Alibaba Cloud
Alibaba Cloud CDN

Domain Management

Issue: 20190716

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⛔	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⛔ Danger: Resetting will result in the loss of user configuration data.
⚠	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	⚠ Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
📋	This indicates warning informatio n, supplementary instructions, and other content that the user must understand.	ⓘ Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	📋 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *`Instance_ID`*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *`[-all|-t]`*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

Legal disclaimer.......... I
Generic conventions.......... I
1 Introduction.......... 1
2 Function overview.......... 3
3 Batch Configure.......... 9
4 Set an alarm rule.......... 12
5 Tags.......... 13
5.1 Tag overview.......... 13
5.2 Attach tags to a domain name.......... 14
5.3 Detach tags from a domain name.......... 14
5.4 Manage domain names by tag.......... 15
5.5 Query domain names by tag.......... 16
5.6 Tag use case.......... 18
6 Content back-to-source settings.......... 19
6.1 Back-to-origin HOST.......... 19
6.2 Back-to-origin with the same protocol.......... 20
6.3 Enable private bucket back-to-origin authentication.......... 22
6.4 Disable private bucket back-to-origin authentication.......... 25
6.5 Back-to-origin SNI.......... 26
6.6 Customize an origin HTTP header.......... 28
7 Node Cache Settings.......... 30
7.1 Cache configuration.......... 30
7.2 Set HTTP code expiration time.......... 32
7.3 Set the HTTP Response Header.......... 35
7.4 Customize the 404 page.......... 36
7.5 Rewrite.......... 38
8 HTTPS Acceleration.......... 41
8.1 What is HTTPS secure acceleration?.......... 41
8.2 Certificate Format.......... 43
8.3 HTTPS Secure Acceleration.......... 48
8.4 HTTP/2.......... 52
8.5 Force Redirect.......... 55
8.6 TLS.......... 56
8.7 HSTS.......... 57
9 Access Control Settings.......... 60
9.1 Anti-leech.......... 60
9.2 Business type.......... 62
9.2.1 Authentication configuration.......... 62

9.2.2 Authentication method A.......... 65
9.2.3 Authentication method B.......... 67
9.2.4 Authentication method C.......... 69
9.2.5 Sample authentication code.......... 71
9.3 IP Blacklist and Whitelist.......... 72
9.4 UA blacklist and whitelist.......... 74
10 Performance Optimization settings.......... 76
10.1 Page Optimization.......... 76
10.2 Intelligent compression.......... 77
10.3 Brotli compression.......... 79
10.4 Filter Parameter.......... 80
11 Advanced settings.......... 82
11.1 Peak Bandwidth.......... 82
12 Video Service Configuration.......... 85
12.1 Back-to-origin of range.......... 85
12.2 Drag/Drop Playback.......... 87

1 Introduction

Quick start

Alibaba Cloud Content Delivery Network(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:

1. Billing method display and change:
2. Key data: the number of domains in normal status and the total traffic for all domains this month
3. This month's data:
    a. Domain peak bandwidth
    b. Top 4 domain names according to the accumulated downstream traffic
    c. Region distribution of users who access the acceleration resources
    d. Real-time cache hit rate of users who access acceleration resources

> Note:
> This month indicates the current calendar month.

You can complete relevant function settings and view data in the left-side navigation pane:

Functions	Brief introduction
Domain name management	Add a CDN domain name, manage, or delete a CDN domain name, and change the basic and configuration information of the CDN domain name.

Functions	Brief introduction
Monitoring	Include Resource Monitoring and Real-time Monitoring.
Refresh	URL refresh and directory refresh are available.
Log	Log downloads, log storage (upcoming), Cloud reports
Tools	Link diagnostic tools, IP queries

2 Function overview

HTTPS secure acceleration

Function	Description	Default
HTTPS secure acceleration	Provides a full link HTTPS secure acceleration scheme, just upload the CDN domain name certificate/private key after you activate secure acceleration mode, and supports viewing , disabling, enabling, editing of certificates.	Disabled
Force redirect	When the "HTTPS secure acceleration" is enabled , the CDN domain name supports custom settings , and redirect the user' s original request in a forcible way.	Disabled
HTTP/2	HTTP/2 can be seen as an advanced edition of HTTP/1.1. It has many advantages, including binary protocol, content security, multiplexing, header compression, and so on.	Disabled
TLS	TLS is a cryptographic protocol designed to ensure communication security and data integrity of a computer network.	TLS Version 1.0, TLS Version 1.1, and TLS Version 1.2 are enabled by default.
HSTS	HSTS is specified in RFC 6797. HSTS instructs clients, such as a browser, that a domain can only be accessed by using HTTPS.	Disabled

Back-to-source settings

Function	Description	Default
Back-to-origin HOST	Specifies the host domain name that a CDN node accesses in the back-to-source process. Three options are available: CDN domain name, original site domain name, and custom domain name.	CDN domain name
Back-to-source with the same protocol	Back-to-source requests for resources use exactly the same protocol as used by the client to request the resources.	Disabled
Private bucket back-to-origin authentication	After authentication is successful and authentication configuration is enabled, domain names enabled with private bucket authentication have the permission to access the private bucket.	Disabled

Cache settings

Function	Description	Default
Cache expiration time	Customizes cache expiration rules for specified resources.	Disabled
Setting the HTTP Request Header	Sets an HTTP request header. Nine parameters are currently available for HTTP request header customization.	Disabled
Custom 404 page	Available in three options: default 404, public welfare 404, custom 404	Default 404 page

Access control

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

Performance optimization

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

Video-related settings

Function	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

Function	Description	Default
Drag/drop playback	Enables random drag or drop playback in a video or audio on-demand scenario .	Disabled

Advanced settings

Function	Description	Default
Peak Bandwidth	If the average bandwidth exceeds the maximum, the domain name automatically goes offline to protect your domain name security	Disabled

Refresh and preload

Function	Description	Default
URL refresh and preload	· Forces specified files on the CDN Cache node to expire in order to update back-to-source again. · 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.	Enabled

Data monitoring and statistical analysis

Function	Description	Default
Data monitoring	You can select Domain Name, Region, Operator , Time Granularity (1 minute, 5 minute or 1 hour) and Time Range (Today, Yesterday, 7 Days, 30 Days or Custom) to view the specific condition.	Enabled
Statistical analysis	In Statistical Analysis, you can check data of PV and UV, Area and ISP, Domain Name Rankings, Popular Referer, and Popular URLs .	Enabled

Usage query

Function	Description	Default
Usage query	You can use this function to obtain the actual usage of traffic, bandwidth, or requests during a certain period.	Enabled
Billing export	You can export actual usage data by day or by month, so as to compare it with the report output from the billing center.	Enabled
Detail data export	You can export detail data for traffic/bps data or request times, so that you can calculate or review the usage you actually paid for .	Enabled

Log management

Function	Description	Default
Log Downloading	You can download the log files within 1 month.	Enabled

Other settings

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

3 Batch Configure

Introduction

You can copy specific configurations of a domain name then apply them to one or more other domain names.

Note:

You can only copy the configuration of a domain name when it is running normally.

Procedure

Make sure that you have configured the domain name that you want to copy.

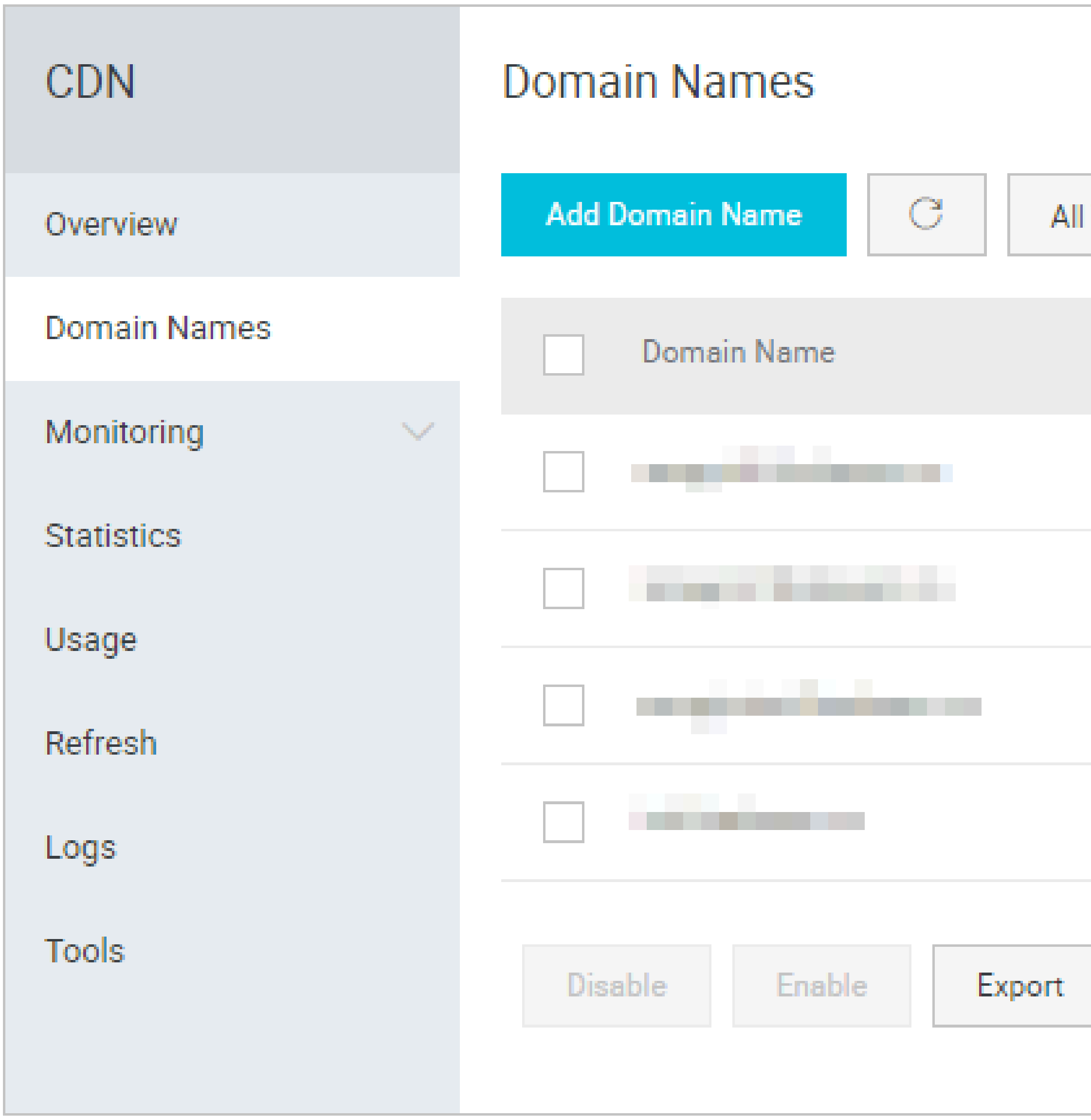
Note:

You cannot copy an HTTPS certificate to another domain name. Configure it independently.

Warning:

You cannot return to the configuration before copying. Make sure the source domain name is on service or has existing configuration, and its bandwidth is large. Copy with caution.

1. On the Domain Names page, select the domain name you want to copy, then click Copy Configuration.



2. Select the configuration items you want to copy, then click Next.

> Note:
> You cannot copy the origin site and other configurations at the same time.

3. Select the target domain name you want to apply configurations to, then click Next Step.

   You can also enter keywords to search for the domain name.

> Note:

> The copied configurations will overwrite any configurations you previously set for the target domain name. Take caution when copying configurations, or your service may become unavailable.

4. Click Confirm.

Note

- For Custom back-to-origin HTTP header, copying means adding configuration to your existing. For example, if Domain A has 2 Custom back-to-origin HTTP header configurations, and you copy 5 configurations from Domain B, you may have 7 configurations in total.
- For HTTP header, copying means covering existing configurations. For example, if Domain A's Cache_Control is set to Private, and you copy Domain B's configuration of Public, then your Cache Control is now set to Public.
- Copying configurations of switches, Referer or IP's blacklist or whitelists cover existing configurations.

4 Set an alarm rule

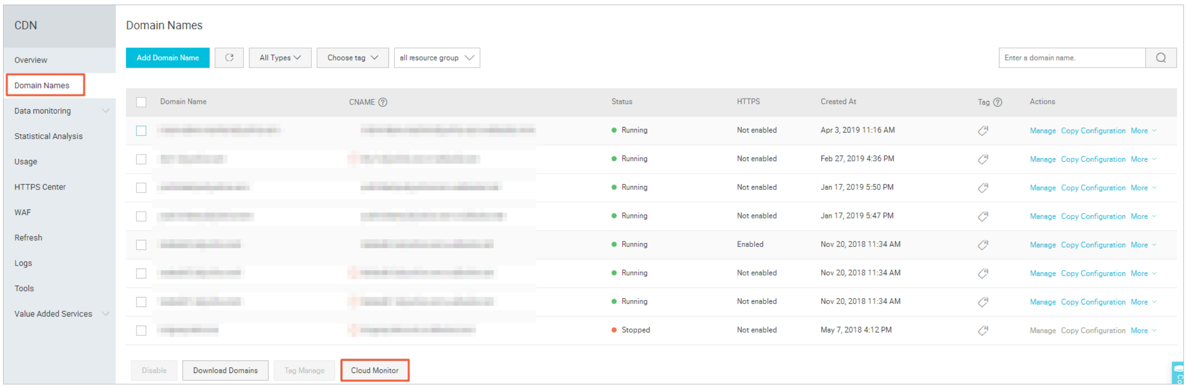
This topic describes how to set an alarm rule for a domain on Alibaba Cloud CDN.

Description

You can use Alibaba CloudMonitor to set alarm rules specific to CDN domain metrics such as the peak bandwidth, the proportion of each returned status code of the 4*xx* or 5*xx* format, and the downlink traffic volume. When an alarm rule is triggered, Alibaba CloudMonitor sends you an alarm by using the notification method (for example, SMS or email) you specify.

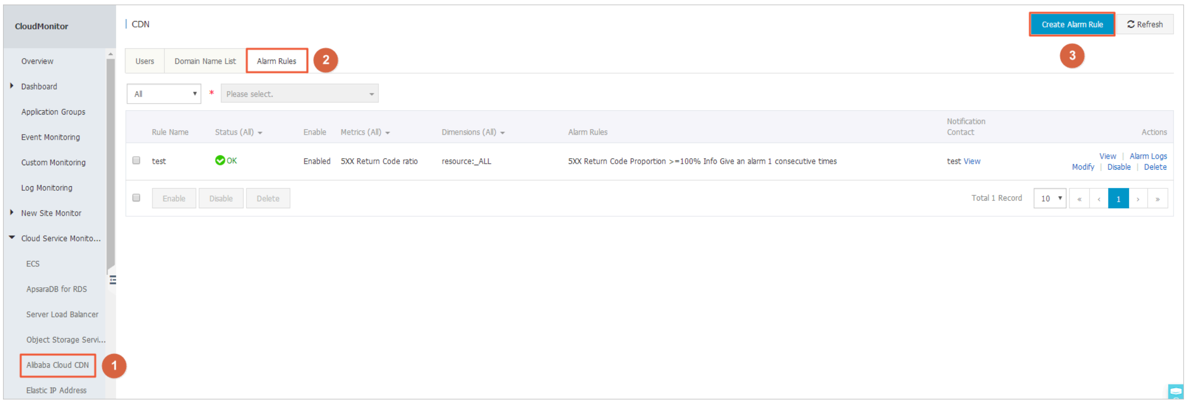
Background

1. Log on to the CDN console, and choose Domain Names from the left pane.
2. In the lower area of the right pane, click Cloud Monitor.



☐	Domain Name	CNAME	Status	HTTPS	Created At	Tag	Actions
☐	[redacted]	[redacted]	● Running	Not enabled	Apr 3, 2019 11:16 AM		Manage Copy Configuration More
☐	[redacted]	[redacted]	● Running	Not enabled	Feb 27, 2019 4:36 PM		Manage Copy Configuration More
☐	[redacted]	[redacted]	● Running	Not enabled	Jan 17, 2019 5:50 PM		Manage Copy Configuration More
☐	[redacted]	[redacted]	● Running	Not enabled	Jan 17, 2019 5:47 PM		Manage Copy Configuration More
☐	[redacted]	[redacted]	● Running	Enabled	Nov 20, 2018 11:34 AM		Manage Copy Configuration More
☐	[redacted]	[redacted]	● Running	Not enabled	Nov 20, 2018 11:34 AM		Manage Copy Configuration More
☐	[redacted]	[redacted]	● Running	Not enabled	Nov 20, 2018 11:34 AM		Manage Copy Configuration More
☐	[redacted]	[redacted]	● Stopped	Not enabled	May 7, 2018 4:12 PM		Manage Copy Configuration More

3. On the CloudMonitor page, choose Cloud Service Monitoring > Alibaba Cloud CDN from the left pane, and click Alarm Rules tab in the right pane.
4. On the Alarm Rules tab page, click Create Alarm rule. Then, create an alarm rule for Alibaba Cloud CDN.



	Rule Name	Status (All)	Enable	Metrics (All)	Dimensions (All)	Alarm Rules	Notification Contact	Actions
☐	test	✓ OK	Enabled	5XX Return Code ratio	resource:_ALL	5XX Return Code Proportion >=100% Info Give an alarm 1 consecutive times	test View	View | Alarm Logs Modify | Disable | Delete

5 Tags

5.1 Tag overview

This topic provides an overview of domain name tags. Each tag is represented by a string of characters. In Alibaba Cloud CDN, you cannot define tags, but you can attach tags to domain names, detach tags from domain names, and use tags to group or filter domain names.

Limits

- Each tag is a key-value pair (`Key : Value`), which consists of a key and a value.
- Up to 20 tags can be attached to a domain name.
- For the same domain name, the key for each tag must be unique. If two tags have the same key but different values, the current tag overwrites the previous tag. For example, if you configure the `Key1 : Value1` tag and then the `Key1 : Value2` tag for the `test . example . com` domain name, only the `Key1 : Value2` tag is attached to the domain name.
- A key cannot start with *aliyun* or *acs*, contain `http ://` or `https ://`, or be left unspecified.
- A value cannot contain `http ://` or `https ://`, but can be left unspecified.
- A key can contain up to 64 Unicode characters.
- A value can contain up to 128 Unicode characters.
- Tags are case-sensitive.

Functions

You can use tags to perform the following operations:

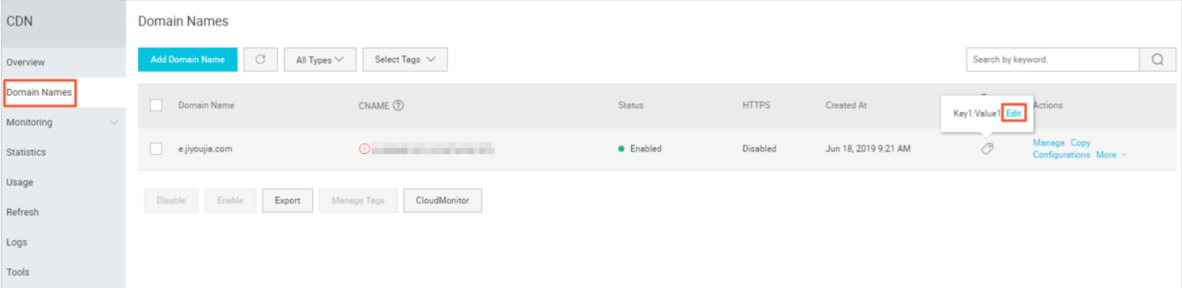
- Attach tags to domain names to identify or group the domain names. For more information, see Attach tags.
- Detach tags from domain names. For more information, see Detach tags.
- Manage domain names based on their tags. For more information, see Manage domain names by tag.
- Query the domain names to which specific tags are attached. For more information, see Filter domain names by tag.

5.2 Attach tags to a domain name

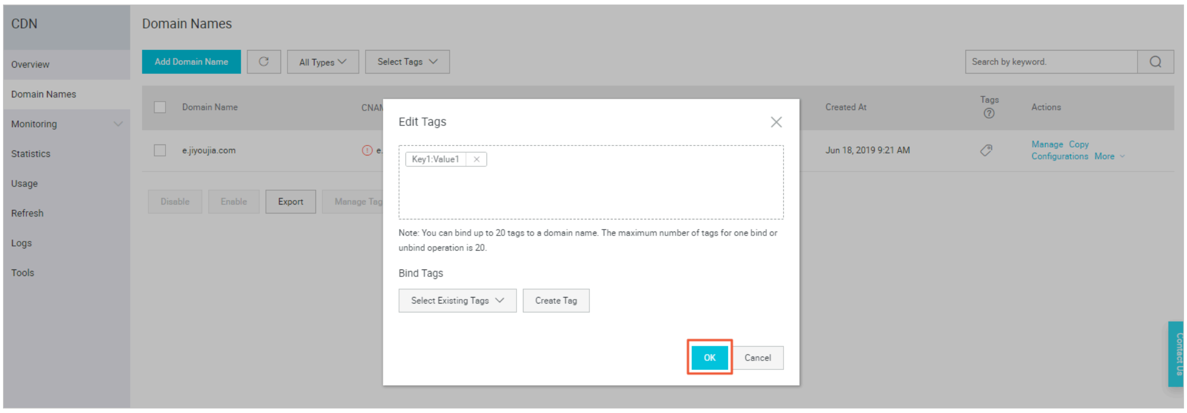
This topic describes how to attach tags to a domain name, which can help you to easily identify and group domain names.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click Domain Names.
3. On the Domain Names page, find the domain name you want to set, and move the pointer over the icon in the Tags column.
4. Click Edit



5. In the Edit Tags dialog box, click Select Existing Tags or Create Tag to attach tags to the domain name.



Note: You can bind up to 20 tags to a domain name. The maximum number of tags for one bind or unbind operation is 20.

6. Click OK.

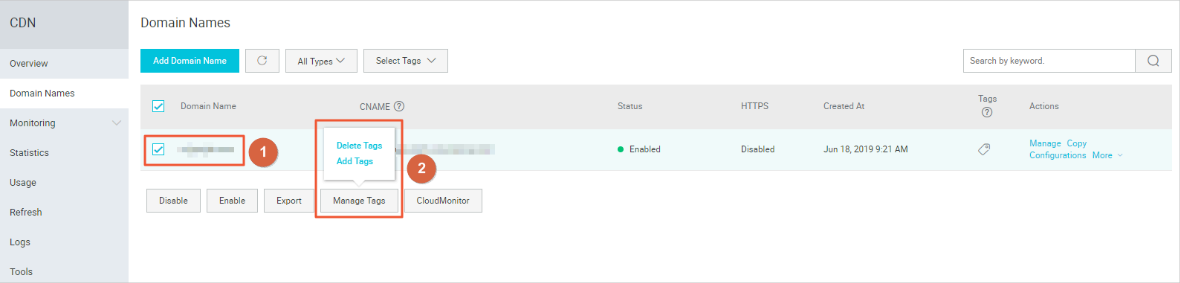
5.3 Detach tags from a domain name

This topic describes how to detach tags from a domain name.

Procedure

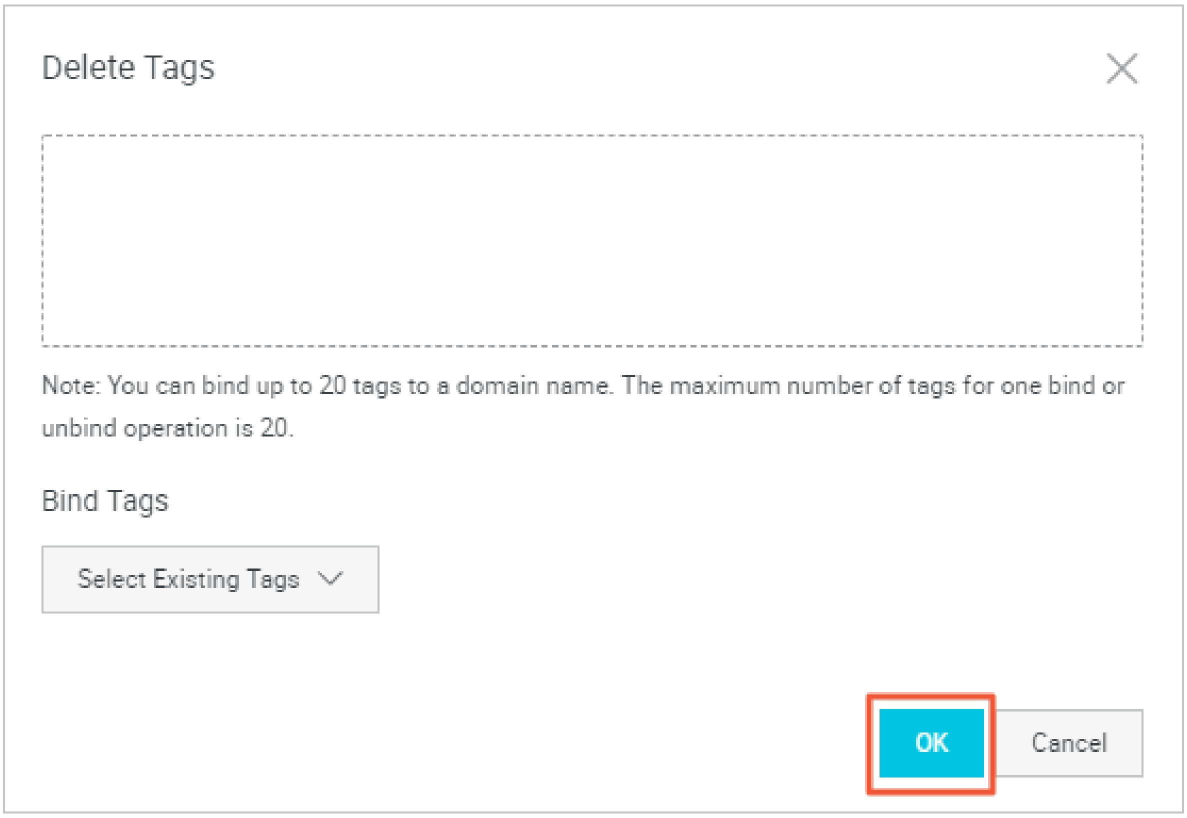
1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click Domain Names.

