

Alibaba Cloud

Alibaba Cloud CDN

Domain Management

Issue: 20190815

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 information, 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 <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Features.....	1
2 Copy configurations.....	7
3 Set an alarm rule.....	10
4 Tags.....	11
4.1 Tag overview.....	11
4.2 Attach tags to a domain name.....	12
4.3 Detach tags from a domain name.....	12
4.4 Manage domain names by tag.....	13
4.5 Query domain names by tag.....	14
4.6 Tag use case.....	16
5 Basic settings.....	17
5.1 Configure origin site.....	17
5.2 Modify basic information.....	20
5.3 Modify origin information.....	20
6 Content back-to-source settings.....	24
6.1 Configure an origin host.....	24
6.2 Back-to-origin with the same protocol.....	25
6.3 Enable private bucket back-to-origin authentication.....	27
6.4 Disable private bucket back-to-origin authentication.....	30
6.5 Back-to-origin SNI.....	31
6.6 Customize an origin HTTP header.....	33
6.7 Set the origin request timeout period.....	34
7 Node Cache Settings.....	36
7.1 Create a cache expiration rule.....	36
7.2 Set HTTP code expiration time.....	40
7.3 Create an HTTP header.....	42
7.4 Customize an error page.....	44
7.5 Rewrite.....	46
8 HTTPS Acceleration.....	48
8.1 What is HTTPS acceleration?.....	48
8.2 Overview of certificate formats.....	54
8.3 Configure HTTPS certificates.....	58
8.4 Enable HTTP/2.....	65
8.5 Enable Force Redirect.....	67
8.6 Configure TLS.....	69
8.7 HSTS.....	71

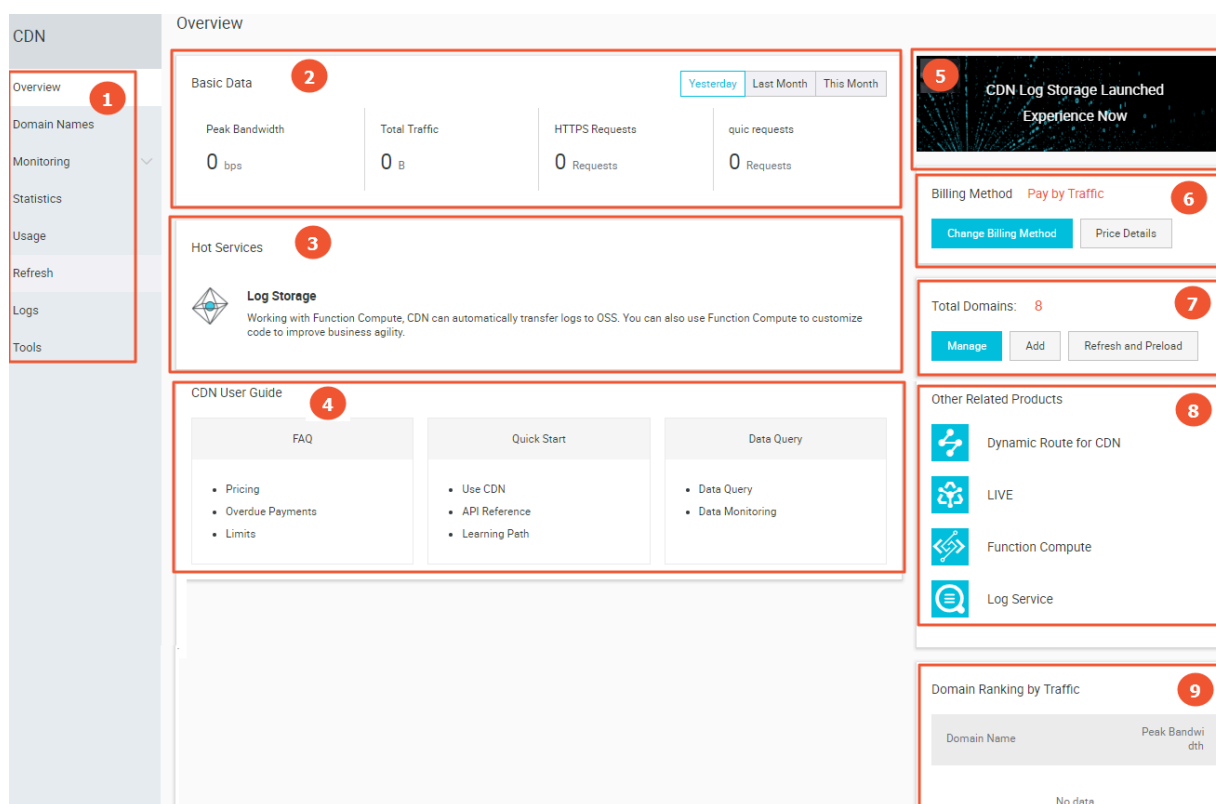
8.8 FAQ.....	73
9 Access Control Settings.....	76
9.1 Anti-leech.....	76
9.2 Business type.....	78
9.2.1 Authentication configuration.....	78
9.2.2 Authentication method A.....	81
9.2.3 Authentication method B.....	83
9.2.4 Authentication method C.....	85
9.2.5 Sample authentication code.....	87
9.3 IP Blacklist and Whitelist.....	88
9.4 UA blacklist and whitelist.....	90
10 Performance Optimization settings.....	92
10.1 Page Optimization.....	92
10.2 Intelligent compression.....	93
10.3 Brotli compression.....	95
10.4 Filter Parameter.....	96
11 Video Service Configuration.....	98
11.1 Back-to-origin of range.....	98
11.2 Drag/Drop Playback.....	100
11.3 Audio extraction.....	101
12 Advanced settings.....	103
12.1 QUIC.....	103
12.1.1 What is the QUIC protocol?.....	103
12.1.2 Configure the QUIC protocol.....	105
12.2 Peak Bandwidth.....	106

1 Features

The Alibaba Cloud CDN console not only allows you to complete basic operations such as domain name configuration, but also provides resource monitoring services for real-time data analysis. You can also learn about your billing information and change the billing method at any time. This topic describes the CDN console and the domain management features.

Console guide

The following figure shows the CDN console interface.



The following table describes the CDN console interface.

No.	Element	Description
1	Left-side navigation pane	Displays the navigation pane for domain management. For more information, see Domain management features .
2	Basic data	Displays the usage status of each billing item based on the billing method of your CDN service. For more information, see Basic Service .

No.	Element	Description
3	Hot services	Shows you how to quickly access the frequently used CDN features.
4	CDN user guide	Displays the links of the CDN help documents to which you can refer. For more information, see CDN Learning Path .
5	Configure log storage	The log storage service uses Function Compute to store logs for a long time period. For more information, see Configure log storage .
6	Billing method	Displays the billing method you have selected. You can also modify the billing method as needed. For more information, see Basic Service and Value-added service .
7	All domains	Allows you to quickly manage the existing domains, add domains, and perform the refresh or preload operation.
8	Other acceleration products	Displays CDN-related products.
9	Traffic-based domain ranking	Displays top five CDN domains by traffic.

Domain management features

The following table lists the CDN domain management features.

Feature	Reference	Description	Default value
Bulk copying	Copy configurations	Allows you to copy one or more configurations of a CDN domain to another one or more CDN domains.	None
Alert settings	Set an alarm rule	Monitors CDN domains by using the following metrics: peak bandwidth, 4xx code proportion, 5xx code proportion, hit rate, Internet downstream traffic, and QPS. When an alert rule is triggered, Alibaba Cloud CloudMonitor sends an alert message through SMS or email based on the settings.	None
Tag management	Attach tags to a domain name	Allows you to add tags to a domain name or group domain names by tags.	None

Feature	Reference	Description	Default value
	Manage domain names by tag	Allows you to use tags to quickly filter domain names for group management.	None
	Query domain names by tag	Allows you to use tags to quickly filter domain names for data query.	None
Basic information settings	Modify basic information	Allows you to modify the accelerated region.	None
	Modify origin information	Allows you to modify the origin information.	None
Back-to-origin settings	Configure an origin host	Allows you to modify the domain name of the origin host.	Enabled
	Configure an origin protocol	CDN communicates with your origin according to the specified origin protocol policy. If you specify the Follow policy, CDN communicates with your origin over HTTP or HTTPS, depending on the protocol of the client request.	Disabled
	Configure the private bucket access control	Grants CDN permissions to access the specified private OSS bucket that serves as the origin.	Disabled
	Back-to-origin SNI	If you have bound your origin IP address to multiple domain names, you must specify the SNI of a specific domain when CDN nodes access your origin site over HTTPS.	Disabled
	Customize an origin HTTP header	If you configure CDN to use HTTP to communicate with your origin, you can add or remove HTTP header fields.	Disabled
	Set the origin request timeout period	Allows you to set the maximum amount of time that CDN waits for a response after it forwards a request to an origin. When CDN does not receive any response before the timeout period expires, the connection between the CDN node and the origin is terminated.	30 seconds

Feature	Reference	Description	Default value
Cache settings	Configure cache expiration	Allows you to customize cache expiration rules for specified resources.	None
	#unique_21	Allows you to customize the expiration rules for the status codes of the resources that are specified by directory or file extension.	None
	Set the HTTP header	Allows you to customize the HTTP request header. Currently, 10 HTTP request header fields are available for customization.	None
	Customize an error page	Allows you to customize a complete URL to redirect for an HTTP or HTTPS response code.	404
	Configure a rewrite rule	Allows you to modify a request URI and perform a 302 redirect to the specified target URI.	None
HTTPS secure acceleration	Configure HTTPS certificates	Provides an end-to-end HTTPS secure acceleration solution. You only need to enable the secure acceleration mode and then upload the certificate and private key for a CDN domain. This feature also allows you to view, disable, enable, or modify certificates.	Disabled
	Enable HTTP/2	The HTTP/2 protocol is binary and has multiple advantages including scalability, security, multiplexing, and header compression.	Disabled
	Enable force redirect	If HTTP secure acceleration is enabled, you can configure CDN to forcibly redirect user requests to HTTPS or HTTP.	Disabled
	Configure TLS	After a TLS protocol version is enabled, the TLS handshake is enabled for the CDN domain. Currently, only TLS version 1.0, TLS version 1.1, TLS version 1.2, and TLS version 1.3 are supported.	Disabled

Feature	Reference	Description	Default value
	Configure HSTS	HSTS is used to force clients (such as browsers) to use HTTPS to create connections with the server.	Disabled
Access control	Configure hotlinking protection	Allows you to configure a referer blacklist or whitelist to identify and filter visitors.	Disabled
	Configure URL authentication	Allows you to configure URL authentication to prevent unauthorized downloads and theft of the resources on the site.	Disabled
	Configure an IP blacklist or whitelist	Allows you to configure an IP blacklist or whitelist to identify and filter visitors.	Disabled
	Configure a User-Agent blacklist or whitelist	Allows you to configure a User-Agent blacklist or whitelist to identify and filter visitors.	Disabled
Performance optimization	Configure HTML optimization	Compresses and removes HTML redundant content, such as blank lines and carriage return characters, to reduce the file size.	Disabled
	Configure intelligent compression	Supports intelligent compression for content in multiple formats to reduce the size of user transmitted content.	Disabled
	Configure Brotli compression	If you want to compress static text files, you can enable this feature. It can reduce the size of the transmitted content and accelerate content delivery.	Disabled
	Configure parameter filtering	After a CDN node receives a URL request that includes the question mark (?) and <i>Parameters</i> , it determines whether the URL request needs to be rerouted to the origin site with the parameters.	Disabled

Feature	Reference	Description	Default value
Advanced settings	Configure a bandwidth cap	Allows you to set the maximum bandwidth value for average bandwidth measured during each statistical cycle (5 minutes). To protect the CDN domain, the domain automatically becomes disabled when the average bandwidth exceeds the maximum value. In this situation, all requests are forwarded to the origin site.	Disabled
Video-related settings	Configure object chunking	Reduces back-to-origin traffic consumption and shortens resource response time.	Disabled
	Configure video seeking	After this feature is enabled, you can drag and drop the playback progress of an audio or video content without affecting the playback effect.	Disabled

2 Copy configurations

This topic describes how to copy and move the configurations of a domain to other domains.

Prerequisites

Ensure that the domain from which you copy configurations has been enabled and appropriately configured.

Context

Note the following points when you copy configurations of a domain:

- The copied configurations will overwrite the existing configurations of the domain. Therefore, exercise cautions when performing the operation.
- The copy operation cannot be undone. The domain from which you copy configurations is enabled and provides a high operational bandwidth. The domain from which you copy configurations is active.

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 from which you want to copy configurations, and click Copy Configurations.

CDN

Overview

Monitoring

Statistics

Usage

Refresh

Logs

Tools

Domain Names

Add Domain Name

All Types

Select Tags

Search by keyword

<input type="checkbox"/>	Domain Name	CNAME	Status	HTTPS	Created At	Tags	Actions
<input type="checkbox"/>	example.com	example.com	Enabled	Disabled	Jun 18, 2019 6:12 PM		<div>ManageCopy ConfigurationsMore</div>
<input type="checkbox"/>	example.com	example.com	Enabled	Disabled	Jun 13, 2019 1:56 PM		<div>ManageCopy ConfigurationsMore</div>
<input type="checkbox"/>	example.com	example.com	Enabled	Disabled	Jun 12, 2019 5:05 PM		<div>ManageCopy ConfigurationsMore</div>
<input type="checkbox"/>	example.com	example.com	Enabled	Disabled	Jun 5, 2019 7:48 PM		<div>ManageCopy ConfigurationsMore</div>

Disable

Enable

Export

Manage Tags

CloudMonitor

4. Select the configuration items you want to copy, and click Next.



Note:

- The origin information cannot be copied at the same time as the other information.
- An HTTPS certificate cannot be copied.

- Custom HTTP origin headers are copied incrementally. For example, if Domain A has two custom HTTP origin headers and you copy another five HTTP origin headers from Domain B to Domain A, Domain A has seven custom HTTP origin headers.
- The HTTP headers are not incrementally copied. For example, if the `cache_control` HTTP header is set to private for Domain A and to public for Domain B and you copy the HTTP header configuration of Domain B to Domain A, the `cache_control` HTTP header of Domain A is set to public.
- If you copy switch-related configurations or Refer or IP address blacklists or whitelists, the new configurations overwrite the original configurations of the target domains.
- The new configurations overwrite the original configurations of the target domains.

CDN < Copy Configurations

You can copy the configurations of the domain to other domains. [Learn more](#)

1 Select Configurations 2 Select Domains 3 Complete

When you choose to copy the origin site information, you cannot copy other configurations. To copy other required configurations, try again after the origin site information is copied.

<input type="checkbox"/> Item	Current Configuration
<input checked="" type="checkbox"/> Origin Information	Configured
<input type="checkbox"/> Origin Protocol Policy	HTTP

Next Cancel

5. Select the domains to which you want to copy the configurations, and click Next.

You can enter a keyword in the search bar to search for a domain.

CDN < Copy Configurations

You can copy the configurations of the domain to other domains. [Learn more](#)

1 Select Configurations 2 Select Domains 3 Complete

Domain Names Selected Domains: 2/50

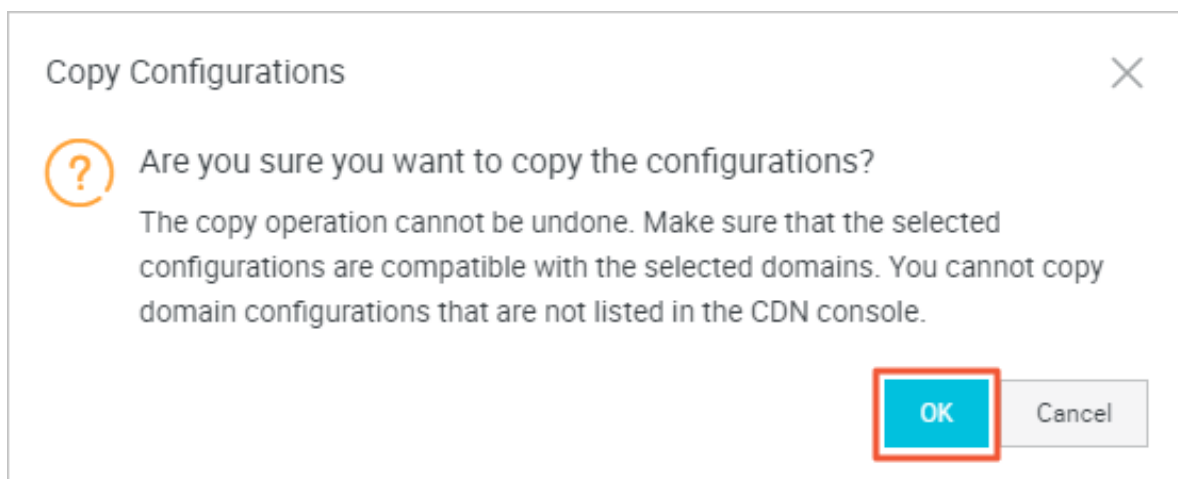
Search by keyword.

<input type="checkbox"/> Domain
<input type="checkbox"/> [Domain Name]
<input checked="" type="checkbox"/> [Domain Name]
<input checked="" type="checkbox"/> [Domain Name]
<input type="checkbox"/> [Domain Name]

▼ Show Selected

Next Cancel

6. In the Copy Configurations dialog box, click OK.

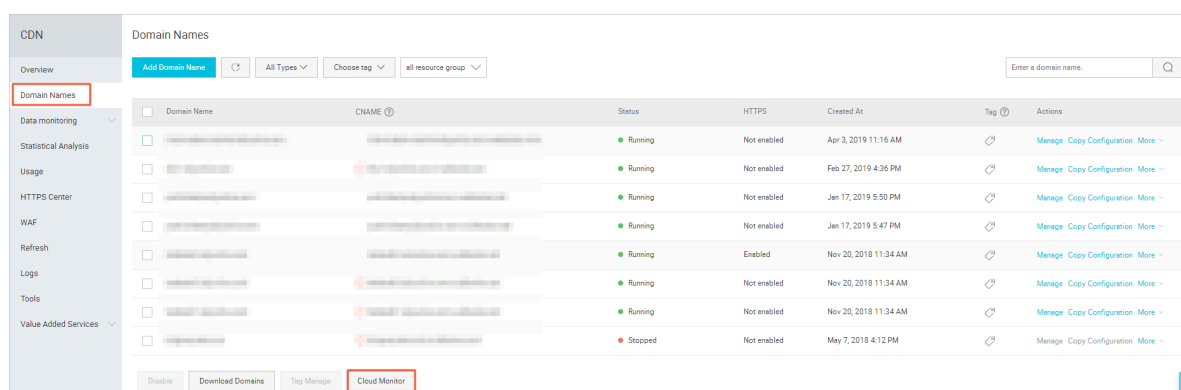


3 Set an alarm rule

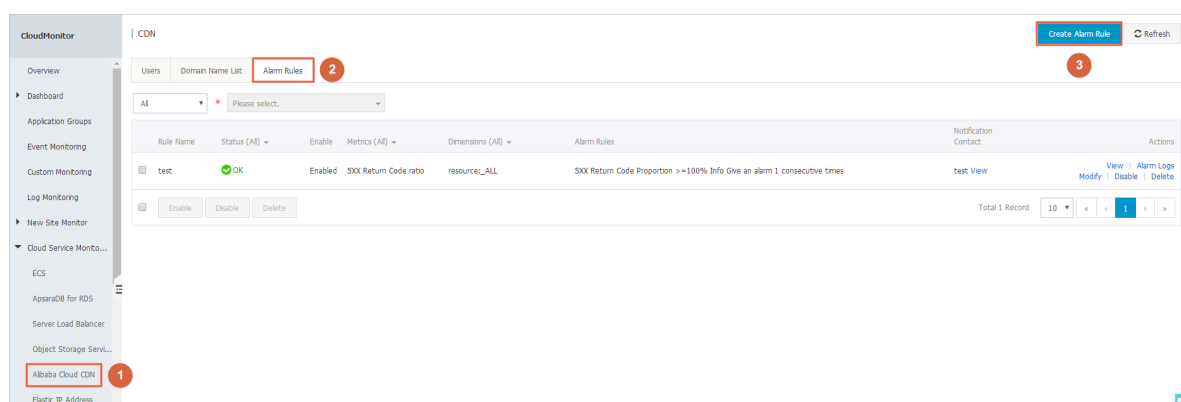
This topic describes how to create an alarm rule on the Alibaba Cloud CDN console. You can use Alibaba CloudMonitor to set alarm rules specific to CDN domain metrics. When an alarm rule is triggered, Alibaba CloudMonitor sends you an alarm by using the notification method (for example, SMS or email) you specify.

