

Alibaba Cloud

Alibaba Cloud CDN

Domain Management

Issue: 20190831

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 alert 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..... | 13 |
| 4.4 Manage domain names by tag..... | 14 |
| 4.5 Query domain names by tag..... | 14 |
| 4.6 Tag use case..... | 15 |
| 5 Basic settings..... | 17 |
| 5.1 Overview of basic settings..... | 17 |
| 5.2 Modify basic information..... | 17 |
| 5.3 Configure an origin..... | 18 |
| 6 Content back-to-source settings..... | 21 |
| 6.1 Overview..... | 21 |
| 6.2 Configure an origin host..... | 21 |
| 6.3 Configure the origin protocol policy..... | 23 |
| 6.5 Disable private bucket back-to-origin authorization..... | 24 |
| 6.6 Configure a back-to-origin SNI..... | 25 |
| 6.7 Customize an origin HTTP header..... | 27 |
| 6.8 Set the origin request timeout period..... | 28 |
| 7 Cache settings..... | 30 |
| 7.1 Overview..... | 30 |
| 7.2 Create a cache expiration rule..... | 30 |
| 7.3 Set status code expiration time..... | 34 |
| 7.4 Create an HTTP header..... | 36 |
| 7.5 Customize an error page..... | 38 |
| 7.6 Configure a rewrite rule..... | 40 |
| 8 HTTPS..... | 43 |
| 8.1 What is HTTPS acceleration?..... | 43 |
| 8.2 Overview of certificate formats..... | 49 |
| 8.3 Configure HTTPS certificates..... | 52 |
| 8.4 Enable HTTP/2..... | 59 |
| 8.5 Enable force redirect..... | 60 |
| 8.6 Configure TLS..... | 62 |

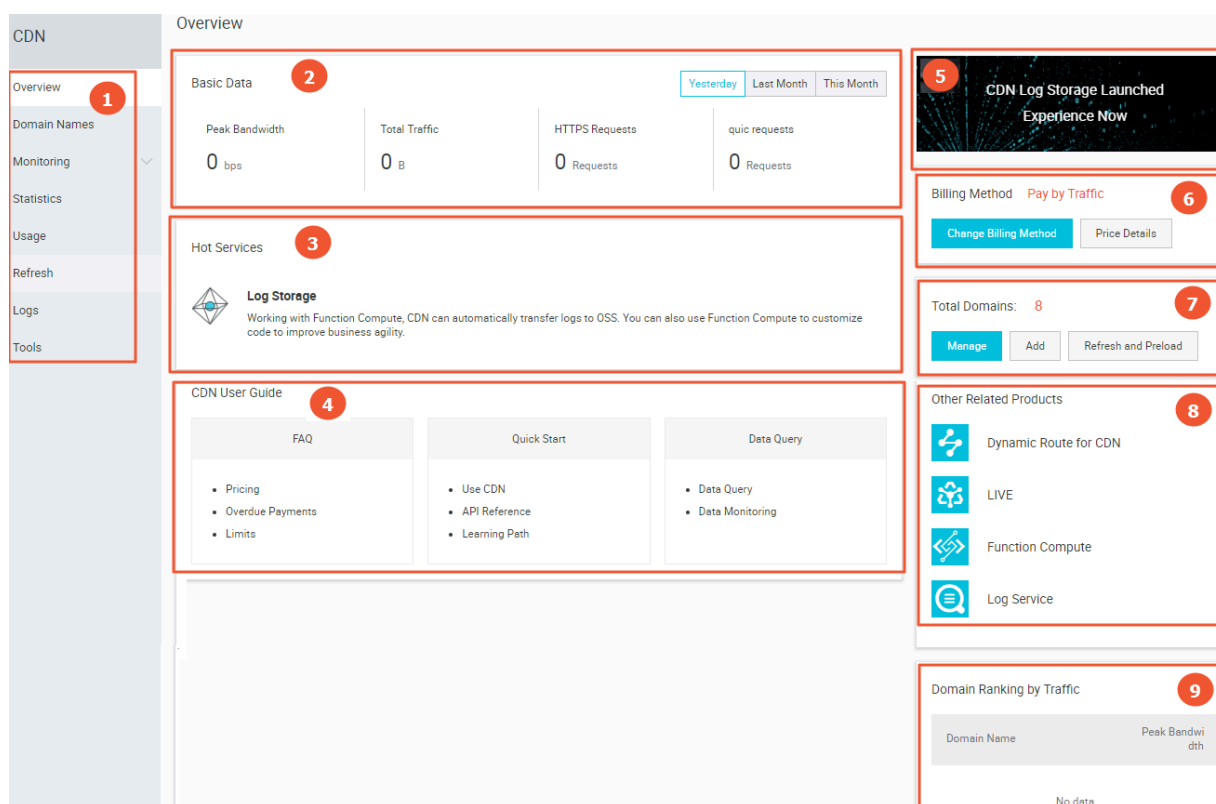
| | |
|---|------------|
| 8.7 Configure HSTS..... | 64 |
| 8.8 FAQ..... | 66 |
| 9 Access control..... | 70 |
| 9.1 Overview..... | 70 |
| 9.2 Configure hotlink protection..... | 70 |
| 9.3 Business type..... | 73 |
| 9.3.1 Configure URL authentication..... | 73 |
| 9.3.2 Authentication method A..... | 77 |
| 9.3.3 Authentication method B..... | 78 |
| 9.3.4 Authentication method C..... | 80 |
| 9.3.5 Sample authentication code..... | 82 |
| 9.4 Configure an IP address blacklist or whitelist..... | 84 |
| 9.5 Configure a User-Agent blacklist or whitelist..... | 86 |
| 10 Performance optimization..... | 89 |
| 10.1 Overview..... | 89 |
| 10.2 Configure HTML optimization..... | 89 |
| 10.3 Configure intelligent compression..... | 90 |
| 10.4 Configure Brotli compression..... | 91 |
| 10.5 Configure parameter filtering..... | 92 |
| 11 Video Service Configuration..... | 97 |
| 11.1 Overview..... | 97 |
| 11.2 Configure object chunking..... | 97 |
| 11.3 Video seeking..... | 99 |
| 11.4 Audio extraction..... | 101 |
| 12 Advanced settings..... | 103 |
| 12.1 Overview..... | 103 |
| 12.2 QUIC..... | 103 |
| 12.2.1 What is the QUIC protocol?..... | 103 |
| 12.2.2 Configure the QUIC protocol..... | 105 |
| 12.3 Configure bandwidth cap..... | 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 #unique_4 . |

| 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 #unique_5 . |
| 6 | Billing method | Displays the billing method you have selected. You can also modify the billing method as needed. For more information, see #unique_4 and #unique_6 . |
| 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 | #unique_7 | Allows you to copy one or more configurations of a CDN domain to another one or more CDN domains. | None |
| Alert settings | #unique_8 | 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 | #unique_9 | Allows you to add tags to a domain name or group domain names by tags. | None |

| Feature | Reference | Description | Default value |
|----------------------------|---|--|---------------|
| | #unique_10 | Allows you to use tags to quickly filter domain names for group management. | None |
| | #unique_11 | Allows you to use tags to quickly filter domain names for data query. | None |
| Basic information settings | #unique_12 | Allows you to modify the accelerated region. | None |
| | #unique_13 | Allows you to modify the origin information. | None |
| Back-to-origin settings | #unique_14 | Allows you to modify the domain name of the origin host. | Enabled |
| | #unique_15 | 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 |
| | #unique_17 | 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 |
| | #unique_18 | If you configure CDN to use HTTP to communicate with your origin, you can add or remove HTTP header fields. | Disabled |
| | #unique_19 | 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 |
| Cache settings | Configure cache expiration | Allows you to customize cache expiration rules for specified resources. | None |

| Feature | Reference | Description | Default value |
|---------------------------|---|--|---------------|
| | Set status code expiration time | 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 |
| | #unique_23 | Allows you to customize a complete URL to redirect for an HTTP or HTTPS response code. | 404 |
| | #unique_24 | Allows you to modify a request URI and perform a 302 redirect to the specified target URI. | None |
| HTTPS secure acceleration | #unique_25 | 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 |
| | #unique_27 | If HTTP secure acceleration is enabled, you can configure CDN to forcibly redirect user requests to HTTPS or HTTP. | Disabled |
| | #unique_28 | 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 |
| | #unique_29 | HSTS is used to force clients (such as browsers) to use HTTPS to create connections with the server. | Disabled |

| Feature | Reference | Description | Default value |
|--------------------------|--|--|---------------|
| 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 |
| | #unique_33 | 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 |
| | #unique_36 | 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 |
| 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 |

| Feature | Reference | Description | Default value |
|------------------------|---|--|---------------|
| 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 / Domain Names / Copy Configurations

← Copy Configurations vediocdn.test.finalexam.cn

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 type="checkbox"/> | Origin Information | Configured |
| <input type="checkbox"/> | Origin Host | Configured |

Next Cancel

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 / Domain Names / Copy Configurations

← Copy Configurations vediocdn.test.finalexam.cn

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: 0/50

| | |
|-------------------------------------|----------------------------|
| <input type="checkbox"/> | Domain |
| <input type="checkbox"/> | isccc.finalexam.cn |
| <input checked="" type="checkbox"/> | vediocdn.test.finalexam.cn |
| <input type="checkbox"/> | 6789.test.com |
| <input type="checkbox"/> | zengyin31.finalexam.cn |

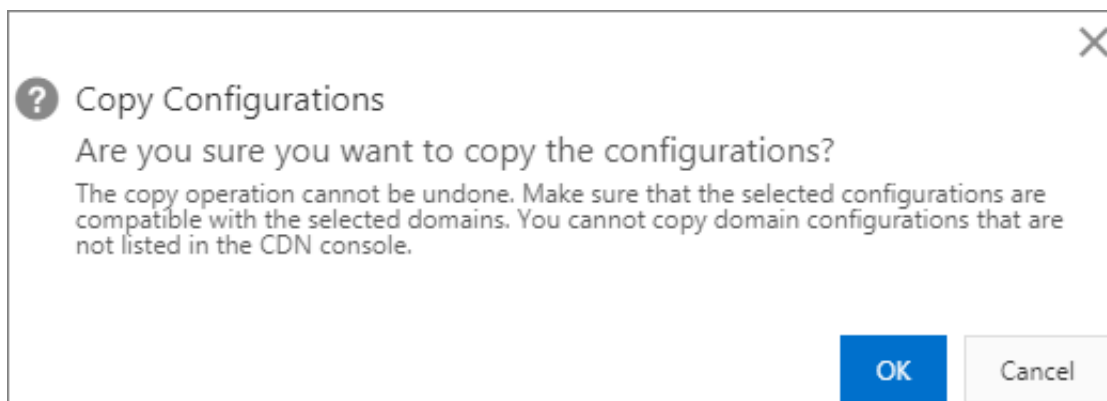
▼ Show Selected

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.



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

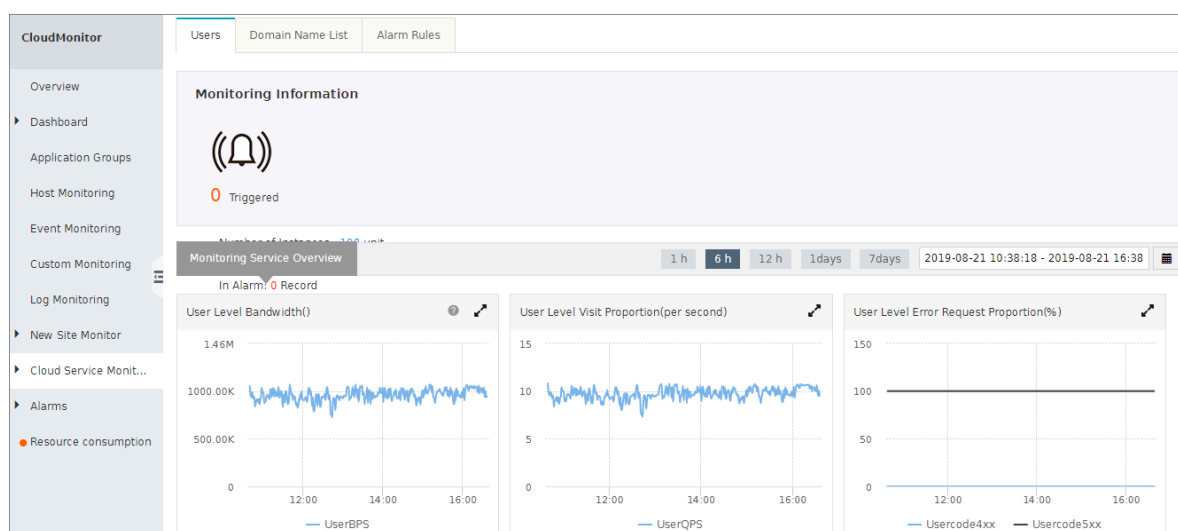
3 Set an alert rule

This topic describes how to create an alert rule in the Alibaba Cloud CDN console.

You can use CloudMonitor to set alert rules specific to CDN domain metrics. When an alert rule is triggered, CloudMonitor sends an alert by using the specified notification method (for example, SMS or email).

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, click Alert Settings to go to the CloudMonitor console.



4. Choose Cloud Service Monitoring > CDN, and click the Alert Rules tab.
5. Click Create Alert Rule.

Alarm Rules

Refresh

Threshold Value Alarm

Event Alarm

Create Alarm Rule

Enter to search.

