligent compress : ○

Source Range : ○

Video Random Drag : ○

Filter parameters : ○

Back-to-source host : test114.macaron.org.cn

Custom 404 Error Page : Default 404

Back-to-source range

Function introduction

The Back-to-source of Rang function allows a client to notify an origin site server to return partial content within a specified range. It is of great help for the accelerated delivery of large files because it can reduce the consumption of back-to-source traffic and improve the resource response speed.

To use the Back-to-source of Range function, the 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.

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. Meanwhile, 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 to the client the content in 101 bytes ranging from 0 to 100.

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 eventually causes 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 while the CDN node will return only 101 bytes to the client. However, because the link is disconnected, the file cannot be cached on the CDN node.

Considerations

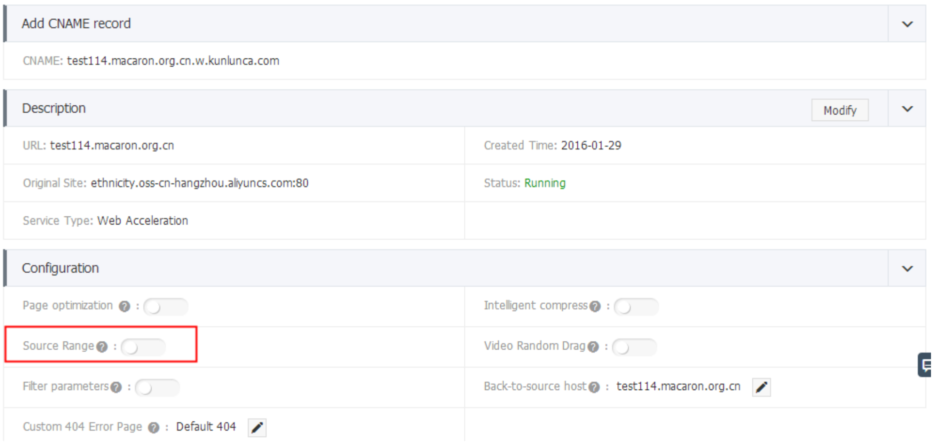
To use the Back-to-source of Range function, an origin site must support Range requests, meaning that the origin site must be able to return correct 206 Partial Content for an HTTP request header containing a Range field.

Configuration guide

This function is optional and is disabled by default.

Change the configuration

Enter the CDN Domain Overview page > Select a domain to enter the management page > Basic information > Enter the basic configuration to enable or disable the Back-to-source of Range function



Add CNAME record

CNAME: test114.macaron.org.cn.w.kunlunca.com

Description

URL: test114.macaron.org.cn	Created Time: 2016-01-29
Original Site: ethnicity.oss-cn-hangzhou.aliyuncs.com:80	Status: Running
Service Type: Web Acceleration	

Configuration

Page optimization : ○	Intelligent compress : ○
Source Range : ○	Video Random Drag : ○
Filter parameters : ○	Back-to-source host : test114.macaron.org.cn
Custom 404 Error Page : Default 404	

Set httpDNS

Function introduction

The traditional DNS resolution is implemented by accessing the local DNS of a carrier to obtain the resolution result, which easily causes DNS hijacking, DNS errors and inter-network traffics and thus leads to failed or slow website accesses.

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

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

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. The domains are separated by whitespaces which can be blank spaces, TABs, and 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. IP addresses of the domains are extracted after resolution and polling can be made among the multiple IP addresses. The TTL cache and expiration rules need to 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
```

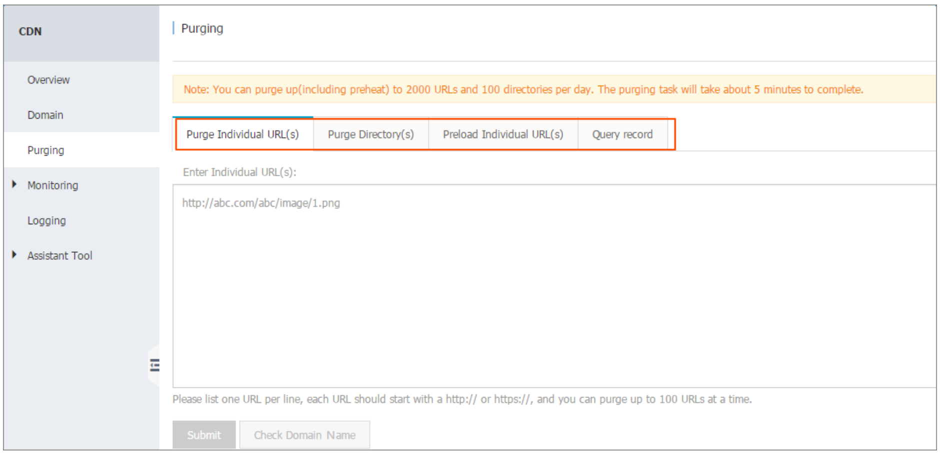
```
' -d 'd.tv.taobao.com vmtstvcdn.alicdn.com'
```

Return example:

```
{"dns":[{"host":"vmtstvcdn.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":"115.238.23.25
0","spdy":0}],"ttl":300,"port":80}],"port":80}
```

Cache Refresh

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



Note: You can purge up(including preheat) to 2000 URLs and 100 directories per day. The purging task will take about 5 minutes to complete.

Enter Individual URL(s):

http://abc.com/abc/image/1.png

Please list one URL per line, each URL should start with a http:// or https://, and you can purge up to 100 URLs at a time.

URL refresh

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

Time to Take Effect: Within 5~10 minutes

Considerations:

- The entered URL must contain http://.
- A total number of 2,000 URLs can be refreshed and warmed up with the same ID each day.

Directory refresh

Principle: Forces the files in the specified directory on the CDN Cache node to expire in order to update back-to-source again. This is suitable for scenarios where there is a large amount of contents.

Time to Take Effect: Generally it takes effect within 30 minutes.

Considerations:

- Up to 100 refresh requests can be submitted each day.
- The entered content must begin with http:// and end with /.

URL push

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

Time to Take Effect: Within 5-10 minutes

Considerations:

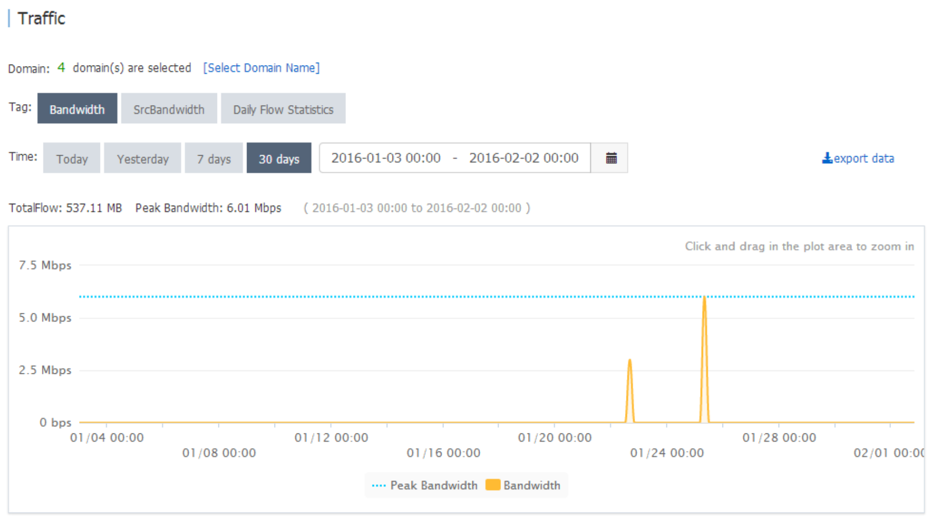
- The entered URL must contain http://.
- A total number of 2,000 URLs can be refreshed and warmed up with the same ID each day.

Resource monitoring

Resource monitoring covers traffic monitoring, user access monitoring, data analysis, and security monitoring.

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

Note: The granularities for collecting original data vary with time spans, which are 300 s, 3,600 s and 14,400 s for daily export, weekly export and monthly export respectively.



Traffic

Domain: 4 domain(s) are selected [Select Domain Name]

Tag: Bandwidth SrcBandwidth Daily Flow Statistics

Time: Today Yesterday 7 days 30 days 2016-01-03 00:00 - 2016-02-02 00:00

export data

TotalFlow: 537.11 MB Peak Bandwidth: 6.01 Mbps (2016-01-03 00:00 to 2016-02-02 00:00)

Item	Metric	Time Span
Traffic monitoring	Network traffic, back-to-source traffic, hit rate, QPS, and HTTP code	Today, yesterday, within 7 days, 30 days, and user-defined 90 days

User access monitoring	PV, UV, regional distribution of users, shares of carriers	Today, yesterday, within 7 days, 30 days, and user-defined 90 days
Data analysis	File response shares, URL access statistics, page reference URL shares	The recent 30 days
Security monitoring	CC monitoring and WAF monitoring	Today, yesterday, within 7 days, 30 days, and user-defined 90 days

Log Management

Log management

- Log files have a delay of 4 hours. In the log management module, you can query log files from over 4 hours ago
- Log files are divided by hour
- Log files are retained up to 2 weeks
- Log field format description

Log content:

```
[9/Jun/2015:01:58:09 +0800] 188.165.15.75 - 1542 "-" "GET http://www.aliyun.com/index.html" 200 191 2830 MISS
"Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)" "text/html"
```

Field content:

Field	Parameter
time	[9/Jun/2015:01:58:09 +0800]
access ip	188.165.15.75
back-to-source ip	-
responsetime	1542
referer	-
method	GET
access url	http://www.aliyun.com/index.html
httpcode	200
requestsize	191

responsesize	2830
cache hit status	MISS
UA header	Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)
File type	text/html

Note:

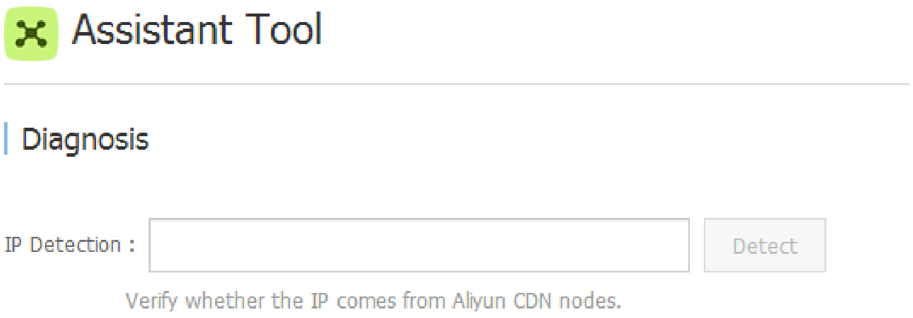
- responsetime (ms)
- requestsize (byte)
- responsesize (byte)

Diagnostic tools

- An IP address detection tool is provided to verify whether a specified IP address is the IP address of an Alibaba Cloud CDN node or not.
- For more diagnostic tools, please visit the website alibench.com

Diagnostic tools

An IP address detection tool is provided to verify whether a specified IP address is the IP address of an Alibaba Cloud CDN node or not.


Assistant Tool
Diagnosis
IP Detection :
Detect
Verify whether the IP comes from Aliyun CDN nodes.