Procedure

1. Log on to the [Alibaba Cloud CDN console](#).
2. In the left-side navigation pane, click Domain Names.
3. In the main workspace, click Cloud Monitor



4. In the left-side navigation pane, choose Cloud Service Monitoring > Alibaba Cloud CDN, then in the main workspace click the Alarm Rules tab.
5. Click Create Alarm Rule.



6. Set the parameters to create a CDN alarm rule. For more information, see [Create a threshold alarm rule](#).

4 Tags

4.1 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:

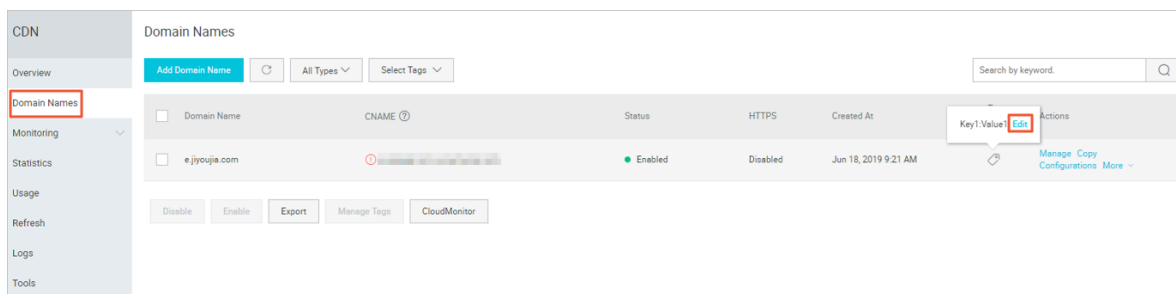
- Attach tags to domain names to identify or group the domain names. For more information, see [Attach tags](#).
- Detach tags from domain names. For more information, see [Detach tags](#).
- Manage domain names based on their tags. For more information, see [Manage domain names by tag](#).
- Query the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

4.2 Attach tags to a domain name

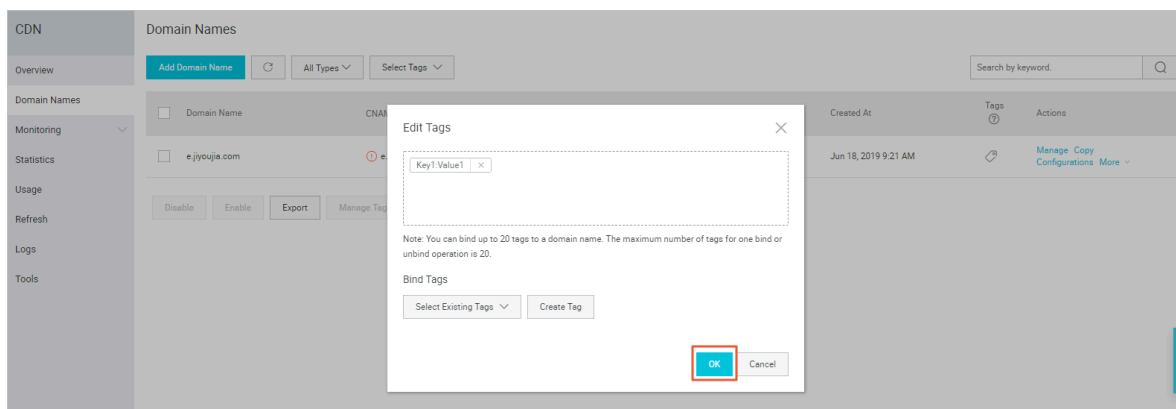
This topic describes how to attach tags to a domain name, which can help you to easily identify and group domain names.

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.



6. Click OK.

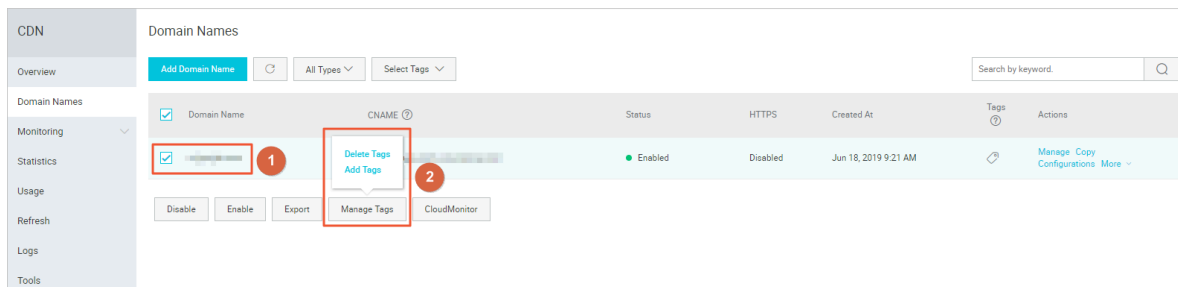
4.3 Detach tags from a domain name

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

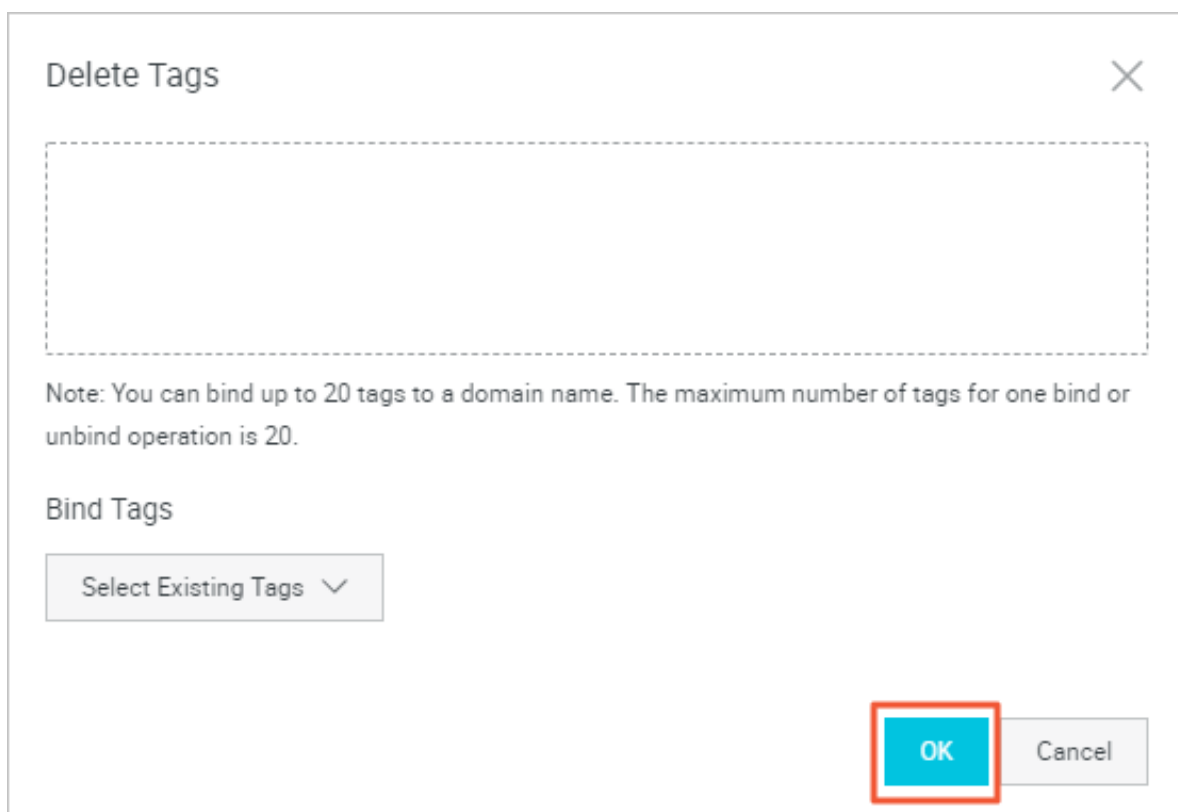
Procedure

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**.



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



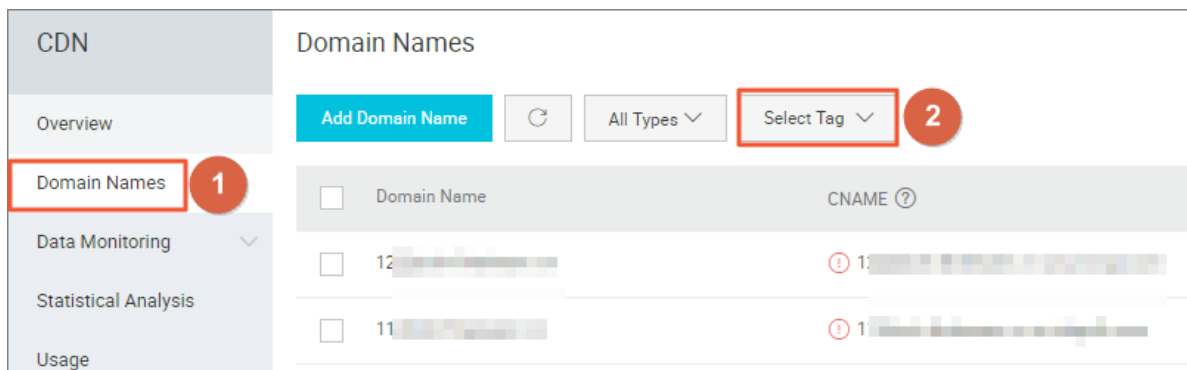
4.4 Manage domain names by tag

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.



4.5 Query domain names by tag

This topic describes how to query domain names by tag.

Procedure

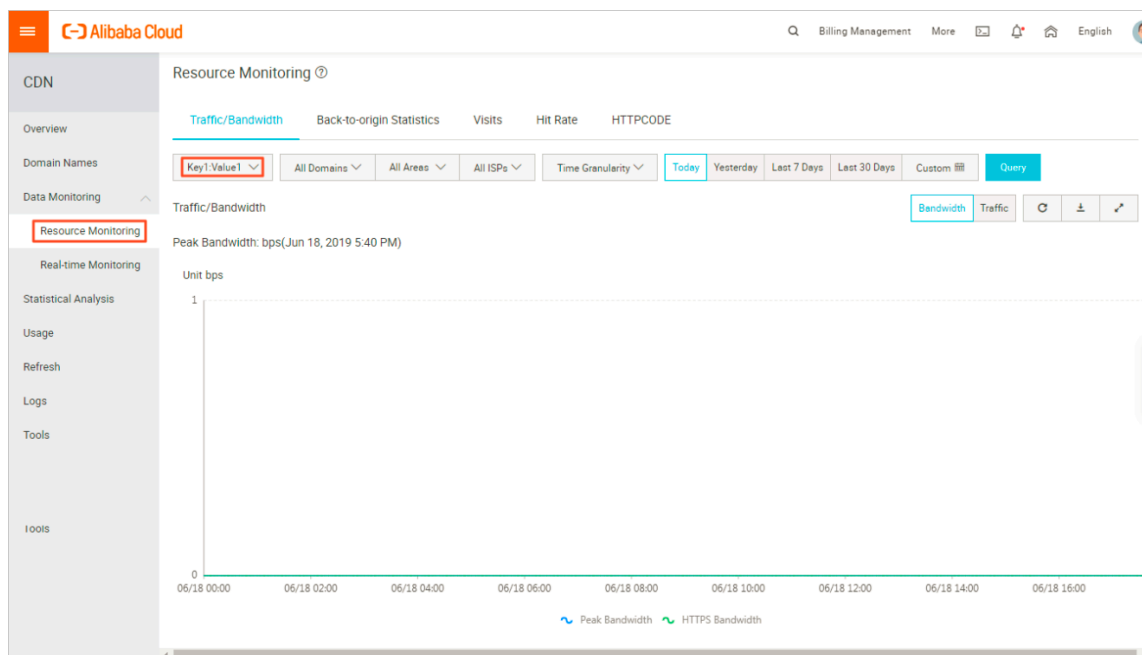
1. Log on to the [CDN console](#).
2. Use one of the following two methods to query the domain names to which specific tags are attached:



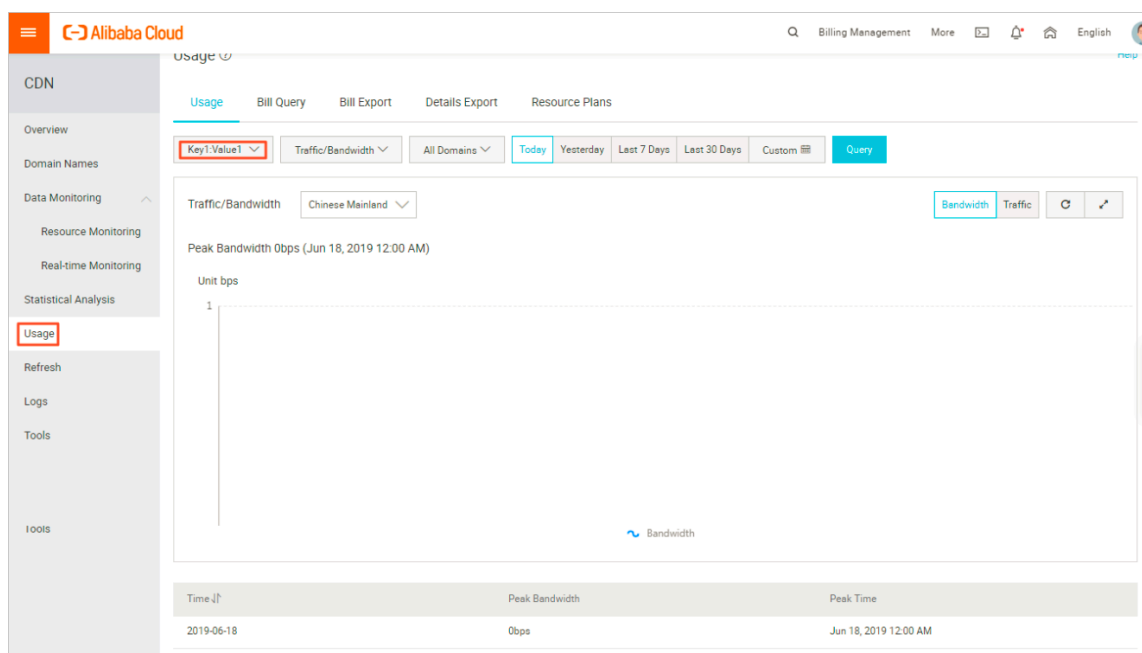
Note:

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.



4.6 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 the `Executive: Tom` tag.
- If the company wants to query the domain names that are managed by John from the Gaming department, it can select the `Department: Gaming` and `Executive: John` tags.

5 Basic settings

5.1 Configure origin site

In this document, you can get abreast of what is origin site and custom port, and how to configure them.

Introduction

Alibaba Cloud CDN supports three types of back-to-origin domain names: OSS back-to-origin domain name, IP address, and custom domain name. Multiple IP addresses and custom domain names are supported, and back-to-origin priority can be configured when multiple origin sites exist.

When the back-to-origin type is IP address or custom domain name, multiple origin sites are allowed and their priorities are configurable. When multiple origin sites are added, the site priority is "main" and "backup", and the priority is "main">"backup".

All back-to-origin traffic is preferentially directed to higher-priority origin sites. If an origin site fails the health check for three consecutive times, all traffic is directed to lower-priority origin sites. If the origin site passes the health check, it is marked as available again and restored to its the original priority. When all origin sites have the same back-to-origin priority, CDN round-robin takes place.

Origin site health check: 4-layer health check is automatically performed on origin sites every 2.5 seconds.

Main supported scenario: Master/Slave origin site switch.

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**.

CDN

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

Add Domain Name

All Types Choose tag 默认资源组

Enter a domain name.

Domain Name	CNAME	Status	HTTPS	Created At	Tag	Actions
<input type="checkbox"/> .1.finalexam.cn	<input type="radio"/> all.1.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
<input type="checkbox"/> .finalexam.cn	<input type="radio"/> all.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
<input type="checkbox"/> private-test.finalexam.cn	<input type="radio"/> private-test.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 23, 2019 11:35 AM		Manage Copy Configuration More
<input type="checkbox"/> time.finalexam.cn	<input type="radio"/> time.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 18, 2019 1:04 PM		Manage Copy Configuration More
<input type="checkbox"/> cuibai2.2.test.cdnp.com	<input type="radio"/> cuibai2.2.test.cdnp.com.w.kunlungr.com	Stopped	Not enabled	Apr 15, 2019 11:02 AM		Manage Copy Configuration More
<input type="checkbox"/> cuibai.2.test.cdnp.com	<input type="radio"/> multi-channel.1.cdnp.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 **Basic** from the left-side navigation pane, and click **Modify** in the **Origin site info** area.

Back .1.finalexam.cn Running Disable

Basic

Back-to-Origin

Cache

HTTPS

Resource Access Control

Performance Optimization

Advanced Settings

Video Related

WAF

Basic Information

CNAME

all.1.finalexam.cn.w.alikunlun.com

You must add CNAME to your DNS record to start using CDN service; After adding or deleting cname, you may wait about 10 minutes to update cname status affected by local DNS record [How to set?](#)

Create Time

Apr 23, 2019 3:21 PM

Acceleration Region

Mainland China

Modify

Origin site info

Type

IP

Address

1.1.1.1.80

Modify

4. In the **Origin Site Configuration** dialog box, set **Type** , **IP** , and **Port** . (You can set **Port** to **Port 80** , **Port 443** , or **Custom Port** .)

- If you set your **Origin site information** to **IP** or **Origin Site** , pay as the internet-caused traffic.
- If you set your **Origin site information** to **OSS domain name** , pay as the intranet-caused traffic. For more information, see [OSS Pricing Details](#).
- If you have set an **OSS domain name** for your **Origin Site**, still pay as the intranet-caused traffic.

5. Click Confirm.

Origin Site Configuration

✕

Origin Site Information

Type

OSS domain name

IP

Origin Site

IP

Priority

Priorities for multiple origins

1.1.1.1

Main

Add

Port

Port 80

Port 443

Custom Port

Custom port does not support follow back-to-origin protocol, please specify back-to-origin protocol to HTTP or HTTPS first.