Search

| Rule Name | Status (All) ▾ | Enable | Metrics (All) ▾ | Dimensions (All) ▾ | Alarm Rules | Product Name (All) ▾ | Notification Contact | Actions |
|---|--|---------|-----------------|-------------------------------------|---|----------------------|-------------------------------|---|
| <input type="checkbox"/> yutan26.test.cdnpe.com | <div><div></div><div>Insufficient Data</div></div> | Enabled | Peak Bandwidth | instancetype:yutan26.test.cdnpe.com | Peak Bandwidth >111000000Bit/sec Warn Give an alarm 3 consecutive times | videolive | 云账号报警联系人 View | View Alarm Logs Modify Disable Delete |
| <input type="checkbox"/> | <div>Enable</div> <div>Disable</div> <div>Delete</div> | | | | | | | |
| Total 1 Record | | | | | | | | <div>10 ▾</div> <div>« < 1 > »</div> |

6. Create a CDN alert rule. For more information, see [#unique_43](#).

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:

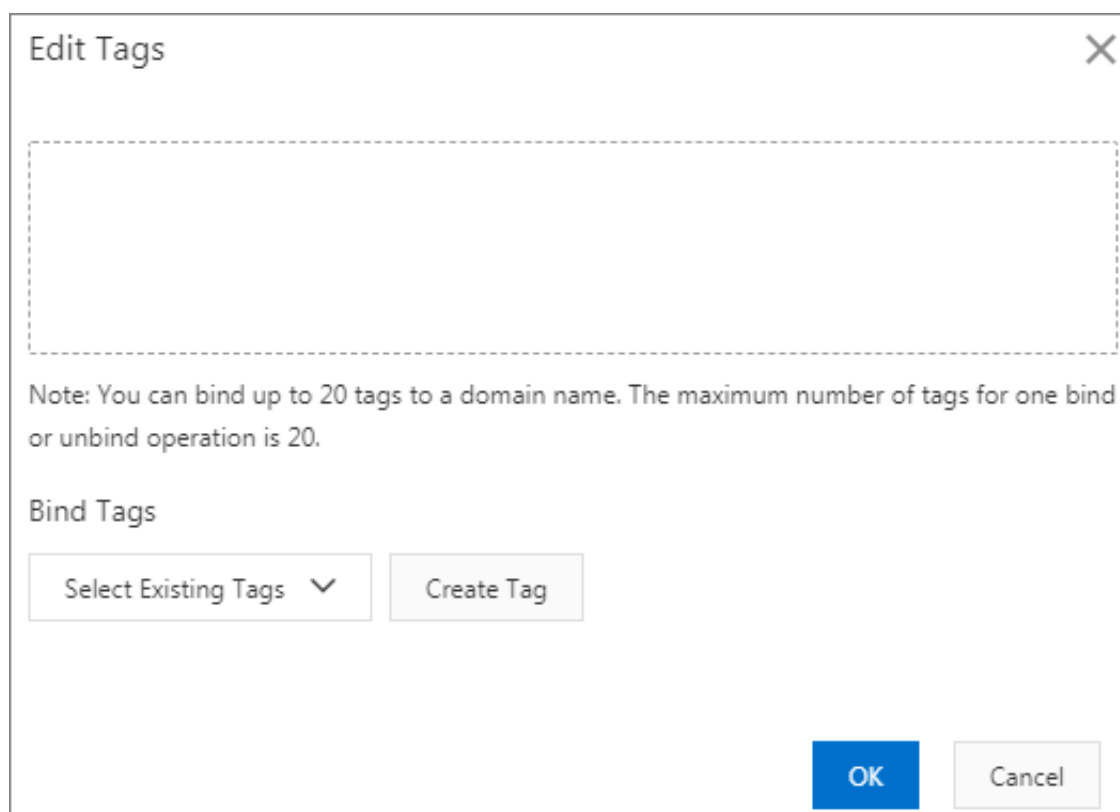
- Attach tags to domain names to identify or group the domain names. For more information, see [Attach tags](#).
- Detach tags from domain names. For more information, see [Detach tags](#).
- Manage domain names based on their tags. For more information, see [Manage domain names by tag](#).
- Query the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

If you want to identify and group domain names, you can attach tags to 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 for which you want to set tags, and move the pointer over the corresponding icon in the Tags column.
4. Click Edit.



Edit Tags

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

Bind Tags

Select Existing Tags ▼ Create Tag

OK Cancel

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

API

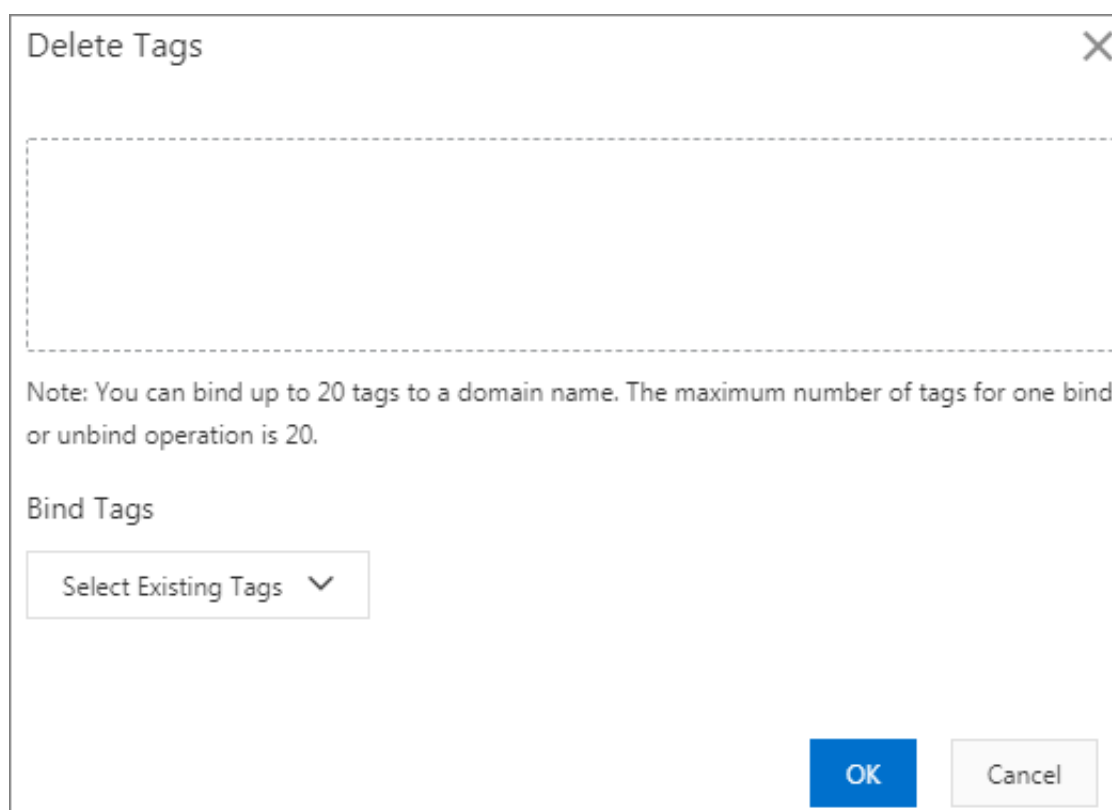
You can call API operations to attach tags to domain names. For more information, see [#unique_49](#).

4.3 Detach tags from a domain name

If the tags no longer apply to one or more domain names, you can detach these tags from the corresponding 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 for which you want to delete tags, and choose Manage Tags > Delete Tags.



4. In the Delete Tags dialog box, select the tags to be deleted, and click OK.

API

You can call API operations to detach tags from domain names. For more information, see [#unique_51](#).

4.4 Manage domain names by tag

After attaching tags to domain names, you can use the tags to quickly filter the corresponding domain names and manage these domain names by group.

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, select tags from the Select Tags drop-down list.

| Domain Names | | | | | | | |
|---------------------------------|----------------------------|--|---------------|--|----------------------|------|--|
| Add Domain Name | | All Types ▾ | Select Tags ▾ | Search by keyword <input type="text"/> | | | |
| <input type="checkbox"/> | Domain Name | CNAME | Status | HTTPS | Created At | Tags | Actions |
| <input type="checkbox"/> | isccc.finalexam.cn | isccc.finalexam.cn.walikulun.com | Enabled | Disabled | Aug 7, 2019 10:49 AM | | Manage Copy Configurations |
| <input type="checkbox"/> | vediocdnstest.finalexam.cn | vediocdnstest.finalexam.cn.walikulun.com | Enabled | Disabled | Jul 31, 2019 5:45 PM | | Manage Copy Configurations |

API

You can call API operations to manage domain names by their tags. For more information, see [#unique_53](#).

4.5 Query domain names by tag

If you want to query the data of some domain names, you can use tags to quickly filter the corresponding domain name and query the data after attaching tags to domain names.

Procedure

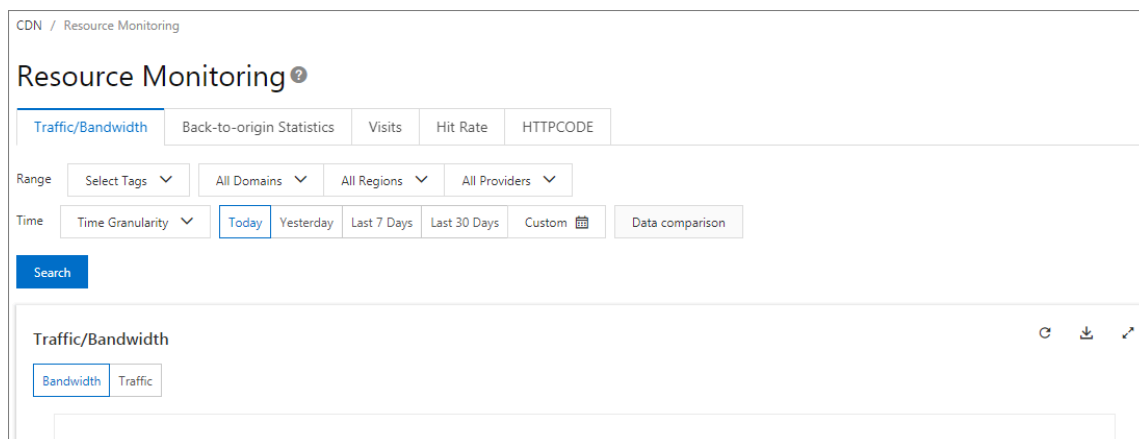
1. Log on to the [Alibaba Cloud CDN console](#).
2. In the left-side navigation pane, click Domain Names.
3. You can use one of the following methods to query the domain names to which specific tags are attached:



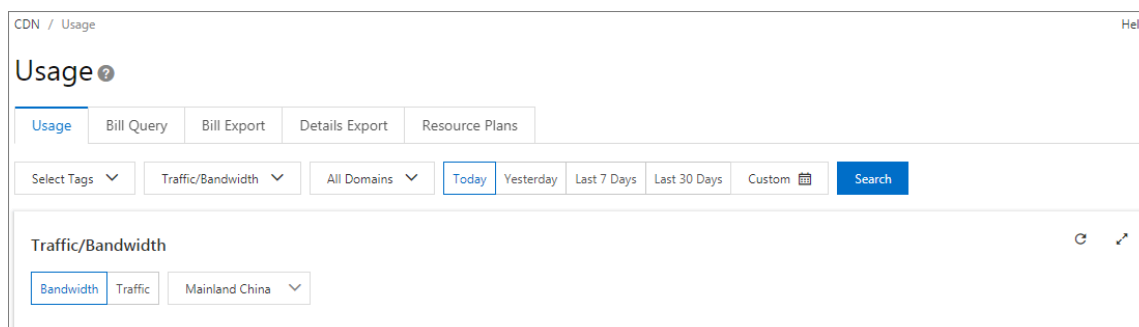
Note:

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

- In the left-side navigation pane, choose **Monitoring > Resource Monitoring**. In the main workspace, select tags from the **Select Tags** drop-down list and click **Search**.



- In the left-side navigation pane, click **Usage**. In the main workspace, select tags from the **Select Tags** drop-down list and click **Search**.



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 Overview of basic settings

This topic describes the basic settings in the Alibaba Cloud CDN console. You can use these settings to obtain and modify the basic information and origin information of a domain.

Settings

On the Basics page, you can:

- Change the region of a domain. For more information, see [Change the region of a domain](#).
- Change the type, IP address, and port of the origin that serves a domain. For more information, see [Configure the origin of a domain](#).

Pricing

When you modify the origin information of a domain:

- If you select IP or Origin Domain for Type, you are billed by Internet traffic.
- If you select OSS Domain for Type, you are billed by intranet traffic. For more information, see [OSS pricing](#).
- If you select OSS Domain for Type and specify a domain name in the Domain Name field, you are billed by Internet traffic.

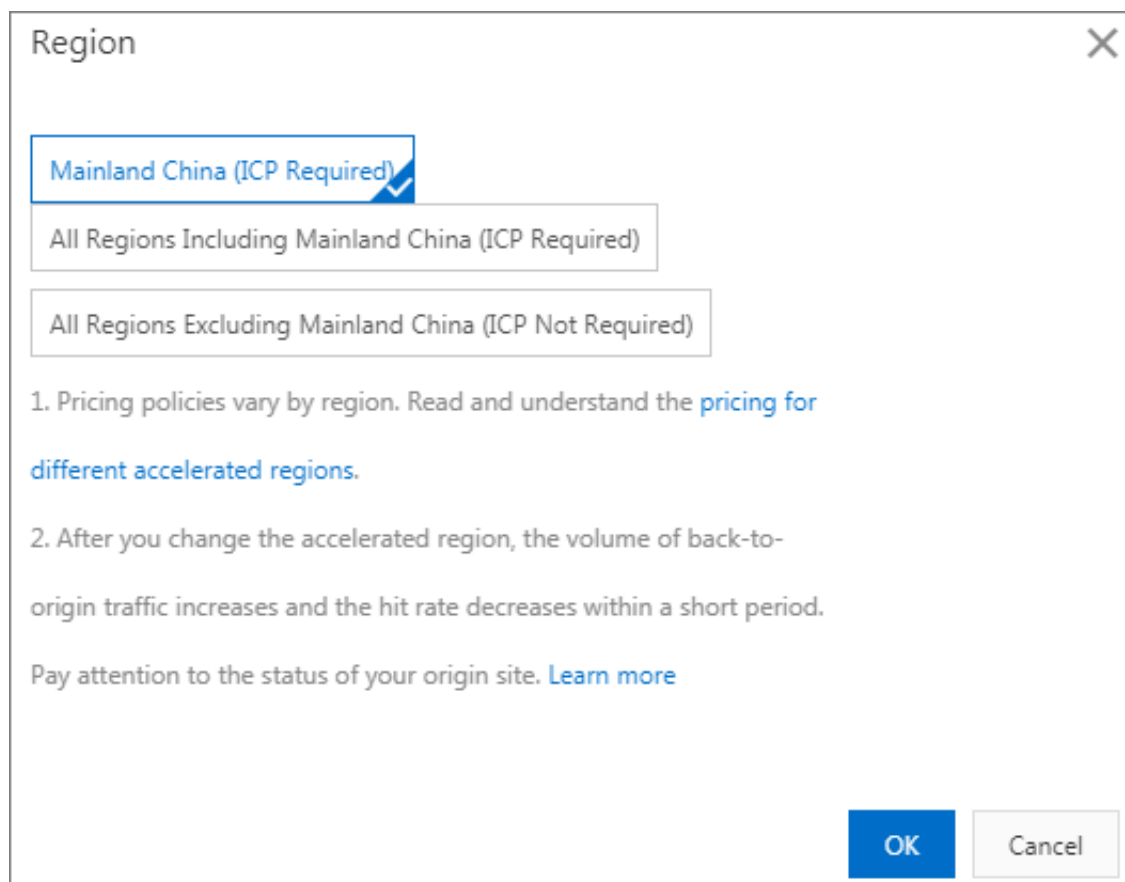
5.2 Modify basic information

You can change the scope of your CDN service by switching between regions.

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 Basic Information section, click Modify.

5. In the Region dialog box, set Region.



The image shows a 'Region' dialog box with a close button (X) in the top right corner. It contains three radio button options: 'Mainland China (ICP Required)' (selected), 'All Regions Including Mainland China (ICP Required)', and 'All Regions Excluding Mainland China (ICP Not Required)'. Below the options, there are two numbered instructions: '1. Pricing policies vary by region. Read and understand the [pricing for different accelerated regions.](#)' and '2. After you change the accelerated region, the volume of back-to-origin traffic increases and the hit rate decreases within a short period.' followed by 'Pay attention to the status of your origin site. [Learn more](#)'. At the bottom right are 'OK' and 'Cancel' buttons.

6. Click OK.

5.3 Configure an origin

This topic describes how to modify the origin type and related precautions.

Context

Origin configuration is not applicable to the acceleration of [#unique_60](#).

Alibaba Cloud CDN supports three types of back-to-origin domains: OSS domain, IP address, and origin domain. Multiple IP addresses and origin domains are supported. You can set priorities for multiple origins.



Note:

The system automatically performs a four-layer health check to test port 80 of each origin every 2.5 seconds. If an origin fails the check for three consecutive times, the system considers the origin unavailable.