3. On the Domain Names page, find the domain name you want to set, and choose Manage Tags > Delete Tags.



Domain Name	CNAME	Status	HTTPS	Created At	Tags	Actions
[redacted]	[redacted]	● Enabled	Disabled	Jun 18, 2019 9:21 AM		Manage Copy Configurations More

4. In the Delete Tags dialog box, select the tags you want to delete, and click OK.



Note: You can bind up to 20 tags to a domain name. The maximum number of tags for one bind or unbind operation is 20.

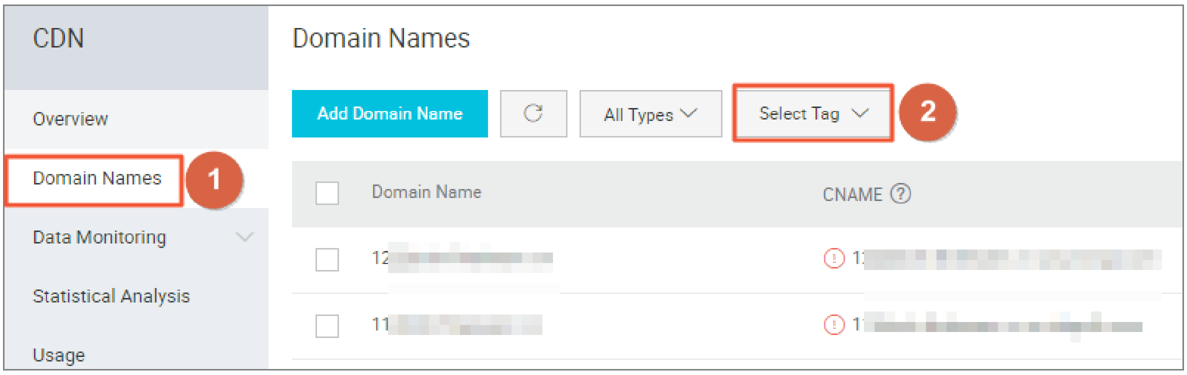
5.4 Manage domain names by tag

This topic describes how to manage domain names by tag.

Procedure

1. Log on to the CDN console.
2. In the left-side navigation pane, click Domain Names.

3. Select tags from the Select Tag drop-down list.



5.5 Query domain names by tag

This topic describes how to query domain names by tag.

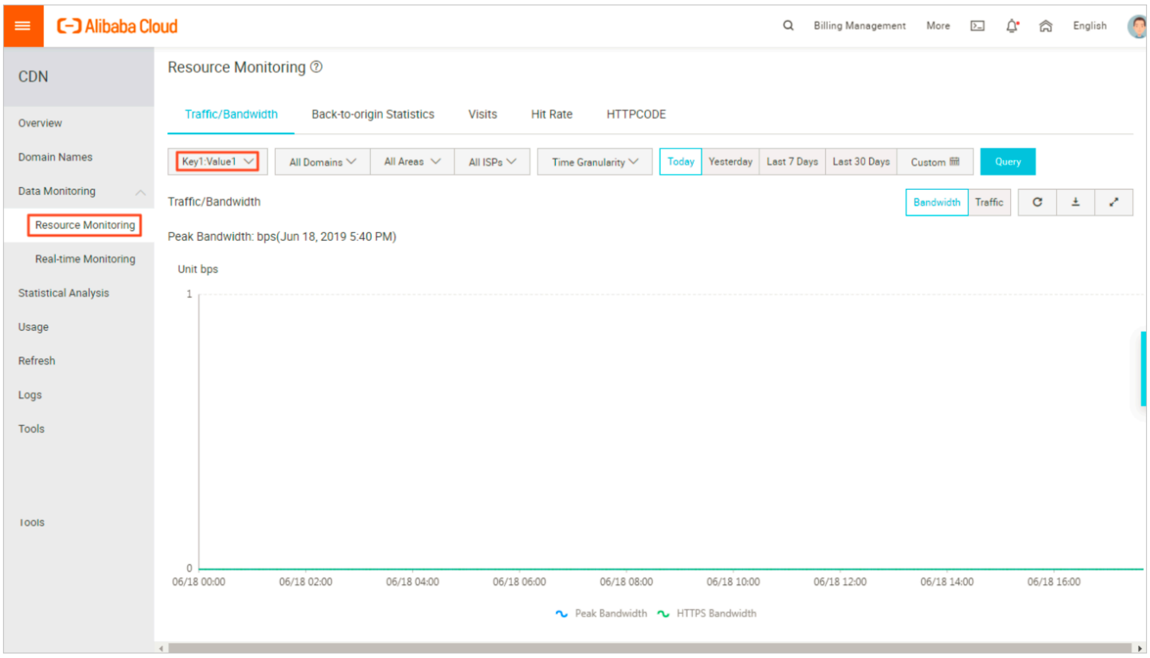
Procedure

1. Log on to the CDN console.
2. Use one of the following two methods to query the domain names to which specific tags are attached:

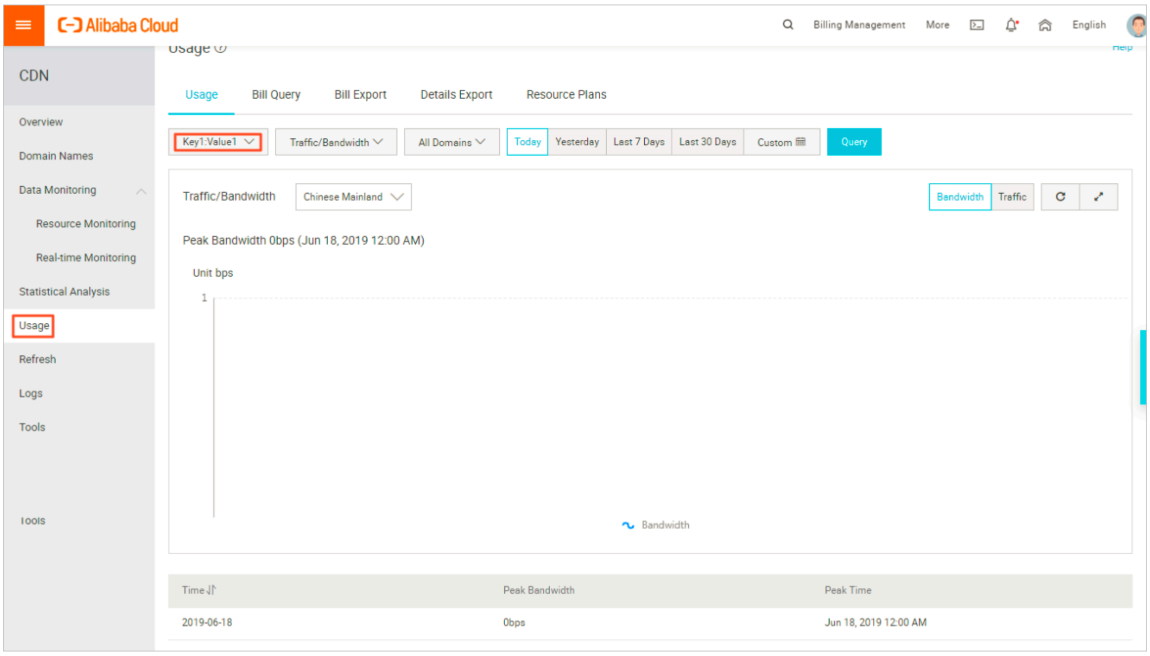
Note:

If you select multiple tags, only the domain names that contain all selected tags are returned by the system.

- In the left-side navigation pane, choose Data Monitoring > Resource Monitoring. In the main workspace, select tags from the Choose tag drop-down list and click Query.



- In the left-side navigation pane, click Usage. In the main workspace, select tags from the Choose tag drop-down list and click Query.



Time	Peak Bandwidth	Peak Time
2019-06-18	0bps	Jun 18, 2019 12:00 AM

5.6 Tag use case

This topic describes how to group and manage domain names with tags by using the example of attaching tags to manage domain names.

Assume the following scenario as a use case for tags. A company has 100 domain names on Alibaba Cloud CDN. These domain names are used by three departments (E-commerce, Gaming, and Entertainment) to supply marketing, gaming (specially for example games A and B), and post-production services. Each department has an executive, whose names are Bob, John, and Tom, respectively.

Define tags

This company defines the following tags, each of which consists of a key and a value. These are used to make grouping and managing domain names easier.

Key	Value
Department	E-commerce, Gaming, and Entertainment
Services	Marketing, Gaming (Games A and B), and Post-production
Executive	Bob, John, and Tom

The company can attach the preceding keys and values to its corresponding domain names.

Use tags to query domain names

- If the company wants to query the domain names that are managed by Tom, it can select theExecutive: Tomtag.
- If the company wants to query the domain names that are managed by John from the Gaming department, it can select theDepartment: GamingandExecutive: Johntags.

6 Content back-to-source settings

6.1 Back-to-origin HOST

Introduction

With this function, you can specify the domain name that the system need to access during CDN back-to-source. You can choose the domain type of acceleration domain, origin domain, or custom domain.

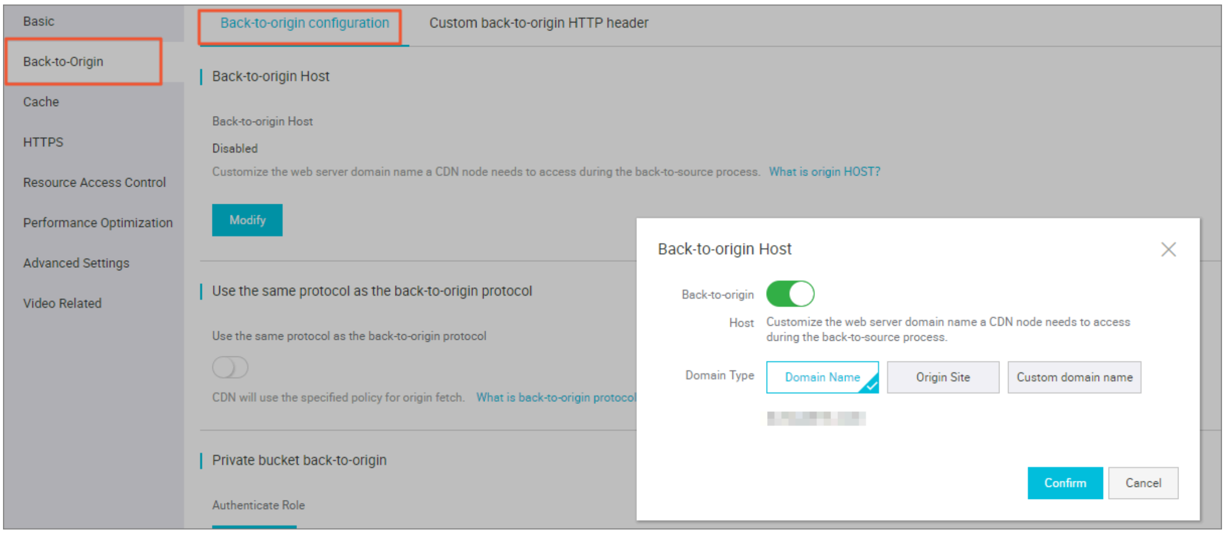
> Note:
> Specify the domain name if your origin site has been bound to multiple sites or domain names. Otherwise, your back-to-source will fail.

- By default, the Back-to-origin HOST is set as the following:
  - If the source site is of IP type, the return source host will by default accelerate the domain name.
  - If the source site is OSS source type, the source host is the source domain name by default.
- The options are: accelerating domain names, source site domain names, and custom domain names.

> Note:
> SNI back-to-origin is unavailable currently.

Configuration

Change configuration: Enter CDN domain name management page, select domain name access configuration page, return to source settings, you can modify the configuration of the returned host.



Back-to-origin Host

Back-to-origin Host

Disabled

Customize the web server domain name a CDN node needs to access during the back-to-source process. What is origin HOST?

Use the same protocol as the back-to-origin protocol

Use the same protocol as the back-to-origin protocol

CDN will use the specified policy for origin fetch. What is back-to-origin protocol

Private bucket back-to-origin

Authenticate Role

Back-to-origin Host

Back-to-origin Host: Customize the web server domain name a CDN node needs to access during the back-to-source process.

Domain Type: Domain Name | Origin Site | Custom domain name

[redacted]

The difference between a source station and a return source host (one IP/host is capable of binding Multiple Domain Names/sites) ,, therefore, you need to specify which domain name/site to return to when the source is returned by setting the feed host):

- Source station: the source station determines which IP to request when the source is returned.
- Back to source host: The back to source host determines which site on the IP to access from Back To The Source request. (If you have an IP source station bound, you need to set up multiple domain names/sites The returned source host specifies which domain name the returned source is to, or the returned source fails).

Note:

- Example 1: The source station is the domain name source for www.a.com the return source host is set to www. B .com, So the actual return source is M. Www.a.com resolve to the IP corresponding to the specific site: www. B .com.
- Example 2: source station is IP source station 1. 1. 1. 1 The return source host is set to www. B .com, and the actual return source is the specific site that corresponds to 1. 1. 1. 1: www. B .com.

6.2 Back-to-origin with the same protocol

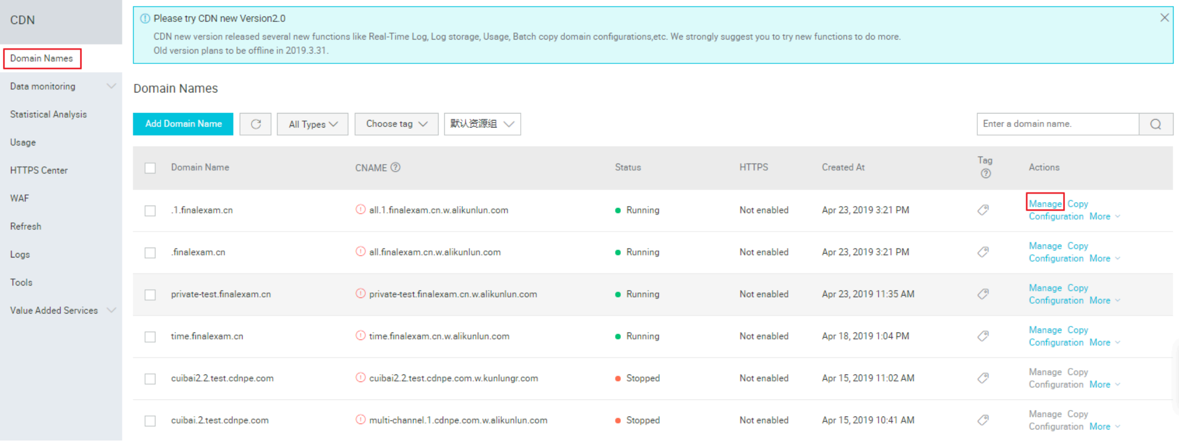
This topic describes the steps to enable the back-to-origin with the same protocol feature. When this feature is enabled, back-to-origin requests for resources uses the same protocol that is used by the client to request resources. If the client makes an HTTPS request for resources, but the resources are not cached on the node, the same back-to-origin 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-origin may fail.

Procedure

1. Log on to the CDN console.
2. In the left-side navigation pane, choose Domain Names. In the main workspace, select a domain, and in the Actions column click Manage.



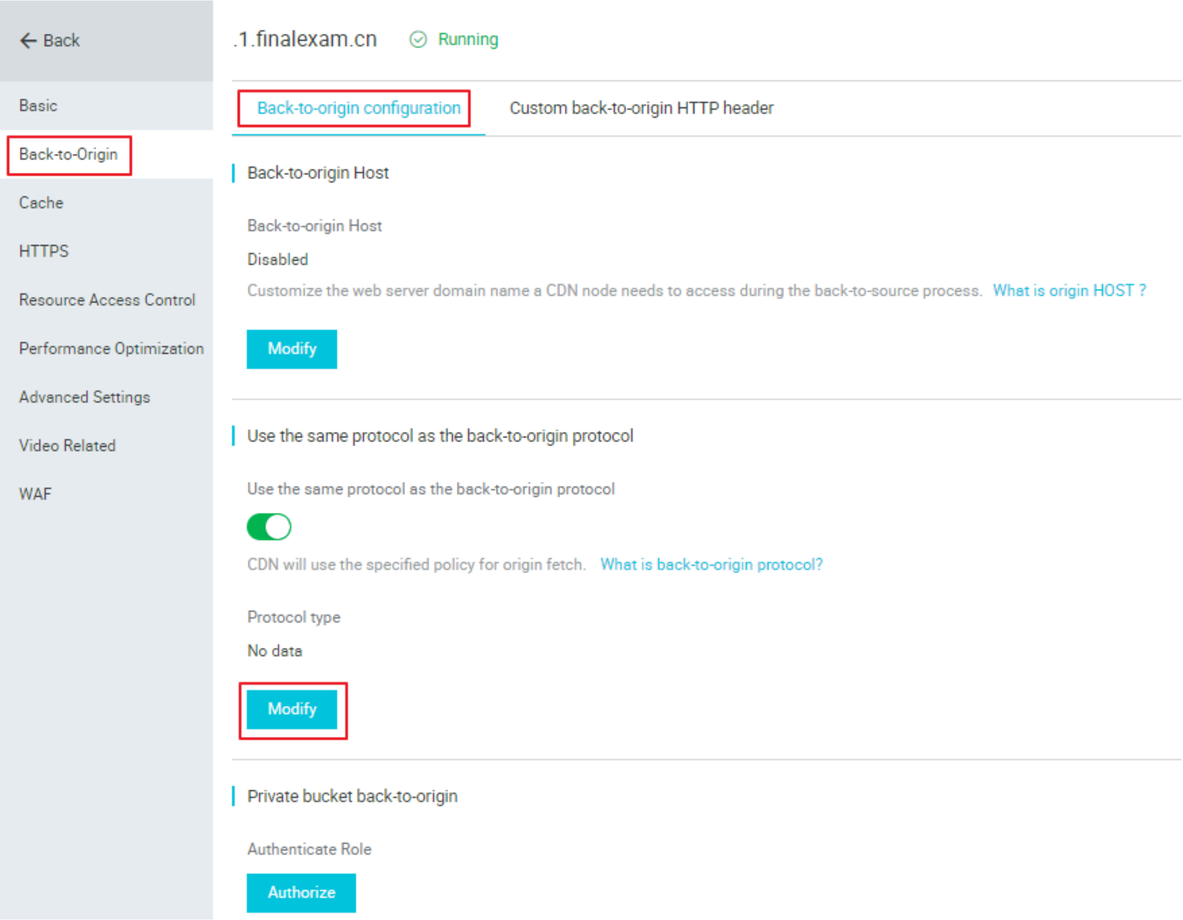
Please try CDN new Version2.0

CDN new version released several new functions like Real-Time Log, Log storage, Usage, Batch copy domain configurations,etc. We strongly suggest you to try new functions to do more.
Old version plans to be offline in 2019.3.31.

Domain Names

Domain Name	CNAME	Status	HTTPS	Created At	Tag	Actions
.1.finalexam.cn	all.1.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
.finalexam.cn	all.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
private-test.finalexam.cn	private-test.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 11:35 AM		Manage Copy Configuration More
time.finalexam.cn	time.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 18, 2019 1:04 PM		Manage Copy Configuration More
cuibai2.2.test.cdnpe.com	cuibai2.2.test.cdnpe.com.w.kunlungr.com	● Stopped	Not enabled	Apr 15, 2019 11:02 AM		Manage Copy Configuration More
cuibai.2.test.cdnpe.com	multi-channel.1.cdnpe.com.w.alikunlun.com	● Stopped	Not enabled	Apr 15, 2019 10:41 AM		Manage Copy Configuration More

3. On the page that is displayed, choose Back-to-Origin from the left-side navigation pane. Then, in the Use the same protocol as the back-to-origin protocol area on the Back-to-origin configuration tab page, enable the function, and click Modify.



.1.finalexam.cn Running

Back-to-origin Host

Back-to-origin Host

Disabled

Customize the web server domain name a CDN node needs to access during the back-to-source process. What is origin HOST ?

Use the same protocol as the back-to-origin protocol

Use the same protocol as the back-to-origin protocol

CDN will use the specified policy for origin fetch. What is back-to-origin protocol?

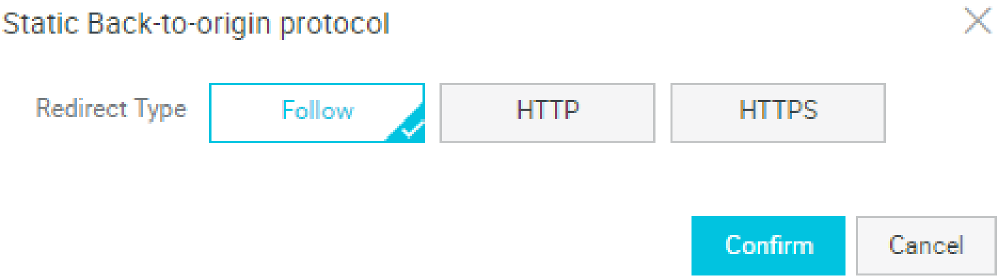
Protocol type

No data

Private bucket back-to-origin

Authenticate Role

4. Choose your Redirect Type, which can be Follow, HTTPS, or HTTP, and click Confirm.



Redirect Type: Follow

6.3 Enable private bucket back-to-origin authentication

Function overview

Private bucket back-to-origin authentication is performed when traffic of a CDN domain is diverted to the bucket marked as private under a user account. After authentication is successful and authentication configuration is enabled, domain names enabled with private bucket authentication have the permission to access the private bucket.

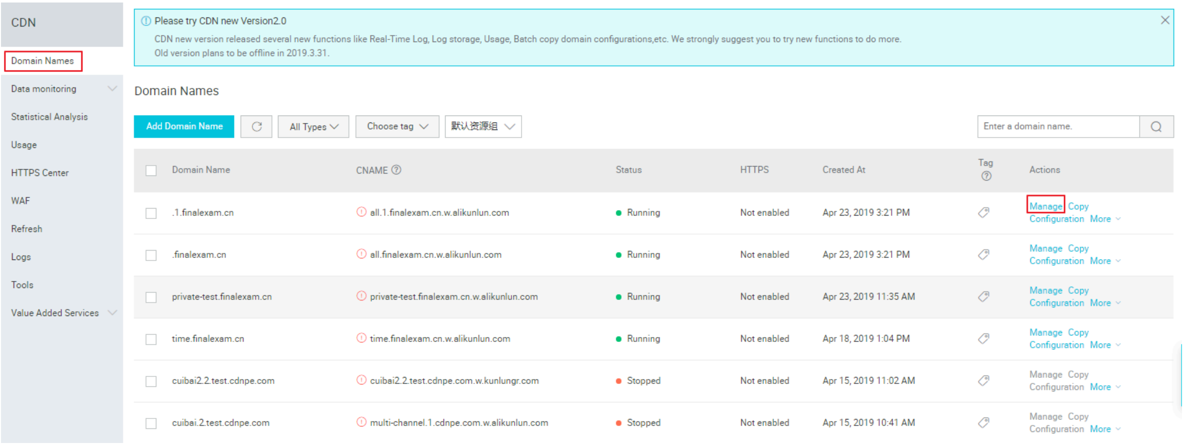
You can use functions such as the referer anti-leech protection and authorization provided by CDN to protect resource security.

> **Warning:**
>
> - After authentication is successful and the private bucket function of correspond ing domains are enabled, the CDN domain can be used to access the resource content in your private bucket. Consider carefully when you decide whether to enable this function. If the content in the private bucket to be authorized is not suitable to function as the back-to-origin content of the CDN domain, do not perform authorization or enable the function.
> - If your website faces attack risks, please buy Anti-DDoS service and do not perform authorization or enable the private bucket function.

Procedure

Enable private bucket back-to-origin authorization

1. Log on to the CDN console
2. In the left-side navigation pane, choose Domain Names. In the main workspace, select a domain, and in the Actions column click Manage.

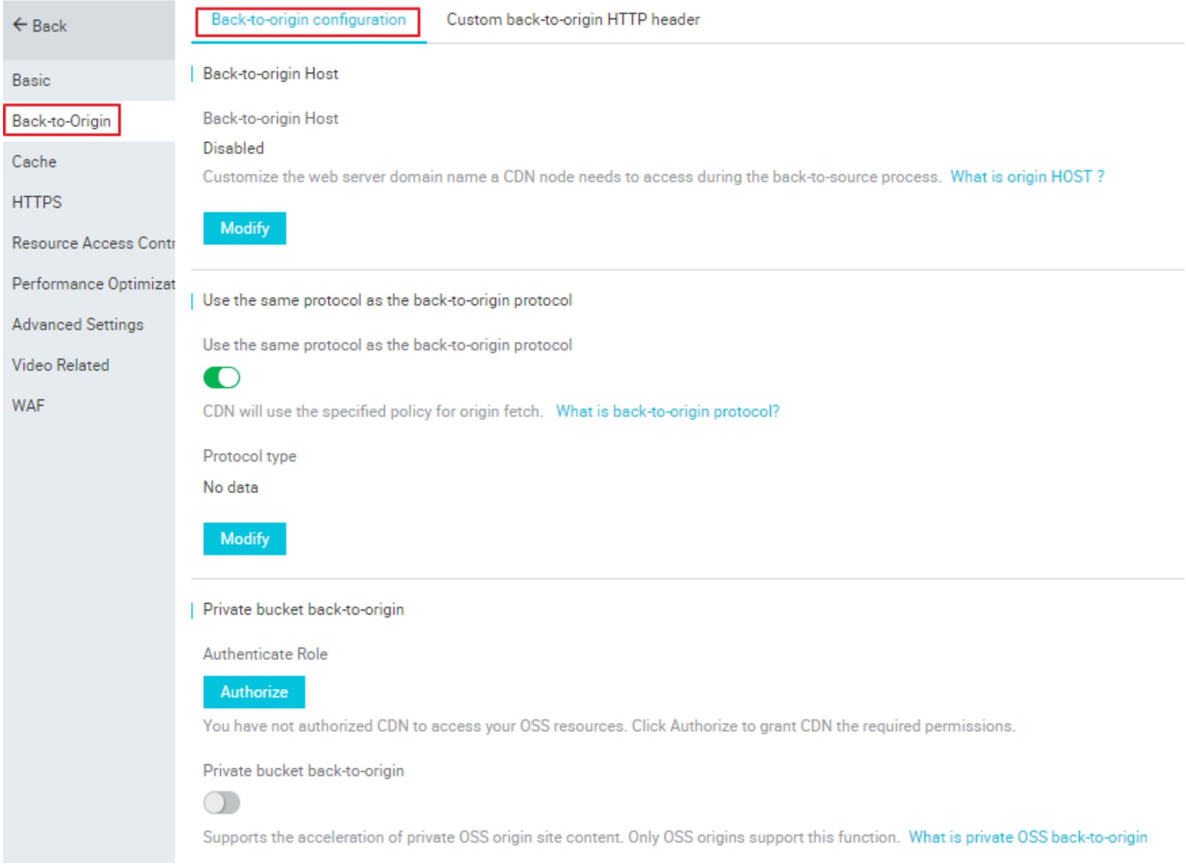


Please try CDN new Version2.0

CDN new version released several new functions like Real-Time Log, Log storage, Usage, Batch copy domain configurations,etc. We strongly suggest you to try new functions to do more.
Old version plans to be offline in 2019.3.31.