Confirm

Cancel



Note:

- Multi-source priority setting is only applicable to the IP address type and origin-site domain name type, but is not applicable to the OSS domain name type. You can select appropriate origin site types and set the reasonable priorities based on your needs.
- Origin site setting is not applicable to acceleration of live video streaming.

Set Custom Port

You can set custom port after enabling the white list. The port number must be between 0 and 65535.

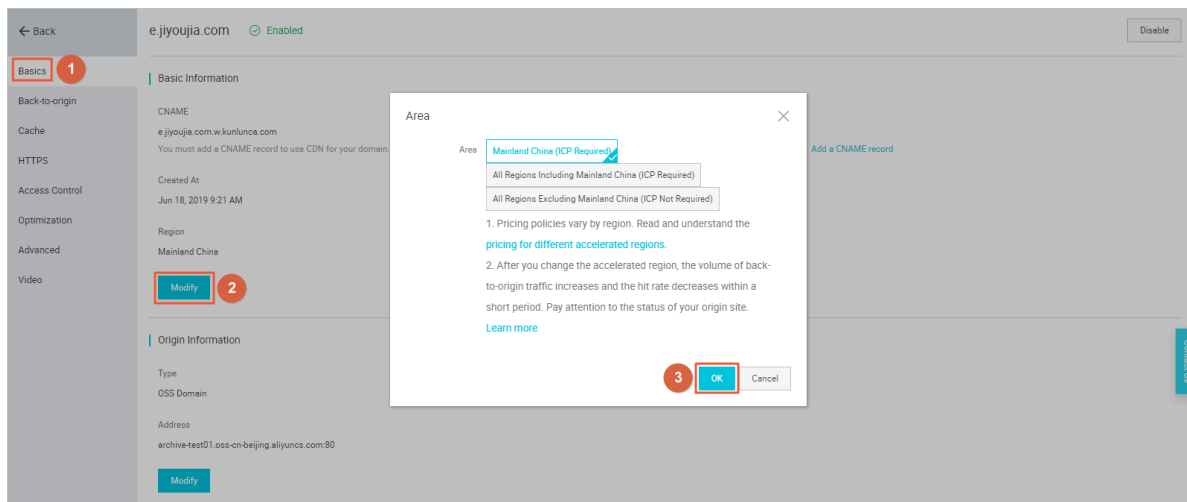
- You cannot set custom port when your static or dynamic protocol is set to Follow.
- Make sure that your back-to-origin protocol and custom port are properly in use if you want to set your back-to-origin protocol to Follow by using OpenAPI.
- Your back-to-origin method will always follow the protocol (HTTP or HTTPS) and custom port you have set by using port, no matter what you have set in console.

5.2 Modify basic information

This topic describes how to modify the basic information of a domain (specifically, the acceleration region) on the Alibaba Cloud CDN console. With this function, you can change the scope of your CDN services.

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 Basic Information section, click Modify.
5. In the Area dialog box, select a region and click OK.



5.3 Modify origin information

This topic describes how to modify the origin information of a domain on the Alibaba Cloud CDN console.

Context

You cannot modify the origin information of a domain whose business type is undefinedundefinedundefined.

Alibaba Cloud CDN supports three types of origin domains: OSS Domain, IP, and Origin Domain. IP allows for multiple IP addresses and Origin Domain allows for multiple domains. If you set Type to IP or Origin Domain, you can also set priorities for multiple origins.

**Note:**

The system automatically performs a four-tier health check to test Port 80 for each origin once per 2.5 seconds. If an origin fails the check for three consecutive times, the system considers it unavailable.

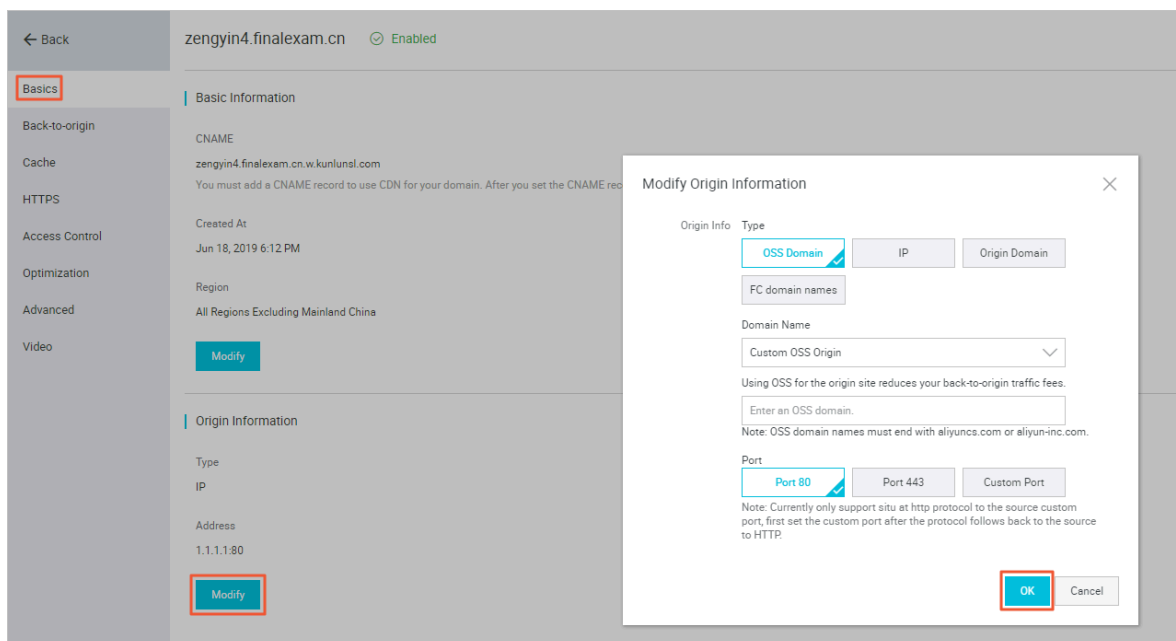
CDN must allow for switchovers between primary and secondary origins. undefined

- When you configure multiple origins and these origins have different priorities, CDN preferably directs requests to the primary origin. If the primary origin fails the health check for three consecutive times, CDN considers the primary origin faulty and then directs requests to the secondary origin. Once the faulty origin passes the health check, CDN considers it available again and restores the priority of this origin to Primary.
- When you configure multiple origins but these origins have the same priority, CDN polls each origin and directs requests to them.

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 Basics.
5. In the Origin Information section, click Modify.

6. In the Modify Origin Information dialog box, set the origin type, IP address, and port number.



The following table describes the Type parameter.

Value	Description
OSS Domain	Allows you to define an OSS origin domain, whose name must end with aliyuncs.com or aliyun-inc.com, for example, xxx.oss-cn-hangzhou.aliyuncs.com. The OSS origin helps you to lower the costs of back-to-origin traffic.
IP	Allows you to configure multiple origin IP addresses and set their priorities.
Origin Domain	Allows you to configure multiple origin domains and set their priorities.

The following table describes the Port parameter.

Value	Description
Port 80	Your origin server returned the requested resources to Port 80 by using HTTP or HTTPS.
Port 443	Your origin server returned the requested resources to Port 443 by using HTTP or HTTPS. If your origin server provides multiple domains for a single IP address, you need to configure Origin SNI. For more information, see Back-to-origin SNI .

Value	Description
Custom Port	<p>Your origin server returned the requested resources to a custom port only by using HTTP. Before you customize a port, you must set Origin Protocol Policy to HTTP. For more information, see Configure an origin protocol.</p> <ul style="list-style-type: none">· If you set Origin Protocol Policy to Follow, you cannot customize a port.· If you set Origin Protocol Policy to Follow through OpenAPI, make sure that your origin protocol and custom port work properly.· If you enable the HTTP or HTTPS origin protocol and customize a port through the Port parameter, your origin server returns the requested resources according to the port settings regardless of the other relevant settings you specify on the Alibaba Cloud CDN console.

7. Click OK.

6 Content back-to-source settings

6.1 Configure an origin host

This topic describes how to configure the origin host of a domain. You can customize the domain name of the server to which CDN routes back-to-origin requests.

Context

An origin host is the domain of the origin server to which CDN routes back-to-origin requests. It determines the IP address to which CDN routes back-to-origin requests. An origin host also determines the server associated with a specific IP address to which CDN routes back-to-origin requests.



Note:

- If your origin is associated with multiple domains or servers, you must specify a domain for receiving back-to-origin requests.
- If you do not specify a domain, back-to-origin requests cannot be routed.

The differences between an origin and an origin host are as follows:

- An origin determines the IP address to which CDN routes back-to-origin requests.
- An origin host determines the server associated with a specific IP address to which CDN routes back-to-origin requests.

The domain types available for an origin host are CDN Domain, Origin Domain, and Custom Domain:

- If your origin type is IP, the default domain type of your origin host is CDN Domain.
- If your origin type is OSS Domain, the default domain type of your origin host is Origin Domain.

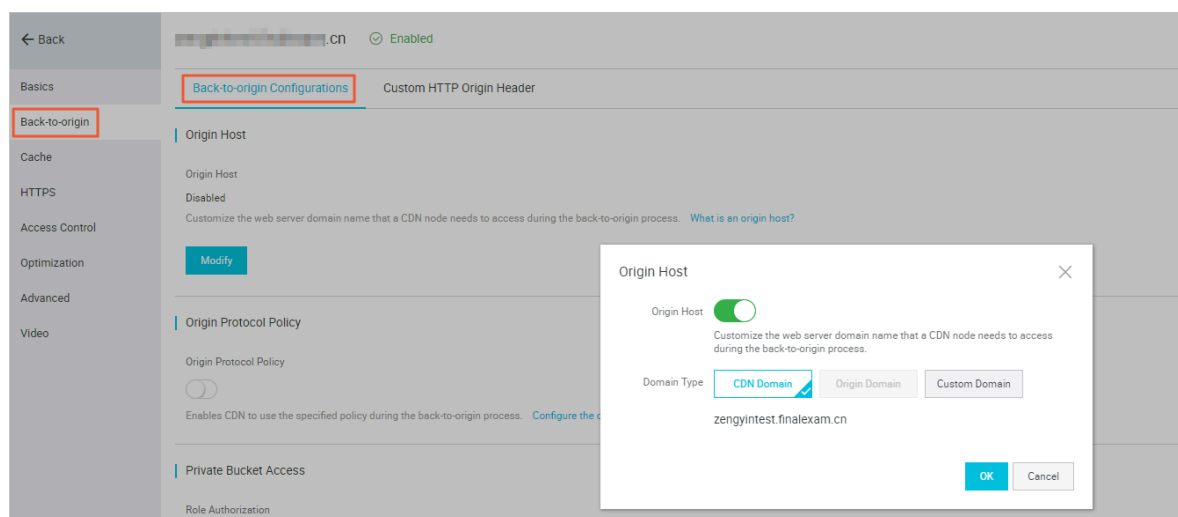
Examples:

- If your origin is `www . a . com` and your origin host is `www . b . com`, CDN routes back-to-origin requests to `www . a . com` but the IP address that CDN obtains through IP address resolution is `www . b . com`.

- If your origin is `1 . 1 . 1 . 1` and your origin host is `www . b . com`, CDN routes back-to-origin requests to `1 . 1 . 1 . 1`, which maps the `www . b . com` origin server on the host.

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 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 Back-to-origin Configurations tab and in the Origin Host section click Modify.
6. Turn on the Origin Host switch, select a domain type, and click OK.



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.

CDN

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.

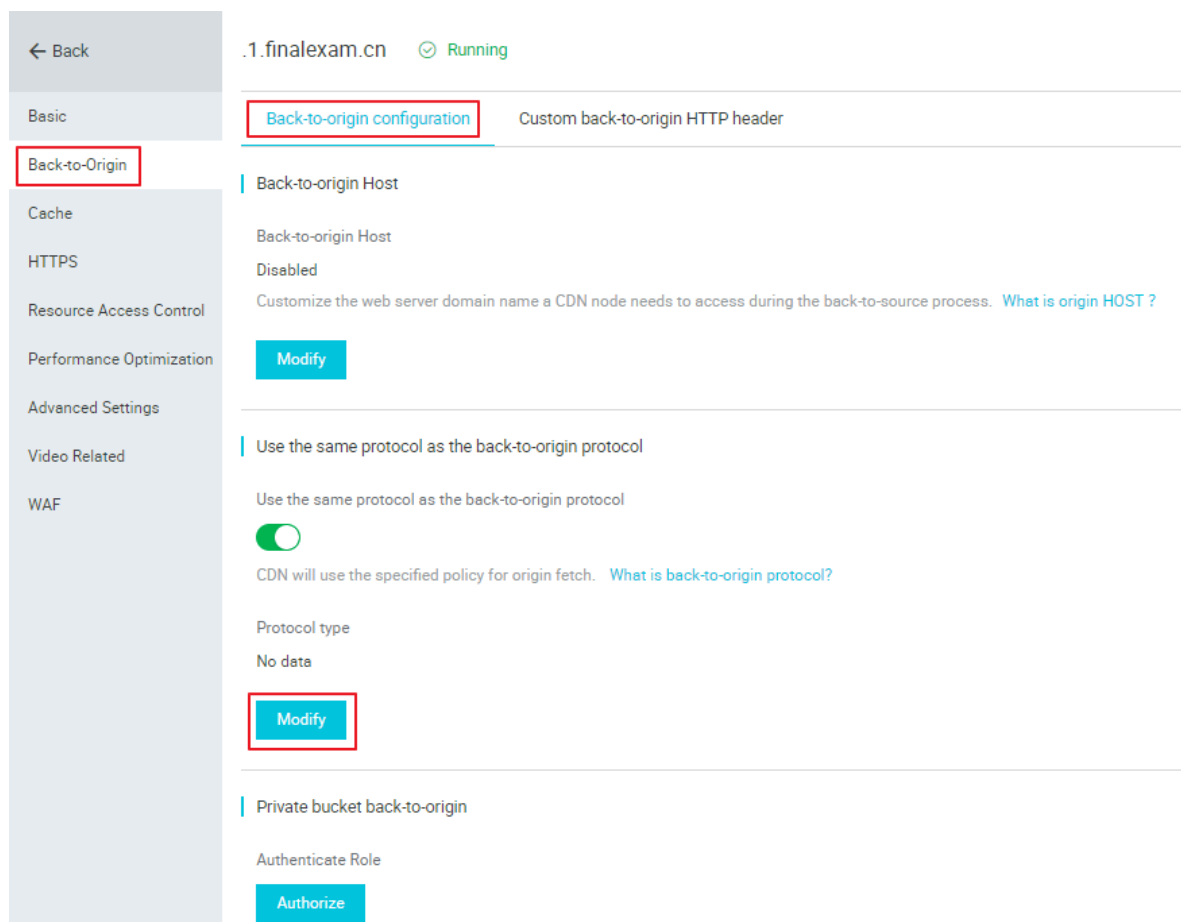
Domain Names

Add Domain Name All Types Choose tag 默认资源组

Enter a domain name.

<input type="checkbox"/>	Domain Name	CNAME	Status	HTTPS	Created At	Tag	Actions
<input type="checkbox"/>	.1.finalexam.cn	all.1.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
<input type="checkbox"/>	.finalexam.cn	all.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
<input type="checkbox"/>	private-test.finalexam.cn	private-test.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 23, 2019 11:35 AM		Manage Copy Configuration More
<input type="checkbox"/>	time.finalexam.cn	time.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 18, 2019 1:04 PM		Manage Copy Configuration More
<input type="checkbox"/>	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
<input type="checkbox"/>	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.



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



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 corresponding 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

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

CDN

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.

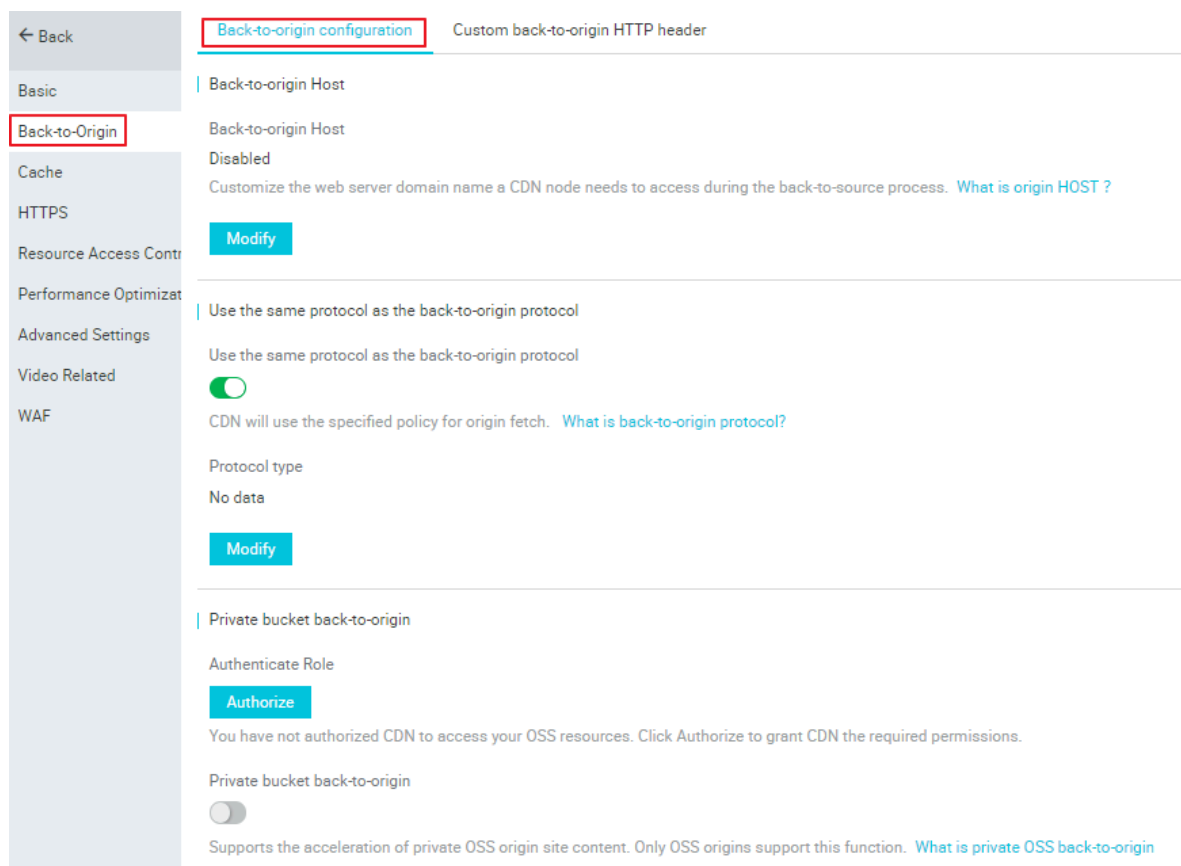
Domain Names

Add Domain Name All Types Choose tag 默认资源组

Enter a domain name.

<input type="checkbox"/>	Domain Name	CNAME	Status	HTTPS	Created At	Tag	Actions
<input type="checkbox"/>	.1.finalexam.cn	ali.1.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
<input type="checkbox"/>	.finalexam.cn	ali.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 23, 2019 3:21 PM		Manage Copy Configuration More
<input type="checkbox"/>	private-test.finalexam.cn	private-test.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 23, 2019 11:35 AM		Manage Copy Configuration More
<input type="checkbox"/>	time.finalexam.cn	time.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 18, 2019 1:04 PM		Manage Copy Configuration More
<input type="checkbox"/>	cuihai2.2.test.cdnpe.com	cuihai2.2.test.cdnpe.com.w.kunlungr.com	Stopped	Not enabled	Apr 15, 2019 11:02 AM		Manage Copy Configuration More
<input type="checkbox"/>	cuihai.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.