CDN supports switchovers between primary and secondary origins. When multiple origins are added, CDN directs requests to the origin whose `Priority` is set to `Primary`. If the primary origin fails the health check for three consecutive times, CDN directs requests to the origin whose `Priority` is set to `Secondary`. Once the primary origin passes the health check, the system considers the origin available again and restores the priority of this origin to `Primary`. If all origins have the same back-to-origin 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 target domain name and click Manage.
4. In the Origin Information section, click Modify.
5. In the Modify Origin Information dialog box, set Type, IP, and Port.

In the Modify Origin Information dialog box, set the following parameters.

- Type
- Port

| Port | Description |
|----------|---|
| Port 80 | Your origin server returns the requested resources to port 80 by using HTTP or HTTPS. |
| Port 443 | Your origin server returns the requested resources to port 443 by using HTTP or HTTPS. If the IP address of your origin server is associated with multiple domains, you must #unique_61 . |

| Port | Description |
|-------------|---|
| Custom Port | <p>Your origin server returns the requested resources to a custom port only by using HTTP. Before you customize a port, you must set the redirect type of Static Origin Protocol Policy to HTTP. For more information, see #unique_15.</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 the API, make sure that the origin protocol and custom port are working properly. - If you enable the HTTP or HTTPS origin protocol and customize a port through the Custom Port parameter, your origin server returns the requested resources based on the port settings regardless of the other settings specified in the Alibaba Cloud CDN console. |

Modify Origin Information

✕

Origin Info

Type

OSS Domain

IP

Origin Domain

FC Domain

IP

Priority

Priorities for multiple origins

1.1.1.1

Primary

Add

Port

Port 80

Port 443

Custom Port

Tip: Custom ports are currently only supported for returning to the source with HTTP protocol.If you need to return to your source's custom port with httpS protocol, submit a ticket configuration.

OK

Cancel

6. Click OK.

6 Content back-to-source settings

6.1 Overview

When you send a resource access request from a client, if CDN cannot find the resource on the CDN node, it retrieves the resource from the origin and then loads the resource to the CDN node. You can configure back-to-origin functions to accelerate access to CDN resources.

CDN supports the following back-to-origin functions.

| Function | Description |
|----------------------------|---|
| #unique_14 | Allows you to specify the domain type of the origin host for CDN nodes retrieving resources from the origin. |
| #unique_15 | Allows you to configure an origin protocol policy for retrieving resources from the origin to CDN nodes when CDN cannot find the resources on CDN nodes. |
| #unique_64 | Allows you to use private Object Storage Service (OSS) buckets as origins in order to prevent resource hotlinking. |
| #unique_65 | You can log on to the RAM console and remove authorization from a specified role to disable private bucket access. |
| #unique_61 | If CDN nodes access your origin over HTTPS and your origin IP address is bound to multiple domain names, then you must select a domain name for CDN by specifying the Server Name Indication (SNI) of the domain name. |
| #unique_18 | If you configure CDN to use HTTP to communicate with your origin, you can add or remove HTTP header fields. |
| #unique_19 | The default timeout period for a resource request sent from a CDN node to an origin is 30 seconds. You can customize the timeout period. If the CDN node does not receive any response before the timeout period expires, the CDN node disconnects from the origin. |

6.2 Configure an origin host

If you want to customize the domain of the server to which CDN initiates back-to-origin requests, you must configure the domain type of the origin host. The domain

types available for an origin host are CDN domain, origin domain, and custom domain.

Context

An origin host is the domain of the origin server to which CDN initiates back-to-origin requests.



Note:

If your origin is bound to multiple domains or servers, you must specify the domain to which the back-to-origin requests are sent. Otherwise, the back-to-origin process fails.

Differences between an origin and an origin host:

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

Default settings for the origin host:

- 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.

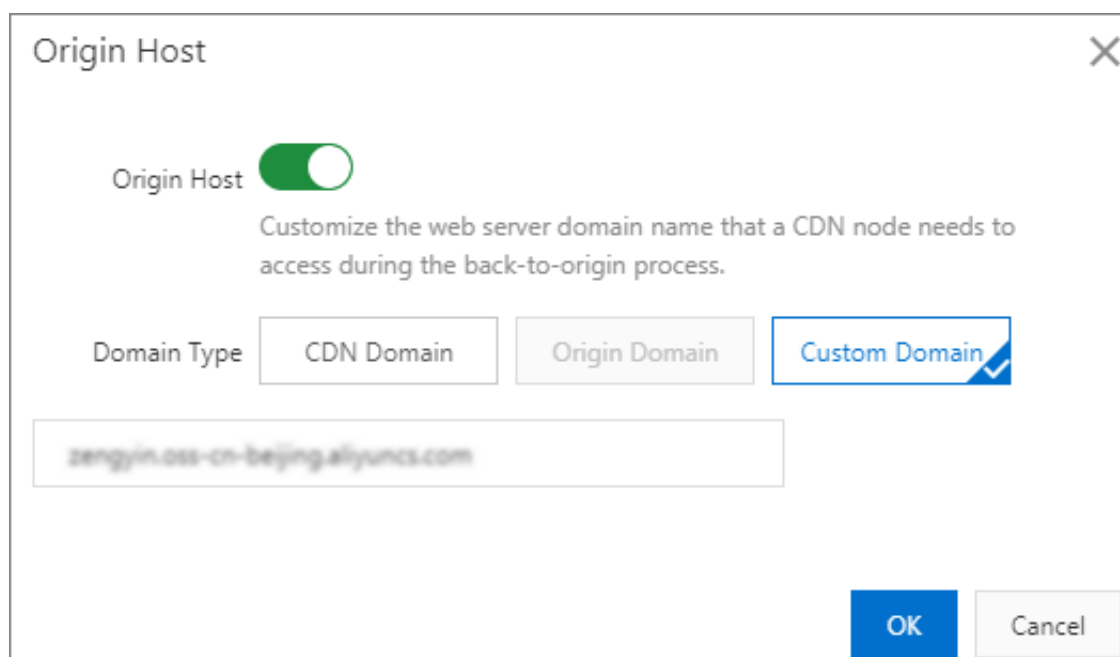
Examples:

- If your origin is `www . a . com` and your origin host is `www . b . com`, CDN initiates 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 initiates 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 target domain name and click Manage.

4. In the left-side navigation pane of the specified domain, click **Back-to-origin**.
5. In the **Origin Host** section, click **Modify**.
6. Turn on **Origin Host**, and set **Domain Type**.



The image shows a dialog box titled "Origin Host" with a close button (X) in the top right corner. Inside the dialog, there is a toggle switch for "Origin Host" which is currently turned on (green). Below the toggle, a text description reads: "Customize the web server domain name that a CDN node needs to access during the back-to-origin process." Underneath this, there is a "Domain Type" section with three buttons: "CDN Domain", "Origin Domain", and "Custom Domain". The "Custom Domain" button is highlighted with a blue border and a checkmark icon. Below the buttons is a text input field containing the domain "zengyin.oss-cn-beijing.aliyuncs.com". At the bottom right of the dialog are two buttons: "OK" (blue) and "Cancel" (gray).

7. Click **OK**.

6.3 Configure the origin protocol policy

If a client requests for resources that are not cached on a CDN node, the node fetches these resources from the origin based on the origin protocol policy and caches these resources on the node. This topic describes how to configure the origin protocol policy.

Context

When origin protocol policy is enabled, back-to-origin requests for resources use the same protocol that is used by the client to request resources. If the client sends an HTTPS request to access resources that are not cached on a CDN node, the node uses the same HTTPS protocol to request for resources from the origin. This origin protocol policy also applies to HTTP requests.

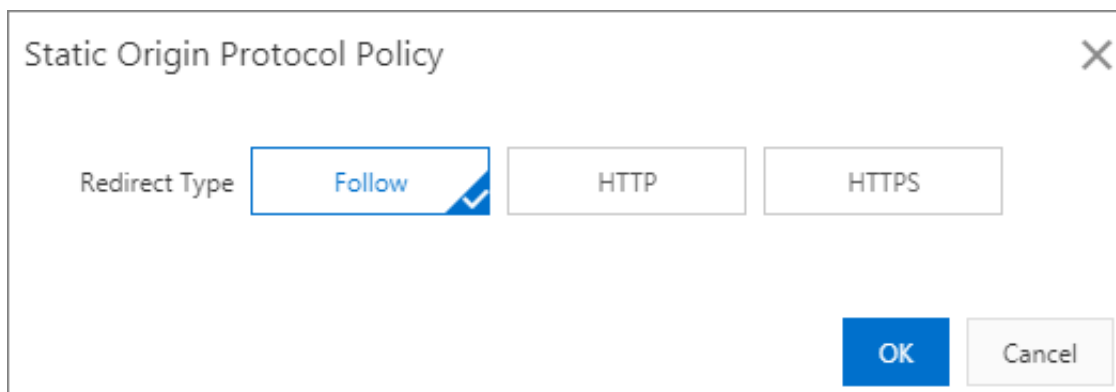


Note:

The origin must support both port 80 and port 443. Otherwise, the back-to-origin process may fail.

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 Back-to-origin.
5. In the Origin Protocol Policy section, turn on Origin Protocol Policy.
6. Click Modify.



7. In the Static Origin Protocol Policy dialog box, set Redirect Type to Follow, HTTP, or HTTPS as needed.
 - Follow: If the client sends HTTP or HTTPS requests to access resources on CDN, CDN uses the same protocol to request for resources from the origin.
 - HTTP: CDN initiates back-to-origin requests only over HTTP.
 - HTTPS: CDN initiates back-to-origin requests only over HTTPS.
8. Click OK.

6.5 Disable private bucket back-to-origin authorization

This topic describes how to revoke access permissions on your private bucket from an origin domain. You can revoke permissions for the corresponding roles to disable private bucket back-to-origin authorization in the Resource Access Management (RAM) console.

Context

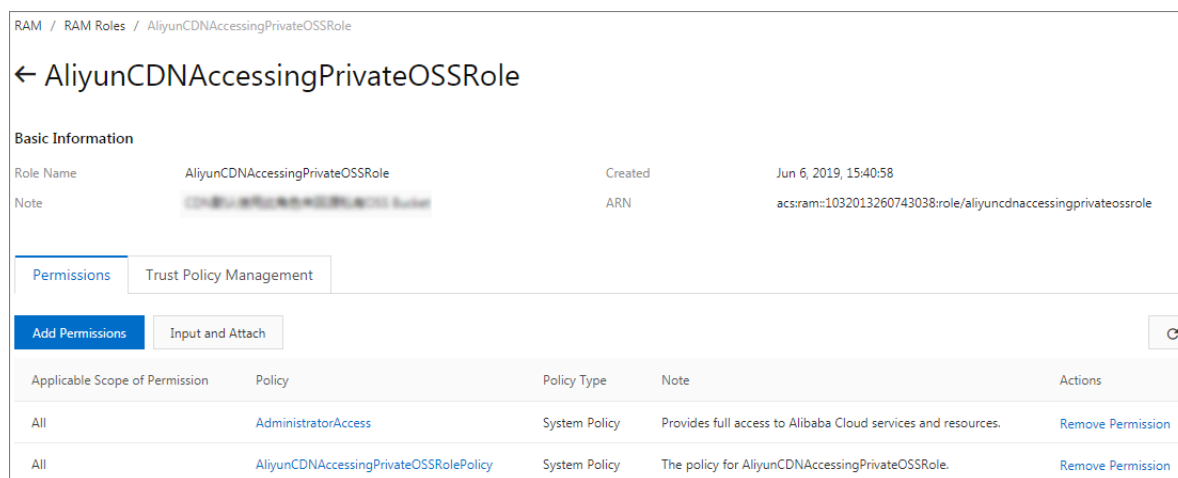


Note:

If your CDN domain uses your private bucket as its origin, do not disable or delete this authorization 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 RAM role name AliyunCDNAccessingPrivateOSSRole.



4. Click Remove Permission in the Actions column corresponding to the RAM role to be deleted.
- In the Remove Permission dialog box, click OK.
5. Return to the RAM Roles page, click Delete in the Actions column corresponding to the RAM role to be deleted.
- In the Delete RAM Role dialog box, click OK.

6.6 Configure a back-to-origin SNI

If your origin IP address is bound to multiple domains, you must configure a back-to-origin Server Name Indication (SNI) to your domain to ensure that the CDN node is able to access your origin site over HTTPS.

Context

SNI is an extension of Transport Layer Security (TLS) by which a client determines which hostname it is attempting to connect to at the beginning of the handshake process. This allows a server to present multiple certificates on the same IP address and TCP port number. This also allows multiple HTTPS websites (or any other service over TLS) that have different certificates to be served by the same IP address.

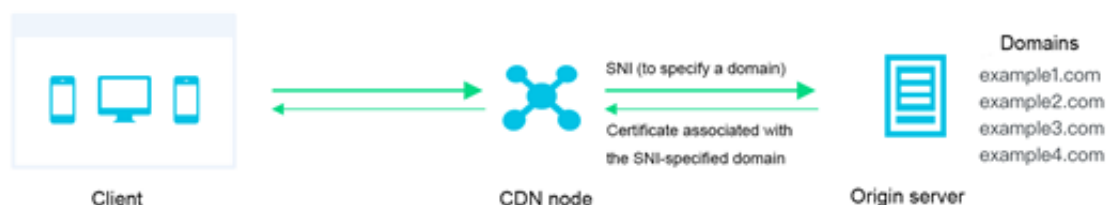
If your origin server uses a single IP address to provide HTTPS services for multiple domains and port 443 is specified for receiving back-to-origin traffic on your CDN, you must configure the back-to-origin SNI of a specific domain. In this way, when a

CDN node requests to access your origin server over HTTPS, the server can return the correct certificates of the requested domains.

**Note:**

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

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

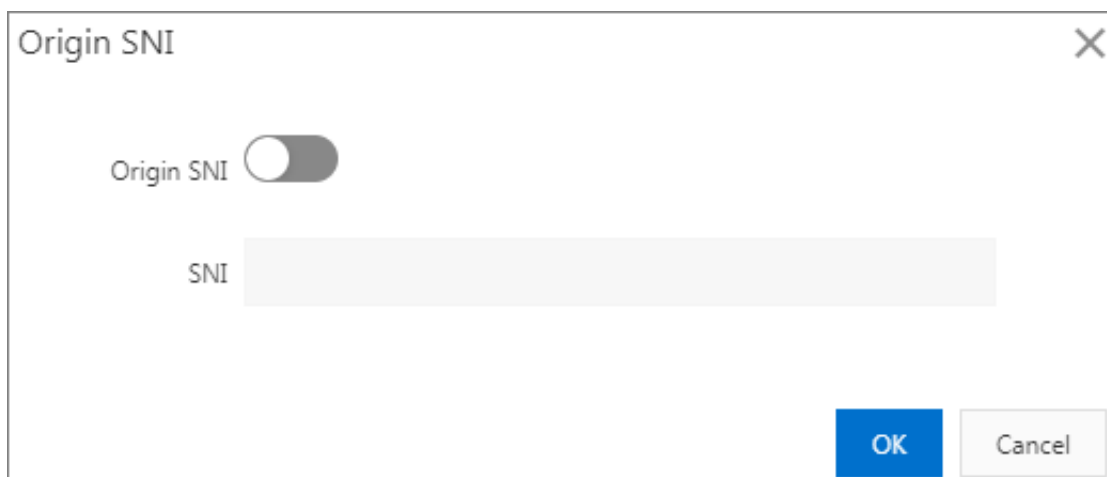


1. The CDN node requests to access the origin server over HTTPS, where the requested domain is specified in the SNI.
2. After receiving the request, the origin server sends the certificate of the requested domain to the CND node.
3. After receiving the certificate, the CDN node establishes a secure connection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

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 Back-to-origin.