□	Domain Name	CNAME	Status	HTTPS	Created At	Tag	Actions
□	.1.finalexam.cn	all.1.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
□	.finalexam.cn	all.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
□	private-test.finalexam.cn	private-test.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 11:35 AM		Manage Copy Configuration More
□	time.finalexam.cn	time.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 18, 2019 1:04 PM		Manage Copy Configuration More
□	cuibai2.2.test.cdnpe.com	cuibai2.2.test.cdnpe.com.w.kunlungr.com	● Stopped	Not enabled	Apr 15, 2019 11:02 AM		Manage Copy Configuration More
□	cuibai.2.test.cdnpe.com	multi-channel.1.cdnpe.com.w.alikunlun.com	● Stopped	Not enabled	Apr 15, 2019 10:41 AM		Manage Copy Configuration More

3. On the page that is displayed, choose Back-to-Origin from the left-side navigation pane, and enable the function in the Private bucket back-to-origin area on the Back-to-origin configuration tab page.



Back-to-origin Host

Back-to-origin Host

Disabled

Customize the web server domain name a CDN node needs to access during the back-to-source process. What is origin HOST ?

Use the same protocol as the back-to-origin protocol

Use the same protocol as the back-to-origin protocol

CDN will use the specified policy for origin fetch. What is back-to-origin protocol?

Protocol type

No data

Private bucket back-to-origin

Authenticate Role

You have not authorized CDN to access your OSS resources. Click Authorize to grant CDN the required permissions.

Private bucket back-to-origin

Supports the acceleration of private OSS origin site content. Only OSS origins support this function. What is private OSS back-to-origin

4. After authorization is successful, enable private bucket back-to-origin configuration for the domain and click Confirm.

Disable private bucket back-to-origin authorization

> **Note:**
> If your CDN domain is sending back-to-origin requests with the private bucket as the origin site, do not disable or delete private bucket authorization.

1. Choose Access Control > Role Management.
2. Delete AliyunCDNAccessingPrivateOSSRole authorization.
3. Private bucket authorization is successfully deleted.

6.4 Disable private bucket back-to-origin authentication

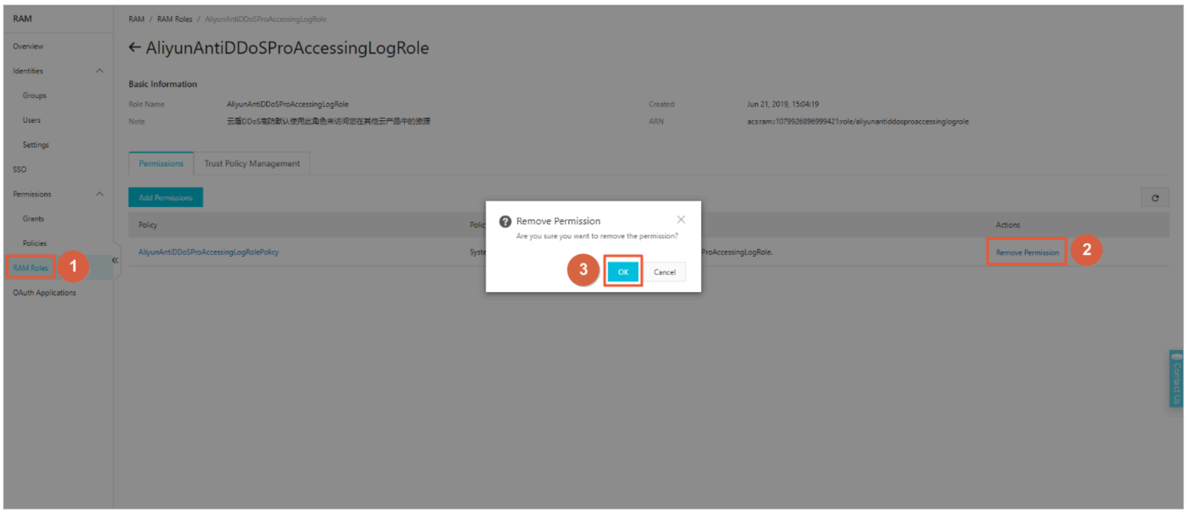
This topic describes how to disable private bucket back-to-origin authentication on the Resource Access Management (RAM) console. This authentication method enables your domain to access the resources in your private bucket.

Context

> **Note:**
> If your domain uses your private bucket as its origin, do not disable or remove this authentication method.

Procedure

1. Log on to the RAM console.
2. In the left-side navigation pane, click RAM Roles.
3. On the RAM Roles page, click the name of your RAM role and in the Actions column click Remove Permission.



← AliyunAntiDDoSProAccessingLogRole

Basic Information

Role Name AliyunAntiDDoSProAccessingLogRole

Note 云盾DDoS高防默认使用此角色来访问您在其他云产品中的资源

Created Jun 21, 2019, 15:04:19

ARN acs:ram::1079926896999421:role/aliyunantiddosproaccessinglogrole

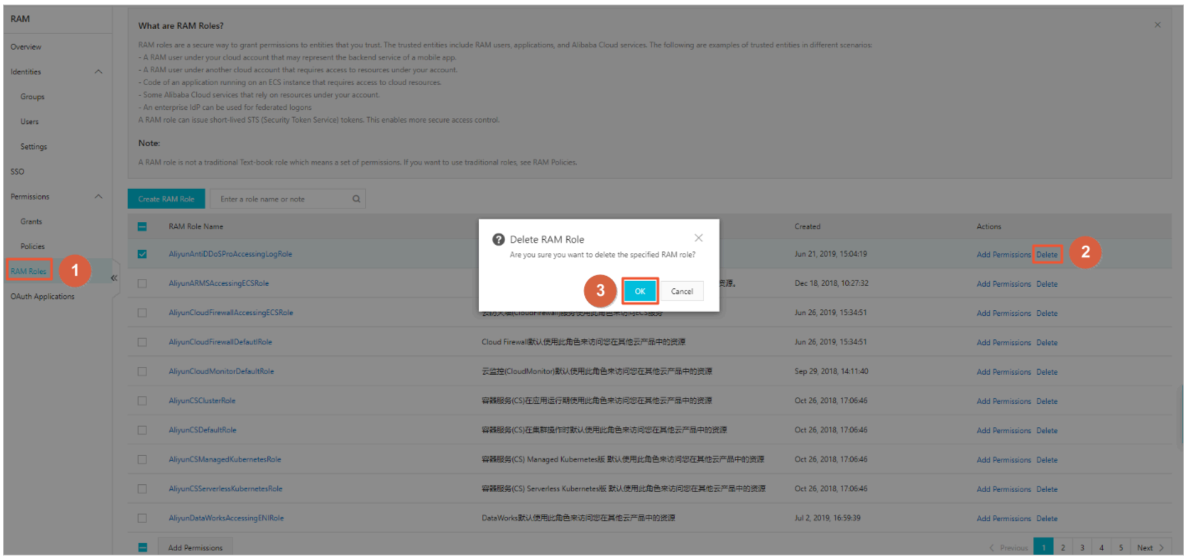
AliyunAntiDDoSProAccessingLogRolePolicy Syste ProAccessingLogRole. Remove Permission

Remove Permission

Are you sure you want to remove the permission?

4. In the Remove Permission dialog box, click OK.
5. Return to the RAM Roles page, find your RAM role, and in the Actions column click Delete.

6. In the Delete RAM Role dialog box, click OK.



What are RAM Roles?

RAM roles are a secure way to grant permissions to entities that you trust. The trusted entities include RAM users, applications, and Alibaba Cloud services. The following are examples of trusted entities in different scenarios:

- A RAM user under your cloud account that may represent the backend service of a mobile app.
- A RAM user under another cloud account that requires access to resources under your account.
- Code of an application running on an ECS instance that requires access to cloud resources.
- Some Alibaba Cloud services that rely on resources under your account.
- An enterprise IdP can be used for federated logons

A RAM role can issue short-lived STS (Security Token Service) tokens. This enables more secure access control.

Note:

A RAM role is not a traditional Text-book role which means a set of permissions. If you want to use traditional roles, see RAM Policies.

Delete RAM Role

Are you sure you want to delete the specified RAM role?

▬	RAM Role Name		Created	Actions
☑	AliyunAntiDDoSProAccessingLogRole	[illegible]	Jun 21, 2019, 15:04:19	Add Permissions Delete
□	AliyunARMSAccessingECSRole	[illegible]资源。	Dec 18, 2018, 10:27:32	Add Permissions Delete
□	AliyunCloudFirewallAccessingECSRole	云防火墙(CloudFirewall)服务使用此角色来访问ECS服务	Jun 26, 2019, 15:34:51	Add Permissions Delete
□	AliyunCloudFirewallDefautlRole	Cloud Firewall默认使用此角色来访问您在其他云产品中的资源	Jun 26, 2019, 15:34:51	Add Permissions Delete
□	AliyunCloudMonitorDefaultRole	云监控(CloudMonitor)默认使用此角色来访问您在其他云产品中的资源	Sep 29, 2018, 14:11:40	Add Permissions Delete
□	AliyunCSClusterRole	容器服务(CS)在应用运行期使用此角色来访问您在其他云产品中的资源	Oct 26, 2018, 17:06:46	Add Permissions Delete
□	AliyunCSDefaultRole	容器服务(CS)在集群操作时默认使用此角色来访问您在其他云产品中的资源	Oct 26, 2018, 17:06:46	Add Permissions Delete
□	AliyunCSManagedKubernetesRole	容器服务(CS) Managed Kubernetes版 默认使用此角色来访问您在其他云产品中的资源	Oct 26, 2018, 17:06:46	Add Permissions Delete
□	AliyunCSServerlessKubernetesRole	容器服务(CS) Serverless Kubernetes版 默认使用此角色来访问您在其他云产品中的资源	Oct 26, 2018, 17:06:46	Add Permissions Delete
□	AliyunDataWorksAccessingENIRole	DataWorks默认使用此角色来访问您在其他云产品中的资源	Jul 2, 2019, 16:59:39	Add Permissions Delete

For information about how to enable private bucket back-to-origin authentication, see Enable private bucket back-to-origin authentication.

6.5 Back-to-origin SNI

This topic describes the working concepts and application scenarios related to back-to-origin Server Name Indication (SNI). The purpose of this topic is to help you decide whether you want to enable back-to-origin SNI.

Description

What is Server Name Indication (SNI)?

SNI is an extension to the Transport Layer Security (TLS) protocol by which a client determines which hostname it is attempting to connect to at the start of the handshaking process. This allows a server to present multiple certificates on the same IP address and TCP port number, and hence allows multiple secure (HTTPS) websites (or any other service over TLS) to be served by the same IP address without requiring all those sites to use the same certificate.

When a server uses a single IP address to provide HTTPS services for multiple domains, the requests for accessing the server must carry SNIs. The server can correctly return the certificates associated with the domains only when the SNIs specify the requested domains.

When do I need to enable back-to-origin SNI?

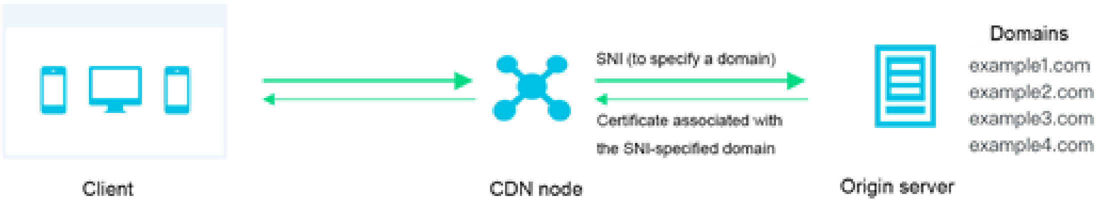
If your origin server uses one IP address to provide HTTPS services for multiple domains and port 443 is specified for receiving back-to-origin traffic on your CDN (CDN nodes communicate with your origin server according to HTTPS), you need to enable back-to-origin SNI and specify the requested domains. When a CDN node communicates with your origin server according to HTTPS, your origin server can correctly return the certificates associated with the requested domains.

Note:

If your origin is Alibaba Cloud OSS, you do not need to enable back-to-origin SNI.

Working concepts

The following figure shows the working concepts of back-to-origin SNI.

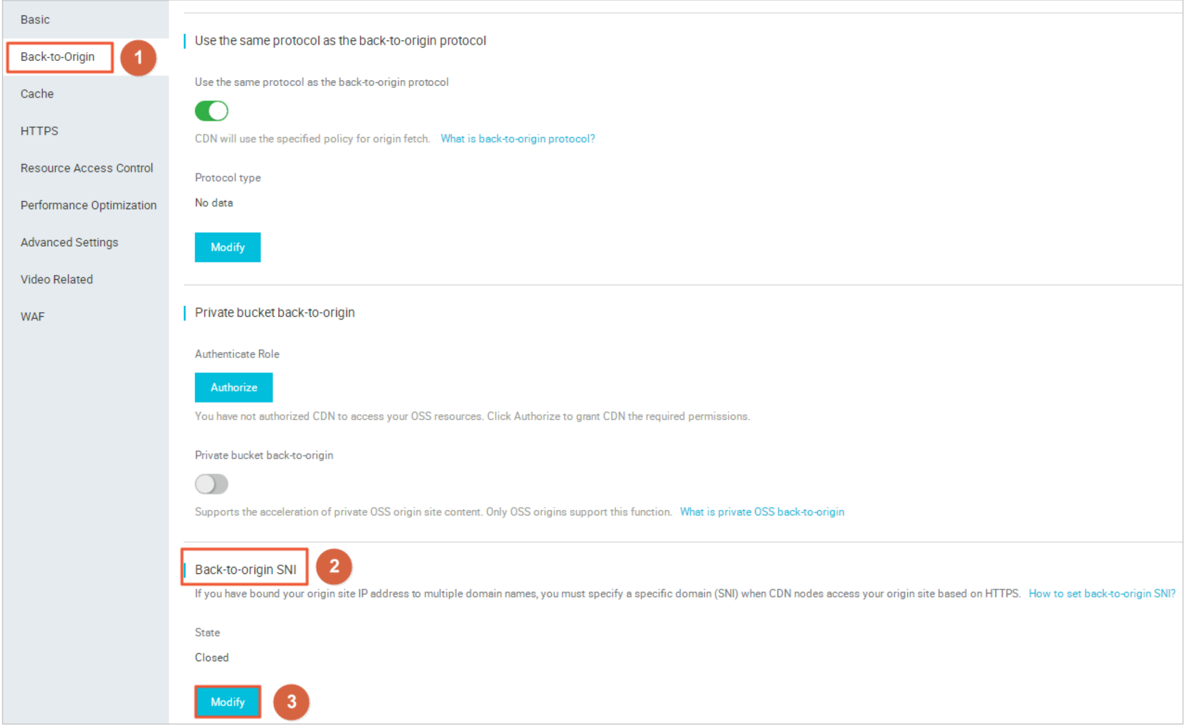


1. The CDN node requests to access the origin server according to HTTPS, where the requested domain name is specified in the SNI.
2. After receiving the request, the origin server sends the certificate associated with the requested domain to the CND node.
3. After receiving the certificate, the CDN node establishes a secure connection with the origin server.

Procedure

1. Log on to the CDN console, and in the left-side navigation pane choose Domain Names.
2. On the Domain Names page, select the target domain for which you want to set SNI, and then in the Actions column click Manage.

3. On the page that is displayed, in the left-side navigation pane choose Back-to-Origin, and in the workspace click the Back-to-origin configuration tab. On the Back-to-origin configuration tab page, click Modify in the Back-to-origin SNI area.



Use the same protocol as the back-to-origin protocol

Use the same protocol as the back-to-origin protocol

CDN will use the specified policy for origin fetch. What is back-to-origin protocol?

Protocol type

No data

Modify

Private bucket back-to-origin

Authenticate Role

Authorize

You have not authorized CDN to access your OSS resources. Click Authorize to grant CDN the required permissions.

Private bucket back-to-origin

Supports the acceleration of private OSS origin site content. Only OSS origins support this function. What is private OSS back-to-origin

Back-to-origin SNI

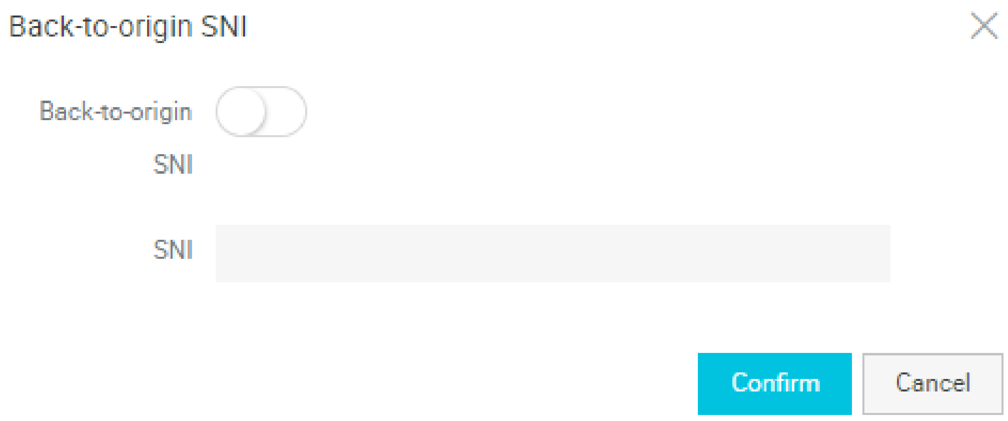
If you have bound your origin site IP address to multiple domain names, you must specify a specific domain (SNI) when CDN nodes access your origin site based on HTTPS. How to set back-to-origin SNI?

State

Closed

Modify

4. In the Back-to-origin SNI dialog box, set Back-to-origin to on, enter the name of the domain served by your origin server, and click Confirm.



Back-to-origin SNI

Back-to-origin SNI

SNI

6.6 Customize an origin HTTP header

This topic describes how to customize an origin HTTP header by adding, modifying, or deleting the header of HTTP requests.

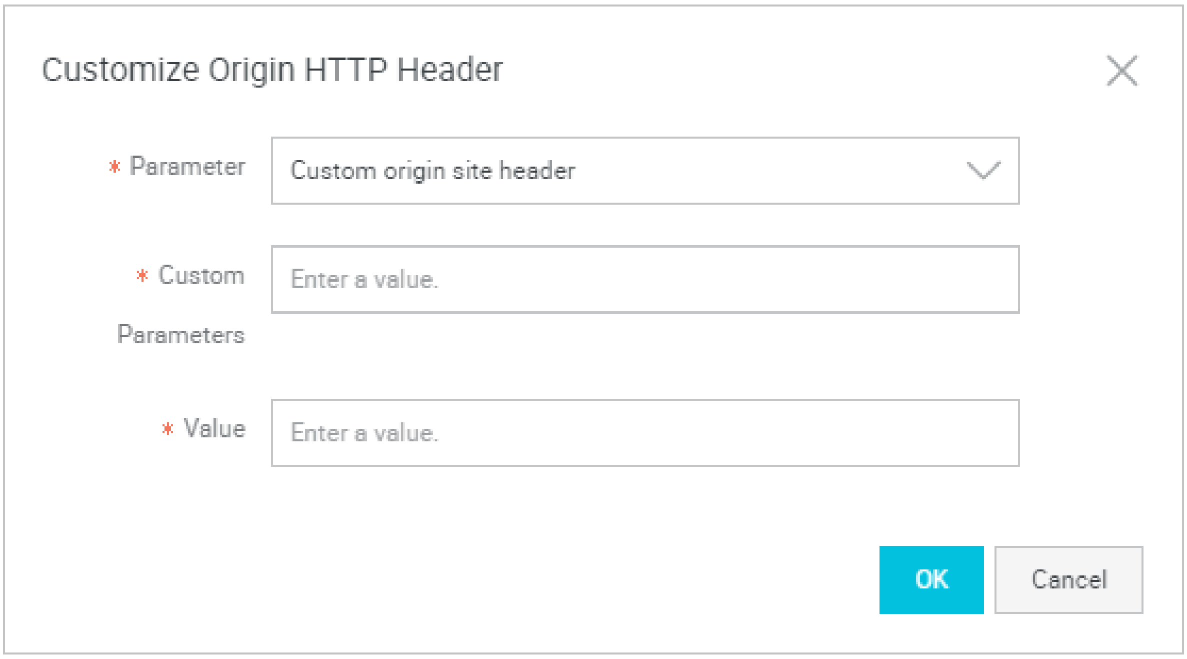
Context

An HTTP header field is a component of the header section in an HTTP request or response message. This field accurately describes the requested resource and the client or server behavior. This field also defines the operating parameters of an HTTP transaction.

HTTP message header fields include `General - header`, `Client Request - header`, and `Server Response - header` fields.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click Domain Names.
3. On the Domain Names page, find the domain name you want to set, and in the Actions column click Manage.
4. In the left-side navigation pane, click Back-to-origin.
5. Click the Custom HTTP Origin Header tab.
6. Click Customize.
7. In the Customize Origin HTTP Header dialog box, select an HTTP header parameter, set the parameter value, and click OK.



Customize Origin HTTP Header

* Parameter: Custom origin site header

* Custom Parameters: Enter a value.

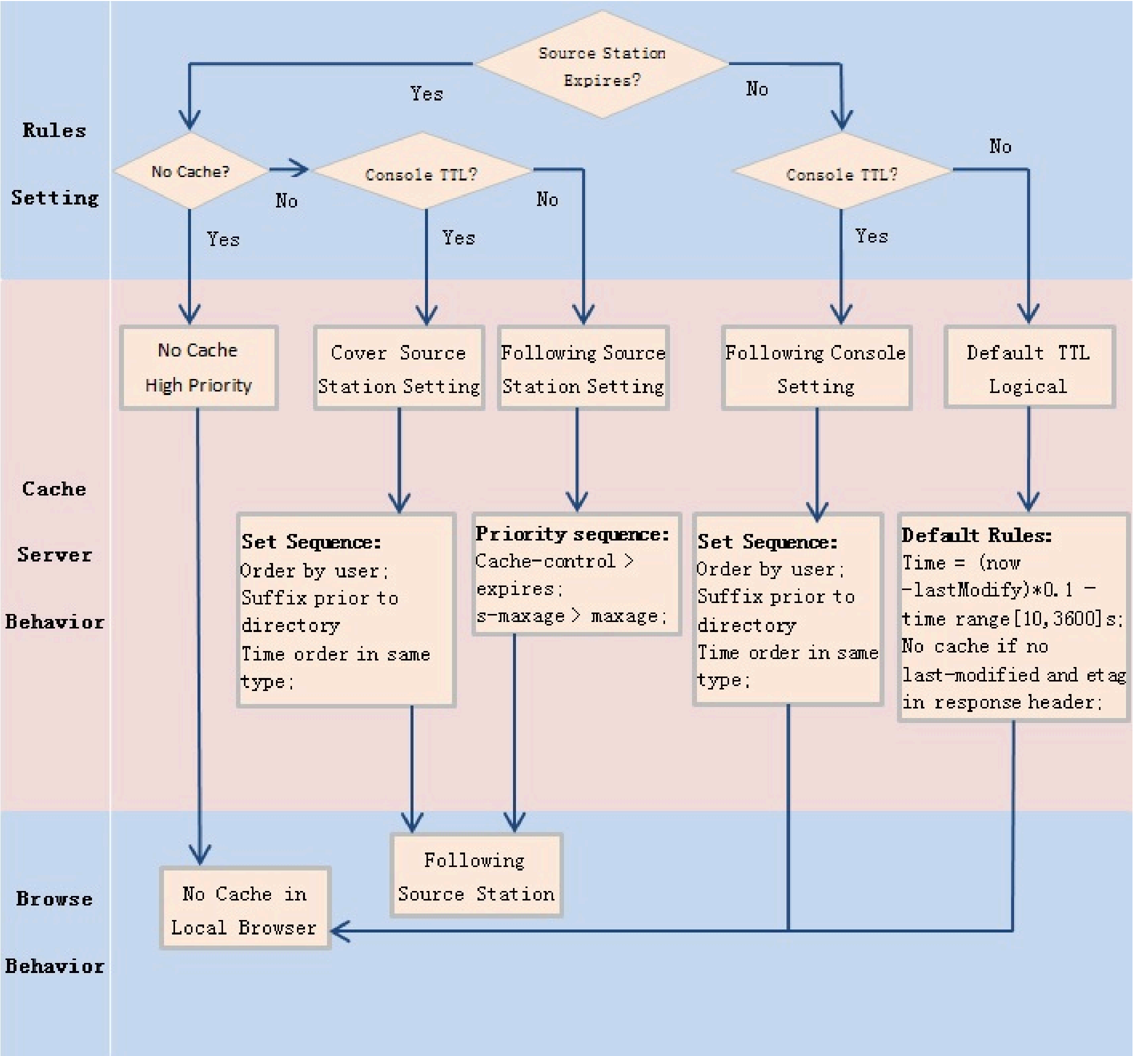
* Value: Enter a value.