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

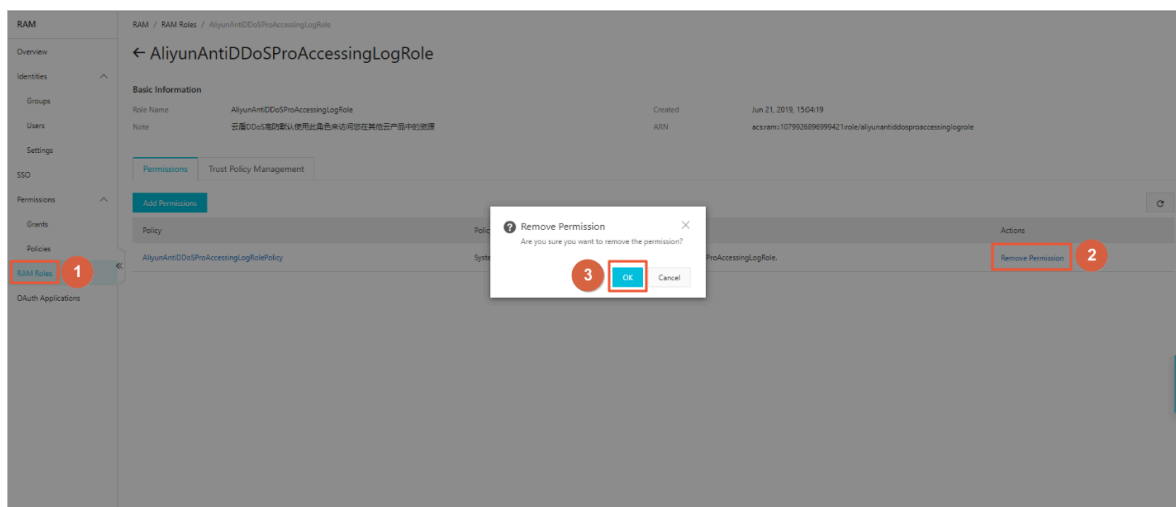


Note:

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

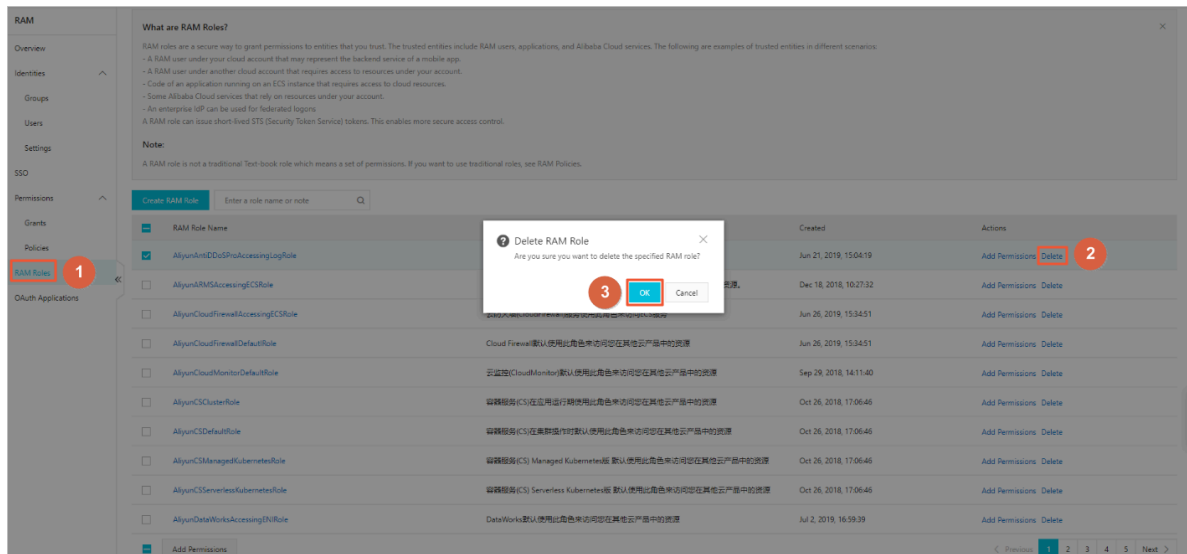
Procedure

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.



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.



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?

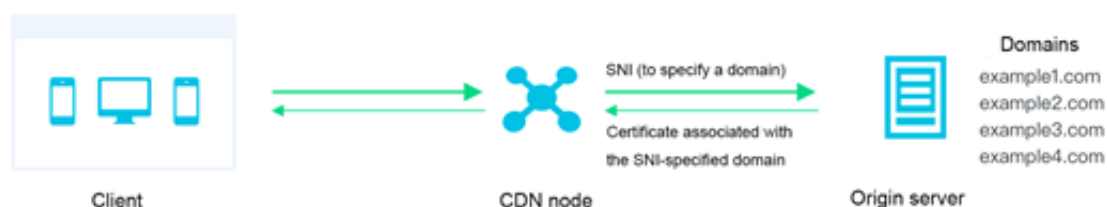
If your origin server uses one IP address to provide HTTPS services for multiple domains and port 443 is specified for receiving back-to-origin traffic on your CDN (CDN nodes communicate with your origin server according to HTTPS), you need to enable back-to-origin SNI and specify the requested domains.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

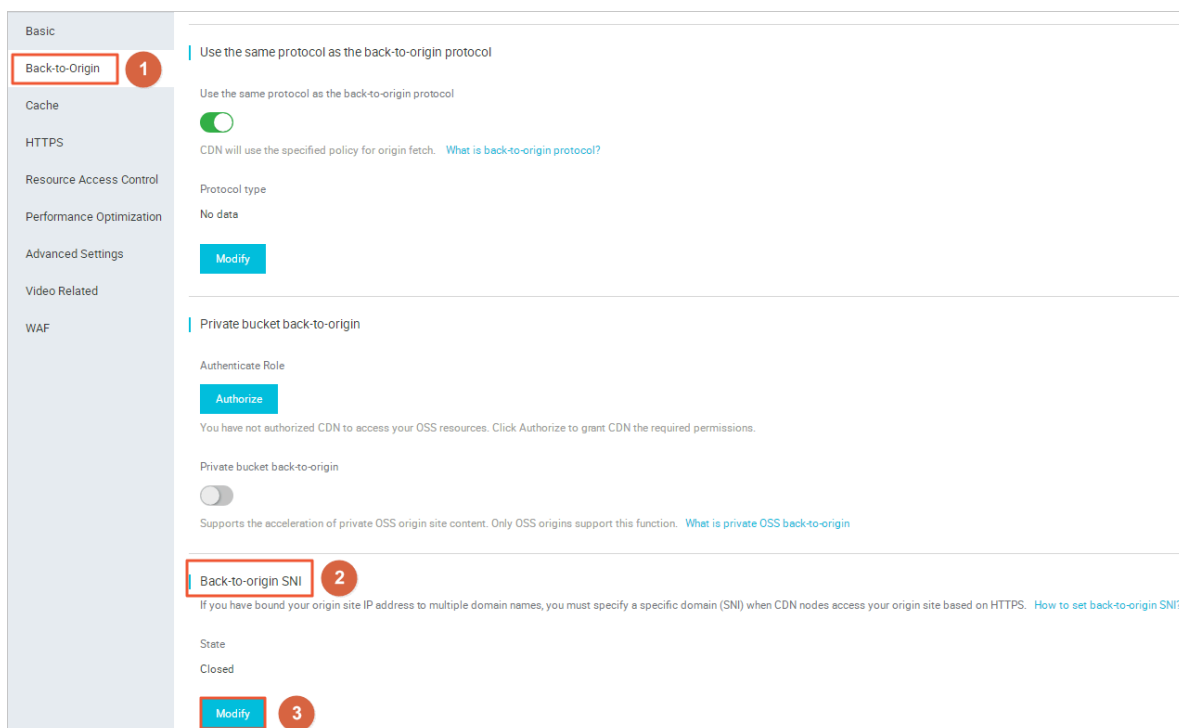


1. The CDN node requests to access the origin server according to HTTPS, where the requested domain name is specified in the SNI.
2. After receiving the request, the origin server sends the certificate associated with the requested domain to the CND node.
3. After receiving the certificate, the CDN node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

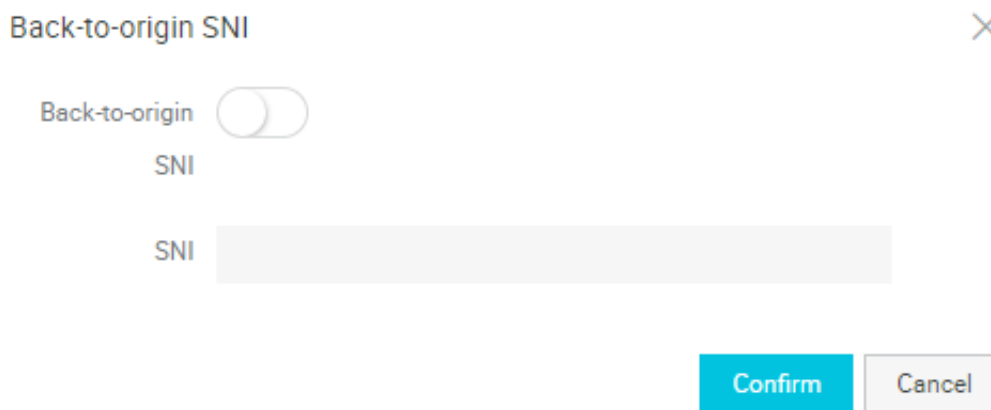
Procedure

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.



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**.



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.

OK Cancel

6.7 Set the origin request timeout period

This topic describes how to set the origin request timeout period. Specifically, the period of time in which CDN nodes wait for back-to-origin requests. The default

timeout period is 30 seconds. Note that if a CDN node does not receive any requests from an origin within the specified timeout period, the CDN node disconnects itself from the origin.

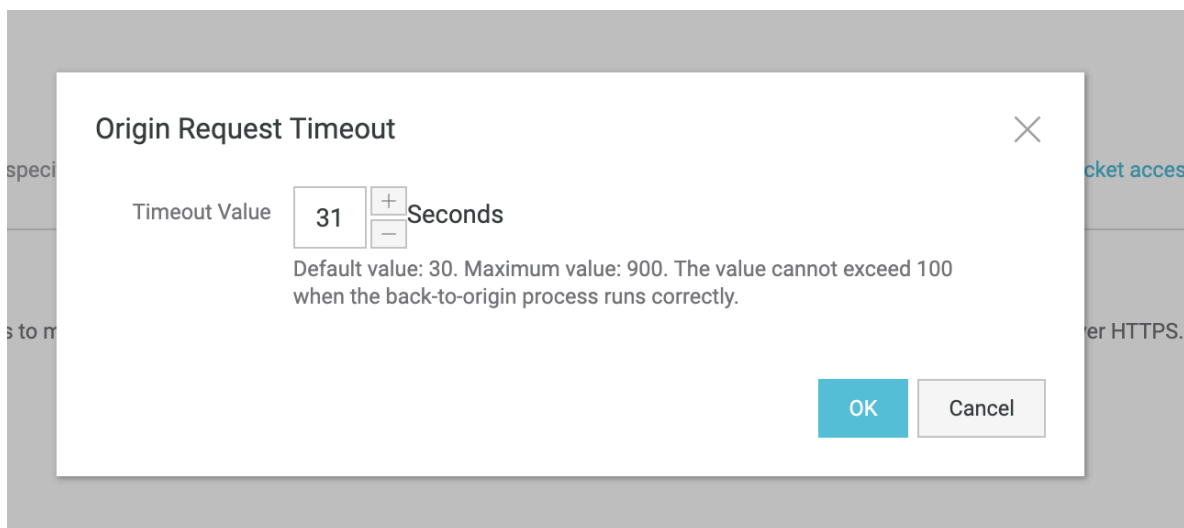
Procedure

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 click Manage in the Actions column.
4. In the left-side navigation pane, click Back-to-origin.
5. In the Origin Request Timeout section, click Modify.
6. In the Origin Request Timeout dialog box, set Timeout Value .



Note:

- The timeout period of back-to-origin requests directed to CDN nodes does not exceed 100 seconds.
- You must set the timeout period to a value less than or equal to 900 seconds.



7. Click OK.

7 Node Cache Settings

7.1 Create a cache expiration rule

This topic describes how to create a cache expiration rule. In each rule, you can set the expiration time of static resources, which are cached in a specified directory or in files with specified file extensions. In addition, you can set the priority of each rule.

Prerequisites

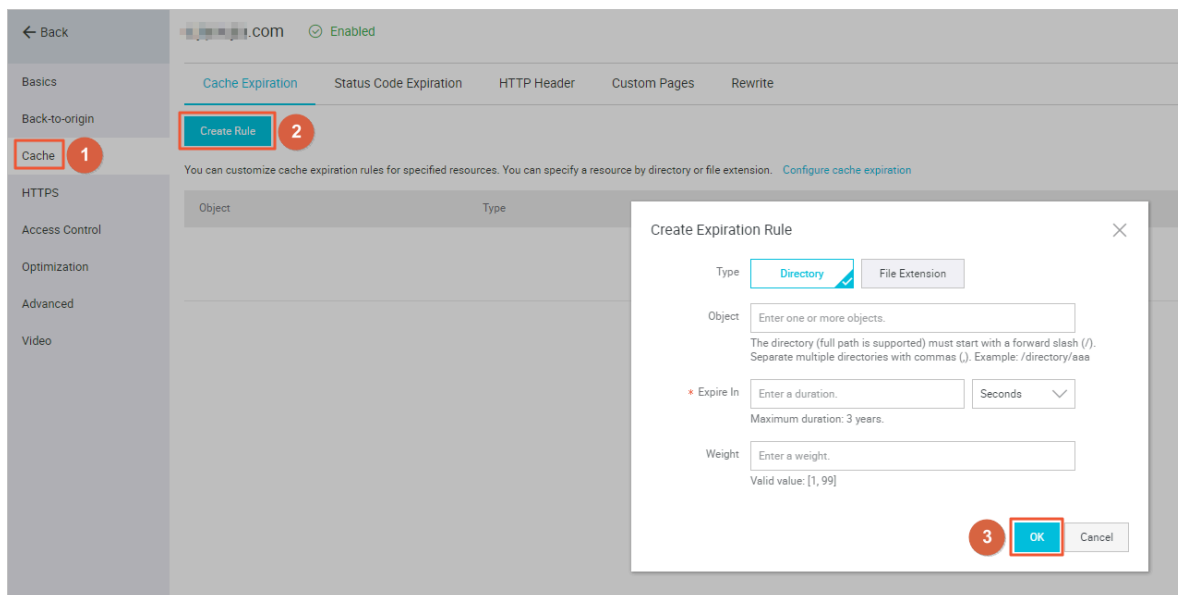
If the following requirement is met, you can follow the steps described in this topic:

The same file name is not used to update content on your origin. If you need to update content on your origin, we recommend that you name the content files by version, for example, *img - v1 . 0 . jpg* and *img - v2 . 1 . jpg* .

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 Cache.
5. On the Cache Expiration tab page, click Create Rule.

6. In the Create Expiration Rule dialog box, select a rule type, set the other parameters as prompted, and click OK.



Parameter	Description
Type	<ul style="list-style-type: none"> Directory: specifies resources cached in a specific directory. File Extension: specifies resources cached in files with specific file extensions.
Object	<ul style="list-style-type: none"> When Type is set to Directory, enter a directory name in the Object field. The directory name must start with a slash (/), for example, <code>/ directory / aaa</code>. When Type is set to File Extension, enter one or more file extensions in the Object field. Multiple file extensions must be separated by using commas (,), for example, <code>jpg,txt</code>.

Parameter	Description
Expire In	<p>Specifies the expiration time of the cached resources. The resource retention duration can reach up to three years. We recommend that you set this parameter in compliance with the following rules:</p> <ul style="list-style-type: none">· Specify a retention duration of one month or longer for static files such as images and applications that are not frequently updated.· Specify a retention duration shorter than one month for static files such as files in JS and CSS format that are frequently updated.· Do not cache dynamic files such as files in PHP, JSP, and ASP formats.

Parameter	Description
Weight	<p>Specifies the priority of the rule.</p> <div>  Note: <ul style="list-style-type: none"> The value of this parameter ranges from 1 to 99. A greater value indicates a higher priority, which in turn means that the rule takes effect preferentially. We recommend that you do not set the same priority for different rules. If different rules have the same priority, they take effect in a random sequence. </div> <p>For example, if you set the following three rules for the <code>example . aliyun . com</code> domain, Rule 1 takes effect preferentially over the other two rules:</p> <ul style="list-style-type: none"> Rule 1: Type is set to File Extension, Object is set to <code>jpg,png</code>, Expire In is set to 1 Months, and Weight is set to 90. Rule 2: Type is set to Directory, Object is set to <code>/ www / dir / aaa</code>, Expire In is set to 1 Hours, and Weight is set to 70. Rule 3: Type is set to Directory, Object is set to <code>/ www / dir / aaa / example . php</code>, Expire In is set to 0 Seconds, and Weight is set to 80.

7. Click OK.

To modify or delete a rule, find the rule and click Modify or Delete in the Actions column.

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.

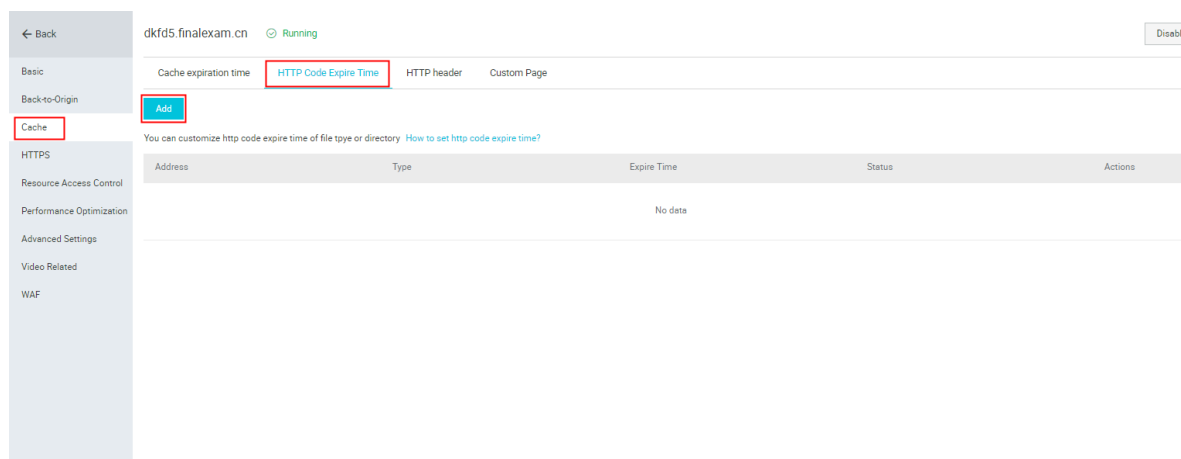


Note:

- 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_ttl` 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.



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?](#)

Confirm

Cancel

Type	Remarks
Directory	<ul style="list-style-type: none"> Add a single directory (full paths are supported). The directory must start with a forward slash (/) (for example, / directory / aaa). Status codes of the 2xx and 3xx formats are not allowed.
File extension	<ul style="list-style-type: none"> 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 2xx and 3xx 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 Create an HTTP header

This topic describes how to create an HTTP header.