5. In the Origin SNI section, click Modify.

A dialog box titled "Origin SNI" with a close button (X) in the top right corner. Inside the dialog, there is a toggle switch labeled "Origin SNI" which is currently turned off. Below the toggle is a text input field labeled "SNI". At the bottom right of the dialog are two buttons: "OK" (blue) and "Cancel" (gray).

6. Turn on Origin SNI, and enter the name of the domain served by your origin server.

7. Click OK.

6.7 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.

Context


HTTP headers are the header component in the request and response messages sent over Hypertext Transfer Protocol (HTTP). HTTP header fields describe the requested resources, the information of the client or server, and the parameters of an HTTP transaction.

HTTP headers include general headers, request headers, and response headers.

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 Back-to-origin.
5. Click the Custom HTTP Origin Header tab.
6. Click Customize.

7. In the Customize Origin HTTP Header dialog box, set Parameter and Value.



8. Click OK.

6.8 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.

Origin Request Timeout

Timeout Value

30

Seconds

Default value: 30. Maximum value: 900. The value cannot exceed 100 when the back-to-origin process runs correctly.

OK

Cancel

7. Click OK.

7 Cache settings

7.1 Overview

If CDN wants to accelerate static resource delivery, it loads the resources on an origin site to the CDN node that is closest to the visitor. When the visitor wants to access the static resources, CDN retrieves the resources from the CDN node instead of retrieving the resources from the origin site, which is time-consuming. This reduces the resource delivery time.

CDN supports the following cache functions.

| Function | Description |
|----------------------------|---|
| #unique_74 | Allows you to configure the time to live (TTL) of static resources in a specified directory or with a specified file extension, and specify their caching priority. CDN then caches the specified static resources based on their priority. |
| #unique_75 | Allows you to configure the TTL of error responses for resources in a specified directory or with a specified file extension. |
| #unique_76 | Allows you to customize HTTP response header fields. |
| #unique_23 | Allows you to specify a custom error page for specific HTTP or HTTPS status codes. |
| #unique_24 | Allows you to redirect request URIs to specified URIs by using 302 redirect. |

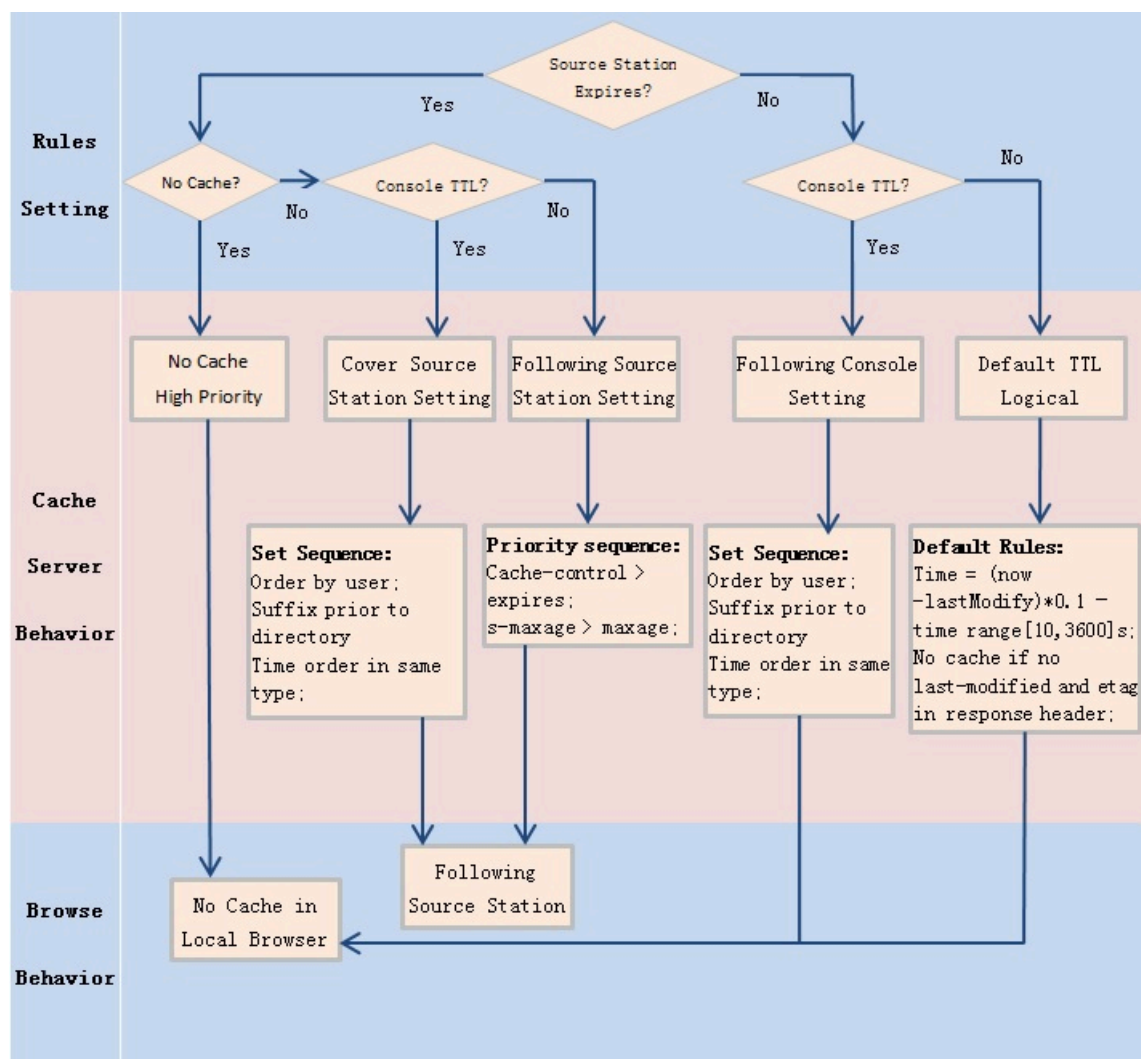
7.2 Create a cache expiration rule

In each cache expiration 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. This topic describes the cache policy of resources on CDN and how to create a cache expiration rule.

Context

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, such as `img - v1 . 0 . jpg` and `img - v2 . 1 . jpg`.

The following figure shows the cache policy of resources on CDN nodes.



Note:

- The default cache policy on edge nodes is used to set the file expiration time. This cache policy has a higher priority than that configured in the origin. If no cache policy is configured on the origin site, you can set a cache policy based on directory or file extension. Full paths are supported.
- The resources cached on CDN nodes can be removed from the nodes ahead of time in case of low popularity.

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 Cache.

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

Create Expiration Rule

Type

Directory

File Extension

Object

Enter one or more objects

The directory (full path is supported) must start with a forward slash (/).
Separate multiple directories with commas (.). Example: /directory/aaa

Expire In

Enter a duration

Seconds

Maximum duration: 3 years.

Weight

Enter a weight


Valid value: [1, 99]

OK

Cancel

6. In the Create Expiration Rule dialog box that appears, select a rule type as prompted.

| 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 forward slash (/), such as / <i>directory</i> / <i>aaa</i> . 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 (,), such as jpg,txt. |

| 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 based on actual business situations for static files such as files in JS and CSS formats that are frequently updated. Do not cache dynamic files such as files in PHP, JSP, and ASP formats. |
| 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 value, they take effect in a random sequence. </div> <p>For example, if you set the following 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.

You can click Modify or Delete in the Actions column corresponding to a cache expiration rule to modify or delete the rule.

7.3 Set status code expiration time

If the specified file extension or directory rule is matched to static resources cached on CDN, you can set the expiration time of these resources based on the specified status code expiration time. This topic describes how to set the status code expiration time.

Context

When you set the status code expiration time, note the following limits:

- 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 status code expiration time is not specified, the default cache time specified by the `negative_ttl` parameter is 1s.
- If you set status code expiration time of both the directory and file extension types, the type you set first takes effect.

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 Cache.
5. Click Status Code Expiration.

6. On the Status Code Expiration tab, click Create Rule.

Create Expiration Rule

Type

Directory

File Extension

Object

Enter one or more objects

The directory (full path is supported) must start with a forward slash (/).
Separate multiple directories with commas (,). Example: /directory/aaa

Expire In

Enter one or more pairs of status code and duration

You can set the duration in seconds for specific 4xx/5xx HTTP status codes. Separate multiple pairs with commas (,). Example: 403=10,404=15 [Configure status code expiration](#)

OK

Cancel

7. In the Create Expiration Rule dialog box that appears, set Type as prompted.

| Type | Consideration |
|-----------|---|
| Directory | <ul style="list-style-type: none">· Add a single directory (full paths are supported). The directory must start with a forward slash (/), such as <code>/www / directory / aaa</code>.· Status codes of the 2xx and 3xx formats are not allowed. |

| Type | Consideration |
|----------------|---|
| File extension | <ul style="list-style-type: none">• Multiple file extensions are separated by commas (,), such as txt,jpg.• Asterisks (*) cannot be used to match all types of files.• Status codes of the 2xx and 3xx formats are not allowed. |

8. Click OK.

You can click Modify or Delete in the Actions column corresponding to a status code expiration rule to modify or delete the rule.

7.4 Create an HTTP header

The HTTP header fields describe the requested resources and the client or server behavior, and also define the operating parameters of an HTTP transaction. This topic describes how to create an HTTP header.

Context

The HTTP header refers to the header component in the request and response messages sent over Hypertext Transfer Protocol (HTTP).

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. |

| Parameter | Description |
|-------------------------------|--|
| 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. |
| Access-Control-Max-Age | Specifies the duration in which the response result can be retained and cached for a prefetch 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. |

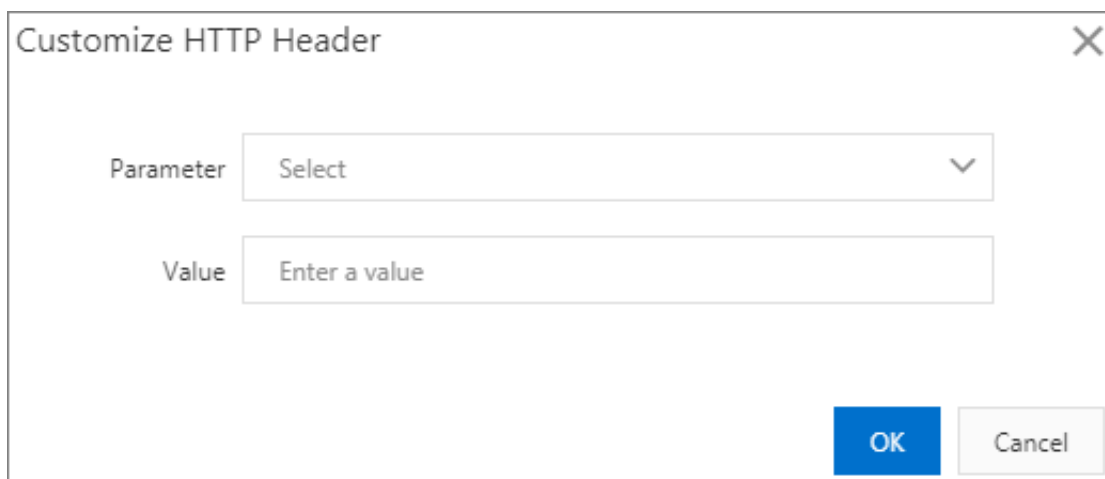
When you create an HTTP response header, note the following limits:

- 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, [submit a ticket](#).
- The Access-Control-Allow-Origin parameter can be set as an asterisk (*) to allow cross-domain requests or a specific domain name such as `www . aliyun . com`.
- 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 target domain name and click Manage.
4. In the left-side navigation pane of the specified domain, click Cache.
5. Click HTTP Header.

6. On the HTTP Header tab, click **Customize**.

A dialog box titled "Customize HTTP Header" with a close button (X) in the top right corner. It contains two input fields: "Parameter" with a dropdown menu showing "Select" and a downward arrow, and "Value" with a text input field containing the placeholder "Enter a value". At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (gray).

7. In the Customize HTTP Header dialog box that appears, set the parameters.

8. Click **OK**.

You can click **Modify** or **Delete** in the **Actions** column corresponding to an HTTP header to modify or delete the HTTP header.

7.5 Customize an error page

When a client requests a Web service through a browser, the website hosting server generates a 404 Not Found page 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 server returns the corresponding web pages when these errors are returned. This topic describes how to customize an error page.

Context

Alibaba Cloud CDN provides two types of error pages: default page and custom page. 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 default 404 Not Found page.
- **Custom page:** When the HTTP response carries the 404 error, the server generates the custom page. You must specify a full URL for the custom page.

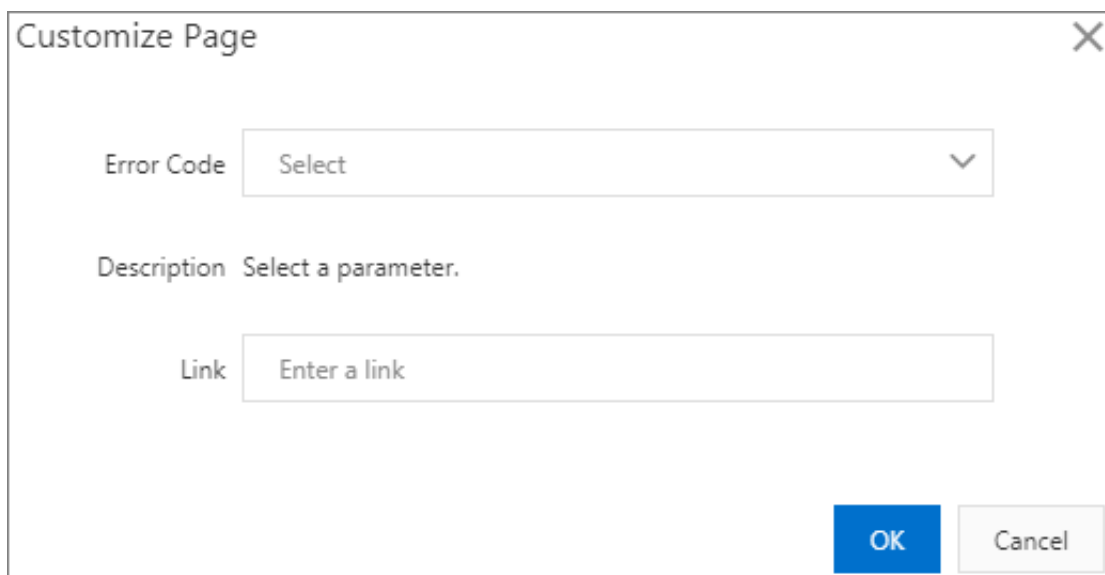


Note:

- Default pages are considered Alibaba Cloud public resources and are free of charge.
- Custom pages are considered personal resources and 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 target domain name and click Manage.
4. In the left-side navigation pane of the specified domain, click Cache.
5. Click Custom Pages.
6. On the Custom Pages tab, click Customize.



7. In the Customize Page dialog box that appears, set the parameters.
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.
8. 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.

7.6 Configure a rewrite rule

The rewrite function allows you to modify the requested Uniform Resource Identifier (URI) and configure destination URIs for 302 redirects. You can configure multiple rewrite rules as needed. This topic describes how to configure rewrite rules in the CDN console.