7 Node Cache Settings

7.1 Cache 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 file name 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:

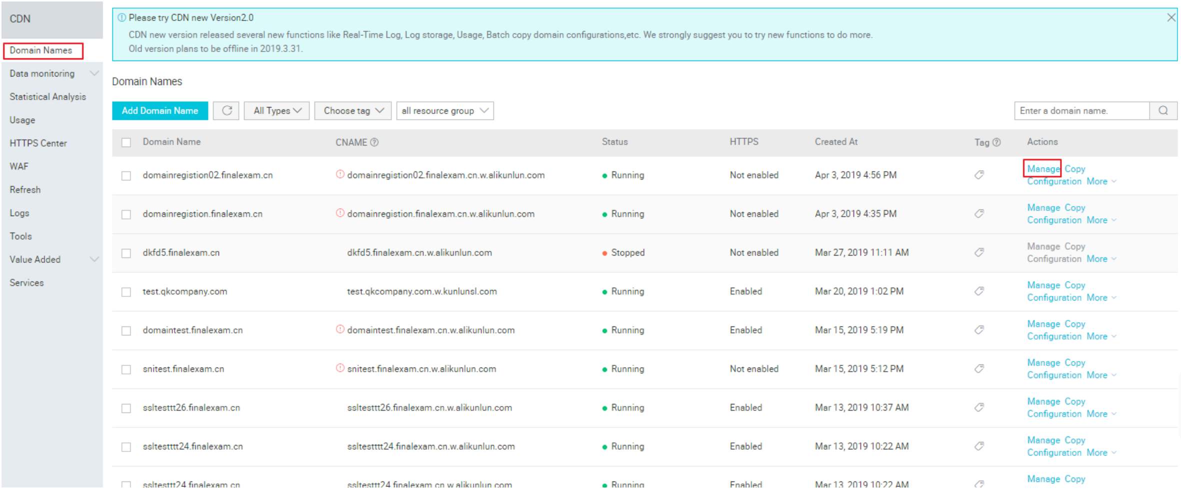
- This function is used to set file expiration time. The priority specified here is higher than that configured on the origin site. If no cache policy is configured on the origin site, you can set a cache policy by directory and file name suffix (the full path mode is supported).
- CDN cached files can be removed from the CDN node if the cached files are not updated frequently.

Notes

- For infrequently updated static files (for example, image files or application download files), we suggest you set a cache time of 1 month or more;
- For static files that must be updated or are updated frequently (for example js and css files), you can set a shorter cache time based on the actual situation;
- For dynamic files (for example, PHP files, JSP files, and ASP files), we recommend that you set the cache duration as 0s, indicating that the files are not cached. If dynamic files such as PHP files are not updated frequently, we recommend that you set the cache duration to a small value.
- We recommend 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.

Configuration guide

1. Log on to the CDN console.
2. In the left-side navigation pane, choose Domain Names. In the main workspace, select a domain, and in the Actions column click Manage.



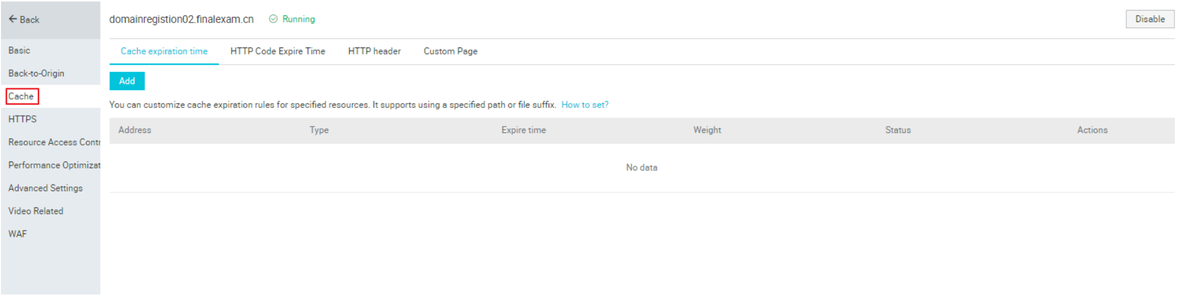
Please try CDN new Version2.0

CDN new version released several new functions like Real-Time Log, Log storage, Usage, Batch copy domain configurations,etc. We strongly suggest you to try new functions to do more.
Old version plans to be offline in 2019.3.31.

Domain Names

□	Domain Name	CNAME	Status	HTTPS	Created At	Tag	Actions
□	domainregistion02.finalexam.cn	domainregistion02.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 3, 2019 4:56 PM		Manage Copy Configuration More
□	domainregistion.finalexam.cn	domainregistion.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 3, 2019 4:35 PM		Manage Copy Configuration More
□	dkfd5.finalexam.cn	dkfd5.finalexam.cn.w.alikunlun.com	● Stopped	Not enabled	Mar 27, 2019 11:11 AM		Manage Copy Configuration More
□	test.qkcompany.com	test.qkcompany.com.w.kunlunsl.com	● Running	Enabled	Mar 20, 2019 1:02 PM		Manage Copy Configuration More
□	domaintest.finalexam.cn	domaintest.finalexam.cn.w.alikunlun.com	● Running	Enabled	Mar 15, 2019 5:19 PM		Manage Copy Configuration More
□	snitest.finalexam.cn	snitest.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Mar 15, 2019 5:12 PM		Manage Copy Configuration More
□	ssltesttt26.finalexam.cn	ssltesttt26.finalexam.cn.w.alikunlun.com	● Running	Enabled	Mar 13, 2019 10:37 AM		Manage Copy Configuration More
□	ssltestttt24.finalexam.cn	ssltestttt24.finalexam.cn.w.alikunlun.com	● Running	Enabled	Mar 13, 2019 10:22 AM		Manage Copy Configuration More
□	ssltesttt24.finalexam.cn	ssltesttt24.finalexam.cn.w.alikunlun.com	● Running	Enabled	Mar 13, 2019 10:22 AM		Manage Copy

3. In the left-side navigation pane, choose Cache.



You can customize cache expiration rules for specified resources. It supports using a specified path or file suffix. How to set?

Address	Type	Expire time	Weight	Status	Actions
No data					

4. Click Modify. You can manage cache policies by perform adding, modifying, and deletion operations.
5. Click Add to add cache policies by directory paths or file name suffixes.

For example, set three cache policies for the CDN domain name `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.
- We 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.

7.2 Set HTTP code expiration time

This topic describes how to set the HTTP code expiration time.

Background

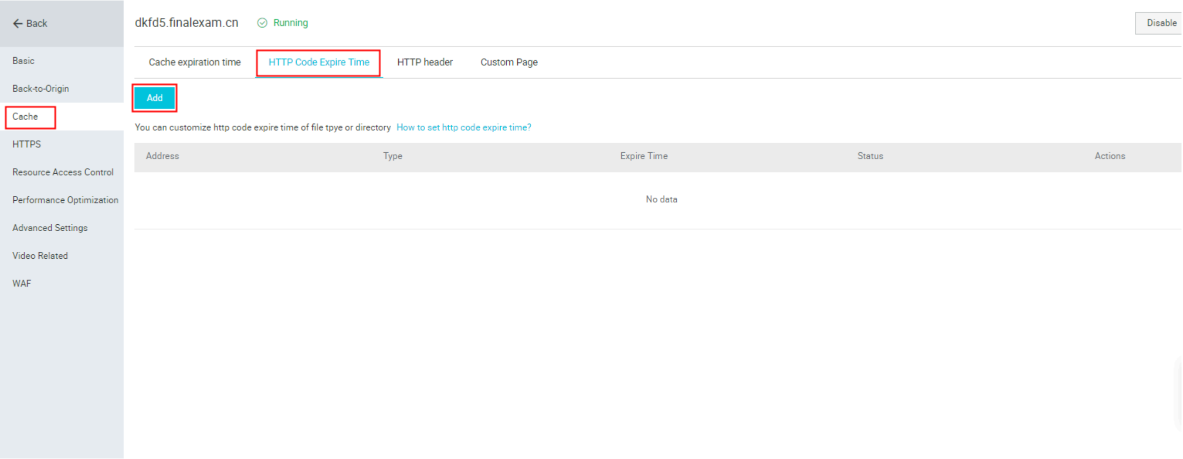
If the specified file extension or directory rule is matched to resources cached on CDN , you can set the expiration time of these resources based on the specified HTTP code expiration time.

Note:

- The system does not cache information about 303, 304, 401, 407, 600, and 601 status codes.
- For 204, 305, 400, 403, 404, 405, 414, 500, 501, 502, 503, and 504 status codes, if a `Cache - Control` header is returned from the origin, the rule specified by the `Cache - Control` parameter is applied. If the HTTP code expiration time is not specified, the default cache time specified by the `negative_t tl` parameter is 1s.

Procedure

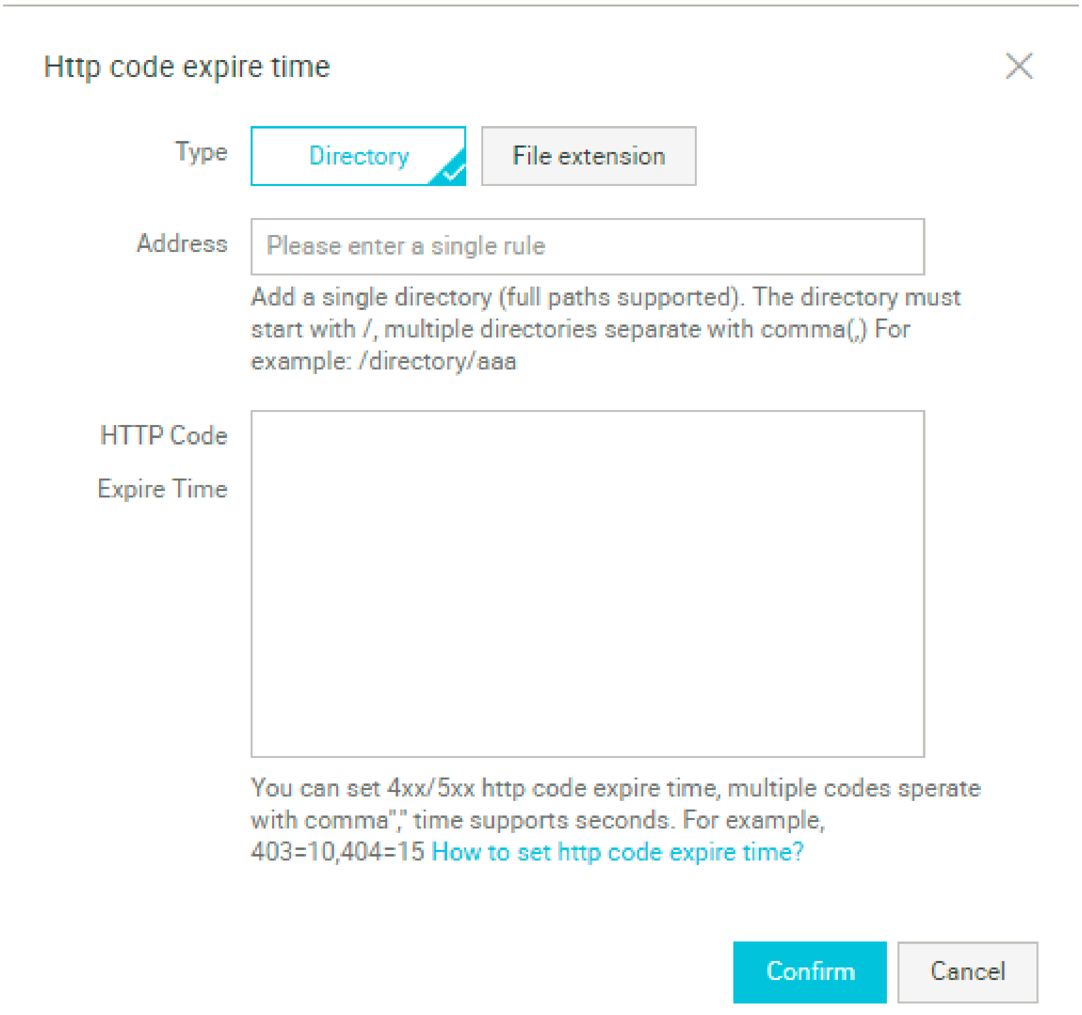
1. Log on to the CDN console.
2. In the left-side navigation pane, click Domain Names.
3. On the Domain Names page, select a domain name, and in the Actions column click Manage.
4. On the page that is displayed, choose Cache from the left pane, and click the HTTP Code Expire Time tab in the right pane.
5. On the HTTP Code Expire Time tab page, click Add.



You can customize http code expire time of file tpye or directory How to set http code expire time?

Address	Type	Expire Time	Status	Actions
		No data		

6. In the Http code expire time dialog box, set Type and other required parameters.



Http code expire time

Type: Directory | File extension

Address: Please enter a single rule

Add a single directory (full paths supported). The directory must start with /, multiple directories separate with comma(,) For example: /directory/aaa

HTTP Code Expire Time

You can set 4xx/5xx http code expire time, multiple codes sperate with comma"," time supports seconds. For example, 403=10,404=15 How to set http code expire time?

Type	Remarks
Directory	· Add a single directory (full paths are supported). The directory must start with a forward slash (/) (for example, `/ directory / aaa`). · Status codes of the 2*xx* and 3*xx* formats are not allowed.
File extension	· Multiple file extensions are separated by commas (,) (for example, `txt` , `jpg`). · Asterisks (*) cannot be used to match all types of files. · Status codes of the 2*xx* and 3*xx* formats are not allowed.

7. Click Confirm.

> Note:
> If you set two types of HTTP code expiration times, for the `Directory` and `File extension`, then the type you set earlier takes effect.

7.3 Set the HTTP Response Header

Introduction

HTTP headers (fields) are components of the header section of request and response messages in the Hypertext Transfer Protocol (HTTP). They define the operating parameters during the HTTP process. HTTP headers can be classified into general headers, request headers, response headers, and so on.

You can set an HTTP Response Header. The following HTTP response header parameters are available for customization:

Parameters	Description
`Content - Type`	Specifies the content type of the client program's response object.
`Cache - control`	Specifies the caching policy that the client program is following when requesting and responding.
`Content - Dispositio n`	Specifies the default file name provided by the client program when it is willing to save the contents accessed by request as a file.
`Content - language`	Specifies the language of the client program's response object.
`Expires`	Specifies the expiration time of the client program's response object.
`Access - Control - Allow - Origin`	Specifies the allowed origin domain of cross-origin requests.
`Access - Control - Allow - Methods`	Specifies the allowed method of cross-origin requests.

Parameters	Description
`Access - Control - Max - Age`	Specifies the length of time the response result is cached for a pre-fetch request initiated by a client program for a particular resource.
`Access - Control - Expose - Headers`	Specifies the custom header information that is allowed to be accessed.

Note

- The HTTP response header configurations will affect the response actions of all client programs of the resource under the CDN domain name, rather than the actions of the cache server.
- For now, you can only customize the HTTP header. Submit a ticket if you have other custom requirements for HTTP header.
- You can type in `*` (indicating all domain names) or a full domain name (such as `www . aliyun . com`) for the `Access - Control - Allow - Origin` parameter.
- For now, you cannot set HTTP headers for an extensive domain name.

Procedure

1. Log on to the CDN console, then go to the Domain Names page. Choose a domain name, then click Manage.
2. Go to Caching Configuration > HTTP Header, then click Modify or Delete for a parameter. You can also click Add, and then choose the parameter and enter value to add a custom HTTP header parameter

7.4 Customize 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:

Take return Code 404 as an example:

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

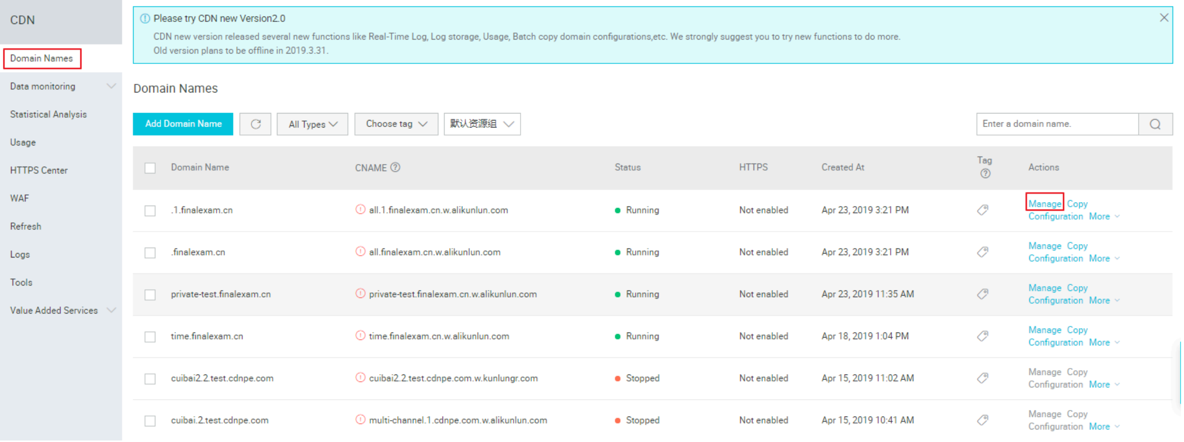
- Public welfare 404 page: when an HTTP an HTTP 404 error is returned, the server returns to the real-time update of the public welfare 404 page, view the public welfare 404 page.
- Custom 404 page: when an HTTP 404 error is returned, the server returns to the 404 page designed and edited by the user. You must costomize complete URL address of the error page.

Attentions

- 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.

Procedure

1. Log on to the CDN console.
2. In the left-side navigation pane, choose Domain Names. In the main workspace, select a domain, and in the Actions column click Manage.



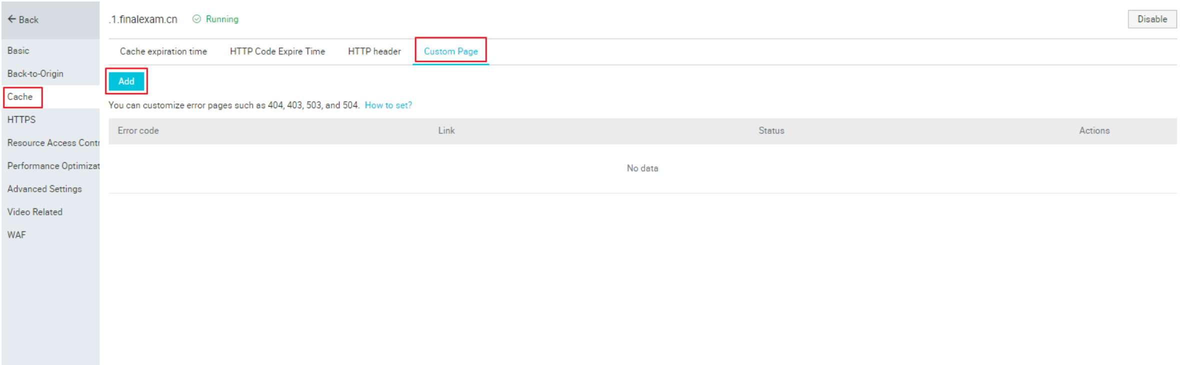
Please try CDN new Version2.0

CDN new version released several new functions like Real-Time Log, Log storage, Usage, Batch copy domain configurations,etc. We strongly suggest you to try new functions to do more.
Old version plans to be offline in 2019.3.31.

□	Domain Name	CNAME	Status	HTTPS	Created At	Tag	Actions
□	.1.finalexam.cn	all.1.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
□	.finalexam.cn	all.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
□	private-test.finalexam.cn	private-test.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 11:35 AM		Manage Copy Configuration More
□	time.finalexam.cn	time.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 18, 2019 1:04 PM		Manage Copy Configuration More
□	cuibai2.2.test.cdnpe.com	cuibai2.2.test.cdnpe.com.w.kunlungr.com	● Stopped	Not enabled	Apr 15, 2019 11:02 AM		Manage Copy Configuration More
□	cuibai.2.test.cdnpe.com	multi-channel.1.cdnpe.com.w.alikunlun.com	● Stopped	Not enabled	Apr 15, 2019 10:41 AM		Manage Copy Configuration More

3. On the page that is displayed, choose Cache from the left-side navigation pane, and in the main workspace select the Custom Page tab.
4. On the Custom Page tab page, click Modify, and you can view and manage the custom error pages.

5. Click Add to add the page content of the custom return code.



You can customize error pages such as 404, 403, 503, and 504. How to set?

Error code	Link	Status	Actions
No data			

If you choose Custom page 404, 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 name 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", and enter `http :// exp . aliyun . com / error404 . html`.

7.5 Rewrite

This topic describes the rewrite function and how to enable it in the CDN console.

Context

With the rewrite function, you can configure multiple rewrite rules. With each rewrite rule, you can specify the requested Uniform Resource Identifier (URI) and the destination URI to which a request is redirected. For example, if a client requests to visit `http :// example . com` through HTTP, you can configure a rewrite rule to redirect the request to `https :// example . com`.

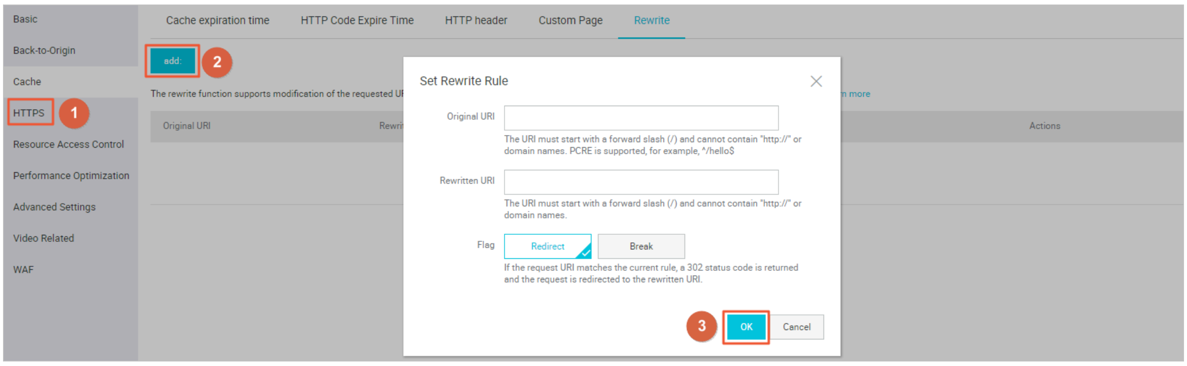
A CDN node uses one of the following two methods to run rewrite rules:

- Redirect: If the requested URI matches the current rule, the CDN node returns a 302 status code and redirects the request to the destination URI.
- Break: If the requested URI matches the current rule, the CDN node returns the content of the requested URI, but does not check whether the requested URI matches the remaining rules.

Procedure

1. Log on to the CDN console.

2. In the left-side navigation pane, click Domain Names.
3. Find the domain name you want to set, and click Manage in the Actions column.
4. In the left-side navigation pane, click Cache.
5. On the Rewrite tab, click add.
6. Set the parameters as needed and click OK. You can select Redirect or Break for the Flag parameter.



The rewrite function supports modification of the requested UI

The URI must start with a forward slash (/) and cannot contain "http://" or domain names. PCRE is supported, for example, ^/hello$

The URI must start with a forward slash (/) and cannot contain "http://" or domain names.

If the request URI matches the current rule, a 302 status code is returned and the request is redirected to the rewritten URI.

Example No.	Requeste URI	Destinati n URI	Rewrite rule flag	Description
1	/hello	/index.html	Redirect	When a client requests the content of `http :// domain . com / hello`, the CDN node returns a 302 status code, asking the client to request the content of `http :// domain . com / index . html`
2	^/hello$	/index.html	Break	When a client requests the content of `http :// domain . com / hello`, the CDN node returns the content of `http :// domain . com / index . html`, but does not check whether the requested URI matches the remaining rewrite rules.

Example No.	Requested URI	Destination URI	Rewrite rule flag	Description
3	^/$	/index.html	Redirect	When a client requests the content of `http :// domain . com`, the CDN node returns a 302 status code, asking the client to request the content of `http :// domain . com / index . html`.

8 HTTPS Acceleration

8.1 What is HTTPS secure acceleration?

This topic describes how HTTPS secure acceleration works, what benefits it brings, how to select certificates for it, and in what scenarios it can be used.

How it works

HTTPS is the secure version of HTTP. In HTTPS, Secure Sockets Layer (SSL) is used as a sublayer under regular HTTP application layering to authenticate users and encrypt data. HTTPS is widely used for such services as transactional payment that involve sensitive user data.

According to a report released by Electronic Frontier Foundation (EFF) in 2017, over 50% of web traffic across the globe is transmitted by using HTTPS.

Benefits

- HTTPS helps to defend against security threats that may be incurred by HTTP, which transmits data in plaintext:
  - Eavesdropping: A third party can intercept the data that is being transmitted.
  - Tamper: A third party can tamper with the data that is being transmitted.
  - Spoofing: A third party can spoof the identify of a user in communication.
  - Traffic hijacking: includes page hijacking and DNS hijacking.
- HTTPS is becoming a trend. An increasing number of leading browsers such as Google Chrome 70 or later and Mozilla Firefox identify HTTP websites as insecure . If an organization insists on using HTTP, they will face security vulnerabilities. Furthermore, when users visit the organization's website by using these browsers , they will be prompted that this website is insecure, which compromises user experience and hence reduces visits to this website.
- HTTPS is more secure, caters to the market, and can make user experience better . Major service providers such as Baidu and Google add search weights to HTTPS websites. Additionally, leading browsers must support HTTPS so that they support HTTP/2. Therefore, we recommend that CDN users upgrade their access protocols to HTTPS.

Certificates

HTTPS certificates are divided into Domain Validation (DV) certificates, Organization Validation (OV) certificates, and Extended Validation (EV) certificates according to levels of certification.

- A DV certificate validates only the ownership of a domain, typically the content of a specified file in the domain, or validates each text (TXT) record for the domain . A safe lock icon is displayed in the address box for a domain after the domain is validated.
- An OV certificate is a standard SSL certificate that requires the validation of an organization's authenticity. OV is more secure and reliable than DV. Furthermore , OV features tighter validation and takes more time to complete validation. Due to these advantages, OV is typically used in sectors such as e-commerce, education, and gaming.
- An EV certificate is an SSL certificate of the highest level. It identifies the requesting entity by using a globally unique object identifier (OID) specified by the CA/Browser Forum and presents the full name of the requesting entity. EV is used mostly in sectors such as financial payment and online banking.

Scenarios

HTTPS is used in the following five scenarios:

- Enterprise application

  HTTPS protects confidential information such as customer relationship management (CRM) data and enterprise resource planning (ERP) data at the website of an enterprise from being hijacked or intercepted. If such data is hijacked or intercepted, the enterprise faces disastrous damages.
- Government website

  HTTPS protects authoritative, correct information at government websites against vulnerabilities such as phishing and hijacking. Leakage of such information may incur a public or trust crisis against the government.
- Payment system

  HTTPS protects sensitive data such as the customer name and phone number involved in a payment against hijacking and spoofing. If HTTPS is not used, the customer may receive details such as the name and address about the order they have placed and then may be tricked into making a duplicate payment, which incurs losses to both the customer and the enterprise.