Context

The HTTP header fields describe the requested resources and the client or server behavior, and also define the operating parameters of an HTTP transaction.

HTTP header fields include General-header, Client Request-header, and Server Response-header fields. The following table describes the 10 HTTP header parameters provided by Alibaba Cloud CDN. You can define the value of each parameter.

Parameter	Description
Content-Type	Specifies the content type of the objects requested by a client program.
Cache-Control	Specifies the caching policy that a client program follows when initiating requests and making responses.
Content-Disposition	Specifies the default file name provided by a client program when the requested content is saved as a file.
Content-Language	Specifies the language of the objects requested by a client program.
Expires	Specifies the expiration time of the objects requested by a client program.
Access-Control-Allow-Origin	Specifies the domains from which cross-domain requests are allowed.
Access-Control-Allow-Headers	Specifies the fields that are allowed in cross-domain requests.
Access-Control-Allow-Methods	Specifies the cross-domain request methods that are allowed.

Parameter	Description
Access-Control-Max-Age	Specifies the duration in which the response result can be retained and 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.

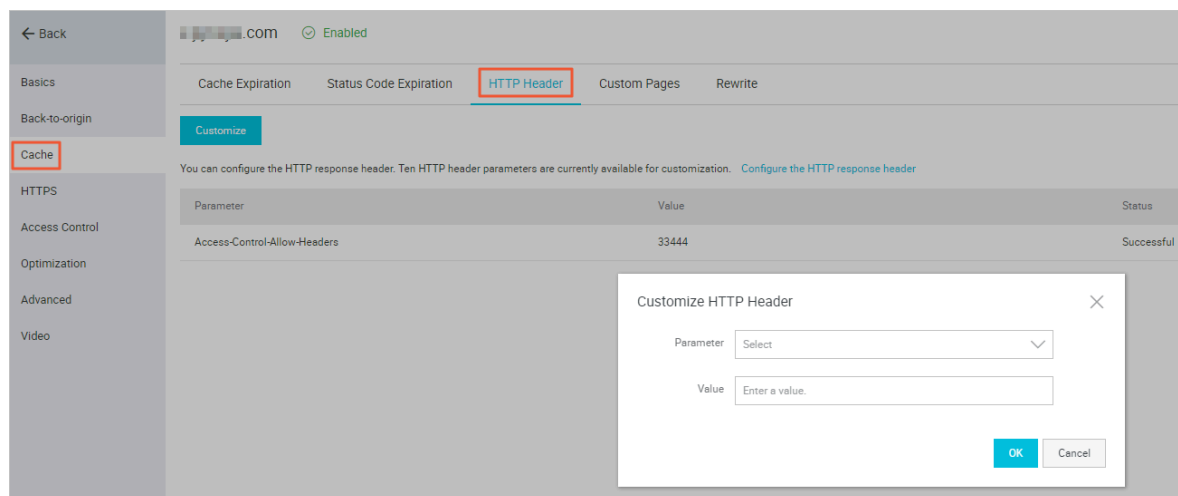
When you create an HTTP header, note the following limits:

- The HTTP response header configurations of a domain affect the response behavior of all client programs such as browsers in this domain. However, the configurations do not affect the behavior of the cache server.
- Alibaba Cloud CDN supports only the 10 HTTP header parameters described in the preceding table. If you require other HTTP header parameters, open a ticket at [Alibaba Cloud Support and Services](#).
- The `Access - Control - Allow - Origin` parameter must be set as a specific domain name or `*` to allow cross-domain requests.
- Alibaba Cloud CDN does not support wildcard domains.

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 Cache.
5. On the HTTP Header tab page, click Customize.

6. In the Customize HTTP Header dialog box, select a parameter and set the parameter value.



7. Click OK.

To modify or delete an HTTP header, find the HTTP header and click **Modify** or **Delete** in the **Actions** column.

7.4 Customize an error page

This topic describes how to customize an error page. When a client requests a web service through a browser, the website hosting server generates a 404 Not Found page by default if the requested URL does not exist. However, you may not like the way the 404 Not Found page looks. To improve user experience, you can associate URLs with errors that are carried in HTTP or HTTPS responses, then the website hosting server generates the corresponding web pages when these errors are returned.

Context

Alibaba Cloud CDN provides two types of error pages: default pages and custom pages. The differences between the default page and custom page are as follows:

- **Default page:** When the HTTP response carries the 404 error, the server generates the 404 Not Found
- **Custom page:** When the HTTP response carries the 404 error, the server generates the custom page.

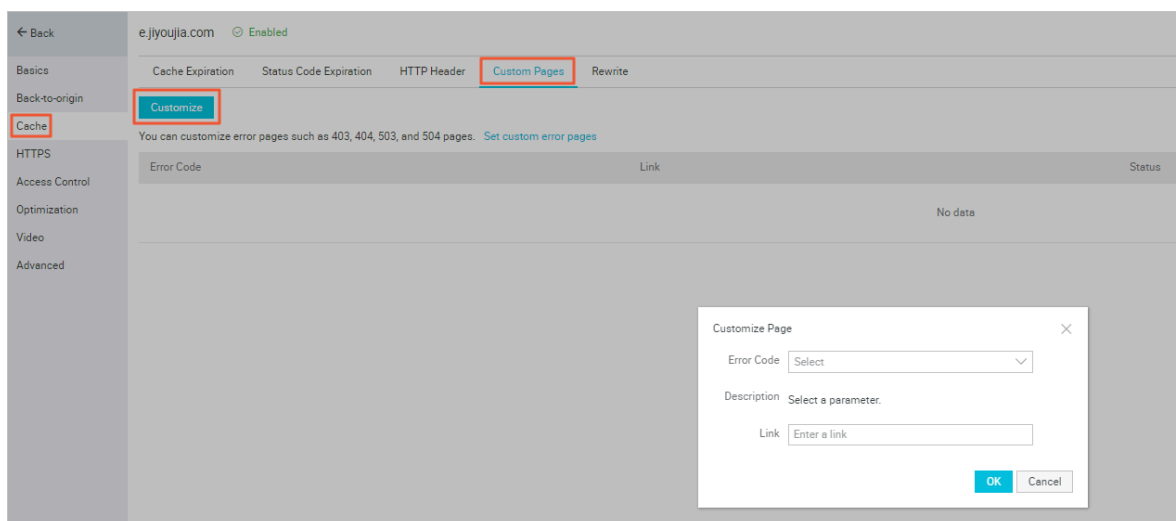


Note:

- Default pages are considered Alibaba Cloud public resources and therefore are free of charge.
- Custom pages are considered personal resources and therefore are charged.

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 Cache.
5. On the Custom Pages tab page, click Customize and in the displayed dialog box set the parameters as prompted.



Assume that you want to store the `error404 . html` page for the 404 error together with other static files to the origin domain and access this web page through the accelerating domain `exp . aliyun . com` . Then you only need to select 404 from the Error Code drop-down list and enter the URL (`http :// exp . aliyun . com / error404 . html`) of the accelerating domain in the Link field.

6. Click OK.

After the custom page is created, you can click Modify or Delete in the Actions column to modify or delete the custom page.

7.5 Rewrite

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

Context

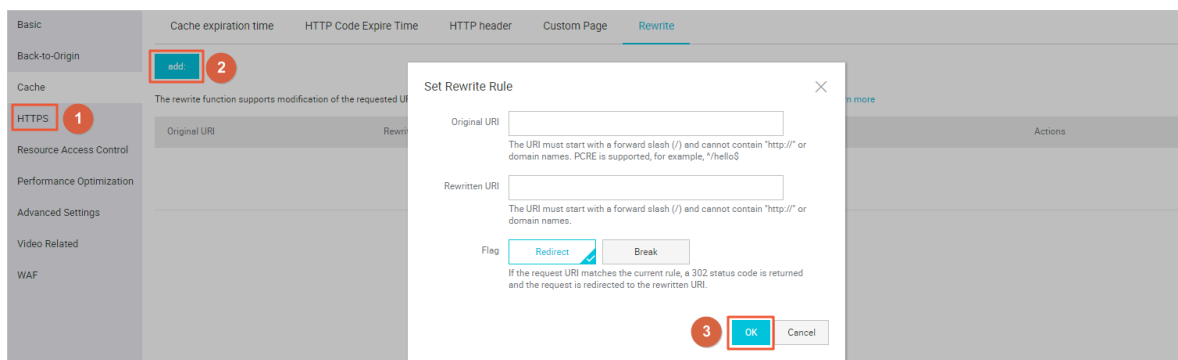
With the rewrite function, you can configure multiple rewrite rules. With each rewrite rule, you can specify the requested Uniform Resource Identifier (URI) and the destination URI to which a request is redirected. For example, if a client requests to visit `http://example.com` through HTTP, you can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



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

8 HTTPS Acceleration

8.1 What is HTTPS acceleration?

This topic provides an overview of HTTPS acceleration, including its working principles, benefits, and considerations. HTTPS acceleration allows HTTPS-based encryption between clients and CDN nodes, ensuring data security during transmission.

What is HTTPS?

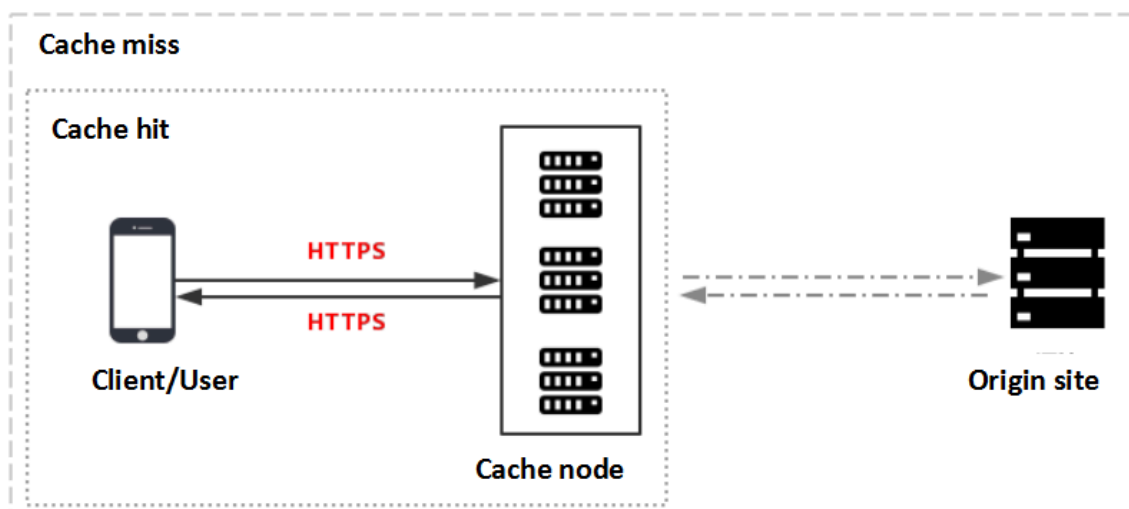
Hypertext Transfer Protocol (HTTP) transmits content in plaintext and does not encrypt data in any form. As an extension of HTTP, Hypertext Transfer Protocol Secure (HTTPS) is an HTTP channel designed to enhance security. Secure Sockets Layer (SSL) or Transport Layer Security (TLS) is used as a sublayer under the regular HTTP application to authenticate users and encrypt data. HTTPS is widely used for services such as payment transactions that involve sensitive user data.

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

Working principles

After you enable HTTPS in the Alibaba Cloud CDN console, the requests from your client to Alibaba Cloud CDN nodes are encrypted by using HTTPS. The CDN node obtains the requested resources from the origin site and then returns them to your client based on the origin configuration. We recommend that you configure and enable HTTPS on the origin site to allow end-to-end HTTPS encryption.

The following figure shows the HTTPS encryption process.



1. The client sends an HTTPS access request.
2. The server generates a public key and a private key, which you can prepare on your own or apply for from a professional organization.
3. The server sends the public key certificate file to the client.
4. The client parses the certificate file to check the file correctness.
 - If the certificate file is correct, the client generates a random number (key) and uses this key to encrypt and transmit data to the server.
 - If the certificate file is incorrect, the SSL handshake between the client and server fails.

**Note:**

A correct certificate file meets the following requirements: The certificate has not expired. The certificate is issued by a trusted certificate authority (CA). The digital signature of the issuer in the certificate can be decrypted by using the public key of the issuer. The domain name in the certificate is the same as that of the server.

5. The server decrypts the private key to obtain a random number (key).
6. The server uses the obtained key to encrypt and transmit data to the client.
7. The client uses the key to decrypt the data.

Benefits

- HTTPS can defend against the following security threats, which are common in HTTP:
 - Eavesdropping: Third parties can intercept the data.
 - Tampering: Third parties can alter the transmitted data.
 - Spoofing: Third parties can impersonate the identity of a user.
 - Hijacking: includes traffic hijacking, link hijacking, and DNS hijacking.
- Benefits of HTTPS transmission:
 - HTTPS encrypts sensitive information such as session IDs and cookies before transmission, preventing security threats caused by sensitive information leakage.
 - HTTPS checks data integrity during transmission to protect your DNS or content against man-in-the-middle (MITM) attacks such as hijacking and tampering.
 - HTTPS is the new norm. An increasing number of mainstream browsers such as Google Chrome and Mozilla Firefox automatically identified HTTP websites as insecure in 2018. 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.
 - Major network service providers such as Google and Baidu prioritize HTTPS websites in the search results. Additionally, mainstream browsers must support HTTPS to support HTTP/2. HTTPS is the more reliable choice in terms of security, market presence, and user experience. Therefore, we recommend that you upgrade your access protocol to HTTPS.

Scenarios

The following table describes the five scenarios of HTTPS.



Scenario	Description
Enterprise application	HTTPS protects confidential information such as customer relationship management (CRM) data and enterprise resource planning (ERP) data on enterprise websites from being hijacked or intercepted.

Scenario	Description
Government website	HTTPS protects authoritative information on government websites against vulnerabilities such as phishing and hijacking. Leakage of such information may cause the public trust in the government to decline.
Payment system	HTTPS protects sensitive data such as the customer names and phone numbers that are involved in payment transactions against hijacking and spoofing. If HTTPS is not used, the customer may receive information about the order they have placed and may be tricked into making a duplicate payment, which causes losses to both the customer and the enterprise.
API	APIs use HTTPS to encrypt important information such as sensitive data and crucial operation instructions, so that the information cannot be hijacked.
Enterprise website	HTTPS makes users feel more secure. Web browsers display a green lock icon in the address bar for websites with domain validated (DV) and organization validated (OV) certificates. The enterprise name is displayed together with the green lock for websites with extended validated (EV) certificates.

Considerations

The following table describes the considerations for using the HTTPS acceleration function.

Category	Consideration
Configuration	<p>The following types of business support HTTPS acceleration:</p> <ul style="list-style-type: none"> - Images and small files <p>Web portals, e-commerce websites, news websites and applications , government or enterprise official websites, and entertainment or gaming websites and applications.</p> <ul style="list-style-type: none"> - Large file download <p>Video or audio applications and websites that provide content for users to download.</p> <ul style="list-style-type: none"> - VOD <p>Websites and applications that provide audio and video content such as movies, online education, news, and social networking.</p> <ul style="list-style-type: none"> - Live Streaming <p>Websites and live streaming platforms of industry verticals that provide live streaming content such as interactive online education, esports, talent show, or event broadcasts.</p> <ul style="list-style-type: none"> • You can enable HTTPS for wildcard domains. • You can enable or disable HTTPS acceleration as needed. - When HTTPS acceleration is enabled: You can modify certificates. The system supports HTTP and HTTPS requests by default. In addition, you can Enable force redirect to customize request methods. - When HTTPS acceleration is disabled: The system no longer supports HTTPS requests and no longer keeps certificate or private key information. To enable certificates again, you must re-upload the certificates or private keys. For more information, see Configure HTTPS certificates. • You can view certificates but not private keys. Keep certificate-related information safe. • You can update certificates. However, exercise caution when performing this operation. HTTPS certificates take effect within one minute after they are updated.

Category	Consideration
Billing	<p>HTTPS acceleration is a value-added service. After you enable HTTPS, HTTPS requests incur additional fee. For more information about the billing standards, see Static HTTPS Requests.</p> <div>  Note: The fee is separately charged based on HTTPS requests and is not covered by the CDN data transfer plan. Before you enable HTTPS acceleration, make sure that your account has a sufficient balance. If your balance becomes empty, the CDN services are suspended. </div>
Certificates	<p>You need to upload certificate and private key files in <code>PEM</code> format for domains for which HTTPS acceleration is enabled.</p> <div>  Note: The Tengine Web server used by CDN is designed based on the NGINX Web server architecture, and therefore supports only certificate files in the NGINX-compatible <code>PEM</code> format. For more information, see Overview of certificate formats. </div> <ul style="list-style-type: none"> • The uploaded certificate file must match the private key. Otherwise, the authentication fails. • A private key cannot carry a password. • Only SSL and TLS handshakes carrying SNIs are supported.

Related functions

You can enable the following functions as needed to increase data security.

Function	Description
Configure HTTPS certificates	Allows for HTTPS acceleration.
Enable HTTP/2	HTTP/2 is the most advanced HTTP protocol, which is used by major browsers such as Google Chrome, Internet Explorer 11, Safari, and Mozilla Firefox.
Enable force redirect	Supports force redirects on original request methods of end users.
Configure TLS	Helps to ensure communication security and data integrity.

Function	Description
Configure HSTS	Forces clients such as browsers to establish HTTPS connections with servers, reducing hijacking risks in the first access requests.

8.2 Overview of certificate formats

This topic provides an overview of the certificates supported by Alibaba Cloud CDN and how to convert various certificates into PEM formats. To access resources through HTTPS secure acceleration, you must configure an HTTPS certificate.

Root CA certificates

Root CA certificates are issued by root CAs including Apache, IIS, Nginx, and Tomcat. Each root CA certificate is unique. Alibaba Cloud CDN uses root CA certificates issued by Nginx. A .crt file contains certificate information and a .key file contains private key information.

A root CA certificate must conform to the following rules:

- It starts from ----- BEGIN CERTIFICATE ----- and ends with ----- END CERTIFICATE -----.
- All lines except the last line must contain 64 characters.
- The last line contains 1 to 64 characters.

The following figure shows an example certificate in PEM format when your system runs a Linux operating system.

[illegible]

Intermediate CA certificates

A certificate file issued by an intermediate CA includes multiple certificates. You must copy and paste them at the end of the server certificate file.



Note:

In most cases, the rules for combining the server certificate with the intermediate certificates are specified when the intermediate CA issues the certificates. Read the rules before you combine the certificates.

The chain of certificates issued by an intermediate CA is as follows:

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

The certificates in the chain must conform to the following rules:

- Blank lines are not allowed between certificates.
- Each certificate must be in the specified format.