Context

If you need to modify the requested URI, create a rewrite rule. For example, if a client requests to visit `http://example.com` through HTTP, you can create a rewrite rule to redirect the request to `https://example.com`.

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 Cache.
5. On the Rewrite tab, click Create.
6. Click Rewrite.

7. On the Rewrite tab, click Create.

Create Rewrite Rule

Original URI

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

Rewritten URI

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

Flag

Redirect

Break

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

OK

Cancel

8. Set the Original URI, Rewritten URI and Flag as needed.

A CDN node uses one of the following 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.

9. Click OK.

After a rewrite rule is configured, you can click **Modify** or **Delete** in the **Actions** column to modify or delete the rewrite rule.

| Example No. | Request URI | Destination URI | Rewrite 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 and redirects the client to <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 and redirects the client to <code>http://domain.com/index.html</code> . |

8 HTTPS

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?

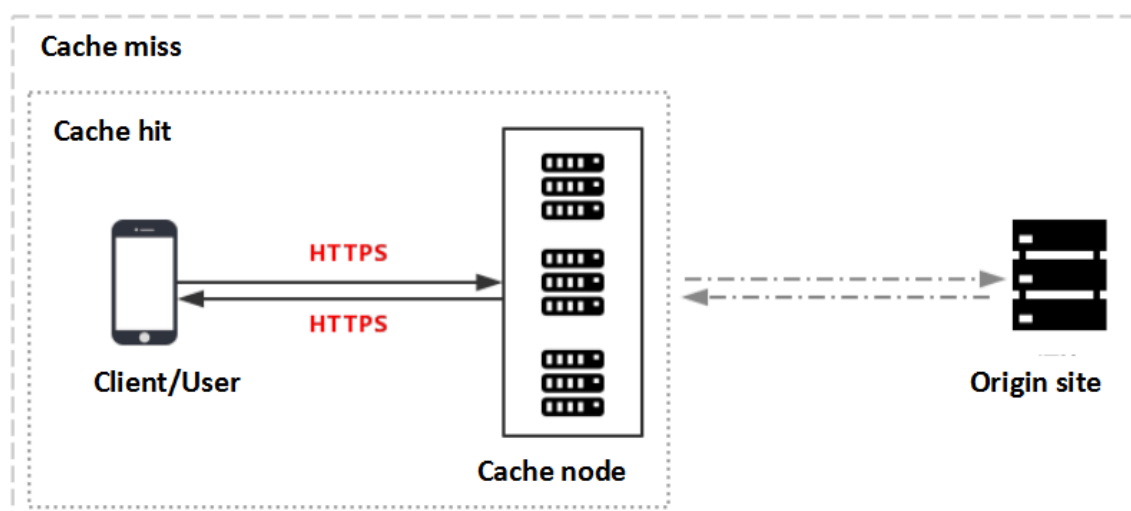
Hypertext Transfer Protocol (HTTP) transmits content in plaintext and does not encrypt data in any form. As an extension of HTTP, Hypertext Transfer Protocol Secure (HTTPS) is an HTTP channel designed to enhance security. Secure Sockets Layer (SSL) or Transport Layer Security (TLS) is used as a sublayer 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"> - #unique_83 <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"> - #unique_84 <p>Video or audio applications and websites that provide content for users to download.</p> <ul style="list-style-type: none"> - #unique_85 <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"> - #unique_60 <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 #unique_27 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 #unique_25. • 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 #unique_6/unique_6_Connect_42_section_jdt_lwl_zdb.</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 #unique_86. </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 |
|-------------------------------|--|
| #unique_25 | 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. |
| #unique_27 | Supports force redirects on original request methods of end users. |
| #unique_28 | Helps to ensure communication security and data integrity. |
| #unique_29 | Forces clients such as browsers to establish HTTPS connections with servers, reducing hijacking risks in the first access requests. |

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-----
MIIEpAIBAAKCAQEAyZiSSSCHH67bmT8mFykAxQ1tKCYukwBiWZwk0StFEbTWHy8K
tTHSFD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A
Xw9SgrqFJMjC1va2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ
/fD0XXyuWoqaIePZtK9Qn957ZEPhtUpVZuhS3409DDM/tJ3Tl8aaNYWhrPBc0
jNcz0Z6XQGF1rZG/Ve520GX6rb5dUYpdcfXzN5WM6xYg8a1L7UHDHPI4AYsatdG
z5TMPnmEf8yZPUYudTLxgMVAovJr09Dq+5Dm3QIDAQABAoIBAGl68Z/nnFyRHRFi
laF6+Wen8ZvNqkm0hAMQwIJh1Vp1f174//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35
cgQ93Tx424WGpCwUshSfxewfbAYGf3ur8W0xq0uU07BAxaKHnCMNG7dGyolUowRu
S+yXLrpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2
06W/zH24YAxwkTYLKGHjoieYs111ah1AJvICVgTc3+LzG2pIpM7I+K0nHC5eswvM
i5x9h/OT/ujZsyX9P0PaAyE2bqy0t080tGexM076Ssv0KVhKFvWjLUnhf6WcqFCD
xqhhxkECgYEA+PftNb6eyXl+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhggHu0edU
ZXIHRJ9u6B1XE1arpijVs/WHmFhYSTm6DbdD7S1tLy0BY4cPTRhziFTKt8AkIXMK
605u0UiWsq0Z8hn1X141ox2cW9ZQa/Hc9udeyQotP4NsMJWgpBV7tC0CgYEAwwNf
0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzFEG8/AR3Md2rhmZi
GnJ5dfde7uY+JsQfX2Q5JjwTad1BW4led0Sa/uKRao4UzVgnYp2aJKxtuWffvVbU
+kf728ZJRA6azSLvGmA8hu/GL6bgFU3fkSkw03ECgYBpYK7TT7JvvnAERMtJf2yS
ICRkbQaB3gPSe/LCgzy1nhtaFOUbNxeuowLAZR0wrz7X3TZqHEDcYoJ7mK346of
QhGLITyoeHkbYkAUtq038Y04EKH6S/IzMzB0frXiPKg9s8UKQzkU+GSE7ootli+a
R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUHKIKcP/+xn
R3kV106MZCFAdqirAjiQWapKh9Bxbp2eHCrB81MFAWLRQSl0k79b/jVmtZMC3upd
EJ/iSWjZKPbw7hCFAeRtPhxyNTJ5idEiu9U8EQid8111giPgn0p3sE0HpDI89qZX
aaIMEQKBgQDK2bsnZE9y0ZWhteu94vziKmFrSkJMGH8pLaTiliw1iRhRYWJysZ9
BOIDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcv0Bh5Hx0yy23m9hFRzfDeQ7z
NTKh193HHF1joNM81LHFYGRFEWWrr0W5gfBudR6USRnR/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

HTTPS is an HTTP channel designed to enhance security. HTTPS provides better protection for content transmission through CDN, allowing clients to browse website

content more securely and effectively at a high speed. This topic describes how to authenticate and configure HTTPS certificates.

Prerequisites

You must purchase an advanced HTTPS certificate or apply for a free HTTPS certificate in the [Alibaba Cloud Security console](#).

Context

Your HTTPS certificate files must be in `PEM` format. For more information, see [#unique_86/unique_86_Connect_42_section_cn2_rql_xdb](#).

HTTPS acceleration is a value-added service. After you enable HTTPS, HTTPS requests incur additional fees. The fee is separately charged based on HTTPS requests and is not covered by the CDN data transfer plan. For more information about the billing standards, see [#unique_6](#).

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

- A domain validated (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.
- An organization validated (OV) certificate is a standard SSL certificate that verifies the identity of an organization. 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.
- An extended validated (EV) certificate follows the guidelines maintained by the Certification Authority Browser Forum, also known as the CA/Browser Forum. An EV certificate is the SSL certificate 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 sectors such 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 target domain name and click Manage.

4. In the HTTPS Certificate section, click **Modify**.

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

Certificate Name

Enter a certificate name

Content

PEM Encoding Reference

Private Key

PEM Encoding Reference

You can go to the SSL Certificates Service console to [manage and upload certificates](#). You can also click [Issue](#).

OK

Cancel

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

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

you whether you want to enable this function. For more information about HTTPS billing standards, see [#unique_6](#).

| Parameter | Description |
|------------------|---|
| Certificate Type | <p>Alibaba Cloud Certificate</p> <p>You can apply for a free certificate or purchase an advanced certificate in the Alibaba Cloud Security console.</p> <p>Custom</p> <p>If you cannot find a suitable certificate,</p> |
| | <p>you can</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 Reference under the Content field. |

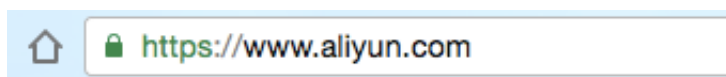
| Parameter | Description |
|-------------|---|
| Private Key | When Certificate Type is set to Custom, you must enter the private key. For more information, click PEM Encoding Reference under the Private Key field. |

6. Click OK.

You can disable, enable, and 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-upload the certificate or private key.

7. Verify that the HTTPS certificate takes effect.

An updated HTTPS certificate takes effect on the entire network within one minute. To verify if 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 acceleration is in effect.



8.4 Enable HTTP/2

HTTP/2 is the latest version of HTTP, which has improved resource access efficiency and security. This topic describes the concept and benefits of HTTP/2, and how to enable it.

Prerequisites

Make sure an HTTPS certificate is configured. For more information, see [#unique_25](#).



Note:

- If this is the first time that you configure an HTTPS certificate, you must wait for the certificate to take effect before enabling HTTP/2.
- If you disable HTTPS acceleration after enabling HTTP/2, HTTP/2 is automatically disabled.

Context

HTTP/2, originally named HTTP 2.0, is the latest version of HTTP. It is supported by all major browsers such as Google Chrome, Internet Explorer 11, Safari, and Mozilla Firefox. HTTP/2 provides optimized performance and is compatible with HTTP/1.1 semantics. HTTP/2 is similar to SPDY but differs greatly from HTTP/1.1.

Benefits of HTTP/2:

- **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, protecting content security while maintaining network performance.
- **Multiplexing:** HTTP/2 allows 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 at the same time. In addition, you can set stream dependencies, which the client uses to inform the server of the importance of a given stream relative to other streams on the same connection, so that resources can be allocated appropriately.

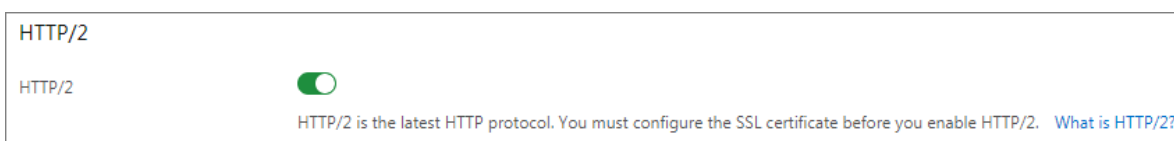
- **Header compression:** HTTP headers carry large volumes of information, which is transmitted repeatedly. HTTP/2 compresses HTTP headers into the HPACK format, allowing both ends of the communications to each cache a copy of the HTTP header indexes and hence transmit only index numbers for duplicate HTTP headers. This increases transmission speed and efficiency.
- **Server push:** Like SPDY, HTTP/2 can push messages to clients. HTTP/2 is widely adopted by many websites, such as Google.com, Amazon.com, and Taobao.com. 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 developed by Google based on TCP. SPDY minimizes network latency to accelerate network access and improve user experience. SPDY is not a replacement for HTTP but serves as an enhancement to HTTP. Similar to 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 target domain name and click Manage.
4. On the HTTP/2 tab, turn on HTTP/2.



8.5 Enable force redirect

You can enable the Force Redirect function to redirect the original requests from a client to L1 as HTTP or HTTPS requests. This topic describes how to enable the Force Redirect function.

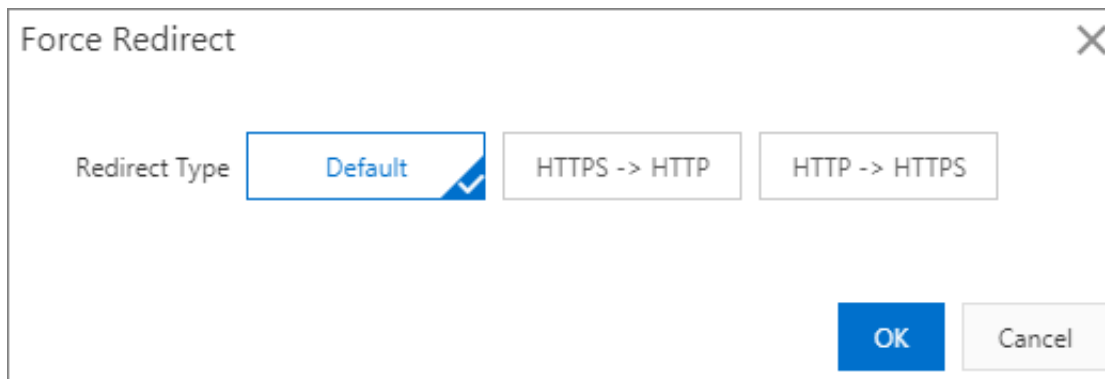
Prerequisites

Make sure an HTTPS certificate is configured. For more information, see [#unique_25](#).

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 Force Redirect section, click Modify.

A dialog box titled "Force Redirect" with a close button (X) in the top right corner. It contains a "Redirect Type" label followed by three buttons: "Default" (highlighted with a blue border and a checkmark), "HTTPS -> HTTP", and "HTTP -> HTTPS". At the bottom right, there are "OK" and "Cancel" buttons.