- API

  HTTPS enables APIs to encrypt important information such as sensitive data and crucial operation instructions, so that the information will not be hijacked when it is being transmitted.

- Enterprise website

  HTTPS makes users feel more secure. When HTTPS is enabled, a safe lock icon is displayed in the address box for DV and OV. For EV, however, a safe lock icon is displayed in the address box, which is in green, with the enterprise name incorporated.

8.2 Certificate Format

Before Enabling the HTTPS service, you must configure certificates. You can directly select managed or purchased certificates in SSL Certificates , apply for free certificates, or manually upload custom certificates. Custom upload only supports certificates in `PEM` format. You must convert certificates and private keys from other formats to the PEM format.

Certificate format requirements

Certificate authorities (CAs) generally provide the following types of certificates. Among these, Alibaba Cloud CDN uses the Nginx format (certificates are .crt files and private keys are .key files):

- If certificates are issued by a root CA, you receive only one certificate.
- If you have obtained a certificate file consisting of multiple certificates from an intermediate CA, you must manually splice the server certificate and intermediate certificate before uploading them together.

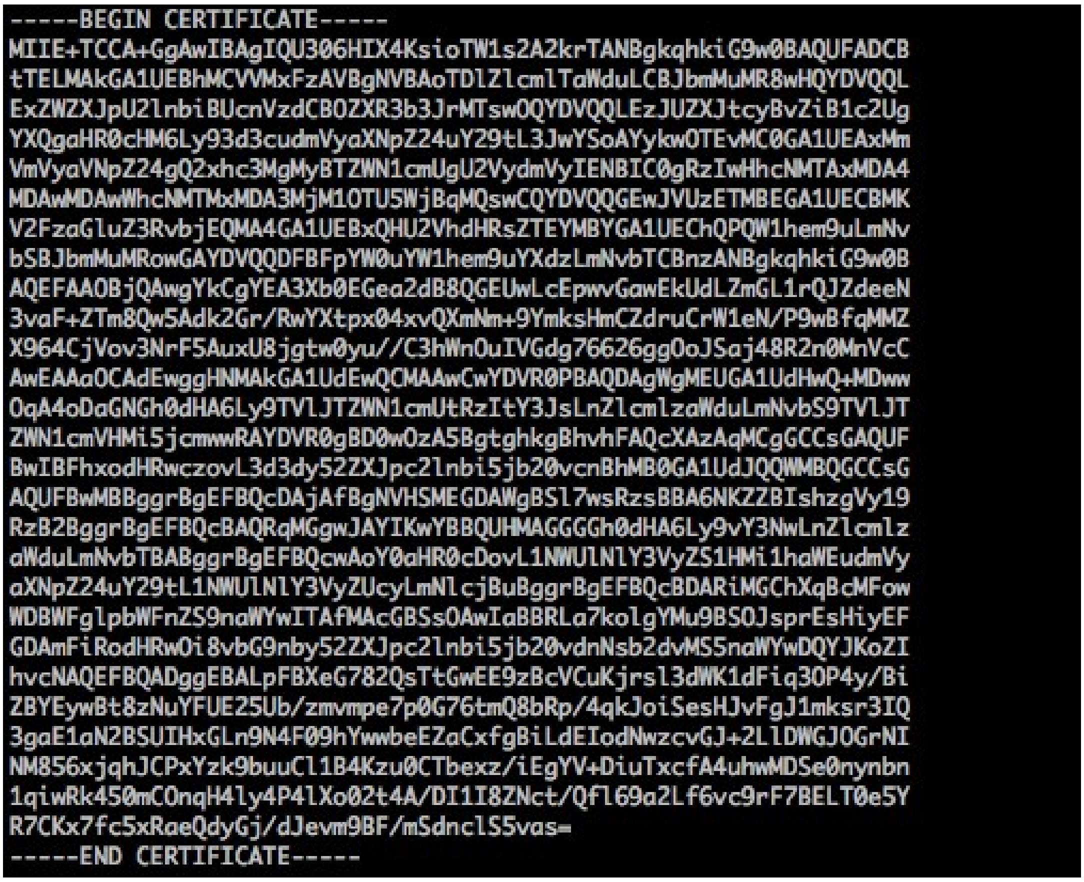
> Note:
> Splicing rules: The server certificate must be followed by the intermediate certificate without any blank line. Generally, the CA provides the relevant description when issuing a certificate. So pay attention to the rule description.

Example

Confirm the format is correct before uploading.

Certificates issued by a root CA

In Linux environments, certificates are in the `PEM` format:



```
-----BEGIN CERTIFICATE-----
MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBICOgRzIwHhcNMTAxMDA4
MDAwMDAwWhcNMTMxMDA3MjM1OTU5WjBqMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
V2FzaGluZ3RvbjEQMA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv
bSBJbmMuMRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWnOuIVGdg76626ggOoJSaj48R2n0MnVcC
AwEAAaOCAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVlJTZWN1cmUtRzItY3JsLnZlcmlzaWduLmNvbS9TVlJT
ZWN1cmVHMi5jcmwwRAYDVR0gBD0wOzA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUF
BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBSl7wsRzsBBA6NKZZBIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWUlNlY3VyZUcyLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFow
WDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEF
GDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq3OP4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2LlDWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

Certificate rules:

- Upload the `----- BEGIN   CERTIFICAT  E -----` and `----- END   CERTIFICAT  E -----` content together.
- Each line has 64 characters, but the last line can have less then 64 characters.

Certificate links issued by intermediate CAs:

`----- BEGIN   CERTIFICAT  E -----`

`----- END   CERTIFICAT  E -----`

`----- BEGIN   Certificat  e  -----`

`----- END   CERTIFICAT  E -----`

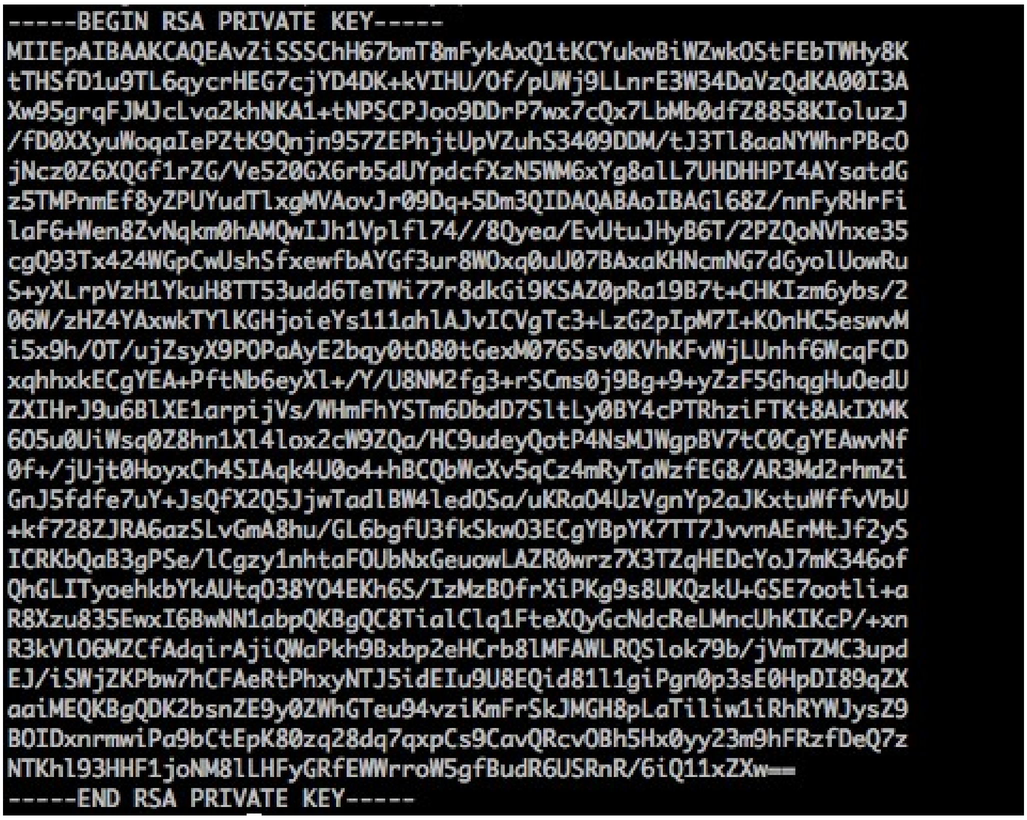
`----- BEGIN   CERTIFICAT  E -----`

`----- END   CERTIFICAT  E -----`

Certificate link rules:

- Do not insert a blank line between certificates.
- Each certificate must comply with the certificate rules.

RSA private key format requirements



```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAvZiSSSChH67bmT8mFykAxQ1tKCYukwBiWZwkOStFEbTWHy8K
tTHSfD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A
Xw95grqFJMJcLva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ
/fD0XXyuWoqaIePZtK9Qnjn957ZEPhjtUpVZuhS3409DDM/tJ3Tl8aaNYWhrPBcO
jNcz0Z6XQGf1rZG/Ve520GX6rb5dUYpdcfXzN5WM6xYg8alL7UHDHHPI4AYsatdG
z5TMPnmEf8yZPUYudTlxgMVAovJr09Dq+5Dm3QIDAQABAoIBAGl68Z/nnFyRHrFi
laF6+Wen8ZvNqkm0hAMQwIJh1Vplfl74//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35
cgQ93Tx424WGpCwUshSfxewfbAYGf3ur8WOxq0uU07BAxaKHNcmNG7dGyolUowRu
S+yXLrpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2
06W/zHZ4YAxwkTYlKGHjoieYs111ahlAJvICVgTc3+LzG2pIpM7I+KOnHC5eswvM
i5x9h/OT/ujZsyX9POPaAyE2bqy0tO80tGexM076Ssv0KVhKFvWjLUnhf6WcqFCD
xqhhxkECgYEA+PftNb6eyXl+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhqgHuOedU
ZXIHrJ9u6BlXE1arpijVs/WHmFhYSTm6DbdD7SltLy0BY4cPTRhziFTKt8AkIXMK
6O5u0UiWsq0Z8hn1Xl4lox2cW9ZQa/HC9udeyQotP4NsMJWgpBV7tC0CgYEAwvNf
0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzfEG8/AR3Md2rhmZi
GnJ5fdfe7uY+JsQfX2Q5JjwTadlBW4ledOSa/uKRaO4UzVgnYp2aJKxtuWffvVbU
+kf728ZJRA6azSLvGmA8hu/GL6bgfU3fkSkwO3ECgYBpYK7TT7JvvnAErMtJf2yS
ICRKbQaB3gPSe/lCgzy1nhtaFOUbNxGeuowLAZR0wrz7X3TZqHEDcYoJ7mK346of
QhGLITyoehkbYkAUtqO38YO4EKh6S/IzMzBOfrXiPKg9s8UKQzkU+GSE7ootli+a
R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUhKIKcP/+xn
R3kVlO6MZCfAdqirAjiQWaPkh9Bxbp2eHCrb8lMFAWLRQSlok79b/jVmTZMC3upd
EJ/iSWjZKPbw7hCFAeRtPhxyNTJ5idEIu9U8EQid81l1giPgn0p3sE0HpDI89qZX
aaiMEQKBgQDK2bsnZE9y0ZWhGTeu94vziKmFrSkJMGH8pLaTiliw1iRhRYWJysZ9
BOIDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcvOBh5Hx0yy23m9hFRzfDeQ7z
NTKhl93HHF1joNM8lLHFyGRfEWWrroW5gfBudR6USRnR/6iQ11xZXw==
-----END RSA PRIVATE KEY-----
```

RSA private key rules:

- Run the `openssl genrsa - out privateKey . pem 2048` command to generate a local private key, with `privateKey . pem` being the private key file.
- `----- BEGIN RSA PRIVATE KEY -----` and ----- `END RSA PRIVATE KEY -----` indicate the beginning and end of the private key file, respectively. Upload the beginning and end content together.
- Each line has 64 characters, but the last line can have less than 64 characters.

If your private key is not generated in the format ----- `BEGIN PRIVATE KEY -----`,

```
—– END PRIVATE
```

```
        KEY -----
```

based on the preceding rules, run the following command to convert the private key:

```
openssl  rsa  - in  old_server  _key . pem  - out  new_server
_key . pem
```

Then, upload `new_server  _key . pem` content together with the certificate.

Certificate format conversion method

CDN HTTPS Secure Acceleration only supports certificates in the PEM format. Certificates in other formats must be converted to the PEM format. We recommend using the OpenSSL tool for conversion. The following shows the methods used to convert other common certificate formats to PEM.

DER to PEM

The DER format is generally used on Java platforms.

- Certificate conversion:

  ```
  openssl  x509  - inform  der  - in  certificat  e . cer  - out
  certificat  e . pem
  ```
- Private key conversion:

  ```
  openssl  rsa  - inform  DER  - outform  pem  - in  privatekey .
  der  - out  privatekey . pem
  ```

P7B to PEM

The P7B format is generally used in Windows Server and Tomcat.

- Certificate conversion:

  ```
  openssl  pkcs7  - print_cert  s  - in  incertific  at . p7b  -
  out  outcertifi  cate . cer
  ```

  In `outcertifi  cat . cer`, Retrieve the `----- BEGIN  CERTIFICAT  E -----`, -----END CERTIFICATE----- `content  and  upload  the  content  as  a  certificat  e`.
- Private key conversion: P7B certificates do not have private keys, so you only have to enter the certificate portion, not the private key portion, in the CDN console.

PFX to PEM

The PFX format is generally used in Windows Server.

- Certificate conversion:

  ```
  openssl  pkcs12 - in  certname . pfx - nokeys - out  cert .
  pem
  ```

- Private key conversion:

  ```
  openssl  pkcs12 - in  certname . pfx - nocerts - out  key .
  pem  - nodes
  ```

Free certificates

The free certificate here is Alibaba Cloud CDN Digicert DV version SSL Free certificate, only available for Alibaba Cloud CDN service. It cannot be managed in the SSL Certificates service of Alibaba Cloud Security. This certificate is only used to enable HTTPS Secure Acceleration in CDN, and you cannot obtain its public and private keys for other use.

- The application process for a free certificate takes 5-10 minutes. While waiting, you can also go back and choose to upload a custom certificate or select a managed certificate.
- You can always switch among custom, managed or free certificate no matter which one you enable at the beginning.
- Free certificates are valid for one year and automatically renewed upon expiration.
- When using this product, if you disable the HTTPS settings and then enable the free certificate option again, the system uses the free certificate you applied for previously, provided it has not expired. If your certificate has expired when you enable the free certificate option, the system reapplies for a free certificate.

Other certificate issues

- You can disable, enable, and modify certificates. After you disable a certificate, the system no longer retains the certificate information. When you re-enable the certificate, you must upload the certificate and private key again. See HTTPS Secure Acceleration settings tutorial.
- Only SSL/TLS "handshakes" with SNI information are supported.
- Ensure that the certificate and private key you upload match.
- Certificate updates take effect in 10 minutes.
- Private keys with passwords are not supported.

8.3 HTTPS Secure Acceleration

Introduction

HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) is an HTTP channel designed to ensure security. It encapsulates HTTP with the SSL/TLS protocol, so the foundation of HTTPS security is SSL/TLS protocol.

HTTPS Acceleration Advantages:

- Encrypt important information during transmission, avoiding attack-caused information leaking, such as session ID or cookies.
- Perform the data integrity during transmission, preventing man-in-the-middle attack (MITM), such as DNS or contents being hijacked by third party.

Alibaba Cloud CDN provides HTTPS Secure acceleration. When you have uploaded certificate and secret keys after enabling HTTPS, so that you can check, disable, enable and edit the certificate.

How it works

The HTTPS Secure Acceleration encrypts your request to Alibaba Cloud CDN nodes. And the CDN nodes still follow your origin site's configuration to access resources in the origin site. We recommend you configure and enable HTTPS on your origin site, encrypting your full-link HTTPS acceleration.

Here is the HTTPS encryption process:

1. You start an HTTPS request.
2. The server generates a public key and a secret key (self-made or apply from professional organization).
3. The server sends the public certificate to your side.
4. You side verify the certificate.
   - If the certificate is correct, a random number (private key) is generated and encrypted with the public key, and transferred to the server.
   - If the certificate is incorrect, the SSL handshake fails.

Note:

The certificate verification includes: the certificate being within the period of validity, the reliability of certificate's CA, the certificate's public key being able to encrypt the number signature of the server's issuer, and the domain name on the server's certificate being matched with its real domain name.

5. The server uses the previous secret key to decrypt and get the random number (private key).
6. The server encrypt the transmitted data by using the private key.
7. You side decrypt the encrypted server date by using private key, and eventually get the data.

Notes

About configuration

- HTTPS secure acceleration is available in the following service types: Image and Small File, Download, Video, and Live Streaming Media.
- HTTPS acceleration for wildcard domain names is available.
- You can Enable or Disable HTTPS acceleration:
  - Enable: you can modify the certificate. The system is compatible with all your HTTP and HTTPS requests by default. You can also customize Forcible redirect for original request method.
  - Disable: the system will neither support HTTPS request nor save the certificate or secret key's information. You need to re-upload the certificate or secret key when you reopen the certificate.
- You can check the certificate, but cannot check the secret key due to its importance . Make sure that you have taken care of certificate information.
- Update your certificate with caution. The update will take effect in 1 minute.

About billing

HTTPS Secure Acceleration is a value-added service, so that you need to pay for the HTTPS requests. For more information, see HTTPS pricing.

Note:
You need to pay for HTTTPS requests separately. Make sure that your account balance is sufficient , otherwise it may affect your CDN service.

About certificate

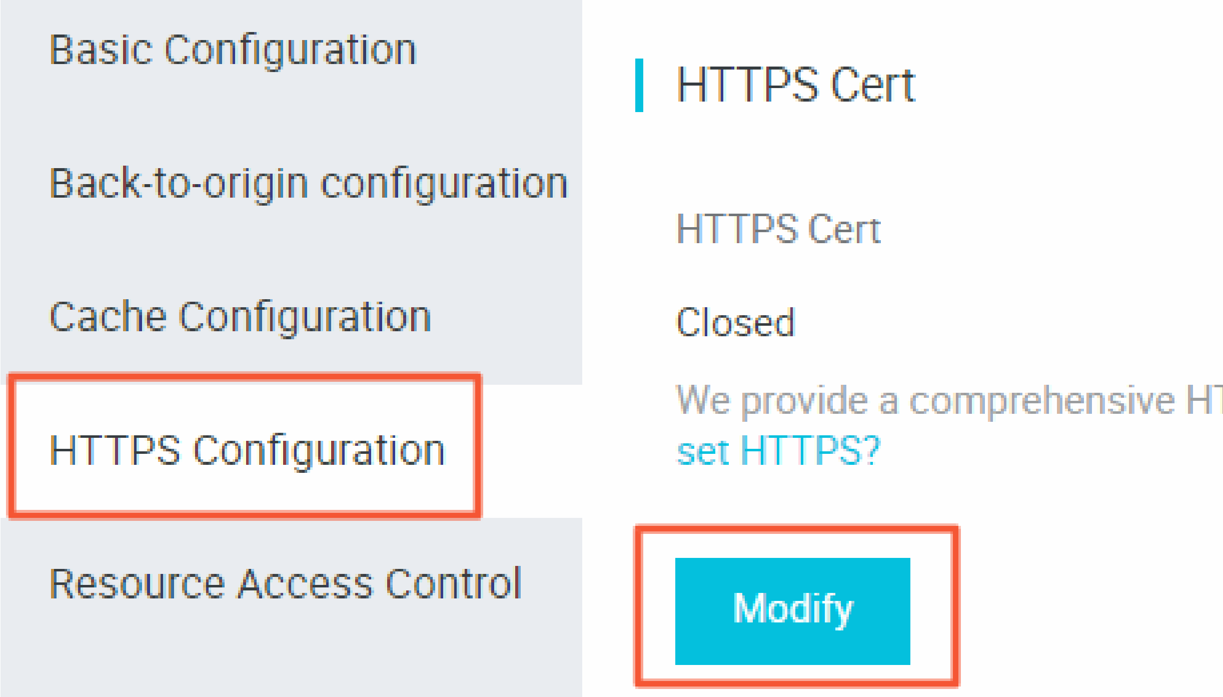
- To enable acceleration domain name with the HTTPS Secure Acceleration feature, you need to upload the certificate and secret key in the `PEM` format.

> Note:
> As Alibaba Cloud CDN only adopts Nginx-based Tengine service, only the certificate in `PEM` format is available. For more information, see Certificate Format.

- Only SSL/TLS handshake with SNI information is available.
- The certificate you upload should be matched with your secret key, otherwise your verification may fail.
- Secret key with a password is unavailable.

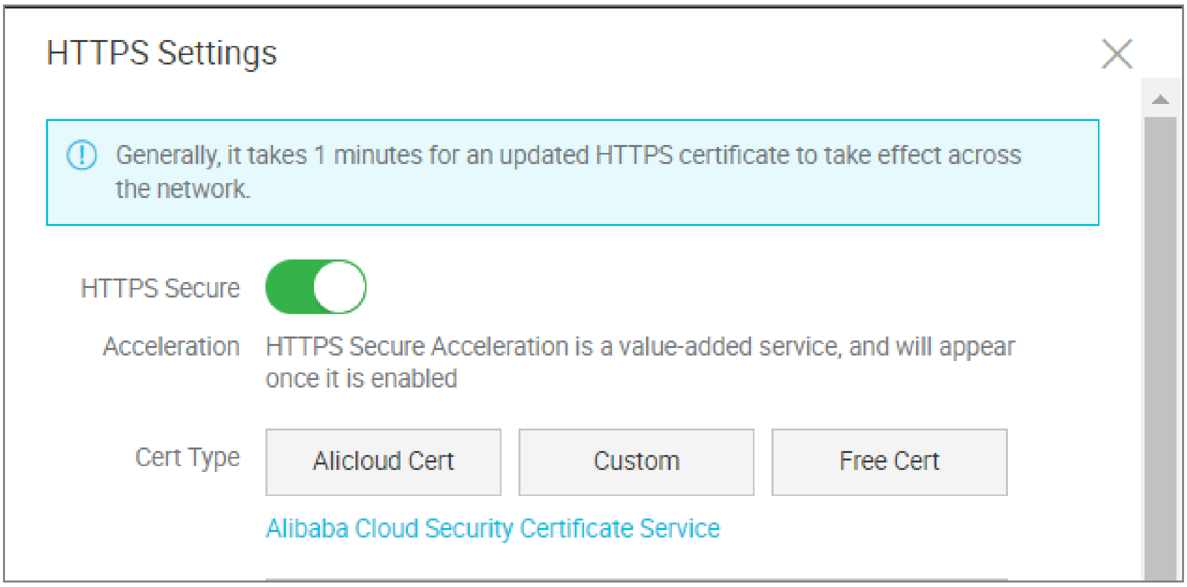
Procedure

1. Purchase a certificate. Only when you own the certificate that is matched with your domain name can you enable HTTPS Secure Acceleration. You can easily purchase Alibaba Cloud Certificate in the SSL Certificate console, or apply for free certificate.
2. Log on to the CDN console, and enter the Domain Names page. Select the domain name, and click Manage.
3. In HTTPS Configurations > HTTPS Cert, click Modify.



4. In the HTTPS Settings dialogue, enable HTTPS Secure.

5. Select your certificate type. You can choose Alibaba Cloud, Custom or Free Cert. Currently, only the `PEM` format is available.



HTTPS Settings

Generally, it takes 1 minutes for an updated HTTPS certificate to take effect across the network.

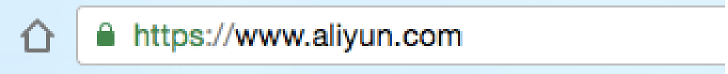
HTTPS Secure Acceleration: HTTPS Secure Acceleration is a value-added service, and will appear once it is enabled

Cert Type: Alicloud Cert | Custom | Free Cert

Alibaba Cloud Security Certificate Service

- You can choose the Alibaba Cloud Certificate. If you have no matched certificate in your list, choose custom certificate. You need to upload the certificate contents and secret key after setting the certificate name. This certificate will be saved in your Alibaba Cloud Security. You can check in My Certificate.
- You can also choose free certificate, namely, Alibaba Cloud CDN Digicert DV version SSL Free certificate. This free certificate is only available for Alibaba Cloud CDN service, and it can't be managed in the SSL Certificates service of Alibaba Cloud Security. This certificate is only used to enable HTTPS Secure Acceleration in CDN, and you cannot obtain its public and private keys for other use. After you choose to use the Free Cert type, it takes about 10 minutes for the certificate to be effective.

6. Verify whether the certificate is effective. You can access resources by using HTTPS after the certificate becomes effective (about 1 hour). Green HTTPS mark indicates that you have established private connection with the website, and HTTPS secure acceleration has comes into effect.



https://www.aliyun.com

Note:

About replacing your certificate:

- If you want to change your certificate to free certificate or Alibaba Cloud certificate, re-choose the target certificate (Free Cert or Alibaba Cloud Cert) in the HTTPS Settings page.
- If you want to change your certificate to custom certificate, choose Custom in the HTTPS Settings page. Enter the target certificate name and contents to the box of the window, then deliver it.

8.4 HTTP/2

Introduction

HTTP/2, the latest HTTP protocol published in 2015, is now available in many browsers, such as Chrome, IE11, Safari, and Firefox. With main features similar to SPDY, HTTP/2 can be seen as an advanced edition of HTTP/1.1.

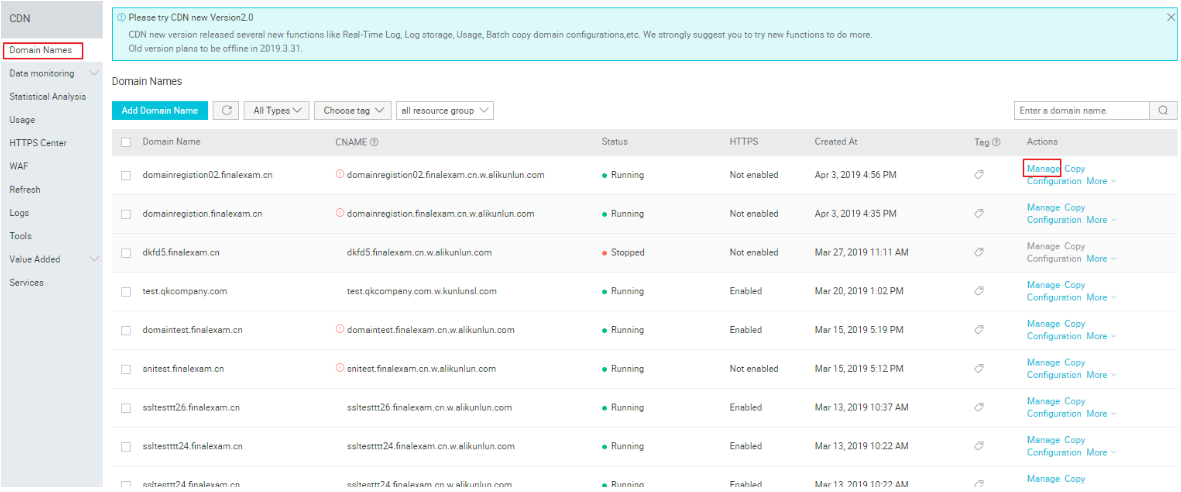
HTTP/2 Benefits

- Binary protocol: Compared with HTTP 1. x, HTTP/2 segments transferring information into smaller frames and messages and encodes them by using binary, which makes the protocol more scalable. For example, data and command can be transferred by frame.
- Content security: Based on HTTPS, HTTP/2 gives considerations to both security and performance.
- Multiplexing: With HTTP/2, your browser can trigger multiple requests in one connection, and receive these requests in any order or at the same time. Moreover , stream dependencies is also available in multiplexing, allowing client servers to define which contents to be transferred in priority.
- Header compression: HTTP/2 compresses and transfers message headers in the HPACK format and creates an index table for the headers. Only the index are transferred, which improves the transferring efficiency and speed.
- Server push: Similar to SPDY, HTTP/2 allows servers to actively push contents to clients without a request, significantly improving web page loading speeds.

Procedure

1. Log on to the CDN console.

2. In the left-side navigation pane, choose Domain Names. In the main workspace, select a domain, and in the Actions column click Manage



Please try CDN new Version2.0

CDN new version released several new functions like Real-Time Log, Log storage, Usage, Batch copy domain configurations,etc. We strongly suggest you to try new functions to do more.
Old version plans to be offline in 2019.3.31.

Domain Names

□	Domain Name	CNAME	Status	HTTPS	Created At	Tag	Actions
□	domainregistion02.finalexam.cn	domainregistion02.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 3, 2019 4:56 PM		Manage Copy Configuration More
□	domainregistion.finalexam.cn	domainregistion.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 3, 2019 4:35 PM		Manage Copy Configuration More
□	dkfd5.finalexam.cn	dkfd5.finalexam.cn.w.alikunlun.com	● Stopped	Not enabled	Mar 27, 2019 11:11 AM		Manage Copy Configuration More
□	test.qkcompany.com	test.qkcompany.com.w.kunlunsl.com	● Running	Enabled	Mar 20, 2019 1:02 PM		Manage Copy Configuration More
□	domaintest.finalexam.cn	domaintest.finalexam.cn.w.alikunlun.com	● Running	Enabled	Mar 15, 2019 5:19 PM		Manage Copy Configuration More
□	snitest.finalexam.cn	snitest.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Mar 15, 2019 5:12 PM		Manage Copy Configuration More
□	ssltesttt26.finalexam.cn	ssltesttt26.finalexam.cn.w.alikunlun.com	● Running	Enabled	Mar 13, 2019 10:37 AM		Manage Copy Configuration More
□	ssltestttt24.finalexam.cn	ssltestttt24.finalexam.cn.w.alikunlun.com	● Running	Enabled	Mar 13, 2019 10:22 AM		Manage Copy Configuration More
□	ssltesttt24.finalexam.cn	ssltesttt24.finalexam.cn.w.alikunlun.com	● Running	Enabled	Mar 13, 2019 10:22 AM		Manage Copy

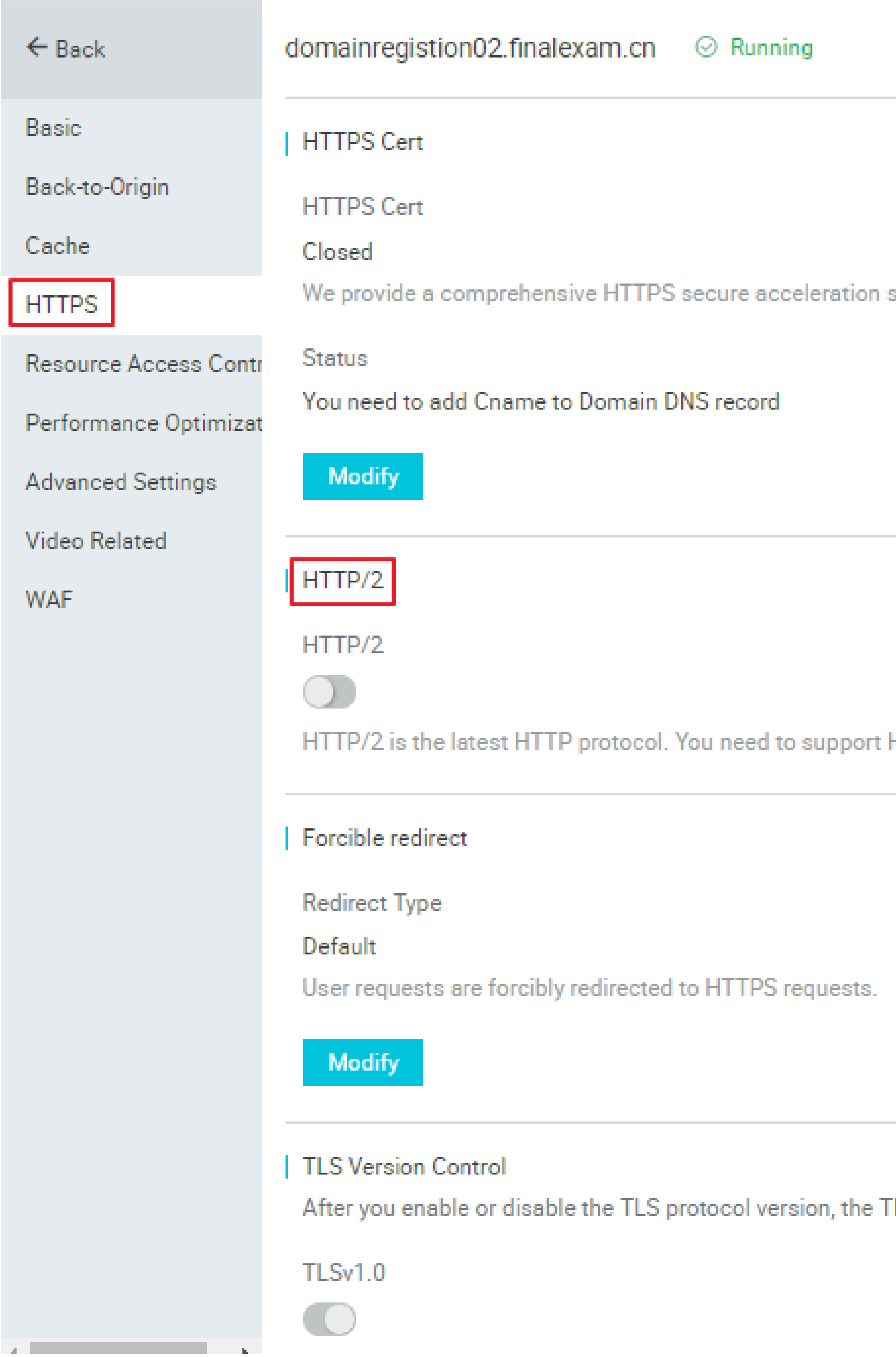
.

Note:

Make sure that you have configured HTTPS certificates before enabling HTTP/2.

- If it is your first time configuring HTTPS certificate, wait for a while until your configuration coming into effect.
- If you disable HTTPS certificates when your HTTP/2 service is running, your HTTP/2 service will be disabled automatically.

3. In the left-side pane, choose HTTPS. In the main workspace, enable HTTP/2.



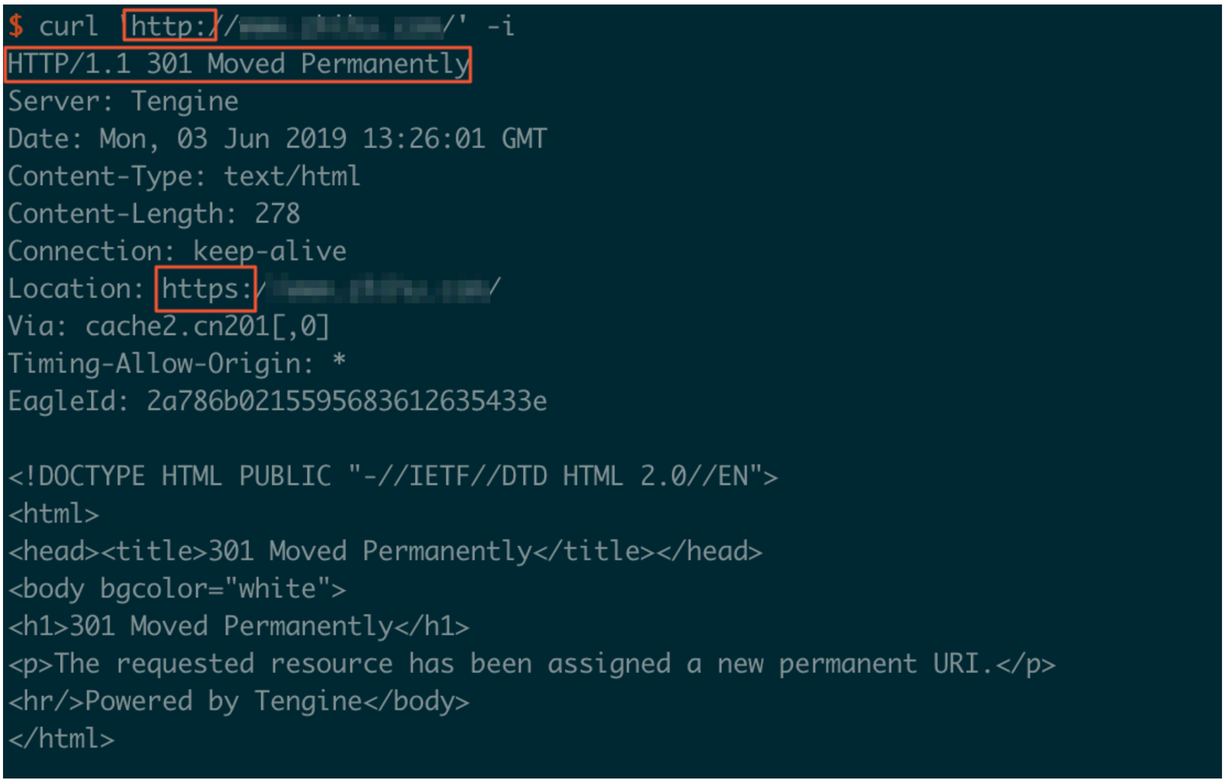
← Back
Basic
Back-to-Origin
Cache
HTTPS
Resource Access Contr
Performance Optimizat
Advanced Settings
Video Related
WAF
domainregistion02.finalexam.cn
Running
HTTPS Cert
HTTPS Cert
Closed
We provide a comprehensive HTTPS secure acceleration s
Status
You need to add Cname to Domain DNS record
Modify
HTTP/2
HTTP/2
HTTP/2 is the latest HTTP protocol. You need to support H
Forcible redirect
Redirect Type
Default
User requests are forcibly redirected to HTTPS requests.
Modify
TLS Version Control
After you enable or disable the TLS protocol version, the TL
TLSv1.0

8.5 Force Redirect

Introduction

When HTTPS Secure Acceleration is enabled for a CDN domain, it supports custom settings to perform force redirects on users' original request methods.

For example, when force HTTPS redirect is enabled and a user initiates an HTTP request, the server returns a 301 redirect response and the original HTTP request is forcibly redirected to an HTTPS request, as shown in the following figure.