RSA private keys

An RSA private key must conform to the following rules:

- In the private key `openssl genrsa - out privateKey . pem 2048` generated on your computer, `privateKey . pem` is your private key file.
- The private key starts with `----- BEGIN RSA PRIVATE KEY -----` and ends with `----- END RSA PRIVATE KEY -----`.
- All lines except the last line must contain 64 characters.
- The last line contains 1 to 64 characters.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAzVSSChH67bmT8mFykAxQ1tKCYukwBiWZwk0StFEbTWHy8K
tTHSFD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A
Xw9SgrqFJMjclva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ
/FD0XXyuWoqaIePZtK9Qn957ZEPhtUpVZuhS3409DDM/tJ3Tl8aaNYWhrPBc0
jNcz0Z6XQGF1rZG/Ve520GX6rb5dUYpdcfXzN5WM6xYg8a1L7UHDHPI4AYsatdG
z5TMPnmEf8yZPUYudTLxgMVAovJr09Dq+5Dm3QIDAQBAoIBAGl68Z/nnFyRHRFi
laF6+Wen8ZvNqkm0hAMQwIjh1Vplf174//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35
cgQ93Tx424WGPcWUshSfxewfbAYGf3ur8W0xq0uU07BAxaKHNCmNG7dGyo1UowRu
S+yXlrpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2
06W/zHZ4YAxwkTYLKGHjoieYs111ah1AJvICVgTc3+LzG2pIpM7I+K0nHC5eswM
i5x9h/OT/ujZsyX9P0PaAyE2bqy0t080tGexM076Ssv0KVhKFvWjLUnhf6WcqFCD
xqhhxkECgYEA+PftNb6eyXl+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhgqHu0edU
ZXIHrJ9u6B1XE1arpijVs/WHmFhYSTm6DbdD7S1tLy0BY4cPTRhziFTKt8AkIXMK
605u0UiWsq0Z8hn1X141ox2cW9ZQa/Hc9udeyQotP4NsMJWgpBV7tC0CgYEAwwNf
0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzFEG8/AR3Md2rhMZi
GnJ5fdfe7uY+JsQfX2Q5JjwTadlBW4led0Sa/ukRa04UzVgnYp2aJKxtuWffvVbU
+kf728ZJRA6azSLvGmA8hu/GL6bgfU3fkSkw03ECgYBpYK7TT7JvvnAERMtJf2yS
ICRkbQaB3gPSe/LCgzy1nh4F0UbNtGeuowLAZR0wrz7X3TZqHEDcYoJ7mK346of
QhGLITyoeHkbYkAUTq038Y04EKH6S/IzMzB0frXiPKg9s8UKQzkU+GSE7ootli+a
R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUhKIKcP/+xn
R3kVL06MZCfAdqirAjiQWapKh9Bxbp2eHCrB81MFAWLRQSl0k79b/jVmTZMC3upd
EJ/iSWjZKPbw7hCFAeRtPhxyNTJ5idEiu9U8EQid8111giPgn0p3sE0HpDI89qZX
aaiMEQKBgQDK2bsnZE9y0ZWhtEu94vziKFrSkJMGH8pLaTiliw1iRhRYWJysZ9
BOIDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcv0Bh5Hx0yy23m9hFRzfDeQ7z
NTKh193HHF1joNM81LHFyGRFEWWrroW5gfBudR6USRnR/6iQ11xZXw==
-----END RSA PRIVATE KEY-----
```

If your private key does not comply with the preceding rules, for example, -----

BEGIN PRIVATE KEY ----- or ----- END PRIVATE KEY -----), you can convert it as follows:

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

Then, upload the new_server_key.pem private key file together with the certificate file.

Convert certificate formats

HTTPS only supports certificates in PEM format. If your certificates are not in PEM format, you must convert them into PEM formats. We recommend that you use OpenSSL to convert certificate formats. The following are methods for converting various certificates into PEM formats:

- Certificates in DER format

These certificates are typically used for Java.

- Convert a certificate from DER to PEM formats as follows:

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

- Convert a private key from DER into PEM formats as follows:

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

- Certificates in P7B format

These certificates are typically used for Windows Server and Tomcat.

- Convert a certificate from P7B to PEM formats as follows:

```
openssl pkcs7 -print_certs -in incertificate.p7b -out outcertificate.cer
```

You must copy the part starting from ----- BEGIN CERTIFICATE ----- to ----- END CERTIFICATE ----- in the outcertificate.cer certificate to the certificate file.

- A certificate in P7B format does not have a private key. When you configure an HTTPS certificate on the Alibaba Cloud console, you only need to enter the certificate information.

- Certificates in PFX format

These certificates are typically used for Windows Server.

- Convert a certificate from PFX to PEM formats as follows:

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

- Convert a private key from PFX to PEM formats as follows:

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

8.3 Configure HTTPS certificates

This topic describes how to configure HTTPS certificates. After you configure HTTP certificates, you must then upload the certificates to CDN in a PEM format to enable HTTP security acceleration.

Prerequisites

- HTTPS certificate files must be in PEM format. For more information, see [Overview of certificate formats](#).
- You must purchase an advanced HTTPS certificate or apply for a free HTTPS certificate at [Alibaba Cloud Security Certificate Service](#).

Context

HTTPS certificates are divided into the following three types based on certification levels:

- Domain Validation (DV) certificates

A DV certificate has a safe lock and authenticates only the ownership of a domain, that is, the content of specified files in the domain or the .txt records related to the domain.

- Organization Validation (OV) certificates

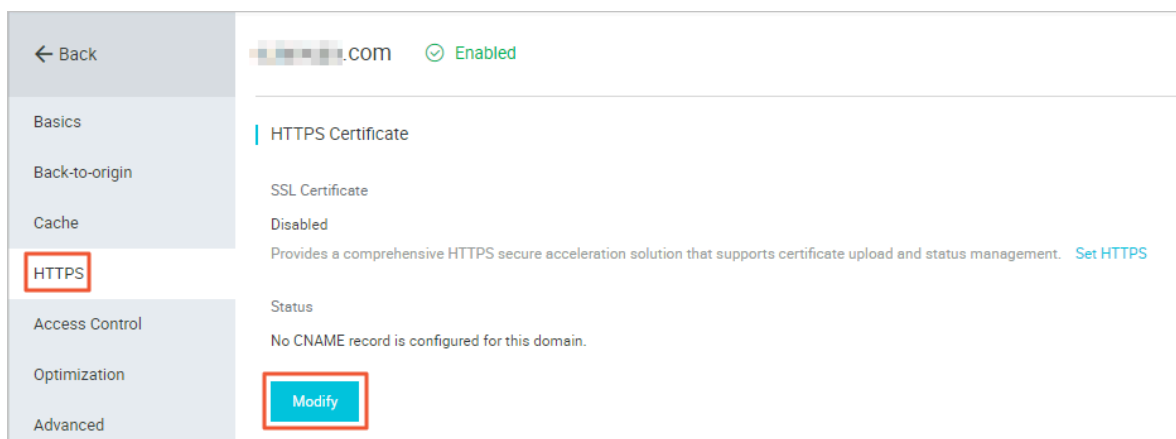
An OV certificate is a standard SSL certificate that verifies the identity of an enterprise. OV certificates feature stricter authentication and a longer authentication period, therefore they are more secure than DV certificates. OV certificates are mostly used in the e-commerce, education, and gaming sectors.

- Extended Validation (EV) certificates

EV certificates follow the guidelines maintained by the Certification Authority Browser Forum, also known as the CA/Browser Forum. They are SSL certificates of the highest certification level. Each EV certificate is identified by an object identifier (OID), which is a complete enterprise name. EV certificates are widely used in such sectors as financial payment and online banking.

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 HTTPS.
5. In the HTTPS Certificate section, click Modify.



6. In the Modify HTTPS Settings dialog box, turn on the HTTPS Secure switch and set the HTTPS certificate parameters.

After you turn on the HTTPS Secure switch, the system displays a message, stating that HTTPS secure acceleration is charged in addition to CDN traffic and asking


you whether you want to enable this function. For more information about HTTPS pricing, see [Value-added service](#).

Parameter	Description
Certificate Type	<p>This parameter has three values:</p> <ul style="list-style-type: none"> Alibaba Cloud Certificate <p>You can apply for a free certificate or purchase an advanced certificate at Alibaba Cloud Security Certificate Service.</p> <ul style="list-style-type: none"> Custom <p>If you cannot find a</p>

Parameter	Description
Certificate Name	When Certificate Type is set to Alibaba Cloud Certificate or Custom, you must enter the certificate name.
Content	When Certificate Type is set to Custom, you must enter the certificate content. For more information, click PEM Encoding Format below the Content field.

Parameter	Description
Private Key	When Certificate Type is set to Custom, you must enter the private key. For more information, click PEM Encoding Format below the Private Key field.

Modify HTTPS Settings

 An updated SSL certificate takes 1 minute to take effect throughout the entire network.

HTTPS Secure

☒

Acceleration

HTTPS secure acceleration is a value-added service. After it is enabled, fees are incurred by HTTPS requests.

Certificate Type

Alibaba Cloud Certificate

Free Certificate

Custom

Alibaba Cloud Security Certificate Service

Certificate Name

Content

PEM Encoding Reference

Private Key

Sensitive information, and the certificate key is invisible

OK

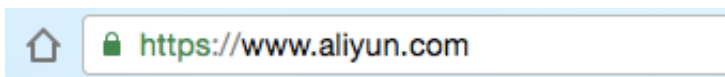
Cancel

7. Click OK.

You can enable, disable, or modify the HTTPS certificate. After the HTTPS certificate is disabled, the system deletes the certificate information. To enable the HTTPS certificate again, you must re-enter the certificate or private key information.

8. Verify that the HTTPS certificate takes effect.

After you update the HTTPS certificate, the updated HTTPS certificate takes effect in 1 minute. To verify that the HTTPS certificate takes effect, use HTTPS to access resources. If the URL in the address bar of the browser displays *https* in green, HTTPS secure acceleration takes effect.



8.4 Enable HTTP/2

This topic describes how to enable HTTP/2.

Prerequisites

An HTTPS certificate is configured. For more information, see [Configure HTTPS certificates](#).



Note:

- If this is the first time that you configure an HTTPS certificate, you must wait until the certificate takes effect before enabling HTTP/2.
- If you disable HTTPS secure acceleration after enabling HTTP/2, HTTP/2 automatically expires.

Context

HTTP/2 also referred to as HTTP 2.0 is the latest version of HTTP, providing optimized performance while maintaining compatibility with the HTTP/1.1 semantics . HTTP/2 is similar to SPDY but differs greatly from HTTP/1.1. Now it is supported by major web browsers such as Google Chrome, Internet Explorer 11.0, Safari, and Mozilla Firefox.

The advantages of HTTP/2 compared to HTTP/1.1 are as follows:

- Binary encoding

Unlike HTTP 1.x that parses data into texts, HTTP/2 splits the data to be transmitted into messages and frames and encodes them into binary formats. Binary encoding makes HTTP/2 more scalable. For example, frames can be introduced to transmit data and instructions.

- Content security

HTTP/2 is designed based on HTTPS to protect content security while maintaining network performance.

- Multiplexing

HTTP/2 allows for multiplexing of multiple concurrent streams on a single connection. Specifically, you can initiate countless requests at the same time over one connection by using a browser, and the server returns the responses to these requests also at the same time. In addition, you can set stream dependencies, based on which the client sends "hints" indicating the importance of a given stream relative to other streams on the same connection, so that resources can be allocated appropriately.

- Header compression

HTTP headers carry large volumes of information, which is transmitted repeatedly. HTTP/2 compresses HTTP headers into HPACK formats, allowing two communication entities each to cache a copy of HTTP header indexes and hence transmit only indexes for duplicate HTTP headers. This increases the transmission speed and efficiency.

- Server push

Like SPDY, HTTP/2 can push messages to clients. Most websites such as Taobao, the most popular shopping website in China, use HTTP/2. You can use Google Chrome to log on to the Alibaba Cloud CDN console and check whether HTTP/2 is enabled.



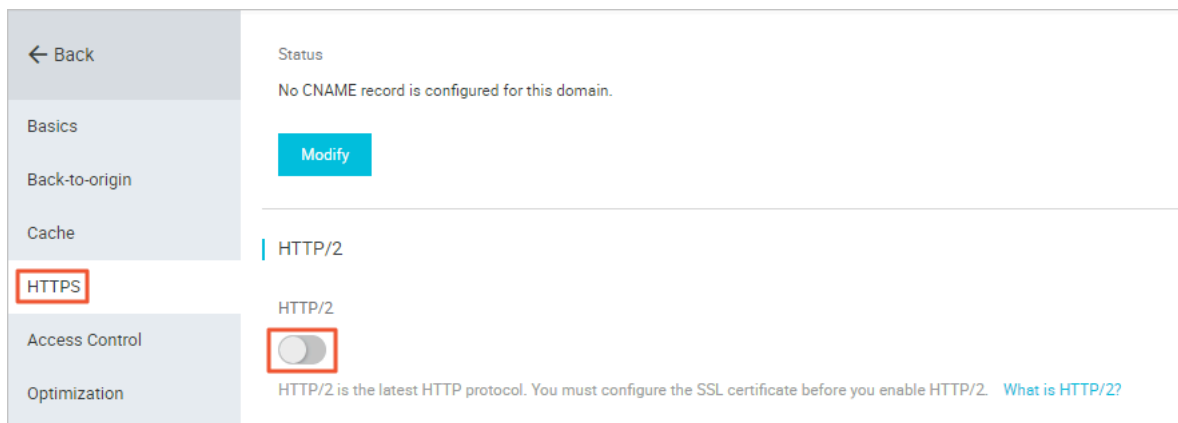
Note:

SPDY is an application layer protocol that Google develops based on TCP. SPDY minimizes network latency to expedite network access and improve user experience. SPDY cannot replace HTTP but serves as an enhancement to HTTP. Like HTTP/2, SPDY also provides multiplexing, request prioritization, and HTTP header compression.

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 HTTPS.
5. In the HTTP/2 section, turn on the HTTP/2 switch.



8.5 Enable Force Redirect

This topic describes how to enable Force Redirect. You can use Force Redirect to customize the settings that redirect users' requests to HTTP or HTTPS.

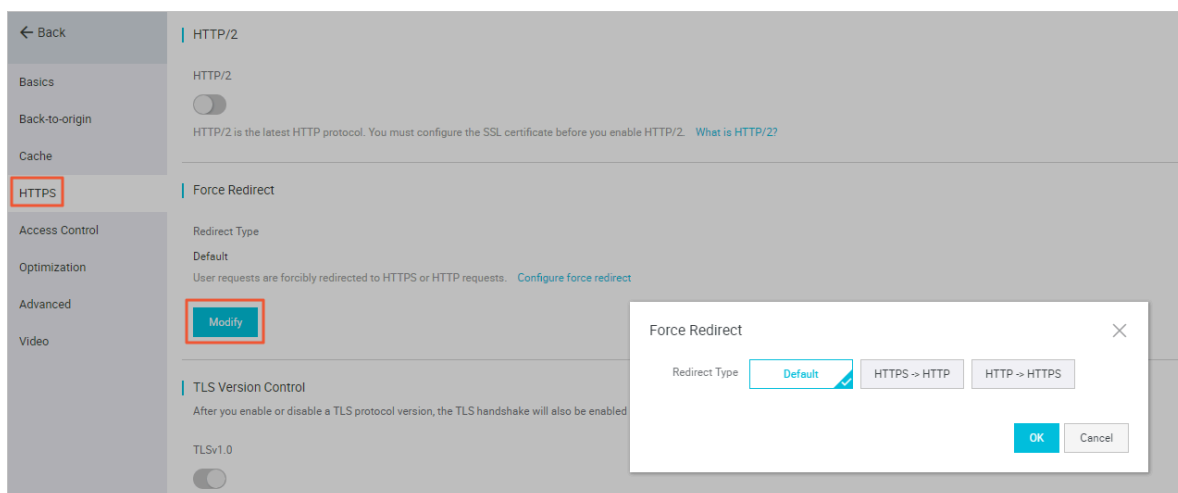
Prerequisites

HTTPS must be configured. For more information, see [Configure HTTPS certificates](#).

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 HTTPS.

5. In the Force Redirect section, click **Modify**.



6. In the Force Redirect dialog box, select a redirect type and click **OK**.

Redirect Type	Description
Default	CDN supports both HTTP and HTTPS requests.
HTTPS -> HTTP	CDN redirects the requests from a client to L1 as HTTP requests.

Redirect Type	Description
HTTP -> HTTPS	CDN redirects the requests from a client to L1 as HTTPS requests.

Assume that you set Redirect Type to HTTP -> HTTPS .

When your client initiates an HTTP request, the server returns a 301 redirect response to redirect the HTTP request as 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>
```

8.6 Configure TLS

This topic describes how to configure Transport Layer Security (TLS) for a domain. You can use the TLS Version Control function of Alibaba Cloud CDN to ensure the security and data security of all Internet services and communications.

Prerequisites

HTTPS certificates are configured. For more information, see [Configure HTTPS certificates](#).

Context

TLS is used at the transport layer to ensure the security and integrity of data transmitted between two entities.

TLS has four versions:

- TLS 1.0

TLS 1.0 was defined in RFC 2246 in 1999 as an upgrade of SSL 3.0. This version is vulnerable to various attacks such as BEAST attacks and POODLE attacks. It is not strong enough to protect today's network connections and does not comply with Payment Card Industry Data Security Standard (PCI DSS). TLS 1.0 supports major browsers including Internet Explorer 6.0 or later, Google Chrome 1.0 or later, and Mozilla Firefox 2.0 or later.

- TLS 1.1

TLS 1.1 was defined in RFC 4346 in 2006 as an update from TLS 1.0. This version fixed some vulnerabilities of TLS 1.0. TLS 1.1 supports major browsers including Internet Explorer 11.0 or later, Google Chrome 22.0 later, Mozilla Firefox 24.0 or later, and Safari 7.0 or later.

- TLS 1.2

TLS 1.2 was defined in RFC 5246 in 2008 and has become the most widely used TLS version. TLS 1.2 supports major browsers including Internet Explorer 11.0 or later , Google Chrome 30.0 or later, Mozilla Firefox 27.0 or later, and Safari 7.0 or later.

- TLS 1.3

TLS 1.3 was defined in RFC 8446 in 2018. As the latest TLS version, TLS 1.3 is faster because it supports the 0-RTT mode. Also, this version is more secure because it only supports perfect forward secrecy key exchange algorithms. TLS 1.3 supports major browsers including Google Chrome 70.0 or later and Mozilla Firefox 63.0 or later.

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 HTTPS.

5. In the TLS Version Control section, enable or disable the TLS versions you want.

← Back

Basics

Back-to-origin

Cache

HTTPS

Access Control

Optimization

Video

Advanced

Status
No CNAME record is configured for this domain.

Modify

HTTP/2

HTTP/2

☐

HTTP/2 is the latest HTTP protocol. You must configure the SSL certificate before you enable HTTP/2. [What is HTTP/2?](#)

Force Redirect

Redirect Type

Default

User requests are forcibly redirected to HTTPS or HTTP requests. [Configure force redirect](#)

Modify

TLS Version Control

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

TLShv1.0

☐

TLShv1.1

☐

TLShv1.2

☐

TLShv1.3

☐



Note:

TLShv1.0, TLShv1.1, and TLShv1.2 are enabled by default.