Force Redirect

Redirect Type

Default HTTPS -> HTTP HTTP -> HTTPS

OK Cancel

5. In the Force Redirect dialog box that appears, set Redirect Type.

| 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>
```

6. Click OK.

8.6 Configure TLS

You can use the TLS Version Control function of Alibaba Cloud CDN to ensure the data security and integrity of all Internet services and communications. You can configure TLS versions based on domain names. This topic describes how to configure TLS for a domain.

Prerequisites

Make sure an HTTPS certificate is configured. For more information, see [#unique_25](#).

Context

Transport Layer Security (TLS) is designed to ensure the security and integrity of data transmitted between two applications. HTTPS is a typical application of TLS. HTTPS, also known as HTTP over TLS, is a secure version of HTTP. HTTPS runs below the top application layer (HTTP) and above the transport layer (TCP), providing data encryption and decryption 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 target domain name and click Manage.
4. In the TLS Version Control section, you can enable or disable specific TLS versions as needed.

The following table describes TLS versions.

| TLS version | Description | Supported browser |
|-------------|---|--|
| 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 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). | <ul style="list-style-type: none"> • Internet Explorer 6 and later • Google Chrome 1 and later • Mozilla Firefox 2 and later |
| TLS 1.1 | TLS 1.1 was defined in RFC 4346 in 2006 as an update for TLS 1.0. This version fixed some vulnerabilities of TLS 1.0. | <ul style="list-style-type: none"> • Internet Explorer 11 and later • Google Chrome 22 and later • Mozilla Firefox 24 and later • Safari 7 and later |
| TLS 1.2 | TLS 1.2 was defined in RFC 5246 in 2008 and has become the most widely used TLS version. | <ul style="list-style-type: none"> • Internet Explorer 11 and later • Google Chrome 30 and later • Mozilla Firefox 27 and later • Safari 7 and later |

| TLS version | Description | Supported browser |
|-------------|---|---|
| TLS 1.3 | TLS 1.3 was defined in RFC 8446 in 2018. TLS 1.3 is faster because it supports the 0-RTT mode. Also, this version is more secure as it only supports perfect forward secrecy key exchange algorithms. | <ul style="list-style-type: none">• Google Chrome 70 and later• Mozilla Firefox 63 and later |

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.

TLSv1.0

☒

TLSv1.1

☒

TLSv1.2

☒

TLSv1.3

☒

**Note:**

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

8.7 Configure HSTS

This topic describes how to configure HTTP Strict Transport Security (HSTS). After HSTS is configured, a client can only establish HTTPS connections.

Prerequisites

An HTTPS certificate is configured. For more information, see [#unique_25](#).

Context

When HTTPS is enabled for your website, all HTTP requests destined for the website are redirected to HTTPS through 301 and 302 errors regardless whether you enter an HTTP URL in the address bar of the browser or directly click an HTTP URL. During the redirection process, the request and response messages may be hijacked and consequently the redirected requests cannot be sent to the server. HSTS is introduced to resolve this issue.

HSTS is a response header, `Strict - Transport - Security : max - age = expireTime [; includeSub Domains] [; preload]`. The following table describes the parameters in the header.

| Parameter | Description |
|---------------------------|---|
| max-age | The maximum time period during which the requested resource is cached. Unit: second. |
| Strict-Transport-Security | Within the time period specified by the <code>max - age</code> parameter, if the <code>Strict - Transport - Security</code> parameter in the HTTP request from the domain has not expired, the browser redirects the HTTP request to HTTPS through a 307 error. This helps to prevent hijacking risks that may arise when the HTTP request is redirected between the server and browser through a 310 or 302 error. |
| includeSubDomains | Optional. If this parameter is set, the preceding parameters take effect on all subdomains of the domain. |
| preload | Optional. This parameter enables you to preload a list. |

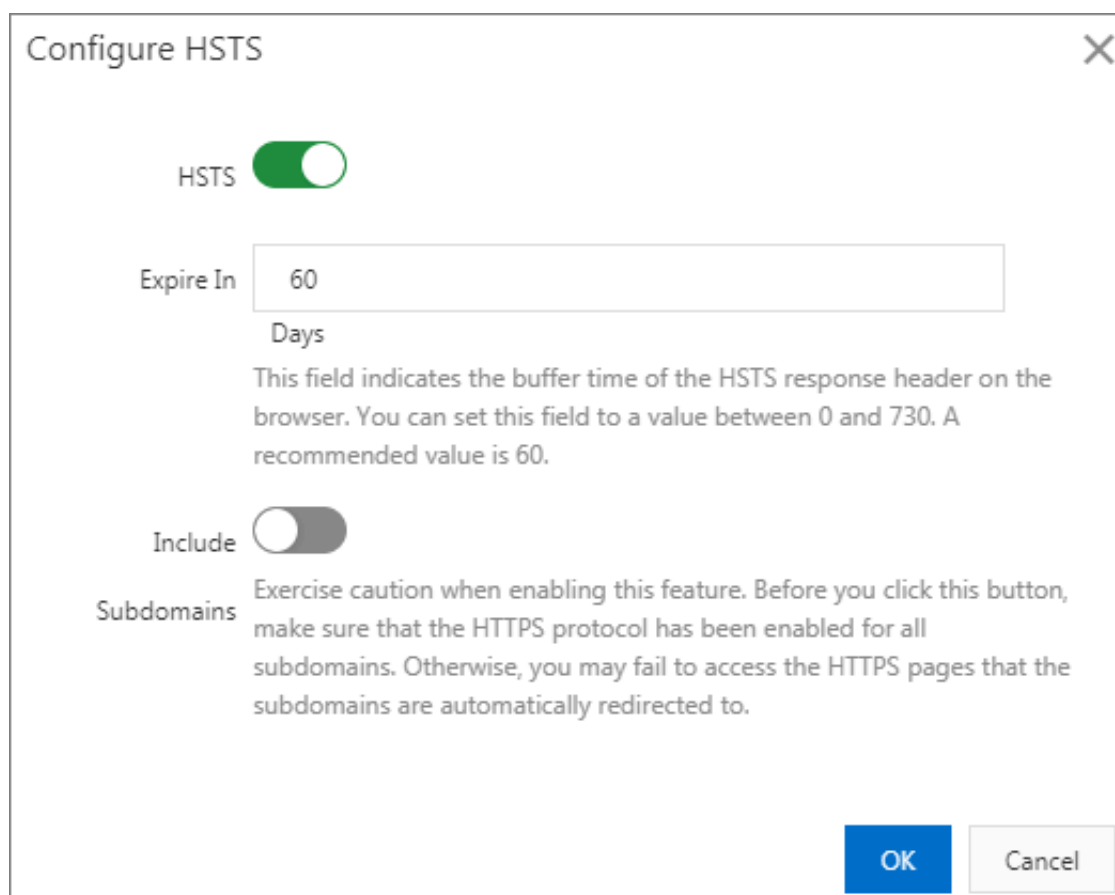
**Note:**

- Before HSTS takes effect, the first HTTP request is redirected to HTTPS through a 301 or 302 error.
- The HSTS response header takes effect on the responses to HTTPS requests but not on the responses to HTTP requests.
- HSTS takes effect only on Port 443 and on domains instead of IP addresses.

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 HSTS section, click **Modify**.



The image shows a 'Configure HSTS' dialog box with a close button (X) in the top right corner. It contains three main settings: 1. 'HSTS' toggle switch, which is currently turned on (green). 2. 'Expire In' text input field containing the value '60', with 'Days' written below it. A descriptive note states: 'This field indicates the buffer time of the HSTS response header on the browser. You can set this field to a value between 0 and 730. A recommended value is 60.' 3. 'Include Subdomains' toggle switch, which is currently turned off (grey). A descriptive note states: 'Exercise caution when enabling this feature. Before you click this button, make sure that the HTTPS protocol has been enabled for all subdomains. Otherwise, you may fail to access the HTTPS pages that the subdomains are automatically redirected to.' At the bottom right, there are two buttons: 'OK' (blue) and 'Cancel' (grey).

5. In the displayed Configure HSTS dialog box, turn on the HSTS switch, and set **Expire In** and **Include** .

6. Click **OK**.

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

9.1 Overview

You can use whitelists, blacklists, and URL authentication to verify the identity of visitors and filter visitors. With these functions, you can control access to CDN resources and improve the security of your CDN service. You can configure Referer, IP, and UserAgent whitelists and Referer, IP, and UserAgent blacklists.

You can use the following functions to implement access control.

| Function | Description |
|----------------------------|---|
| #unique_96 | Allows you to configure a Referer blacklist or whitelist to identify and filter visitors so that you can control access to CDN resources. |
| #unique_97 | Allows you to configure URL authentication to prevent unauthorized downloads and use of resources on origin sites. URL authentication is more secure than Referer-based hotlink protection. |
| #unique_98 | Allows you to configure an IP blacklist or whitelist to identify and filter visitors so that you can control access to CDN resources. |
| #unique_33 | Allows you to configure a UserAgent blacklist or whitelist to identify and filter visitors so that you can control access to CDN resources. |

9.2 Configure hotlink protection

You can configure a referer blacklist or whitelist to identify and filter users, restricting access to CDN resources and improving CDN security. This topic describes how to configure hotlink protection.

Context

- Hotlink protection is implemented by the HTTP referer mechanism. Referer is used to track and identify where requests come from.
- Hotlink protection enables you to configure a blacklist or whitelist. After you send a request to access resources, the request is directed to a CDN node. The CDN node will filter users based on the configured blacklist or whitelist. If the domain names of users are whitelisted, users can access the requested resources. If the domain

names of users are blacklisted, users cannot access the requested resources, and a 403 error is returned.

**Notice:**

- Hotlink protection is optional. By default, hotlink protection is disabled.
- The blacklist and whitelist are mutually exclusive. Only either of them can take effect at any time.
- After hotlink protection is configured, CDN automatically adds a wildcard (*) to domain names. For example, if you enter a.com, the domain name will be configured as *.a.com. Hotlink protection takes effect on all the subdomains of a.com.
- You can specify whether to allow requests with an empty referer header to access CDN resources. You can access CDN resources by entering a URL into a web browser.

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 Access Control.

5. In the Hotlinking Protection section, click Modify.

Configure Hotlinking Protection

Type

Blacklist

Whitelist

The blacklist and whitelist cannot be configured at the same time.

Rules

Press Enter to separate multiple referers. Wildcard "*" is supported.
Example: a.*b.com can match aliyun.b.com or a.img.b.com.

☐ Allow resource URL access from browsers

Allow empty referers to access CDN resources.

OK

Cancel

6. Configure Blacklist or Whitelist as prompted.

| Parameter | Description |
|-----------|--|
| Type | <p>The following two types are supported:</p> <ul style="list-style-type: none">• Blacklist <p>Blacklisted domain names cannot be used to access CDN resources</p> <ul style="list-style-type: none">• Whitelist <p>Only whitelisted domain names can be used to access CDN resources.</p> <p>The blacklist and whitelist are mutually exclusive. Only either of them can take effect at any time.</p> |

| Parameter | Description |
|-----------|---|
| Rules | Separate multiple domain names in a referer blacklist or whitelist with carriage return characters. You can use wildcards (*) to perform fuzzy matching. For example, a.*b.com can match a.aliyun.b.com or a.img.b.com. |

7. Click OK.

9.3 Business type

9.3.1 Configure URL authentication

The URL authentication feature protects origin server resources from unauthorized download and access. You can prevent some hotlinking issues by configuring a referer blacklist or whitelist with hotlink protection. However, this method cannot completely protect resources on the origin server because referer content can be forged. URL authentication is a more secure and effective method to protect resources on the origin server.

Context

URL authentication is a more secure and reliable method that integrates CDN nodes with the origin server to protect resources on the origin server.

- The origin server provides encrypted URLs that contain permission verification information.
- You can send a request to a CDN node by accessing an encrypted URL.
- The CDN node authenticates the permission information in the encrypted URL to determine whether the request is valid. If the request is valid, the CDN node returns a successful response. If the request is invalid, the CDN node rejects the request.

For more information about sample Python authentication code, see [#unique_102](#).

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 Access Control.
5. Click URL Authentication.

6. In the URL Authentication section, click Modify.

Set URL Authentication

URL ☐

Authentication

Type

Type A

Type B

Type C

Primary Key

Enter a primary key

The key must be 6 to 32 characters in length and can contain uppercase letters, lowercase letters, and numbers.

Secondary Key

Enter a secondary key

The key must be 6 to 32 characters in length and can contain uppercase letters, lowercase letters, and numbers.

OK

Cancel

7. Turn on the URL Authentication switch as prompted to configure URL authentication.

| Parameter | Description |
|---------------|--|
| Type | CDN supports three authentication types. You can select an authentication type based on your need to protect resources on the origin server. The following URL authentication types are supported: <ul style="list-style-type: none">• #unique_103• #unique_104• #unique_105 |
| Primary Key | The primary password corresponding to the selected authentication type. |
| Secondary Key | The secondary password corresponding to the selected authentication type. |

8. Click OK.

What's next

You can perform the following steps to generate a signed URL.

1. In the Generate Signed URL section, configure Original URL and authentication information.

| Parameter | Description |
|-------------------|--|
| Original URL | The complete original URL. For example, https://www.aliyun.com . |
| Type | The authentication type. Select one of the following URL authentication types: <ul style="list-style-type: none">• #unique_103• #unique_104• #unique_105 |
| Cryptographic Key | The authentication password. Cryptographic Key can be Primary Key or Secondary Key configured in the Set URL Authentication dialog box. |

| Parameter | Description |
|-----------------|--|
| Validity Period | The validity period for URL authentication. Unit: seconds. Example value: 1,800. |

Generate Signed URL

Original URL

Type

Type A

Type B

Type C

Cryptographic Key

Validity Period

Generate

2. Click Generate.

Obtain Authentication URL and Timestamp.

Signed URL

https://cdn.console.aliyun.com?auth_key=1586805148-0-0-95b0a8fccc1a17994ac4f223d4f2e9294

Copy

Timestamp

1586805148

9.3.2 Authentication method A

How it works

Formats of the encrypted URL for user access

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

Authentication fields

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

| Field | Description |
|-----------|---|
| timestamp | The expiration time. It is a positive integer with a fixed length of 10 and a time in seconds from January 1, 1970. This 10-digit integer is used to control the expiration time. Effective time is 1,800 seconds. |
| rand | random number, we recommend that you use UUID (not including hyphen “-”, for example, 477b3bbc253f467b8def6711128c7bec format) |
| uid | Not used yet (set to 0). |
| md5hash | Verification string calculated by the MD5 algorithm, which is a combination of numbers 0 to 9 and lowercase English letters a to z, with a fixed length of 32 characters |

When the CDN server receives a request, it first determines whether the

`timestamp` in the request is earlier than the current time.

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

file is returned. Otherwise, the request fails the authentication, and an HTTP 403 error is returned.

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

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

An instance of authorization

1. Request object by `req_auth` :

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

2. Set key to: aliyuncdnexp1234 (you can configure yourself)
3. The expiration date of the authentication configuration file is October 10, 2015 00:00:00. The calculated number of seconds is 1,444,435,200.
4. The CDN server constructs a signature string for the calculation of HashValue:

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

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

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

6. When requested, the URL is:

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

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

9.3.3 Authentication method B

Principles

Formats of the encrypted URL for user access

* The user access URL is as follows:

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

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

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

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

Authentication fields

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

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

Example

1. Back-to-source request object.

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

2. The key is set to aliuncdnexp1234 (user-defined).

3. The time for the user to access the client source server is 201508150800 (format: YYYYMMDDHHMM).

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

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

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

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

6. The URL to request CDN:

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

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

9.3.4 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.

9.3.5 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 ()
```

9.4 Configure an IP address blacklist or whitelist

You can configure an IP address blacklist or whitelist to identify and filter users, restricting access to CDN resources and improving CDN security. This topic describes how to configure an IP address blacklist or whitelist.

Context

- **IP address blacklist:** Blacklisted IP addresses are not allowed to access CDN resources.

If your IP address is blacklisted, requests from your IP address can be sent to a CDN node. However, the CDN node will reject the requests and return a 403 error. The requests from blacklisted IP addresses are recorded in CDN logs.

- **IP address whitelist:** Only whitelisted IP addresses are allowed to access CDN resources.



Note:

- Both IP address blacklists and whitelists support IPv6 addresses.
- Both IP address blacklists and whitelists support CIDR block notations. For example, in the CIDR block 192.168.0.0/24, /24 indicates that the first 24 bits are network bits. The remaining 8 bits are host bits. The subnet can accommodate 254 hosts. 192.168.0.0/24 indicates that IP addresses range from 192.168.0.1 to 192.168.0.254.

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 Access Control.
5. Click IP Blacklist/Whitelist.

6. On the IP Blacklist/Whitelist, click Modify.

Configure Blacklist/Whitelist

Type

Blacklist

Whitelist

The blacklist and whitelist cannot be configured at the same time.

Rules

Up to 100 unique entries (IP address or CIDR block) are supported. Press Enter to separate entries.