```
$ curl 'http://[redacted]/' -i
HTTP/1.1 301 Moved Permanently
Server: Tengine
Date: Mon, 03 Jun 2019 13:26:01 GMT
Content-Type: text/html
Content-Length: 278
Connection: keep-alive
Location: https://[redacted]/
Via: cache2.cn201[,0]
Timing-Allow-Origin: *
EagleId: 2a786b0215595683612635433e

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<h1>301 Moved Permanently</h1>
<p>The requested resource has been assigned a new permanent URI.</p>
<hr/>Powered by Tengine</body>
</html>
```

Force Redirect is disabled by default. When you enable the feature, both HTTP and HTTPS requests are enabled simultaneously by default.

Options: Default, Force HTTPS redirect, and Force HTTP Redirect.

- Force HTTPS redirect: User requests are forcibly redirected to HTTPS requests.
- Force HTTP redirect: User requests are forcibly redirected to HTTP requests.

Procedure

1. Go to Domain Namespage, select the domain name, then click Manage.
2. Enable the function in HTTPS Configuration > Forcible redirect .

8.6 TLS

This document describes the features of Transport Layer Security (TLS) and how to use TLS.

Features

TLS is a cryptographic protocol designed to ensure communication security and data integrity of a computer network. HTTP Strict Transport Security (HSTS) is a typical application of TLS. HTTPS, also known as HTTP over TLS, is a secure version of HTTP . HTTPS runs under the top application layer HTTP and above the transport layer TCP . HTTPS encrypts and decrypts user page requests.

TLS has four versions:

- TLS Version 1.0: TLS Version 1.0 was published as RFC 2246 in 1999 based on SSL Version 3.0. This version is vulnerable to various attacks, such as BEAST attacks and POODLE attacks. RFC 2246 provides weak encryption that is not strong enough to protect the current network connection. TLS Version 1.0 is not compliant with Payment Card Industry Data Security Standard (PCI DSS). Supported browsers include IE 6.0 or later, Chrome 1.0 or later, and Firefox 2.0 or later.
- TLS Version 1.1: TLS Version 1.1 was published as RFC 4346 in 2006. This version fixed some vulnerabilities of TLS Version 1.0. Supported browsers include IE 11.0 or later, Chrome 22.0 later, Firefox 24.0 or later, and Safari 7.0 or later.
- TLS Version 1.2: TLS Version 1.2 was published as RFC 5246 in 2008. This is currently the most widely used version. Supported browsers include IE 11.0 or later, Chrome 30.0 or later, Firefox 27.0 or later, and Safari 7.0 or later.
- TLS Version 1.3: TLS Version 1.3 was published as RFC 8446 in 2018. As the latest TLS version, RFC 8446 is faster because it supports the 0-RTT mode. Also, this version is more secure as it only supports perfect forward secrecy key exchange algorithms. Supported browsers include Chrome 70.0 or later and Firefox 63.0 or later.

Note:

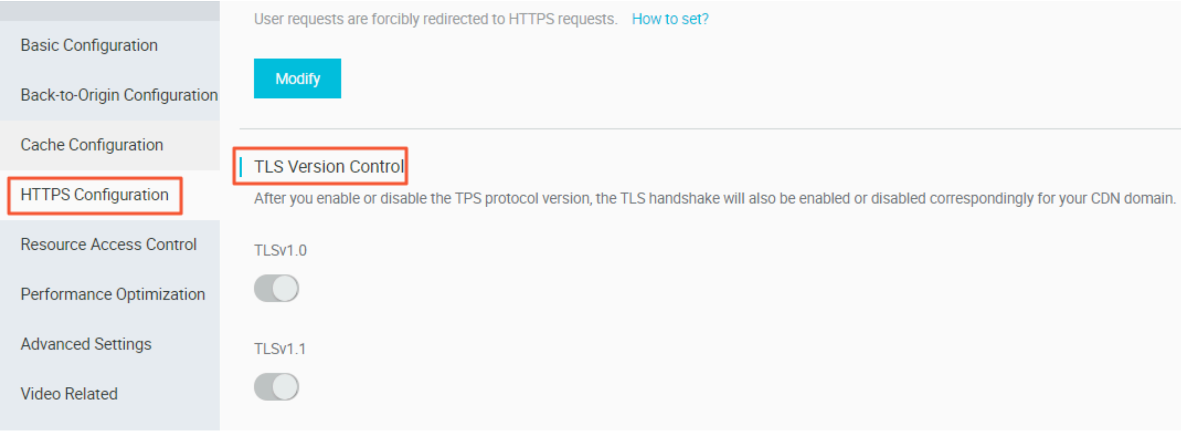
Currently, TLS Version 1.0, TLS Version 1.1, and TLS Version 1.2 are enabled by default.

Procedure

Note:

You must configure the HTTPS certificate and then enable TLS.

1. Log on to the CDN console.
2. In the left-side navigation pane, click Domain Names.
3. Select a domain name to be configured, and click Manage.
4. In the left-side navigation pane, click HTTPS Configuration.



User requests are forcibly redirected to HTTPS requests.

TLS Version Control

After you enable or disable the TPS protocol version, the TLS handshake will also be enabled or disabled correspondingly for your CDN domain.

TLSv1.0

TLSv1.1

5. In TLS Version Control, you can enable or disable a specific TLS version based on your needs.

8.7 HSTS

This document describes the technical details and scenarios of HTTP Strict Transport Security (HSTS), and how to operate HSTS in the Alibaba Cloud console.

Features

HSTS is specified in RFC 6797. HSTS instructs clients, such as a browser, that a domain can only be accessed by using HTTPS.

Scenarios

After you have enabled HTTPS on the entire website, redirect your users and search engines to the HTTPS page with 301 or 302 HTTP redirects. If you enter an HTTP URL in a Web browser or click an HTTP URL in another location, the server will redirect the HTTP request to HTTPS. When redirecting the requests to HTTPS, a man-in-the-middle (MITM) can still hijack the connection before the redirect. As a result, the requests cannot be sent to the specified server. To address this issue, you can set the HTTP HSTS header to standardize all client connections on HTTPS.

HSTS is a response header: Strict-Transport-Security: max-age=expireTime [; includeSubDomains] [; preload]. The parameters are described as follows:

- max-age is expressed in seconds.
- Strict-Transport-Security: HSTS is a Web security mechanism that restricts browsers to access Web servers over HTTPS for only a given amount of time. If a website accepts a connection through HTTP and the amount of time specified for the Strict-Transport-Security mechanism is not passed, the browser starts a 307 internal redirect from HTTP to HTTPS. This helps to avoid hijacks occurred in the 301 and 302 redirects.
- includeSubDomains is optional. If this parameter is specified, this rule applies to all subdomains of the site as well.
- preload is optional. The site owner can submit a website to the preload list.

Note:

- Before HSTS takes effect, you still need to use the 301 or 302 redirect for the first redirect.
- The HSTS response header is valid in response to the HTTPS requests and invalid in response to HTTP requests.
- The HSTS response header is only valid to the 443 port.
- The HSTS response header is valid to domain names and invalid to IP addresses.
- After enabling HSTS, if the website certificate is incorrect, the certificate may need more time to process.

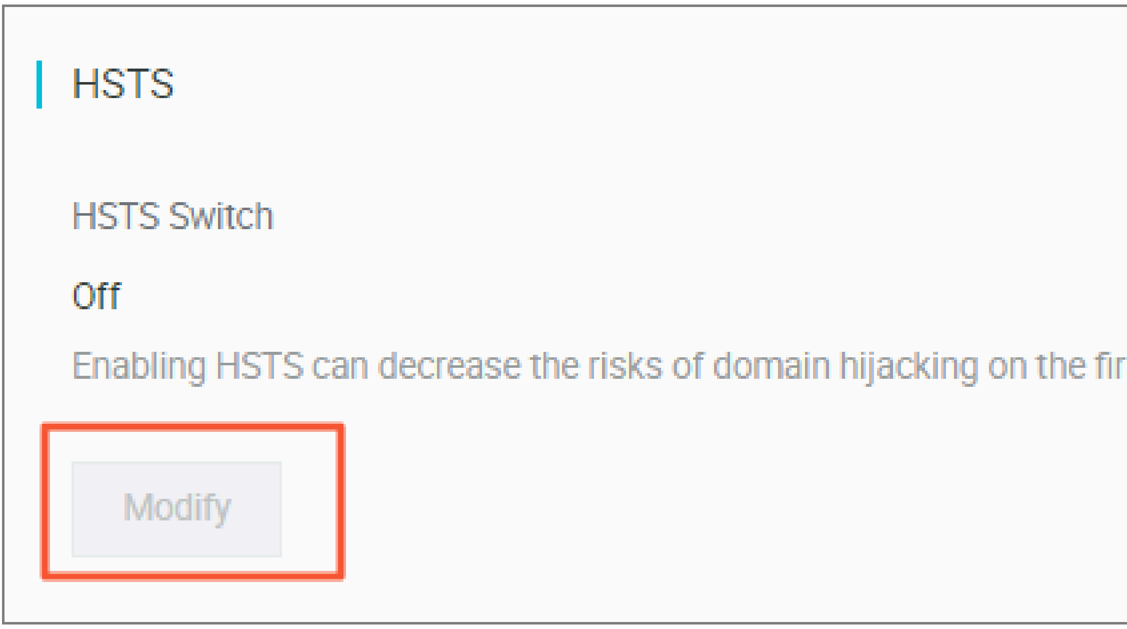
Procedure

Note:

Configure the HTTPS certificate and then enable the TLS feature.

1. Log on to the CDN console.
2. In the left-side navigation pane, clickDomain Names.
3. Select a domain name, and click Mange.

4. In the left-side navigation pane, click HTTPS Configuration.



HSTS

HSTS Switch

Off

Enabling HSTS can decrease the risks of domain hijacking on the fir

5. In HTST, click Modify. to complete the configuration.

9 Access Control Settings

9.1 Anti-leech

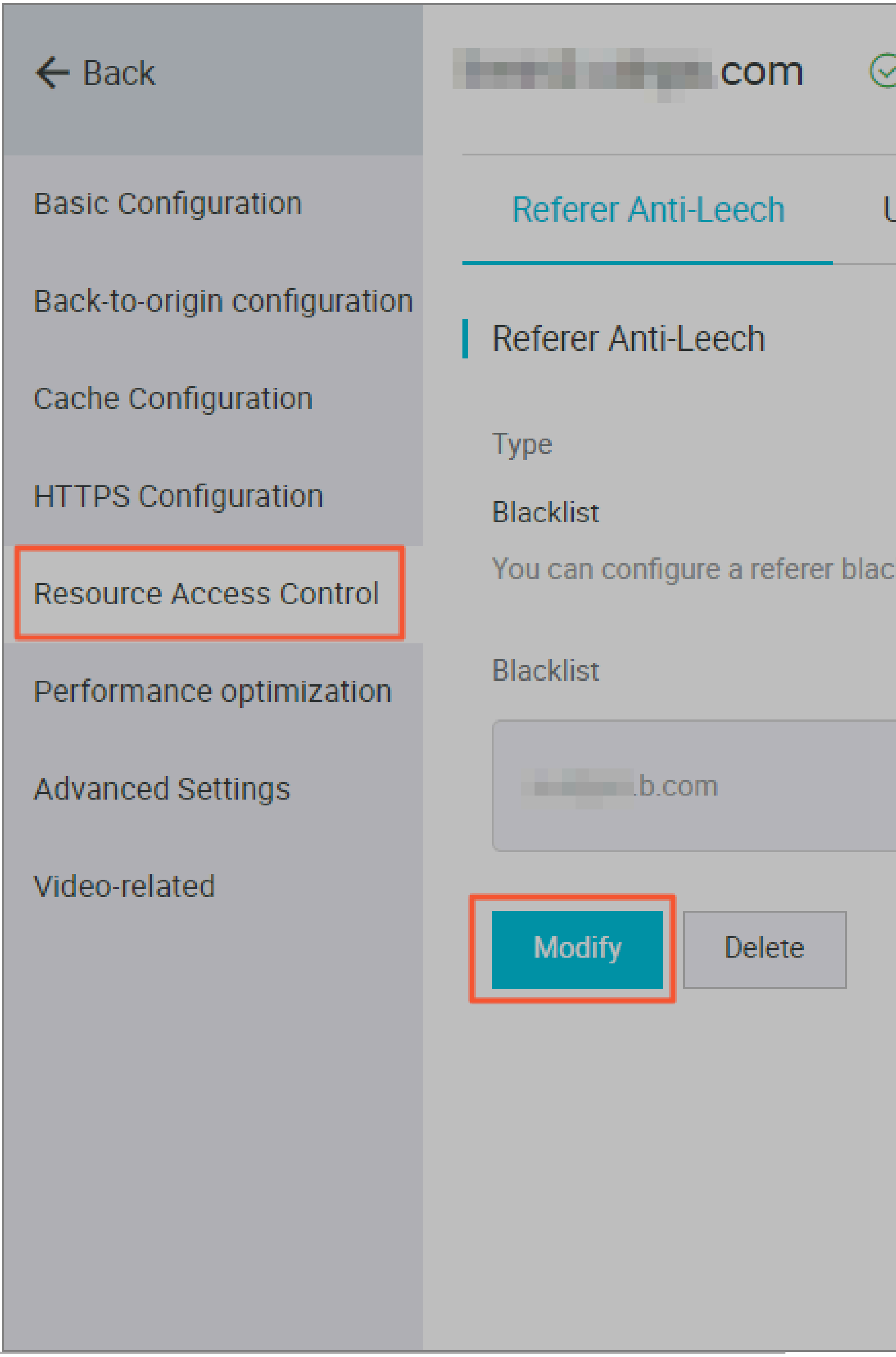
Introduction

- 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 whitelist to identify and filter visitors in order to limit access to your CDN resources.
- Currently, the anti-leech function supports the black list or whitelist 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 configuration of the anti-leech black list or whitelist.
    - 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.

Procedure

1. Go to Domain Namespage, select the domain name, then click Manage.

2. On Resource Access Control > Anti-leech, click Modify.



3. ChooseBlacklist or Whitelist, and add the IP network segment in the box below.
4. Click Confirm.

Notes

- This function is optional and is disabled by default.
- You can only select one of Refer Blacklist or Refer Whitelist to edit at the same time .
- After configuration, wildcard domain name support is added automatically. For example, if you enter `a.com`, all sub-domain names under `*.a.com` take effect.
- You can set a null Referer field to access resources on a CDN node (that is, allowing to access the resource URL by typing the address in browser).

9.2 Business type

9.2.1 Authentication configuration

The URL authentication feature is designed to protect user's origin server resources from unauthorized downloading and misappropriation. Referer blacklist and whitelist with anti-leech can protect video content from some leeching attacks too some degree. However, it cannot completely protect site resources, as the referer contents can be forged. As a result, it is a more secure and effective way to protect your resources by using URL authentication.

How it works

URL authentication uses Alibaba Cloud CDN nodes together with client resource sites to provide more secure and reliable anti-leech protection for origin site resources.

1. The CDN client site provides an encrypted URL including verification information of permissions.
2. You use the encrypted URL to initiate a request to the CDN node.
3. The accelerated node authenticates the permission information in the encrypted URL to determine the legitimacy of the request. A normal response to a legitimate request will reject an illegal request.

Authentication method

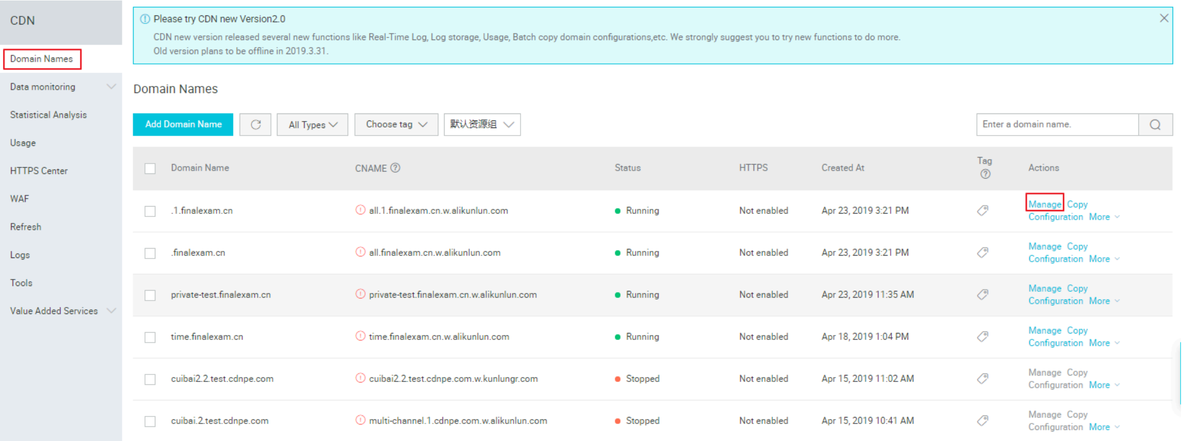
Alibaba Cloud CDN supports 3 authentication methods: A, B, and C. You can choose the authentication method based on your business need, so that it will help protect your origin site.

Sample authentication code

You can check Sample authentication code.

Procedure

1. Log on to the CDN console.
2. In the left-side navigation pane, choose Domain Names. In the main workspace, select a domain, and in the Actions column click Manage.



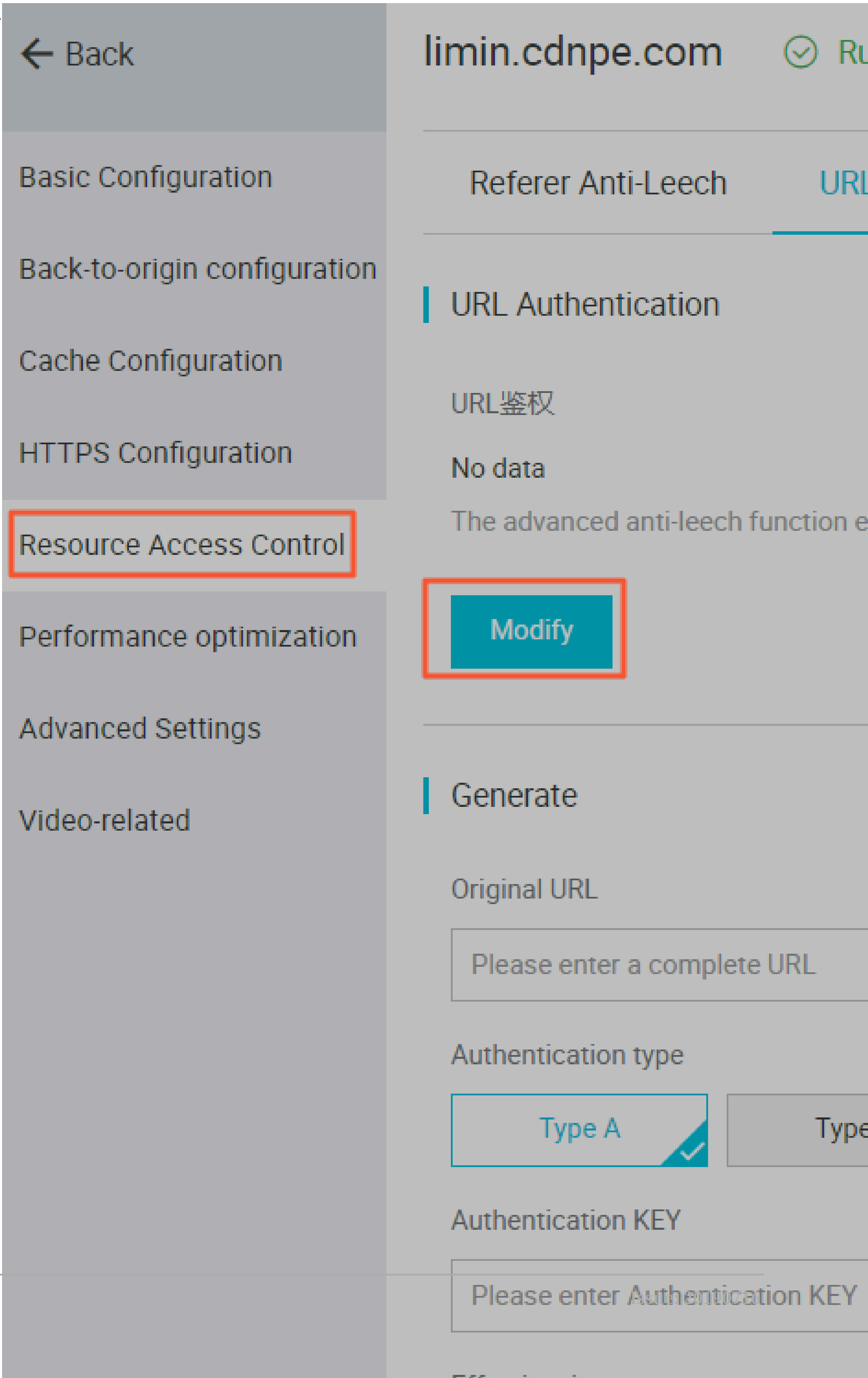
Please try CDN new Version2.0

CDN new version released several new functions like Real-Time Log, Log storage, Usage, Batch copy domain configurations,etc. We strongly suggest you to try new functions to do more.
Old version plans to be offline in 2019.3.31.

□	Domain Name	CNAME	Status	HTTPS	Created At	Tag	Actions
□	.1.finalexam.cn	all.1.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
□	.finalexam.cn	all.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
□	private-test.finalexam.cn	private-test.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 11:35 AM		Manage Copy Configuration More
□	time.finalexam.cn	time.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 18, 2019 1:04 PM		Manage Copy Configuration More
□	cuibai2.2.test.cdnpe.com	cuibai2.2.test.cdnpe.com.w.kunlungr.com	● Stopped	Not enabled	Apr 15, 2019 11:02 AM		Manage Copy Configuration More
□	cuibai.2.test.cdnpe.com	multi-channel.1.cdnpe.com.w.alikunlun.com	● Stopped	Not enabled	Apr 15, 2019 10:41 AM		Manage Copy Configuration More

3. On the page that is displayed, choose Resource Access Control from the left-side navigation pane, and then click Modify in

the URL Authentication area on the URL authentication tab page.



4. In the Authentication URL dialog box, switch on Authentication URL, select an Authentication type, and enter Master Key and Backup Key.
5. Click Confirm.

9.2.2 Authentication method A

How it works

Formats of the encrypted URL for user access

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

Authentication fields

- You can set the `PrivateKey` field.
- The validity period 1,800 seconds indicates that the authentication fails when the user fails to access the client source server 1,800 seconds after the preset access time. For example, if the user sets the access expiration time to 2020-08-15 15:00:00, the link actually fails at 2020-08-15 15:30:00.

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. Effective time is 1,800 seconds.
rand	random number, we recommend that you use UUID (not including hyphen “-” , for example, 477b3bbc253f467b8def6711128c7bec format)
uid	Not used yet (set to 0).

Field	Description
md5hash	Verification string calculated by the MD5 algorithm , which is a combination of numbers 0 to 9 and lowercase English letters a to z, with a fixed length of 32 characters

When the CDN server receives a request, it first determines whether the `timestamp` in the request is earlier than the current time.

- If the `Timestamp` is earlier than the current time, the URL is regarded as expired, and the CDN server returns an HTTP 403 error.
- If the `timestamp` is later than the current time, the CDN server constructs an equivalent string (see the construction of the sstring field described later). Use the MD5 algorithm to calculate `HashValue`, and compare it with `md5hash` . If they are consistent, the request passes the authentication and the requested file is returned. Otherwise, the request fails the authentication, and an HTTP 403 error is returned.

- The ` `HashValue` ` is calculated based on the following string:

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

An instance of authorization

1. Request object by `req_auth` :

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

2. Set key to: aliyuncdnexp1234 (you can configure yourself)
3. The expiration date of the authentication configuration file is October 10, 2015 00:00:00. The calculated number of seconds is 1,444,435,200.

4. The CDN server constructs a signature string for the calculation of HashValue:

```
/ video / standard / 1K . html - 1444435200 - 0 - 0 - aliyuncdne
 xp1234 "
```

5. Depending on the signature string, the CDN server evaluates hashvalue:

```
HashValue  =  md5sum ("/ video / standard / 1K . html - 1444435200
- 0 - 0 - aliyuncdne  xp1234 ") =  80cd3862d6  99b7118eed
99103f2a3a  4f
```

6. When requested, the URL is:

```
http :// cdn . example . com / video / standard / 1K . html ?
auth_key = 1444435200 - 0 - 0 - 80cd3862d6  99b7118eed  99103f2a3a
4f
```

If the calculated HashValue matches the value of md5hash = 80cd3862d6 99b7118eed99103f2a3a4f that is carried in the user request, authentication succeeds.

9.2.3 Authentication method B

Principles

Formats of the encrypted URL for user access

* 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 fields

- Note: `PrivateKey` is set by CDN clients.
- * Validity period of 1,800 seconds: The user fails the authentication if attempting to access the client source server 1,800 seconds (specified in the Timestamp field) later than the preset access time. For example, if the preset access time is 15:00:00 on August 15, 2020, the link expires at 15:30:00 on the same day.

Field	Description
DomainName	CDN client domain name.
timestamp	Resource failure time, as part of the URL and as a factor in the calculation of `md5hash` , is formatted: `YYYYMMDDHH MM` , effective time 1800 s
md5hash	//md5hash: The "timestamp", "FileName", and preset "PrivateKey" are used in the MD5 algorithm to get this string, i.e., (`PrivateKey` + `timestamp` + `FileName`)"
FileName	The actual URL of the origin access. Note that FileName must start with a slash (/) in authentication.

Example

1. Back-to-source request object.

```
http :// cdn . example . com / 4 / 44 / 44c0909bcf  c20a01afaf
256ca99a8b  8b . mp3
```

2. The key is set to aliyuncdnexp1234 (user-defined).
3. The time for the user to access the client source server is 201508150800 (format: YYYYMMDDHHMM).
4. The CDN server constructs a signature string used to calculate the "md5hash":

```
aliyuncdne  xp12342015  08150800 / 4 / 44 / 44c0909bcf  c20a01afaf
256ca99a8b  8b . mp3
```

5. The CDN server calculates the "md5hash" according to the signature string:

```
md5hash  =  md5sum (" aliyuncdne  xp12342015  08150800 / 4 / 44
/ 44c0909bcf  c20a01afaf  256ca99a8b  8b . mp3 ") =  9044548ef1
527deadafa  49a890a377  f0
```

6. The URL to request CDN:

```
http :// cdn . example . com / 2015081508  00 / 9044548ef1
527deadafa  49a890a377  f0 / 4 / 44 / 44c0909bcf  c20a01afaf
256ca99a8b  8b . mp3
```

The calculated "md5hash" is the same as the "md5hash = 9044548ef1527deadafa 49a890a377f0" value in the user request, so the request passes authentication

9.2.4 Authentication method C

Principles

Formats of the encrypted URL for user access

Format 1

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

Format 2

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

- The content in braces represents the encrypted information that is added based on the standard URL.
- `< md5hash >` is the MD5 encrypted string of authentication information.
- `< timestamp >` is a non-encrypted string expressed in plaintext.. The fixed length is 10 bits. It is the number of seconds since January 1, 1970, Coordinated Universal Time (UTC), expressed in hexadecimal format.
- Use format 1 to encrypt a URL, for example:

  ```
  http :// cdn . example . com / a37fa50a5f  b8f71214b1  e7c95ec7a1
  bd / 55CE8100 / test . flv
  ```

  `< md5hash >` a37fa50a5fb8f71214b1e7c95ec7a1bd`< timestamp >` is 55CE8100.

Authentication fields

- Field description for `< md5hash >`:

Field	Description
PrivateKey	Interference string. Different clients use different interference strings.
FileName	The actual URL of the origin fetch access. Note that the path must start with a slash (/) in authentication.
time	The UNIX time of the user's access to the origin server, expressed in hexadecimal format.

- PrivateKey value: `aliyuncdne  xp1234`
- FileName value: `/ test . flv`

- time value: `55CE8100`
- So the "md5hash" value is:

  ```
  md5hash  =  md5sum ( aliyuncdne  xp1234 / test . flv55CE810  0 ) =
  a37fa50a5f  b8f71214b1  e7c95ec7a1  bd
  ```

- Plaintext: `timestamp  =  55CE8100`

  The encrypted URL is then generated as follows:

  Format 1:

  ```
  http :// cdn . example . com / a37fa50a5f  b8f71214b1  e7c95ec7a1
  bd / 55CE8100 / test . flv
  ```

  Format 2:

  ```
  http :// cdn . example . com / test . flv ? KEY1 = a37fa50a5f
  b8f71214b1  e7c95ec7a1  bd & KEY2 = 55CE8100
  ```

Example

The user accesses the acceleration node using the encrypted URL. The CDN server first extracts the encrypted string 1, obtains

`< FILENAME >`

After this process, the CDN server authenticates the URL.

1. Use `< FileName >`of the original URL, request time, and PrivateKey to do MD5
2. Compare whether the encrypted string 2 and the encrypted string 1 are the same. The access request is rejected if the two strings are inconsistent.
3. Use the current time on the CDN server 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 1,800s means that authentication fails when the user fails to access the client source server 1,800s after the preset access time. For example, if the preset access time is 2020-08-15 15:00:00, the actual link expiry time is 2020-08-15 15:30:00
5. If the time difference is less than the preset time limit, the request is valid, and the CDN acceleration node responds normally. Otherwise, the request is rejected and an HTTP 403 error is returned.

9.2.5 Sample authentication code

For URL authentication rules, see URL Authentication Document. Using this demo, you can perform URL authentication based on your business needs. The demo provides three authentication methods and describes the composition of requested URLs and hash strings for each method.

Python version