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



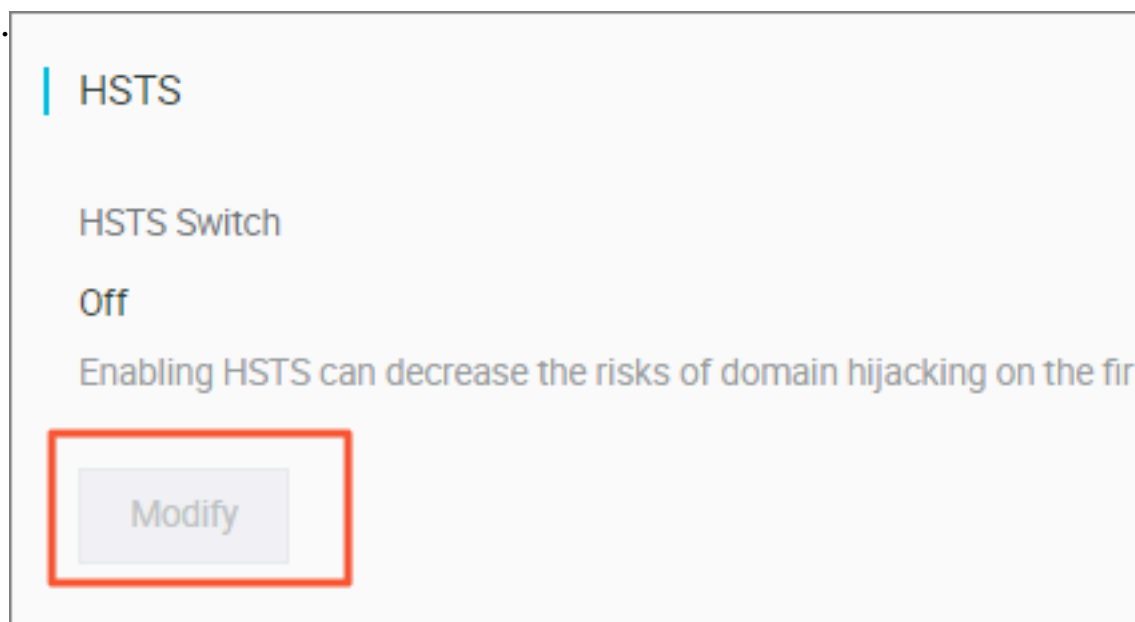
Note:

Configure the HTTPS certificate and then enable the TLS feature.

1. Log on to the [CDN console](#).
2. In the left-side navigation pane, click **Domain Names**.

3. Select a domain name, and click Manage.
4. In the left-side navigation pane, click HTTPS

Configuration.



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

8.8 FAQ

- [Does HTTPS secure acceleration incur additional fees?](#)
- [Will my access speed drop and resource usage increase after I enable HTTPS secure acceleration?](#)
- [Should I enable HTTPS only for when I log on to a website?](#)
- [What are common HTTP attacks?](#)

Does HTTPS secure acceleration incur additional fees?

Yes. HTTPS secure acceleration takes effect on the link from the client to the serving edge node. The SSL handshakes and content encryption and decryption all require computation, which makes the CDN server consume more CPU resources. However, the number of resources consumed on the origin server remains unchanged because the link from the serving edge node to the client still uses HTTP.

- If you purchase a certificate, you are charged for additional fees.



Note:

You can apply for [free certificates](#) on the [CDN console](#). Free certificates provided by Alibaba Cloud CDN are of the DV certification level. You can apply for one free certificate for each accelerating domain. The validity period of a free certificate

is one year. When a free certificate is about to expire, the system automatically renews it.

- After you configure an HTTPS certificate for an accelerating domain, you are charged 0.008 USD for every 10,000 static HTTPS requests destined for CDN nodes in this domain.

Will my access speed drop and resource usage increase after I enable HTTPS secure acceleration?

No, overall your access speed will remain the same, and the number of resources used will not increase as a result of enabling HTTPS secure acceleration. However, note that your access speed may drop by 10% the first time you access a website after you enable HTTPS because an initial Secure Sockets Layer (SSL) connection takes more time. After an HTTPS connection has been established, the access speed will return to normal.

Should I enable HTTPS only for when I log on to a website?

We do not recommend that you enable HTTPS only for when you log on to a website because this will negatively affect overall your website security and network performance. Specially, in terms of website security, if HTTPS is enabled for only some web pages, then there is the possibility that resources may be leaked while you are using HTTPS or an unsecure CDN service. Next, in terms of network performance, enabling HTTPS for only some web pages will cause the server to need to continually switch from HTTPS and HTTP, which can result in access speed decreases.

What are common HTTP attacks?

HTTPS is only one of the many ways to guarantee secure access. To ensure the overall network security, you need to deploy web application firewalls (WAFs) and defend against threats such as distributed denial-of-service (DDoS) attacks. Common HTTPS attacks are as follows:

- SQL injection

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into entry fields for execution in an SQL database. As a result, SQL statements are not executed as what developers have expected.

- Cross-site scripting (XSS)

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages. When other users surf on these web pages, their identities and permissions are exploited to execute the injected scripts, which are intended to tamper with or even steal the user information.

- Cross-site request forgery (CSRF)

Cross-site request forgery (CSRF) enables attackers to forge a request, in which a user submits a form, thereby tampering with the user data or executing a specific task. To spoof a user's identity, CSRF is often launched with XSS or by using means such as tricking the user into clicking a link into which CSRF is embedded.

- HTTP header injection

When you use a browser to visit a website, HTTP is used no matter what technology and framework were used to design this website. According to HTTP, a blank line lies between the header and content of a response message. This blank line, which is equivalent to two sets of CRLF (0x0D 0A), marks the end of the header and the start of the content. Attackers can exploit this vulnerability to inject any characters into the header.

- Open redirect

Open redirect is typically launched by using a phishing attack. Attackers masquerade as a trusted entity to send a user a link. When the user clicks this link, they are redirected to a malicious website, where the user data is stolen. We recommend that all redirection operations must be authenticated, so that users will not be redirected to malicious websites. One solution to this vulnerability is to add trusted URLs to a whitelist. Any redirections to domains that are not included in the whitelist will be denied. The other solution is to add redirection tokens to trusted URLs, which will be verified based on the tokens when users are to be redirected to these URLs.

9 Access Control Settings

9.1 Anti-leech

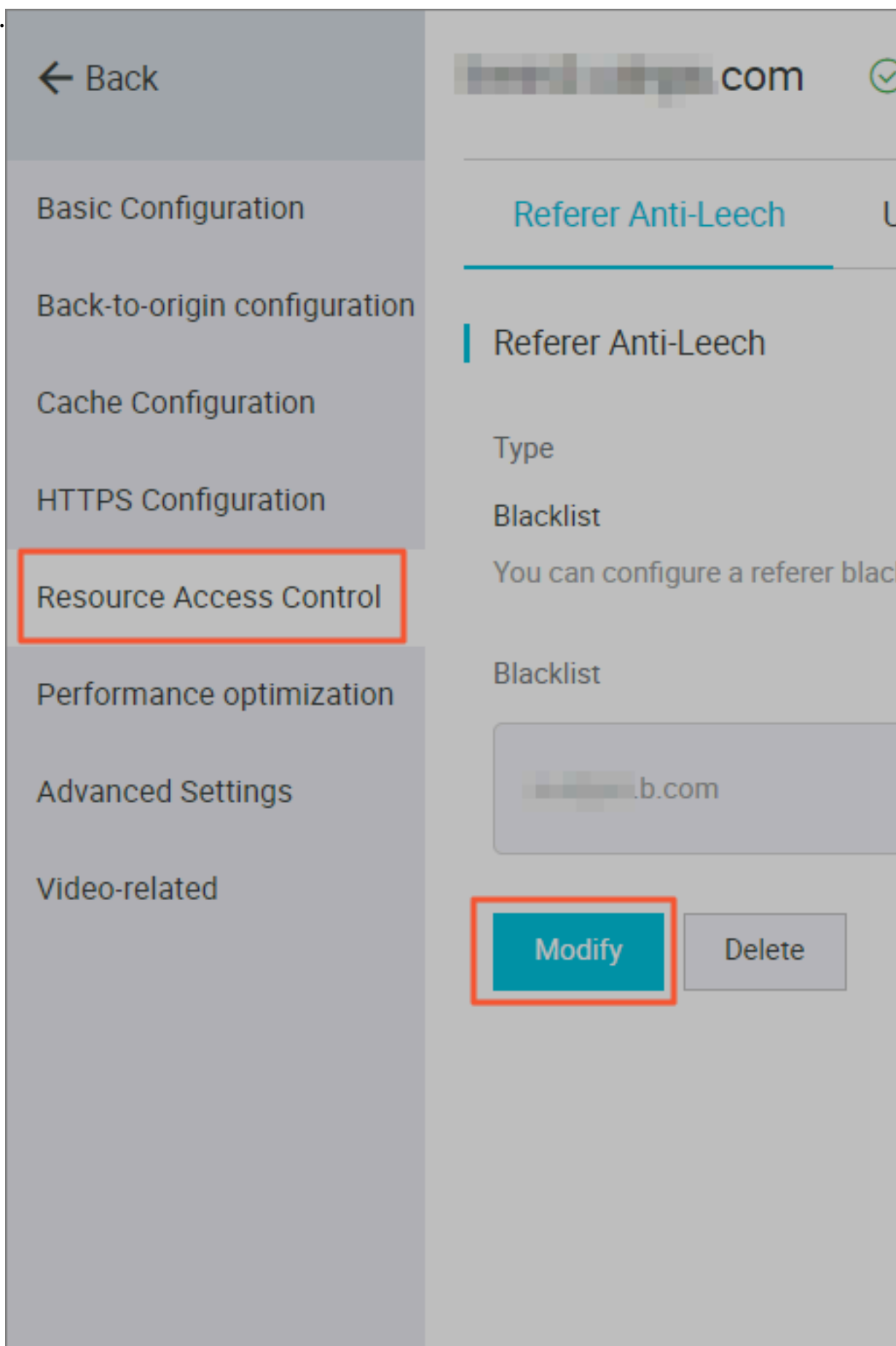
Introduction

- 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. Choose Blacklist 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 to 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

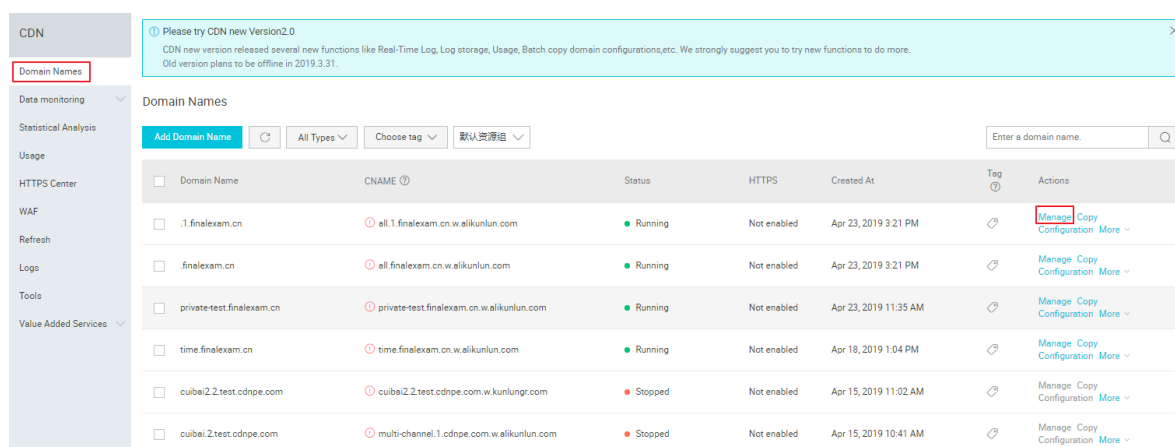
Alibaba Cloud CDN supports 3 authentication methods: A, B, and C. You can choose the authentication method based on your business need, so that it will help protect your origin site.

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.



CDN

Domain Names

Domain Names

Add Domain Name

All Types

Choose tag

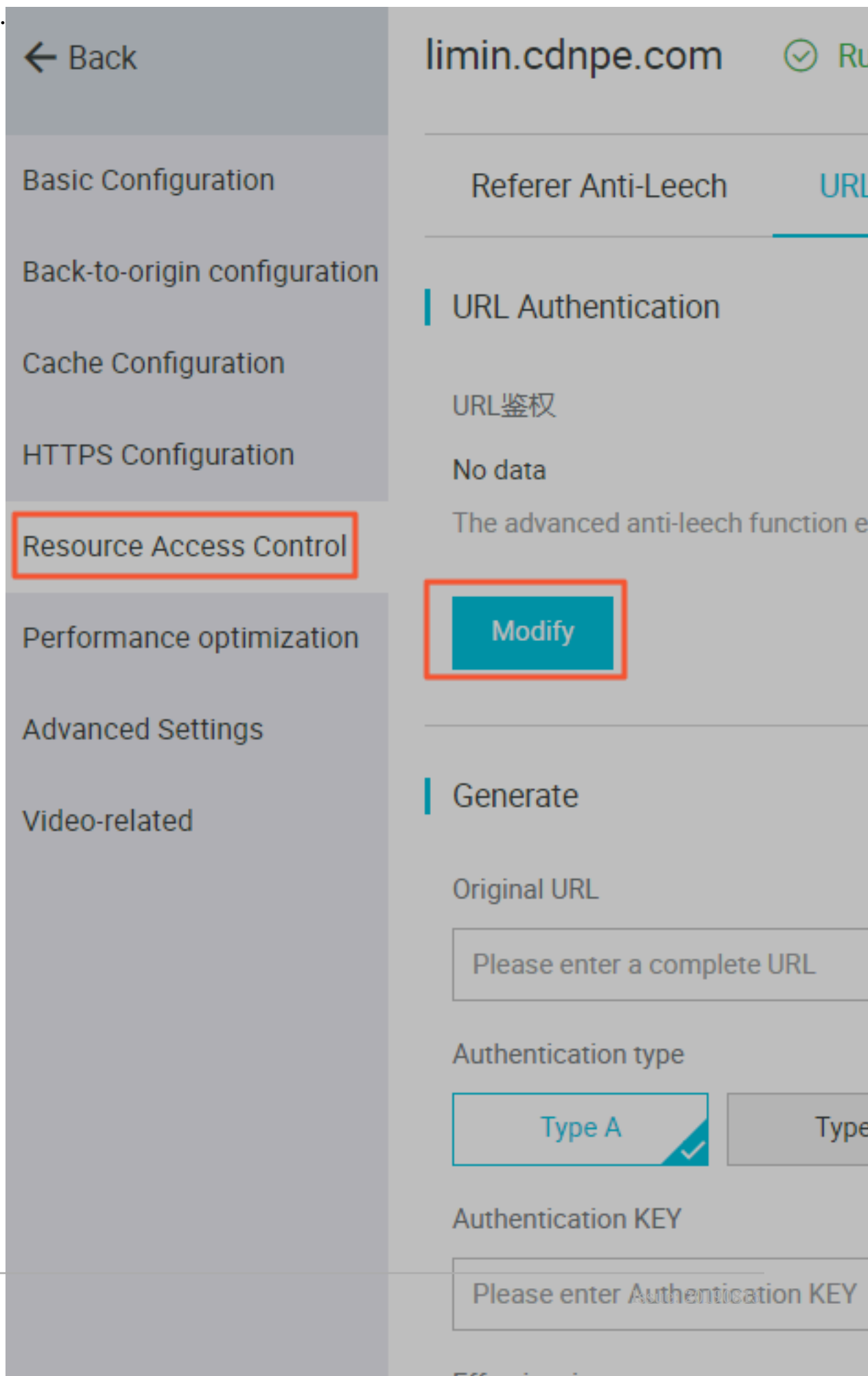
默认资源组

Enter a domain name.

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
cuibai2.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	<p>The expiration time. It is a positive integer with a fixed length of 10 and a time in seconds from January 1, 1970.</p> <p>This 10-digit integer is used to control the expiration time. Effective time is 1,800 seconds.</p>
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 - aliyncdne
xp1234 "
```

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

```
HashValue = md5sum ("/ video / standard / 1K . html - 1444435200
- 0 - 0 - aliyncdne 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 <code>md5hash</code> , is formatted: <code>YYYYMMDDHHMM</code> , effective time 1800 s
md5hash	//md5hash: The "timestamp", "FileName", and preset "PrivateKey" are used in the MD5 algorithm to get this string, i.e., (<code>PrivateKey</code> + <code>timestamp</code> + <code>FileName</code>)"
FileName	The actual URL of the origin access. Note that <code>FileName</code> must start with a slash (/) in authentication.

Example

1. Back-to-source request object.

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

2. The key is set to aliyncdnexp1234 (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":

```
aliyncdne xp12342015 08150800 / 4 / 44 / 44c0909bcfc20a01afaf256ca99a8b8b.mp3
```

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

```
md5hash = md5sum("aliyncdne xp12342015 08150800 / 4 / 44 / 44c0909bcfc20a01afaf256ca99a8b8b.mp3") = 9044548ef1527deadafa49a890a377f0
```

6. The URL to request CDN:

```
http://cdn.example.com/201508150800/9044548ef1527deadafa49a890a377f0/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
```

The calculated "md5hash" is the same as the "md5hash = 9044548ef1527deadafa49a890a377f0" 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
    nexptime = datetime . datetime . fromtimestamp ( exp ) . strftime
('% Y % m % d % H % M ')
    sstring = key + nexptime + path
    hashvalue = md5sum ( sstring )
    return "% s % s /% s /% s % s % s " %( scheme , host , nexptime ,
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.

CDN

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

Add Domain Name All Types Choose tag all resource group

Enter a domain name.

Domain Name	CNAME	Status	HTTPS	Created At	Tag	Actions
<input type="checkbox"/> domainregio02.finalexam.cn	<input type="radio"/> domainregio02.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 3, 2019 4:56 PM		Manage Copy Configuration More
<input type="checkbox"/> domainregio.finalexam.cn	<input type="radio"/> domainregio.finalexam.cn.w.alikunlun.com	Running	Not enabled	Apr 3, 2019 4:35 PM		Manage Copy Configuration More
<input type="checkbox"/> dkfd5.finalexam.cn	<input type="radio"/> dkfd5.finalexam.cn.w.alikunlun.com	Stopped	Not enabled	Mar 27, 2019 11:11 AM		Manage Copy Configuration More
<input type="checkbox"/> test.qkcompany.com	<input type="radio"/> test.qkcompany.com.w.alikunlun.com	Running	Enabled	Mar 20, 2019 1:02 PM		Manage Copy Configuration More
<input type="checkbox"/> domaintest.finalexam.cn	<input type="radio"/> domaintest.finalexam.cn.w.alikunlun.com	Running	Enabled	Mar 15, 2019 5:19 PM		Manage Copy Configuration More
<input type="checkbox"/> snitest.finalexam.cn	<input type="radio"/> snitest.finalexam.cn.w.alikunlun.com	Running	Not enabled	Mar 15, 2019 5:12 PM		Manage Copy Configuration More
<input type="checkbox"/> sstesttt26.finalexam.cn	<input type="radio"/> sstesttt26.finalexam.cn.w.alikunlun.com	Running	Enabled	Mar 13, 2019 10:37 AM		Manage Copy Configuration More
<input type="checkbox"/> sstesttt24.finalexam.cn	<input type="radio"/> sstesttt24.finalexam.cn.w.alikunlun.com	Running	Enabled	Mar 13, 2019 10:22 AM		Manage Copy Configuration More
<input type="checkbox"/> sstesttt74.finalexam.cn	<input type="radio"/> sstesttt74.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.

Back sstesttt24.finalexam.cn Running Disable

Basic Referer Anti-Leech URL authentication IP Address Blacklists/Whitelists

Back-to-Origin

Cache

HTTPS

Type

Not Set

Configure a whitelist or blacklist for access control. IPv6 addresses are supported. [Configure a whitelist or blacklist](#)

Performance Optimization

Advanced Settings

Video Related

WAF

Modify

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

Confirm Cancel

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.