OK

Cancel

7. Configure Blacklist or Whitelist as prompted.

| Parameter | Description |
|-----------|--|
| Type | <p>The following two types of IP address lists are supported:</p> <ul style="list-style-type: none">• Blacklist <p>The blacklisted IP addresses are not allowed to access CDN resources.</p> <ul style="list-style-type: none">• Whitelist <p>Only the whitelisted IP addresses are allowed to access CDN resources.</p> <p>The blacklist and whitelist are mutually exclusive. Only either of them can take effect at any time.</p> |

| Parameter | Description |
|-----------|---|
| Rules | You can configure a maximum of 100 IP addresses or CIDR blocks and separate them with carriage return characters. Each CIDR block must be unique. For example, if the IP address 192.168.0.1/24 is already configured, it cannot be configured again. |

8. Click OK.

9.5 Configure a User-Agent blacklist or whitelist

You can configure a User-Agent blacklist or whitelist to identify and filter visitors, restricting access to CDN resources and improving CDN security. This topic describes how to configure a User-Agent blacklist or whitelist.

Context

If you want to implement access control based on the User-Agent field, you must configure a User-Agent blacklist or whitelist to filter requests.

- **User-Agent blacklist:** The User-Agent fields on the blacklist cannot be used to access resources.

If your User-Agent field is added to the blacklist, a request with the User-Agent field can still be sent to a CDN node. However, the request will be rejected by the CDN node, and a 403 error will be returned. Requests that contain the User-Agent fields on the blacklist are still recorded in CDN logs.

- **User-Agent whitelist:** Only User-Agent fields on the whitelist can be used to access resources.

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 Access Control.
5. Click UserAgent Blacklist/Whitelist.

6. On the UserAgent Blacklist/Whitelist tab, click Modify.

Configure Blacklist/Whitelist

Type

Blacklist

Whitelist

The blacklist and whitelist cannot be configured at the same time.

Rules

Supports the wildcard "*" and multiple values. The wildcard can match any string and values are separated with vertical bars (|). Example:
curl|*IE*|*chrome*|*firefox*

OK

Cancel

7. Configure Blacklist or Whitelist as prompted.

| Parameter | Description |
|-----------|---|
| Type | <p>The following two types are supported:</p> <ul style="list-style-type: none">• Blacklist <p>The User-Agent fields on the blacklist cannot be used to access resources.</p> <ul style="list-style-type: none">• Whitelist <p>Only User-Agent fields on the whitelist can be used to access resources.</p> <p>The blacklist and whitelist are mutually exclusive. Only either of them can take effect at any time.</p> |

| Parameter | Description |
|-----------|--|
| Rules | When you configure the User-Agent field, use vertical bars () to separate multiple values. The User-Agent field can contain wildcards (*). For example, *curl* *IE* *chrome* *firefox*. |

8. Click OK.

10 Performance optimization

10.1 Overview

CDN provides multiple optimization functions for you to reduce the size of the content that you want to access, accelerate content delivery, and improve the readability of the requested Web pages.

CDN supports the following optimization functions.

| Function | Description |
|-----------------------------|---|
| #unique_114 | Removes comments and whitespaces in HTML pages to reduce the payload size and improve the readability. |
| #unique_115 | Automatically compresses static content with gzip. This significantly reduces the size of the transmitted content and accelerates content delivery. |
| #unique_36 | Enable Brotli compression if you want to compress static text files . It can reduce the size of the transmitted content and accelerate content delivery. |
| #unique_116 | If a CDN node receives a URL request with a question mark (?) followed by <i>request parameters</i> , it determines whether the URL request needs to be rerouted to the origin with the parameters. |

10.2 Configure HTML optimization

When you enable the HTML optimization feature, CDN automatically removes redundant comments and duplicate spaces from all HTML pages. This helps reduce file size and improve page readability. This topic describes how to enable the HTML optimization feature.

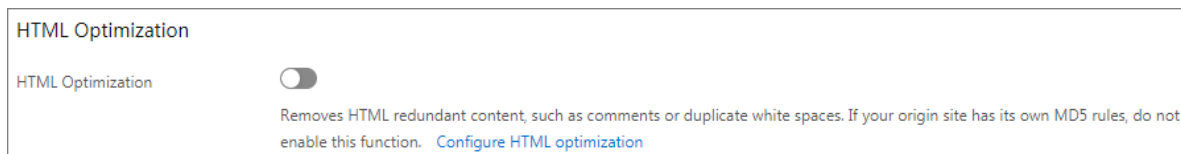
Context

When you enable the HTML optimization feature, CDN automatically removes redundant comments and duplicate spaces from all HTML pages. This helps reduce file size and improve the efficiency of content delivery.

If MD5 validation is configured for a file in the origin server, do not enable this feature. When pages are optimized, the MD5 value of the optimized file is different from that of the file in the origin server, which causes MD5 validation to fail.

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 Optimization.
5. In the HTML Optimization section, turn on HTML Optimization.



10.3 Configure intelligent compression

When you enable the intelligent compression feature, static files will be automatically GZIP compressed. GZIP compression reduces the size of the transmitted files and accelerates content delivery. This topic describes how to enable the intelligent compression feature.

Context

- Intelligent compression supports the following formats: 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, and application/xmltext.
- If a request from the client includes the `Accept - Encoding : gzip` request header, the client expects the requested resource to be GZIP compressed.
- If a response from a CDN node includes the `Content - Encoding : gzip` response header, the requested resource is GZIP compressed.



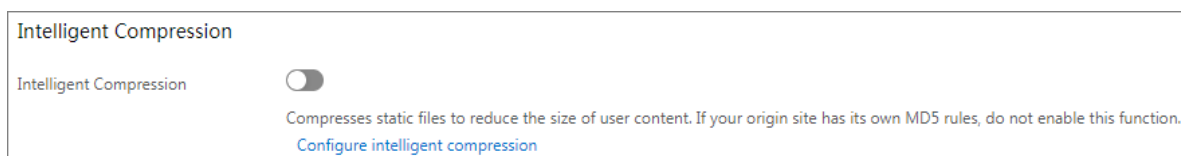
Notice:

- If MD5 validation is configured for a file in the origin server, do not enable this feature. When a static file is compressed, the MD5 value of the compressed file is different from that of the file in the origin server, which will cause MD5 validation to fail.
- Files in the origin server will be GZIP compressed only when the file size exceeds 1,024 B.

- Internet Explorer 6 is not fully compatible with GZIP. If your customers expect to use Internet Explorer 6, we recommend you disable the intelligent compression feature.

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 Optimization.
5. In the Intelligent Compression section, turn on Intelligent Compression.



10.4 Configure Brotli compression

When you want to compress static text files, you can enable the Brotli compression feature to reduce the size of the transmitted content and accelerate content delivery. This topic describes how to enable the Brotli compression feature.

Context

Brotli is a new open-source compression algorithm. With Brotli compression enabled, CDN nodes can compress the text files such as HTML, JavaScript, and CSS when it returns the requested resource. The efficiency of Brotli compression is 15 to 25% higher than that of intelligent compression.

- If a request includes the `Accept - Encoding : br` request header, the client expects the requested resource to be Brotli compressed.
- If a response from a CDN node includes the `Content - Encoding : br` response header, the requested resource is Brotli compressed.

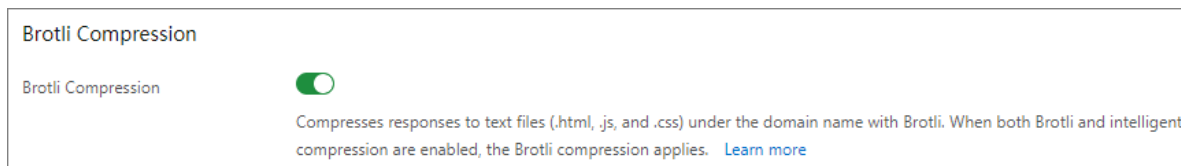


Notice:

If both Brotli compression and GZIP compression are enabled, and the `Accept - Encoding` request header includes `br` and `gzip`, Brotli compression takes priority.

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



10.5 Configure parameter filtering

If a request URL contains a question mark (?) and *parameters*, such as `http://alibaba.com/content?a=10`, CDN nodes will determine whether to retrieve content from the origin server based on the entire request URL. This topic describes how to configure parameter filtering.

Context

- Enable parameter filtering

When a request is sent to a CDN node, the CDN node removes the parameters after the question mark (?) in the URL when retrieving content from the origin server. The CDN node caches only one copy of the requested content.

- Most HTTP requests contain parameters. However, parameters can be ignored when they have low priorities. After you enable parameter filtering, the file cache hit rate and delivery efficiency are improved.
- If a parameter contains important information such as the file version, we recommend you set Retain Parameters to retain this parameter. You can retain up to 10 parameters. If the request URL contains a retained parameter, the CDN node will retrieve content from the origin server based on the URL with the retained parameter.

- Disable parameter filtering

Different copies of the requested content corresponding to different parameters in URLs will be cached.

Parameter filtering consists of Retain Parameters feature and Ignore Parameters feature.

- **Retain Parameters:** You can specify one or more parameters to be retained. You must separate multiple parameters with commas (.). Unspecified parameters are not retained.
- **Ignore Parameters:** You can specify one or more parameters to be ignored. You must separate multiple parameters with spaces. Unspecified parameters are not ignored.



Note:

The URL authentication feature takes priority over parameter filtering. The authentication information in authentication type A contains parameters of an HTTP request. Therefore, CDN nodes perform URL authentication first. The CDN node caches a copy of the requested content after the URL authentication succeeds. For more information about how to configure URL authentication, see [Configure URL authentication](#).

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 Optimization.

5. In the Parameter Filtering section, click **Modify** below **Retain Parameters** or **Ignore Parameters**.

Filter Parameters

Parameter Filtering

☒

Parameter Filtering

Removes the parameters after the question mark (?) from the URL during the back-to-origin process to increase the file cache hit rate and delivery efficiency. [Configure parameter filtering](#)

Retain Parameters

Enter one or more parameters

Up to 10 parameters. Separate two parameters with a blank space.

Retain Origin Parameters

☐

Retain Origin Parameters

Retains all back-to-origin parameters.

OK

Cancel

Filter Parameters

Parameter Filtering

☒

Parameter Filtering

Ignores only the specified parameters. Other parameters will not be ignored. Multiple parameters are separated with blank spaces. [Specify ignored parameters](#)

Ignore Parameters

Enter one or more parameters

Separate two parameters with a blank space.

Retain Origin Parameters

☐

Retain Origin Parameters

Retains all back-to-origin parameters.

OK

Cancel

6. You can configure Retain Parameters or Ignore Parameters as needed.

- Retain Parameters

| Parameter | Description |
|--------------------------|--|
| Parameter Filtering | The switch used to retain parameters. After the Parameter Filtering switch is turned on, the parameters that follow question marks (?) in the URL are filtered out during the back-to-origin process. This helps increase the file cache hit rate. |
| Retain Parameters | The parameters to be retained. Up to 10 parameters can be configured. Separate multiple parameters with commas (,). |
| Retain Origin Parameters | The switch used to retain origin parameters. After the Retain Origin Parameters switch is turned on, all parameters are retained during the back-to-origin process. |

- Ignore Parameters

| Parameter | Description |
|---------------------|--|
| Parameter Filtering | The switch used to ignore parameters. After the Parameter Filtering switch is turned on, the specified parameters are ignored during the back-to-origin process. Unspecified parameters are not ignored. |
| Ignore Parameters | The parameters to be ignored. Up to 10 parameters can be configured. Separate multiple parameters with spaces. |

| Parameter | Description |
|--------------------------|---|
| Retain Origin Parameters | The switch used to retain origin parameters. After the Retain Origin Parameters switch is turned on, all parameters are retained during the back-to-origin process. |

Example:

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

- If the Retain Parameters feature is enabled:
 - a. The CDN node initiates the `http://www.abc.com/a.jpg` request to the origin server. The parameter `x=1` is ignored.
 - b. The origin server returns a response to the CDN node.
 - c. The CDN node caches a copy of the content requested by the `http://www.abc.com/a.jpg` request and then returns the content to the client.
 - d. The CDN node caches a copy of the requested content for the `http://www.abc.com/a.jpg` request, and returns the requested content to all requests similar to `http://www.abc.com/a.jpg?parameters`.
- If the Retain Parameters feature is disabled: `http://www.abc.com/a.jpg?x=1` and `http://www.abc.com/a.jpg?x=2` contain different parameters. Therefore, requested contents are returned based on the parameters following the question mark (?) in the URL.

7. Click OK.

11 Video Service Configuration

11.1 Overview

The object chunking and video seeking functions of CDN can help you reduce data transfer usage and improve the quality of video and audio playback.

With these functions, you can perform the following tasks.

| Function | Description |
|-----------------------------|---|
| #unique_123 | Reduces the amount of data forwarded back to the origin and the data delivery time. |
| #unique_124 | Allows you to seek to a specified position when playing video or audio, without affecting the playback effects. |

11.2 Configure object chunking

Object chunking allows the client to notify the origin server to return partial content within a specified range. It helps accelerate delivery of large files. This feature also helps reduce the consumption of back-to-origin traffic and improve resource response speed. This topic describes how to enable object chunking and related precautions.

Context

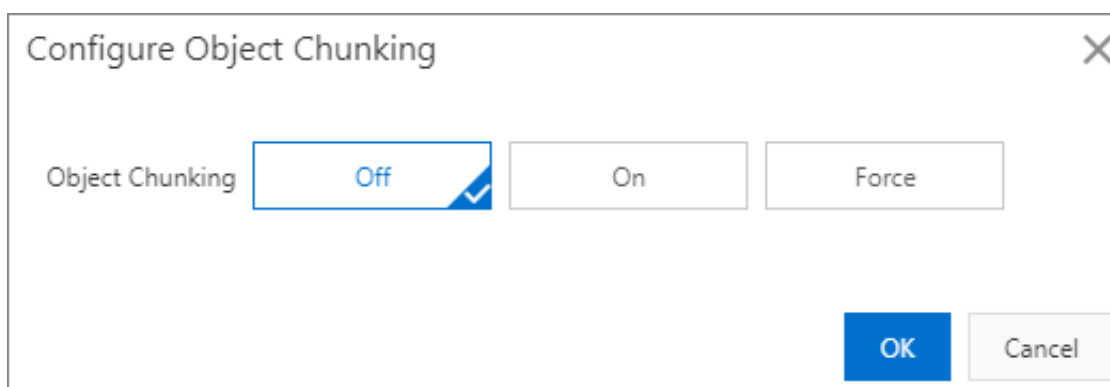
When you configure object chunking, take note of the following points:

- Ensure that the origin server supports range requests. If the HTTP request header contains the range field, the origin server must be able to return 206 Partial Content.
- Object chunking is optional and is disabled by default.

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. In the Object Chunking section, click **Modify**.



The dialog box titled "Configure Object Chunking" has a close button (X) in the top right corner. It contains three radio buttons for "Object Chunking": "Off" (selected with a blue checkmark), "On", and "Force". At the bottom right, there are "OK" and "Cancel" buttons.

6. Object Chunking can be set to On , Off , or Force .

| Object chunking | Description | Example |
|-----------------|--|---|
| On | Requests with the Range parameter can be sent to the origin server. The origin server returns a file that has the number of bytes within the range specified by the Range parameter. CDN nodes return the file to the client. | When a request sent from the client to a CDN node contains <code>range : 0 - 100</code> , the request received by the origin server also contains <code>range : 0 - 100</code> . The origin server returns a file with 101 bytes in the range of 0 to 100 to the CDN node. Then, the CDN node returns this file to the client. |
| Off | A CDN node redirects a request for the entire file on the origin server. The client automatically disconnects the HTTP connection to the CDN node after receiving a file that has the number of bytes within the range specified by the Range parameter. The requested file is not cached on the CDN node . This results in a low cache hit rate and large back-to-origin traffic. | When a request sent from the client to a CDN node contains <code>range : 0 - 100</code> , the request received by the origin server does not contain the Range parameter. The origin server returns a complete file to the CDN node. However, the CDN node returns a file with the first 101 bytes to the client. Because the HTTP connection is disconnected, this file is not cached on the CDN node. |
| Force | The requests with the range parameter are forcibly sent to the origin server. | When you set Object Chunking to Force , make sure that the origin server supports the Range parameter. |



Note:

When you set Object Chunking to Force, all chunked requests are forcibly sent to the origin server.