```
 import   re
 import   time
 import   hashlib
 import   datetime
 def   md5sum ( src ):
     m  =  hashlib . md5 ()
     m . update ( src )
     return   m . hexdigest ()
 def   a_auth ( uri ,  key ,  exp ):
     p  =  re . compile ("^( http ://| https ://)?([ ^/?] +)(/[^?] *)?
( \\?. *)?$")
     if   not   p :
         return   None
     m  =  p . match ( uri )
     scheme ,  host ,  path ,  args  =  m . groups ()
     if   not   scheme :  scheme  = " http ://"
     if   not   path :  path  = "/"
     if   not   args :  args  = ""
     rand  = " 0 "      # " 0 "  by   default ,  other   value   is
 ok
     uid  = " 0 "       # " 0 "  by   default ,  other   value   is
 ok
     sstring  = "% s -% s -% s -% s -% s " %( path ,  exp ,  rand ,
 uid ,  key )
     hashvalue  =  md5sum ( sstring )
     auth_key  = "% s -% s -% s -% s " %( exp ,  rand ,  uid ,
 hashvalue )
     if   args :
         return  "% s % s % s % s & auth_key =% s " %( scheme ,  host
 ,  path ,  args ,  auth_key )
     else :
         return  "% s % s % s % s ?  auth_key =% s " %( scheme ,  host
 ,  path ,  args ,  auth_key )
 def   b_auth ( uri ,  key ,  exp ):
     p  =  re . compile ("^( http ://| https ://)?([ ^/?] +) (/[^?]
 *)? ( \\?. *)? $ ")
     if   not   p :
         return   None
     m  =  p . match ( uri )
     scheme ,  host ,  path ,  args  =  m . groups ()
     if   not   scheme :  scheme  = " http ://"
     if   not   path :  path  = "/"
     if   not   args :  args  = ""
    #  convert   unix   timestamp   to  " YYmmDDHHMM "  format
     nexp  =  datetime . datetime . fromtimest  amp ( exp ). strftime
 ('% Y % m % d % H % M ')
     sstring  =  key  +  nexp  +  path
     hashvalue  =  md5sum ( sstring )
     return  "% s % s /% s /% s % s % s " %( scheme ,  host ,  nexp ,
 hashvalue ,  path ,  args )
 def   c_auth ( uri ,  key ,  exp ):
     p  =  re . compile ("^( http ://| https ://)?([ ^/?] +) (/[^?]
 *)? ( \\?. *)?$")
     if   not   p :
         return   None
     m  =  p . match ( uri )
     scheme ,  host ,  path ,  args  =  m . groups ()
     if   not   scheme :  scheme  = " http ://"
     if   not   path :  path  = "/"
     if   not   args :  args  = ""
     hexexp  = "% x " % exp
     sstring  =  key  +  path  +  hexexp
     hashvalue  =  md5sum ( sstring )
     return  "% s % s /% s /% s % s % s " %( scheme ,  host ,
 hashvalue ,  hexexp ,  path ,  args )
 def   main ():
     uri  = " http :// xc . cdnpe . com / ping ? foo = bar " #
 original   uri
     key  = "< input   private   key >"                        #
 private   key   of   authorizat  ion
     exp  =  int ( time . time ()) +  1  *  3600                   #
 expiration   time :  1   hour   after   current   itme
     authuri  =  a_auth ( uri ,  key ,  exp )                     #
 auth   type :  a_auth  /  b_auth  /  c_auth
     print (" URL  : % s \ nAUTH : % s " %( uri ,  authuri ))
 if   __name__  == " __main__ ":
     main ()
```

9.3 IP Blacklist and Whitelist

Introduction

CDN supports the blacklist and whitelist rules. You can add IP addresses on the IP blacklist. An IP address on the blacklist cannot access the target domain. Likewise, only IP addresses on the whitelist can access the target domain.

Note:

If you add one IP address to the blacklist, it can still access to CDN node. But it will be refused with 403. As a result, these request logs will still exist in your CDN logs.

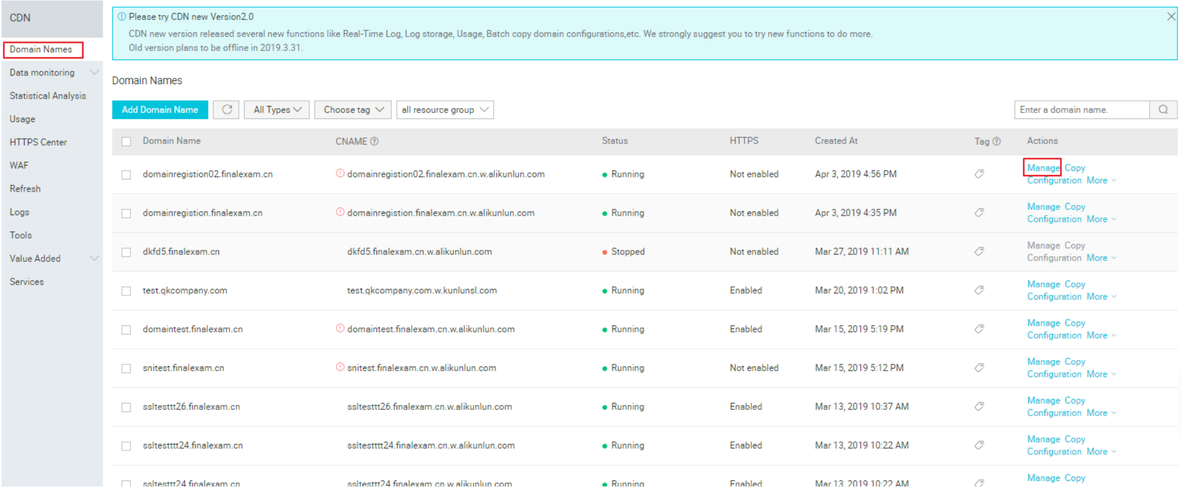
Example

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

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 127.0.0.1/24 indicates the IP network segment scope of 127.0.0.1~127.0.0.255.

Procedure

1. Log on to the CDN console.
2. In the left-side navigation pane, choose Domain Names. In the main workspace, select a domain, and in the Actions column click Manage.



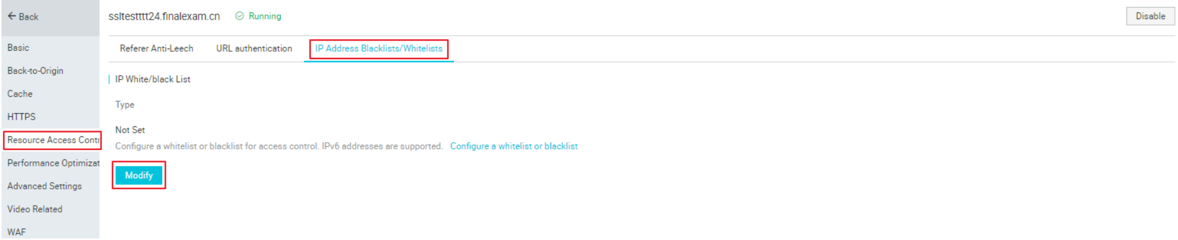
Please try CDN new Version2.0

CDN new version released several new functions like Real-Time Log, Log storage, Usage, Batch copy domain configurations,etc. We strongly suggest you to try new functions to do more.
Old version plans to be offline in 2019.3.31.

Domain Names

□	Domain Name	CNAME	Status	HTTPS	Created At	Tag	Actions
□	domainregistion02.finalexam.cn	domainregistion02.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 3, 2019 4:56 PM		Manage Copy Configuration More
□	domainregistion.finalexam.cn	domainregistion.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 3, 2019 4:35 PM		Manage Copy Configuration More
□	dkfd5.finalexam.cn	dkfd5.finalexam.cn.w.alikunlun.com	● Stopped	Not enabled	Mar 27, 2019 11:11 AM		Manage Copy Configuration More
□	test.qkcompany.com	test.qkcompany.com.w.kunlunsl.com	● Running	Enabled	Mar 20, 2019 1:02 PM		Manage Copy Configuration More
□	domaintest.finalexam.cn	domaintest.finalexam.cn.w.alikunlun.com	● Running	Enabled	Mar 15, 2019 5:19 PM		Manage Copy Configuration More
□	snitest.finalexam.cn	snitest.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Mar 15, 2019 5:12 PM		Manage Copy Configuration More
□	ssltesttt26.finalexam.cn	ssltesttt26.finalexam.cn.w.alikunlun.com	● Running	Enabled	Mar 13, 2019 10:37 AM		Manage Copy Configuration More
□	ssltestttt24.finalexam.cn	ssltestttt24.finalexam.cn.w.alikunlun.com	● Running	Enabled	Mar 13, 2019 10:22 AM		Manage Copy Configuration More
□	ssltesttt24.finalexam.cn	ssltesttt24.finalexam.cn.w.alikunlun.com	● Running	Enabled	Mar 13, 2019 10:22 AM		Manage Copy

3. In the left-side navigation pane, choose Resource Access Control. In the main workspace, choose the IP Address Blacklists/Whitelists tab, and on the IP Address Blacklists/Whitelists tab page click Modify.



ssltestttt24.finalexam.cn Running

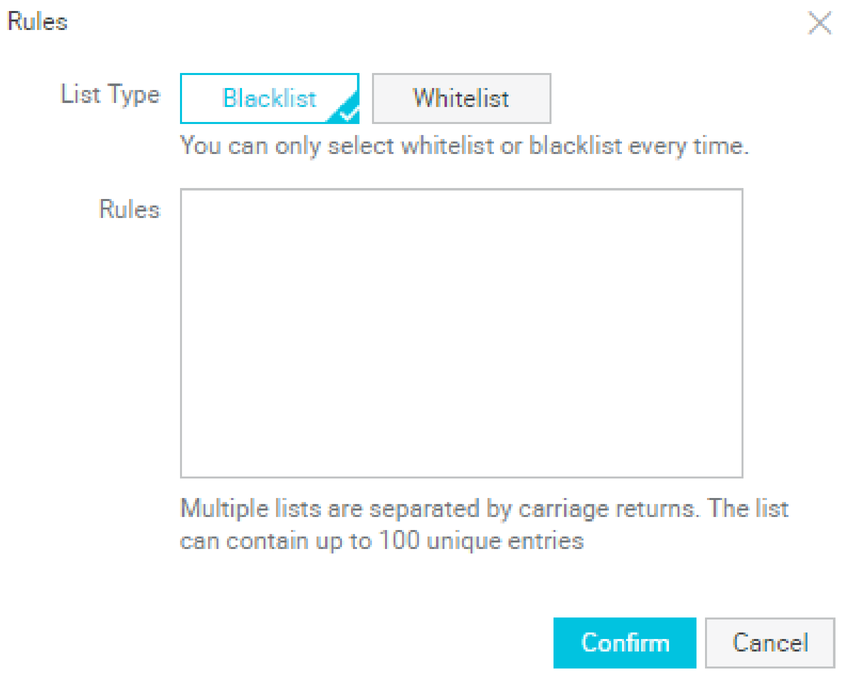
IP White/black List

Type

Not Set

Configure a whitelist or blacklist for access control. IPv6 addresses are supported. Configure a whitelist or blacklist

4. In the dialog box that is displayed, set `List Type` to `Blacklist` or `Whitelist`, add the IP network segment in the text box below, and click Confirm.



Rules

List Type: Blacklist ☑ | Whitelist

You can only select whitelist or blacklist every time.

Rules:

Multiple lists are separated by carriage returns. The list can contain up to 100 unique entries

9.4 UA blacklist and whitelist

This topic describes UA blacklists and whitelists and how to configure them in the CDN console.

Context

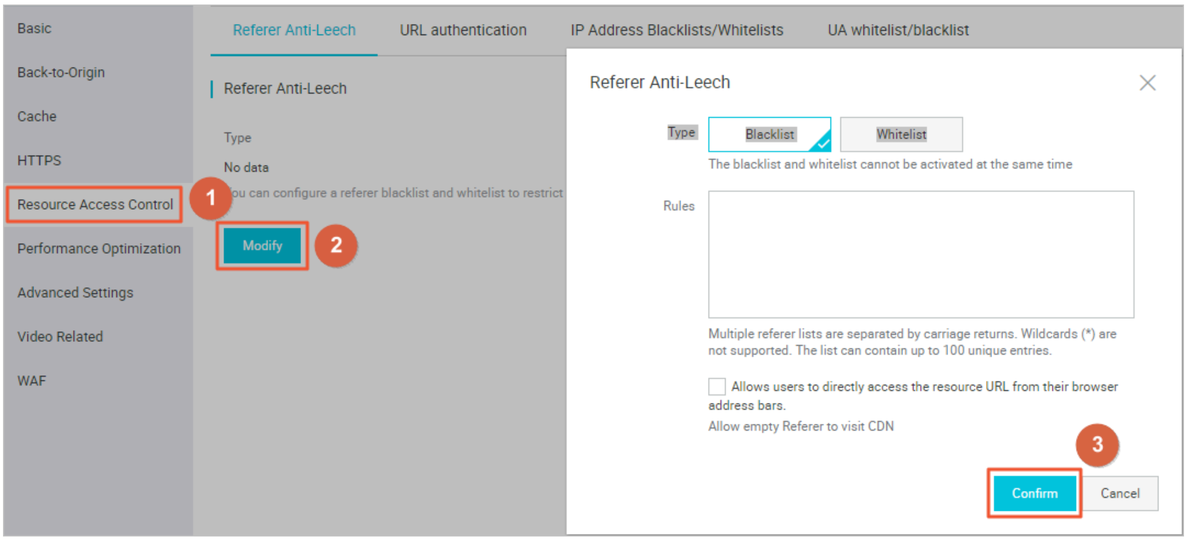
Both UA blacklists and whitelists contain `Usage - Agent` information elements (IEs), which are carried in request messages. After you configure UA blacklists or whitelists for a CDN node, the CDN node filters request messages and permits only the access requests from specific clients.

Note:

- `Usage - Agent` IEs are not case-sensitive and can contain wildcard characters (*). The multiple options in a `Usage - Agent` IE are separated by using vertical bars (|). An example `Usage - Agent` IE is as follows: `* curl *|* IE *|* chrome *|* firefox *`.
- Only the UA blacklist or whitelist can be enabled at a specific time point.

Procedure

1. Log on to the CDN console.
2. In the left-side navigation pane, click Domain Names.
3. Find the domain name you want to set, and click Manage in the Actions column.
4. In the left-side navigation pane, click Resource Access Control.
5. On the UA whitelist/blacklist tab, click Modify.
6. Configure the blacklist or whitelist as needed, and click Confirm.



ou can configure a referer blacklist and whitelist to restrict

The blacklist and whitelist cannot be activated at the same time

Multiple referer lists are separated by carriage returns. Wildcards (*) are not supported. The list can contain up to 100 unique entries.

□ Allows users to directly access the resource URL from their browser address bars.

Allow empty Referer to visit CDN

10 Performance Optimization settings

10.1 Page Optimization

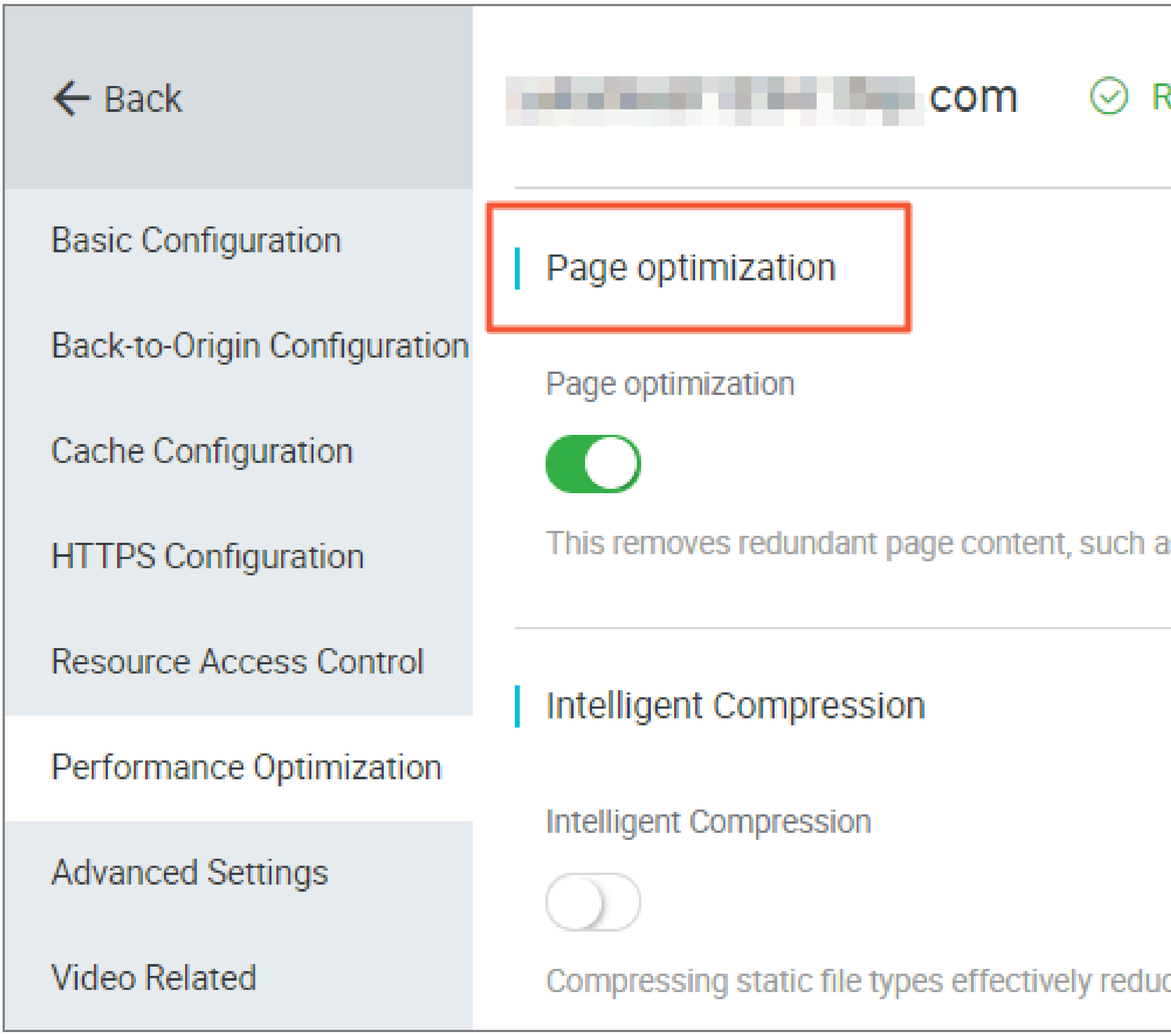
Introduction

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

Procedure

> **Notice:**
>
> When we are optimizing your page, the file's md5 value will be changed. It will be different from that of the file I your origin site. Do not enable this feature if your origin site has some verification.

1. Go to Domain Namespage, select the domain name, then click Manage.

2. 

Page optimization

Page optimization

This removes redundant page content, such a

Intelligent Compression

Intelligent Compression

Compressing static file types effectively reduc

3. Enable the function in Performance Optimization > Page Optimization.

10.2 Intelligent compression

After enabling Intelligent Compression function, you can compress most types of static files, so as to reduce the size of content transmitted by users and accelerates the content delivery.

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

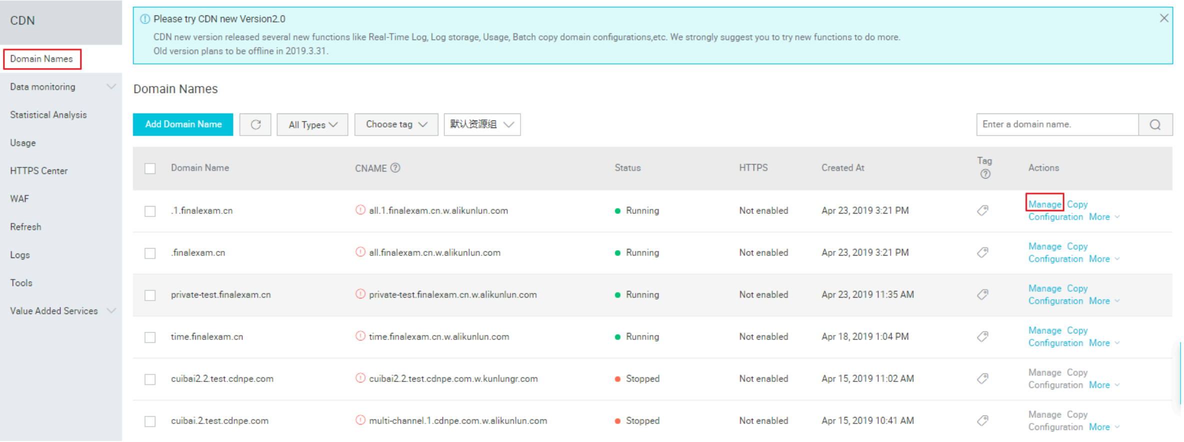
Applicable business type: All.

Procedure

Notice:

When we are optimizing your page, the file's md5 value will be changed. It will be different from that of the file I your origin site. Do not enable this feature if your origin site has some verification.

1. Log on to the CDN console.
2. In the left-side navigation pane, choose Domain Names. In the main workspace, select a domain, and in the Actions column click Manage.



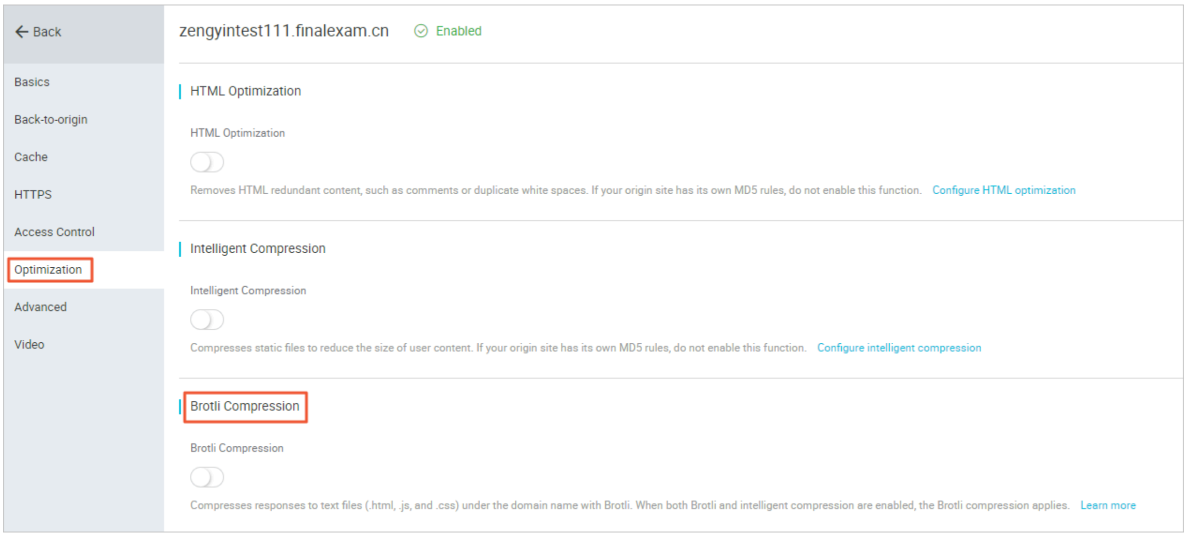
Please try CDN new Version2.0

CDN new version released several new functions like Real-Time Log, Log storage, Usage, Batch copy domain configurations,etc. We strongly suggest you to try new functions to do more.
Old version plans to be offline in 2019.3.31.

Domain Names

□	Domain Name	CNAME	Status	HTTPS	Created At	Tag	Actions
□	.1.finalexam.cn	all.1.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
□	.finalexam.cn	all.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
□	private-test.finalexam.cn	private-test.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 23, 2019 11:35 AM		Manage Copy Configuration More
□	time.finalexam.cn	time.finalexam.cn.w.alikunlun.com	● Running	Not enabled	Apr 18, 2019 1:04 PM		Manage Copy Configuration More
□	cuibai2.2.test.cdnpe.com	cuibai2.2.test.cdnpe.com.w.kunlungr.com	● Stopped	Not enabled	Apr 15, 2019 11:02 AM		Manage Copy Configuration More
□	cuibai.2.test.cdnpe.com	multi-channel.1.cdnpe.com.w.alikunlun.com	● Stopped	Not enabled	Apr 15, 2019 10:41 AM		Manage Copy Configuration More

3. On the page that is displayed, choose Performance Optimization from the left-side navigation pane, and in the Intelligent Compression area enable the function.



zengyintest111.finalexam.cn Enabled

HTML Optimization

HTML Optimization

Removes HTML redundant content, such as comments or duplicate white spaces. If your origin site has its own MD5 rules, do not enable this function. Configure HTML optimization

Intelligent Compression

Intelligent Compression

Compresses static files to reduce the size of user content. If your origin site has its own MD5 rules, do not enable this function. Configure intelligent compression

Brotli Compression

Brotli Compression

Compresses responses to text files (.html, .js, and .css) under the domain name with Brotli. When both Brotli and intelligent compression are enabled, the Brotli compression applies. Learn more

10.3 Brotli compression

This topic describes Brotli compression and how to enable it in the CDN console. Brotli compression helps to reduce content size and expedite content delivery.

Context

Brotli is a new, open-source compression algorithm. It enables a CDN node to compress and optimize the requested HTML, JS, and CSS, and other static text files at speeds that are 15% to 25% higher than Gzip.

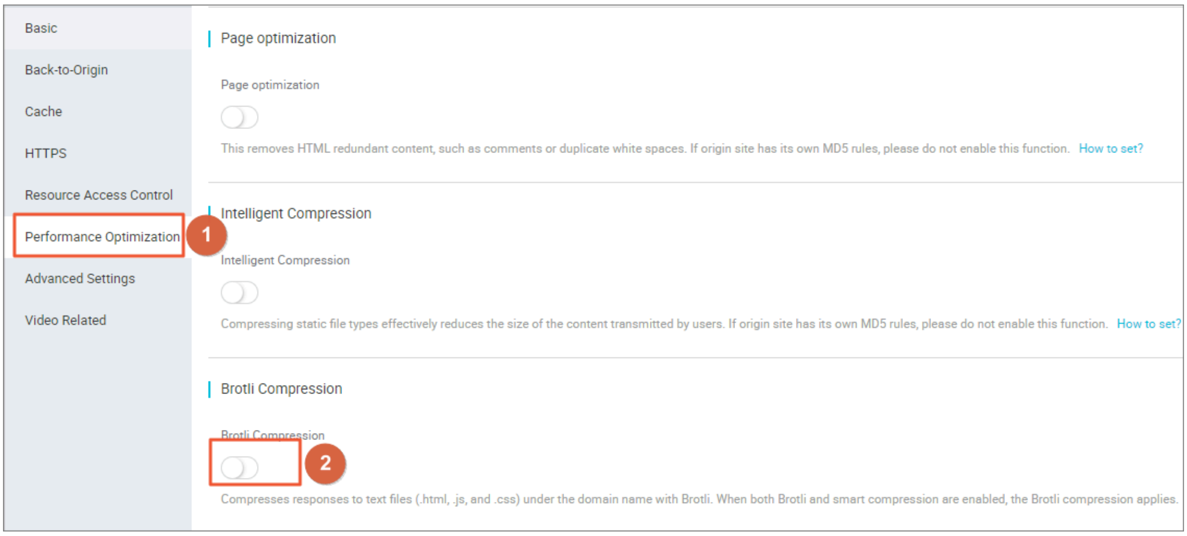
- If the request message from a client carries the `Accept - Encoding : br` request header, the client wants the requested resources to be compressed by using Brotli.
- If the response message from the server carries the `Content - Encoding : br` response header, the server returns the requested resources that are compressed by using Brotli.

> **Notice:**
> If Brotli compression and Gzip compression are both enabled and the `Accept - Encoding` request header in the request message from the client carries both the `br` and `gzip` options, the CDN node as a priority uses Brotli to compress the requested content.

Procedure

1. Log on to the CDN console.
2. In the left-side navigation pane, click Domain Names.
3. Locate the domain name you want to set, and click Manage in the Actions column.
4. In the left-side navigation pane, click Performance Optimization.

5. In the Brotli Compression section, turn on Brotli compression.


Basic
Back-to-Origin
Cache
HTTPS
Resource Access Control
Performance Optimization
1
Advanced Settings
Video Related
Page optimization
Page optimization
This removes HTML redundant content, such as comments or duplicate white spaces. If origin site has its own MD5 rules, please do not enable this function. How to set?
Intelligent Compression
Intelligent Compression
Compressing static file types effectively reduces the size of the content transmitted by users. If origin site has its own MD5 rules, please do not enable this function. How to set?
Brotli Compression
Brotli Compression
2
Compresses responses to text files (.html, .js, and .css) under the domain name with Brotli. When both Brotli and smart compression are enabled, the Brotli compression applies.

10.4 Filter Parameter

Introduction

When a URL request carrying? and request parameters are sent to a CDN node, the CDN node determines whether to send the request to the origin site.

- If you enable Filter Parameter function: after the request arrives at the CDN node, the URL without parameters is intercepted and requested against the origin site. Additionally, the CDN node retains only one copy.
  - 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 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), we recommend that you disable this function.
- If you disable Filter Parameter function, different copies are cached on the CDN node for different URLs.

Applicable business type: All.

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 to the origin site the `http :// www . abc . com / a . jpg` request (ignore parameter x = 1). After the origin site returns a response, the CDN node retains a copy. Then, the origin site continues to respond to the terminal `http :// www . abc . com / a . jpg` . For all requests similar to `http :// www . abc . com / a . jpg ? parameters` , the origin site responds to the CDN copy `http :// www . abc . com / a . jpg` .
- If the Filter Parameter function is disabled, `http :// www . abc . com / a . jpg ? x = 1` and `http :// www . abc . com / a . jpg ? x = 2` respond to the response content of different parameter origin site.

> Note:
>
> 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.

Procedure

1. Go to Domain Namespage, select the domain name, then click Manage.
2. Enable the function in Performance Optimization > Filter Parameter.

11 Advanced settings

11.1 Peak Bandwidth

Introduction

The bandwidth cap function sets the maximum bandwidth value for average bandwidth measured during each statistical cycle (five minutes). If the average bandwidth exceeds the maximum, the domain name automatically goes offline to protect your domain name security. In this situation, all requests are sent back to the origin site. When the bandwidth cap is reached, CDN stops acceleration services to avoid excessive fees produced by abnormal traffic volumes. After your domain name goes offline, you can restart it in the console.

Note:
The bandwidth cap function is not currently available for wildcard domain names, so the function has no effect even it is enabled.

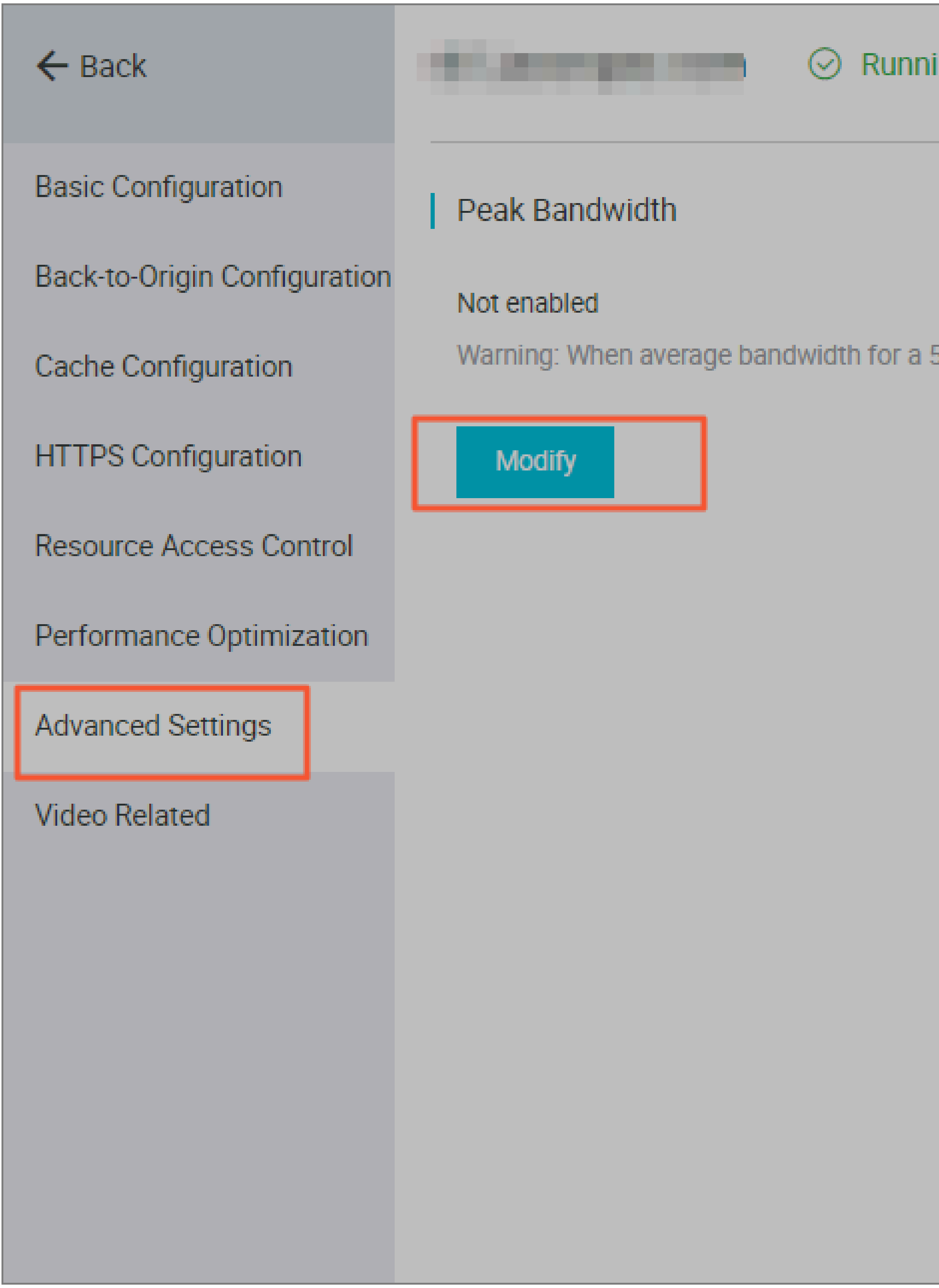
RAM subaccounts require CloudMonitor authorization to use this function. To grant authorization, use the AliyunCloudMonitorFullAccess policy group.

Procedure

Note:
After you have enabled the peak bandwidth function, your services are limited by the bandwidth cap and go offline if it is exceeded. To guarantee your services running continuously on your domain name, we recommend you set the cap value with discretion based on reasonable estimation.

1. Log on to the CDN console.
2. On the Domain Names page, choose the domain name, then click Manage.

3. Choose Advanced Settings, then click Modify under the Peak Bandwidth label.



Peak Bandwidth

Not enabled

Warning: When average bandwidth for a 5

4. Enable the bandwidth cap function. Choose the unit from Mbps, Gbps, or Tbps.

> **Note:**
> Bandwidth value can be set in powers of thousand.

5. Click Confirm. Then the peak bandwidth is successfully enabled.

You can choose to enable or disable the peak bandwidth function based on the actual usage of your domain name.

12 Video Service Configuration

12.1 Back-to-origin of range

Introduction

The Back-to-origin 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-origin traffic and improving the resource response speed.

The origin site must support the range request, that is, the range field is included in the HTTP request header, and the origin site can respond to the correct 206 file slice.

When the Back-to-origin of Range is	Description	Instances
Enable	A parameter request can be returned to an origin site. In this case, based on the Range parameter, the origin site returns the file byte range, while the CDN node returns the content in the byte range to the client.	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-origin of Range is	Description	Instances
Disable	A CDN higher-level node requests 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-origin traffic.	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.

Note:

To use the Back-to-origin 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.

Procedure

Back-to-origin of Range feature is optional and is disabled by default. You can change the configuration to enable it.

1. Go toDomain Namepage,selete your domain name, and click Manage.
2. Click Modify Configuration in Video-related > Back-to-origin of Range.
3. Select Enable, Disable or Force.

Go to the CDN domain name management page, click Configure, select Enable/ Disable/Force Back-to-origin of Range function.

Note:

You can enable Force if your origin site is capable of using this feature. After enabling it, all requests will be forced to perform Back-to-origin of range.

See Back-to-origin of Range for more API information.

12.2 Drag/Drop Playback

Introduction

In a video-on-demand scenario, when the playback progress bar is dragged, the end user will send a URL request, such as `http :// www . aliyun . com / test . flv ? start = 10` , to the server. The server returns the data from the key frame prior to the10th second to the client (If start=10 is not the key frame).

After receiving such a request from an end user and the Drag/Drop Playback function is enabled, a CDN node can directly return the data from the key frame prior to the10th second (If start=10 is not the key frame) (FLV format) or from the 10th second to the end user.

Note

- 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.
- Two available file format: MP4 and FLV.
- Currently, FLV format only supports the coding formats with the audio format of aac and video format of avc.

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 request http: // domain/video.mp4 ?start=10 playing a video from the 10th second.

File Format	Meta Information	start Parameter	Example
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.	For http: //domain/video.flv, the request http://domain/video.flv? start=10 playing a video from the key frame prior to the10th byte(If start=10 is not the position of the key frame) .

Procedure

1. Go to Domain Namespage, select the domain name, then click Manage.
2. Enable the function in Video-related > Drag/Drop Playback.