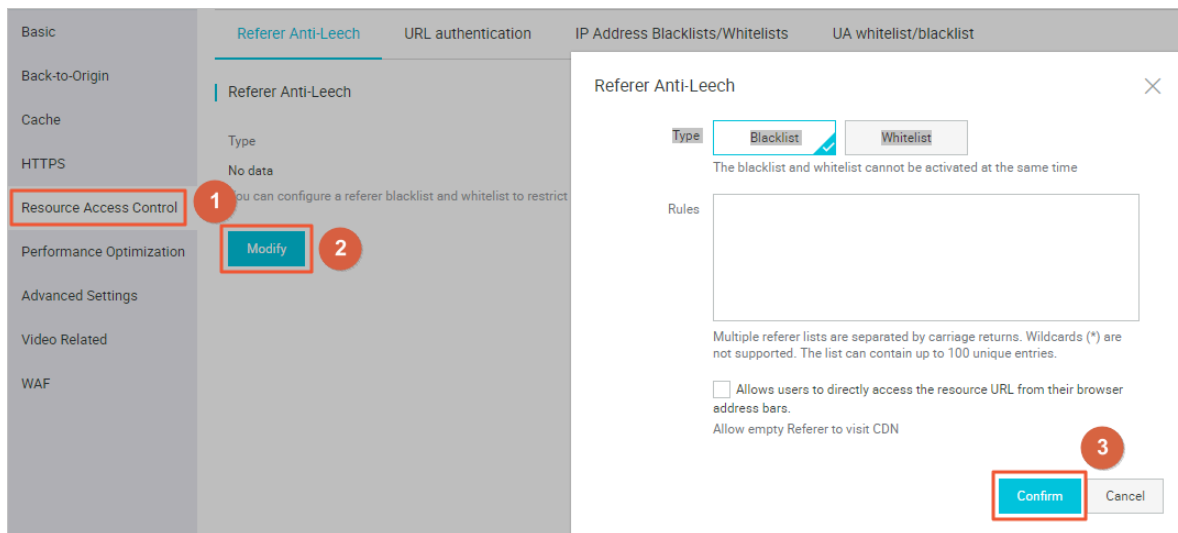


Note:

- **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.



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.

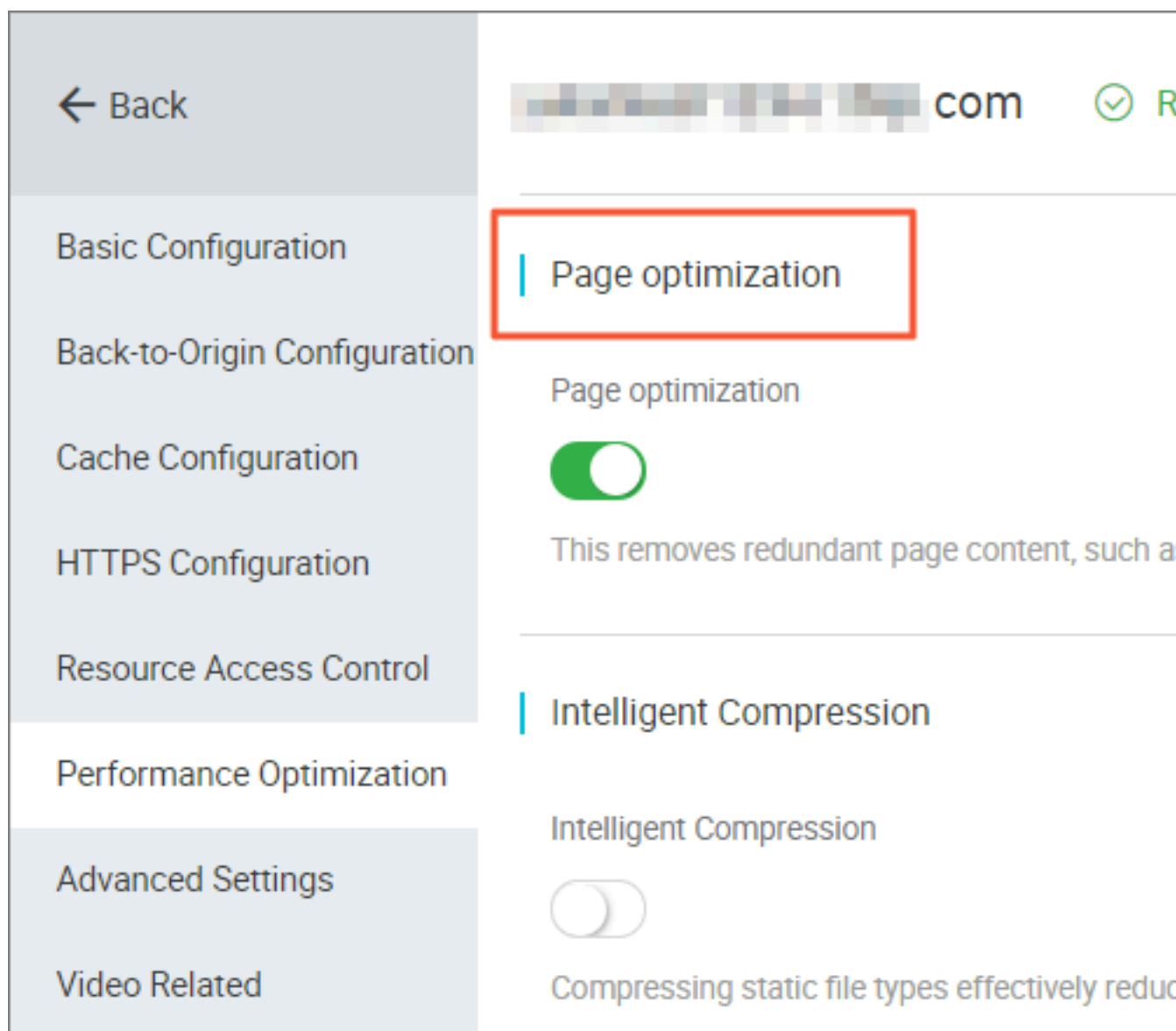
Procedure

**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.



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.

CDN

Domain Names

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
cuibai2.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.

← Back

zengyintest111.finalexam.cn Enabled

Basics

Back-to-origin

Cache

HTTPS

Access Control

Optimization

Advanced

Video

HTML Optimization

HTML Optimization

Intelligent Compression

Intelligent Compression

Brotli Compression

Brotli Compression

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.



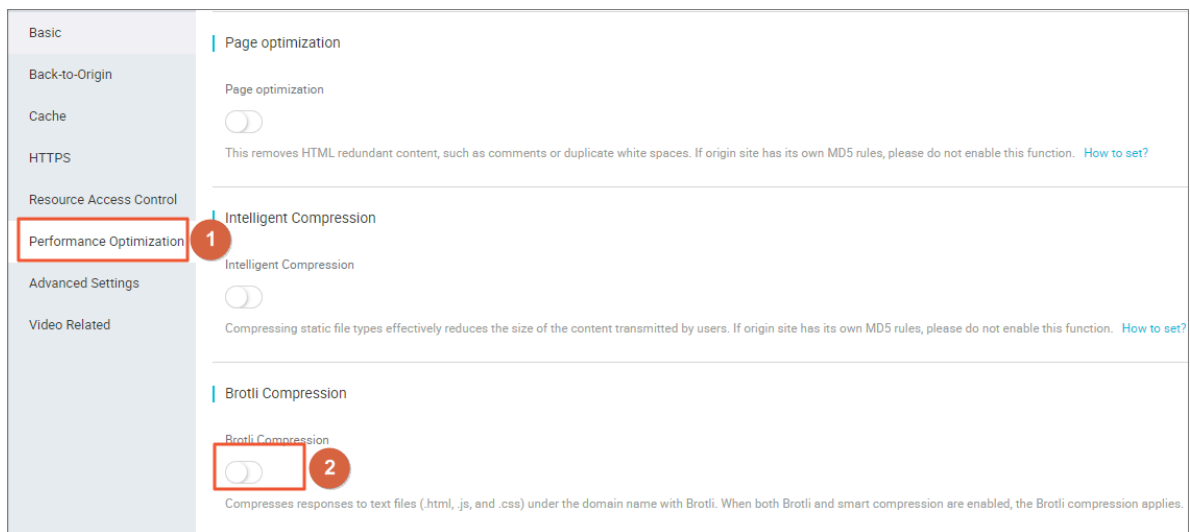
Notice:

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.



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 is recommended to enable the Filter Parameter function. This improves the file cache hit rate and the delivery efficiency.
 - If a parameter has important indicators (for example, if it contains file version information), 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 Video Service Configuration

11.1 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 to Domain Name page, select 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.

11.2 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 the 10th 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 the 10th 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 <code>http://domain/video.mp4?start=10</code> 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 <code>http://domain/video.flv</code> , the request <code>http://domain/video.flv?start=10</code> playing a video from the key frame prior to the 10th byte(If <code>start=10</code> 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.

11.3 Audio extraction

Audio extraction allows you to request the audio data in a video file. With audio extraction enabled, a CDN node extracts audio data from a video file and then returns only the audio data to the client. This reduces network traffic usage. This topic describes how to enable audio extraction.

Context

When a client requests a video file, it sends a request to the CDN server. The request contains the URL of the video file, for example, `http://www.aliyun.com/test.flv?ali_audio_only=1`. After the CDN server receives the request, it returns the audio data in the video file to the client.

The client must support this transmission method: `Transfer-Encoding: chunked`.

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 target domain name and click Manage.
4. In the left-side navigation pane of the specified domain, click Video.

5. Click the Audio Extraction switch to enable audio extraction.

After audio extraction is enabled, add the `ali_audio_only` parameter to the video file URL in a request to perform audio extraction. Audio extraction supports the following file formats:

Format	Metadata	ali_audio_only parameter	Example
MP4	Only MP4 video files with the metadata contained in their header support audio extraction. MP4 video files with the metadata contained in their footer do not support audio extraction.	Set the <code>ali_audio_only</code> parameter to 1 to require the CDN server to return only the metadata and audio data of the requested video. The video data is not returned. If you do not specify this parameter or set the parameter to other values, audio extraction is not performed.	<code>http : // domain / video . mp4 ? ali_audio_ only = 1 .</code>
FLV	No requirements.	Set the <code>ali_audio_only</code> parameter to 1 to require the CDN server to return only the metadata and audio data of the requested video. The video data is not returned. If you do not specify this parameter or set the parameter to other values, audio extraction is not performed.	<code>http : // domain / video . flv ? ali_audio_ only = 1 .</code>

12 Advanced settings

12.1 QUIC

12.1.1 What is the QUIC protocol?

If the connection between a client and a CDN node uses the QUIC protocol for data communication, the connection can ensure the security of data transmission and improve the resource access efficiency. This topic describes what is QUIC, how QUIC works, and client requirements and billing of the QUIC protocol.

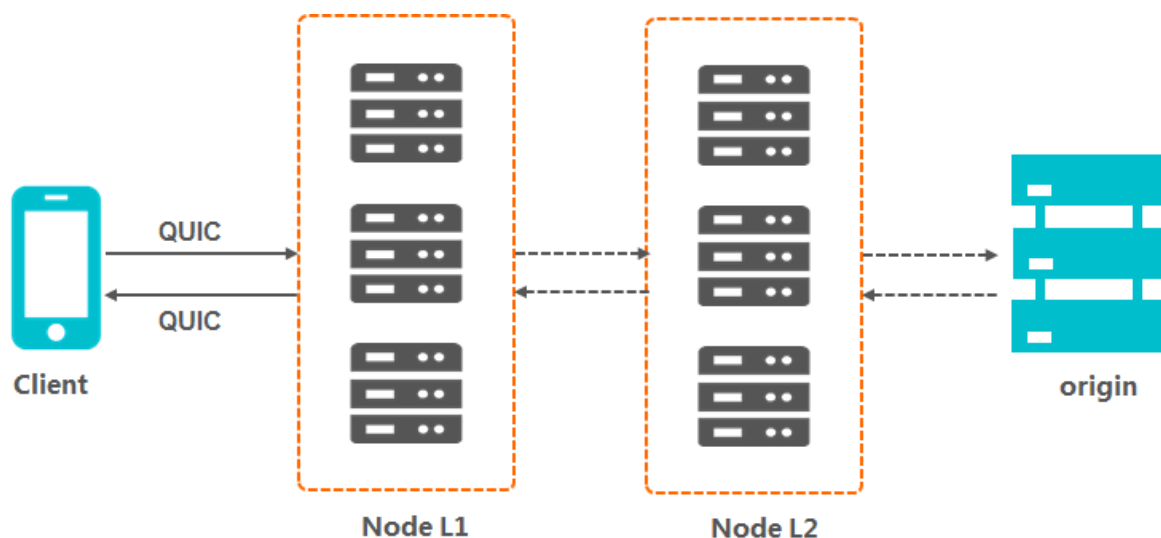
What is QUIC?

Quick UDP Internet Connections (QUIC) is an experimental transport layer network protocol that provides the same security as TLS/SSL and has reduced connection and transmission latency. Based on UDP, QUIC has excellent performance in case of weak network connections. When packet loss and network latency are severe, QUIC can still provide available services. QUIC can implement different congestion control algorithms at the application layer without the support of the operating system and the kernel. Compared with the traditional TCP protocol, QUIC allows future changes to be made more easily. This protocol is very suitable for businesses that encounter bottlenecks in TCP protocol optimization.

Currently, Alibaba Cloud CDN supports the layer-7 QUIC (HTTP over QUIC) protocol. The version number is Q39.

How QUIC works

The following figure shows how QUIC is used in Alibaba Cloud CDN.



Client requirements

The QUIC protocol has the following requirements for a client:

- If you use Google Chrome, only version Q43 is supported. The QUIC protocol supported by Alibaba Cloud CDN is version Q39. You cannot use Google Chrome to directly send QUIC requests to Alibaba Cloud CDN.
- If you use a self-developed app, the app must integrate a network library that supports the QUIC protocol, such as lsquic-client or Cronet.

QUIC billing

The QUIC protocol is a value-added service and incurs additional fees for the number of QUIC requests. For more information, see [CDN pricing](#).



Note:

For a QUIC request whose protocol header is HTTPS, it will not be repeatedly charged in both HTTPS requests and QUIC requests. The HTTPS request billing and the QUIC request billing are mutually exclusive. One request is charged for only one type of requests.

- QUIC requests are not identified by the request header. Whether a request is a QUIC request is determined by the UDP protocol.
- CDN first checks whether the request is a QUIC request. If yes, the request is billed according to the QUIC billing rules. CDN will no longer check whether the request is an HTTPS request. If no, CDN continues to check whether the request is an HTTPS request.

12.1.2 Configure the QUIC protocol

The QUIC protocol is as secure as TLS/SSL, with reduced connection and transmission latency. If you want to improve resource access efficiency and ensure data transmission security, enable the QUIC protocol. This topic describes how to enable the QUIC protocol.

Prerequisites

Make sure that you have enabled the HTTPS protocol and uploaded the SSL certificate. For more information, see [Configure HTTPS certificates](#).

Context

A preview of QUIC is currently available. Follow the prompts to scan the QR code to join the DingTalk group. After you join the group, follow the group announcements to provide domain information. Alibaba Cloud IT administrators will help you enable the QUIC protocol. After you enable the QUIC protocol in Alibaba Cloud CDN, Alibaba Cloud CDN will process user requests according to the QUIC protocol.

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 target domain name and click Manage.
4. In the left-side navigation pane of the specified domain, click Advanced.

5. In the QUIC Protocol section, enable the `QUIC Protocol` function.

Follow the prompts below to enable the QUIC protocol.



12.2 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

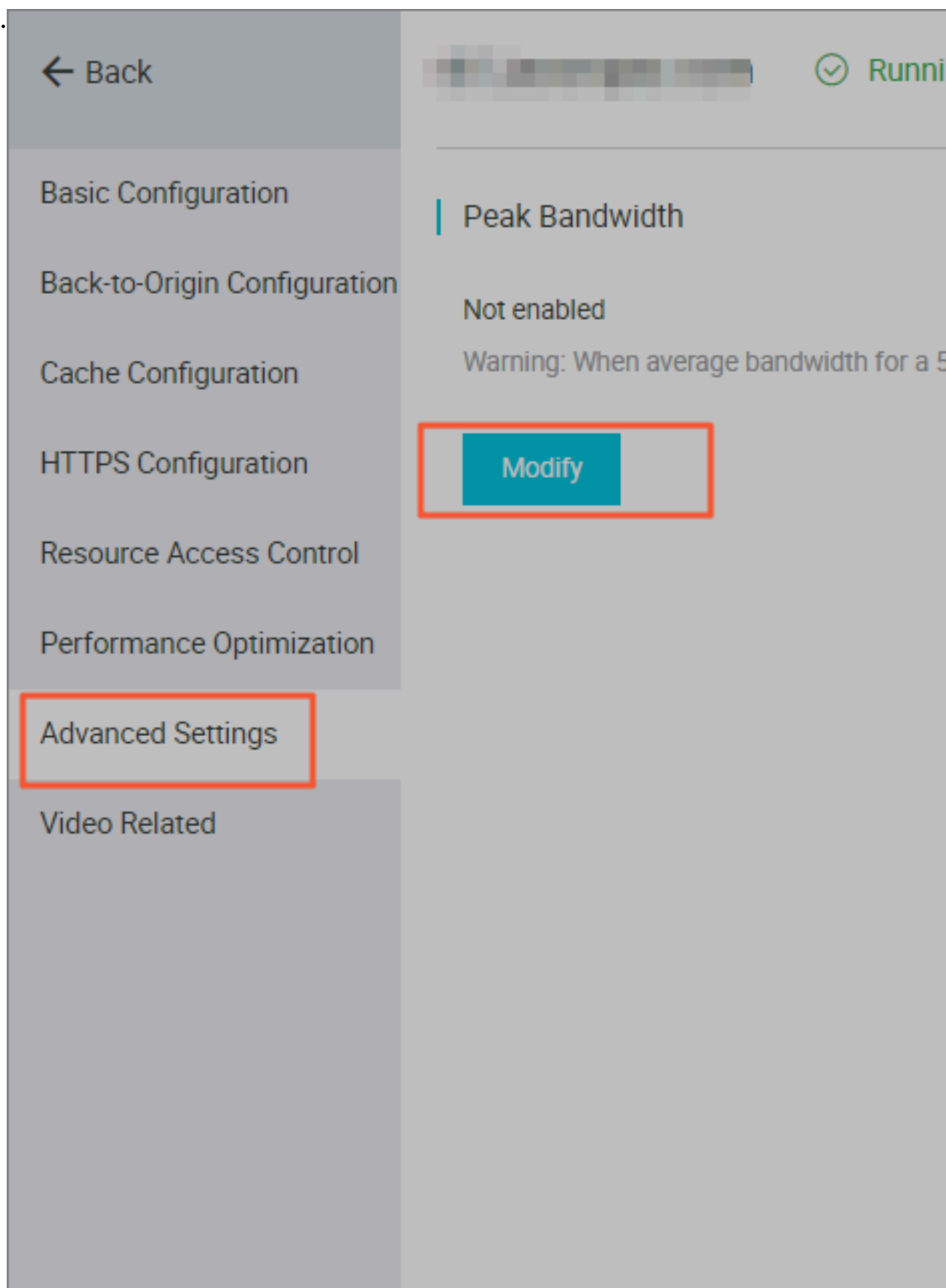


Note:

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.



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.