7. Click OK.

11.3 Video seeking

With video seeking enabled, you can seek to a specified position when you play video and audio. This topic describes how to configure video seeking.

Context

With video seeking enabled, if you seek to a specified position when you play video or audio on demand, the client sends a request to the server. The request contains the URL of the video or audio file, for example, `http://www.aliyun.com/test.flv?start=10`. The start parameter specifies the position that you want to seek to. After the server receives the request, it seeks to the keyframe at the specified position and then returns the content starting from this keyframe. If no keyframe can be found at the specified position, the server seeks to the last keyframe before the specified position.

- Before you configure video seeking, make sure that the origin site supports HTTP range requests. If an HTTP request contains the Range field in its header, then an origin site must return a 206 partial content status message.

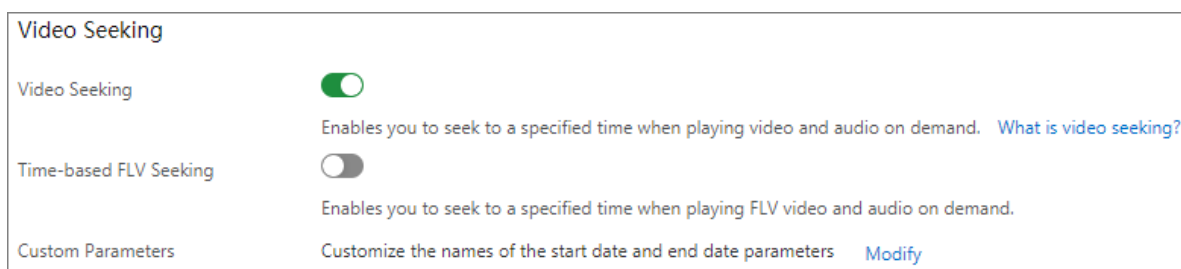
- The file formats supported by video seeking and the sample URLs are as follows:

| File format | Metadata | Start parameter | Example |
|-------------|---|--|---|
| MP4 | Only MP4 video files with the metadata contained in their header support video seeking. MP4 video files with the metadata contained in their footer do not support video seeking. | The <code>start</code> parameter specifies the time that you want to seek to, in seconds. Milliseconds are expressed with decimals. For example, <code>start =1.01</code> represents 1.01 second. If CDN cannot find the keyframe at the time specified by <code>start</code> , it seeks to the last keyframe before the specified time. | The request URL <code>http : // domain / video . mp4 ? start = 10</code> is to seek forward by 9 seconds. |
| FLV | FLV video files must contain metadata. | The <code>start</code> parameter specifies the byte that you want to seek to. If CDN cannot find the keyframe at the byte specified by the <code>start</code> parameter, it seeks to the last keyframe before the specified byte. | For video file <code>http : // domain / video . flv</code> , the request URL <code>http : // domain / video . flv ? start = 10</code> is to seek to the tenth byte. If no keyframe can be found at the tenth byte, then CDN seeks to the last keyframe before the tenth byte. |

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 **Video Seeking** switch under **Video Seeking** to enable the function.



Video Seeking

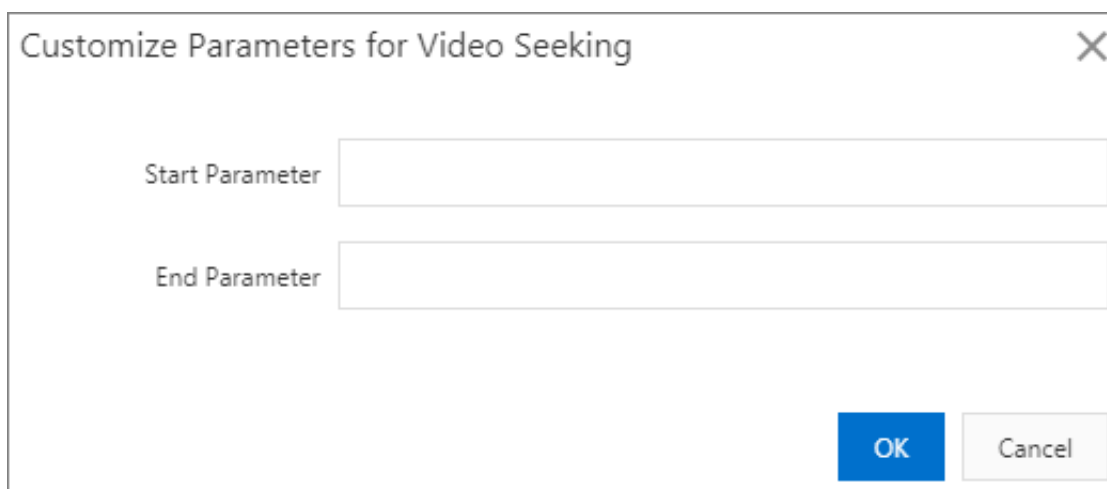
Video Seeking ☒ Enables you to seek to a specified time when playing video and audio on demand. [What is video seeking?](#)

Time-based FLV Seeking ☐ Enables you to seek to a specified time when playing FLV video and audio on demand.

Custom Parameters Customize the names of the start date and end date parameters [Modify](#)

6. Click the **Time - based FLV Seeking** switch to enable the function.

7. Click **Modify**.



Customize Parameters for Video Seeking

Start Parameter

End Parameter

OK Cancel

8. Set the **Start Parameter** and **End Parameter** for video seeking.

9. Click **OK**.

11.4 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 Overview

You can configure Quick UDP Internet Connections (QUIC) and bandwidth cap to guarantee the security of data transmission and CDN domain names.

CDN advanced configuration supports the following functions:

| Function | Description |
|-----------------------------|--|
| #unique_130 | If you want to accelerate resource delivery and ensure data transmission security, enable QUIC. |
| #unique_131 | If the specified bandwidth threshold is reached, the system automatically disables your CDN domain name to protect the domain name. All requests are rerouted to the origin. The CDN service is temporarily suspended. |

12.2 QUIC

12.2.1 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.

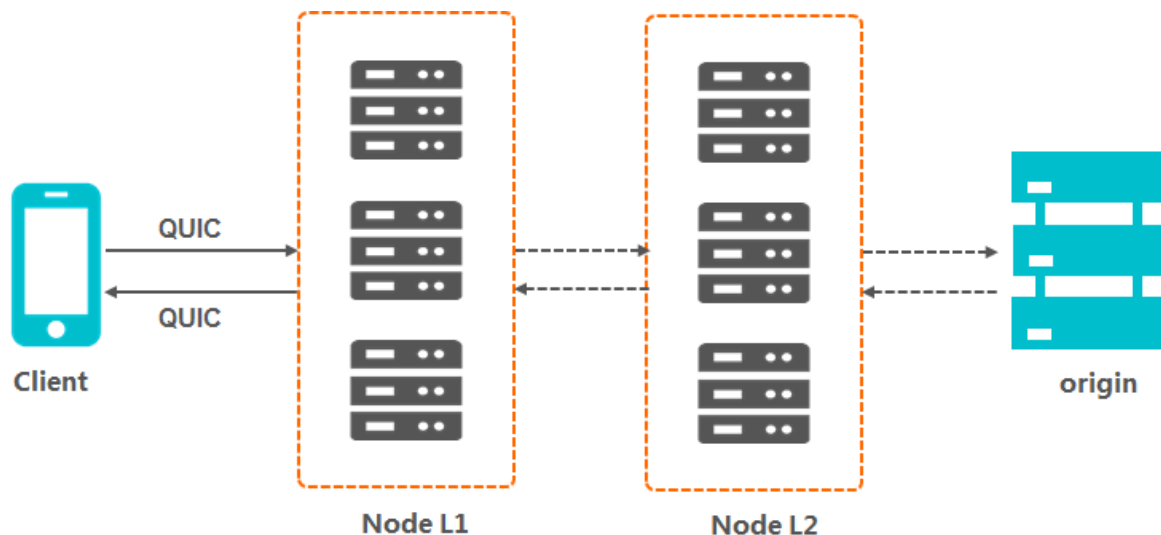
What is QUIC?

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.

12.2.2 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 [#unique_25](#).

Context

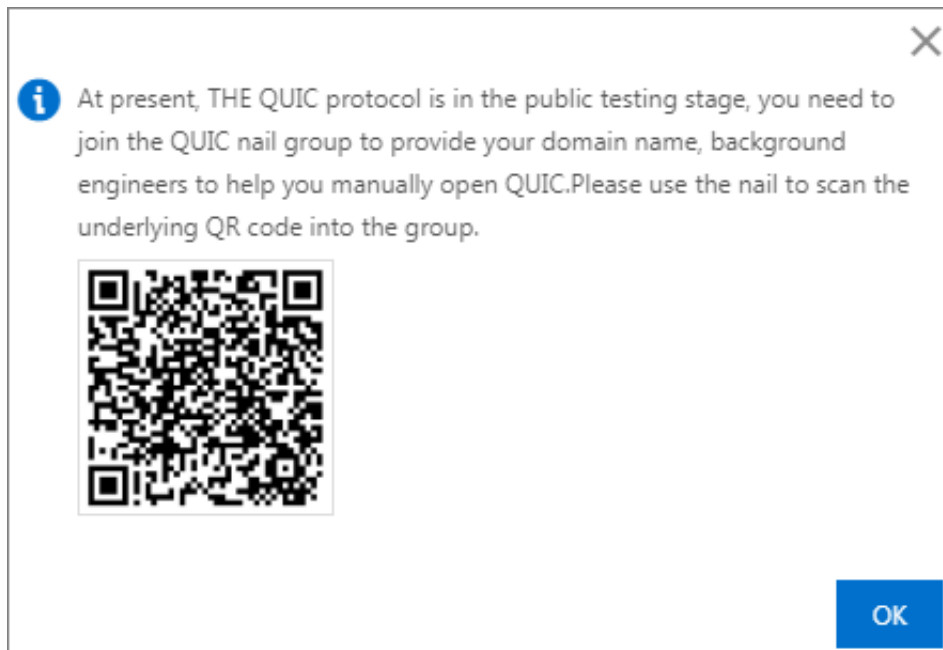
A preview of QUIC is currently available. Follow the prompts to scan the QR code to join the DingTalk group. After you join the group, follow the group announcements to provide domain information. Alibaba Cloud IT administrators will help you enable the QUIC protocol. After you enable the QUIC protocol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



12.3 Configure bandwidth cap

The bandwidth cap feature specifies the maximum bandwidth for a domain name. When the average bandwidth measured during each statistical cycle (five minutes) exceeds the specified maximum bandwidth, your domain name will automatically go offline to protect itself. All requests will be redirected to the origin server, and CDN will stop acceleration services to avoid excessive fees produced by abnormal traffic. After your domain name goes offline, you can re-enable it in the console. This topic describes how to enable the bandwidth cap feature and related precautions.

Context

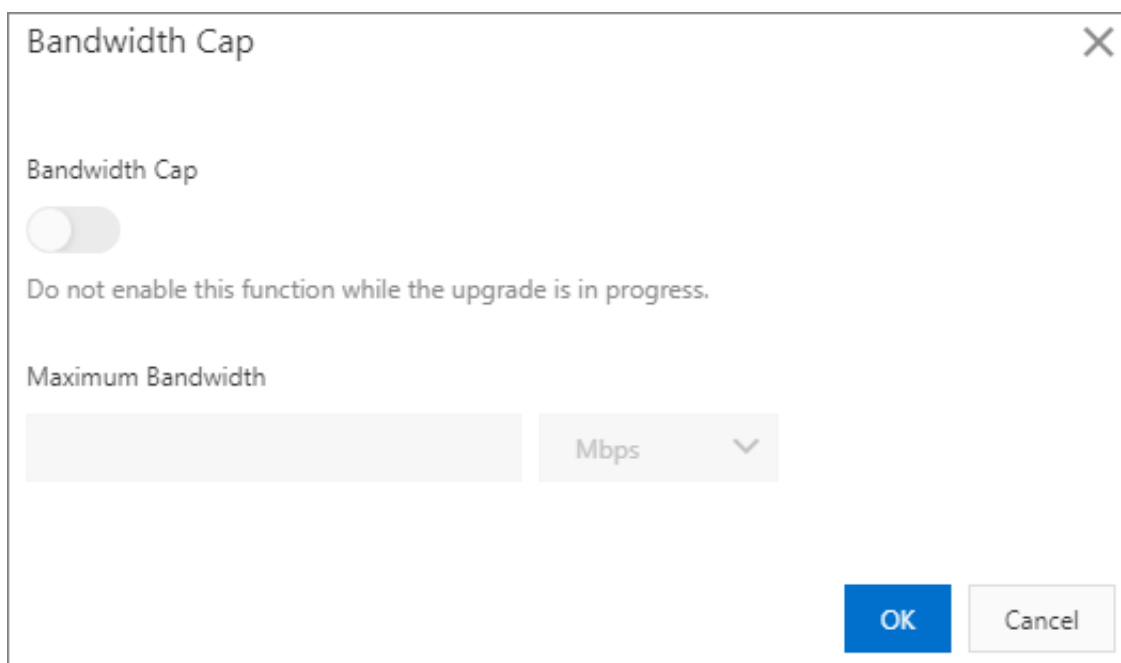
When you configure the bandwidth cap feature, take note of the following points:

- If you intend to enable this feature by using a RAM user account, you must log on to the [RAM console](#) to create the `AliyunCDNFullAccess` policy. This policy grants the RAM user account permission to manage CDN.
- This feature is not applicable to wildcard domain names. Even if you set this feature for a wildcard domain name, this feature does not take effect.
- After you enable this feature, your services may go offline due to the bandwidth cap. To ensure that your domain name can provide normal services, we recommend you set the maximum bandwidth based on a reasonable estimation.

- If your CDN service goes offline due to the bandwidth cap, you can go to the Domain Names page in the CDN console, select the check box corresponding to the domain name, and then click Enable.

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 Bandwidth Cap section, click Modify.
6. Turn on Bandwidth Cap to set the maximum bandwidth.



The screenshot shows a 'Bandwidth Cap' dialog box with a close button (X) in the top right corner. Inside the dialog, there is a section titled 'Bandwidth Cap' with a toggle switch that is currently turned off. Below the toggle, a message states: 'Do not enable this function while the upgrade is in progress.' Underneath this message is a section titled 'Maximum Bandwidth' which contains a text input field and a unit selector dropdown menu currently set to 'Mbps'. At the bottom right of the dialog are two buttons: 'OK' (in blue) and 'Cancel' (in light gray).



Note:

- You can only specify units at intervals of 1000. For example, 1 Tbit/s is equal to 1000 Gbit/s, and 1 Gbit/s is equal to 1000 Mbit/s.
- You can choose to enable or disable this feature based on the actual usage of your domain name.
- If this feature is being upgraded, you cannot enable it.

7. Click OK.