

Content Delivery Network

User Guide

Issue 04
Date 2024-06-06



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 Domain Name Management	1
1.1 Functions	1
1.2 Enabling/Disabling CDN for a Domain Name	2
1.3 Deleting a Domain Name	3
1.4 Domain Name Quota Management	4
2 Domain Name Settings	5
2.1 Overview	5
2.2 OBS Authorization	9
2.3 Basic Settings	10
2.3.1 Service Type	10
2.3.2 Origin Server Settings	10
2.3.3 Host Header	15
2.3.4 IPv6	18
2.4 Origin Settings	19
2.4.1 Overview	19
2.4.2 Origin Protocol	20
2.4.3 Origin SNI	21
2.4.4 Origin URL Rewriting	22
2.4.5 Advanced Origins	26
2.4.6 Range Requests	29
2.4.7 Redirect from Origin	30
2.4.8 ETag Verification	31
2.4.9 Origin Response Timeout	32
2.4.10 Origin Request Headers	33
2.4.11 FAQ	39
2.5 HTTPS Settings	40
2.5.1 Overview	40
2.5.2 HTTPS Certificates	41
2.5.3 HTTPS Certificate Requirements	46
2.5.4 HTTPS Certificate Format Conversion	49
2.5.5 TLS Versions	50
2.5.6 Force Redirect	51
2.5.7 HSTS	53

2.5.8 HTTP/2.....	55
2.5.9 OCSP Stapling.....	56
2.5.10 QUIC.....	57
2.5.11 FAQ.....	58
2.6 Cache Settings.....	59
2.6.1 Overview.....	59
2.6.2 Cache Rules.....	59
2.6.3 Browser Cache TTL.....	67
2.6.4 Status Code Cache TTL.....	70
2.7 Access Control.....	72
2.7.1 Overview.....	72
2.7.2 Referer Validation.....	72
2.7.3 IP ACL.....	76
2.7.4 User-Agent ACL.....	79
2.7.5 Token Authentication.....	80
2.7.5.1 Signing Method A.....	81
2.7.5.2 Signing Method B.....	86
2.7.5.3 Signing Method C1.....	91
2.7.5.4 Signing Method C2.....	96
2.7.6 Remote Authentication.....	101
2.7.7 IP Access Frequency.....	106
2.8 Advanced Settings.....	107
2.8.1 HTTP Header Settings (Cross-origin Requests).....	108
2.8.2 Custom Error Pages.....	114
2.8.3 Smart Compression.....	116
2.8.4 Request Rate Limiting.....	117
2.9 Video Settings.....	119
2.9.1 Video Seek.....	119
2.10 Tag Management.....	120
3 Cache Purge and Prefetch.....	124
3.1 Overview.....	124
3.2 Cache Prefetch.....	124
3.3 Cache Purge.....	126
3.4 Viewing Task Progresses.....	128
3.5 FAQ.....	129
4 Statistical Analysis.....	132
4.1 Statistics Description.....	132
4.2 Utilization Statistics.....	132
4.3 Access Statistics.....	133
4.4 Origin Server Statistics.....	134
4.5 Data Analysis.....	136
4.6 Region & Carrier Statistics.....	137

4.7 Status Codes.....	139
5 Resource Package Management.....	141
6 Log Management.....	142
7 Permissions Management.....	145
7.1 Creating a User and Granting CDN Permissions.....	145
7.2 Creating a Custom Policy.....	146
8 Enterprise Projects.....	148
A Change History.....	149

1 Domain Name Management

1.1 Functions

After a domain name is added, you can enable and disable CDN for the domain name, remove the domain name, and copy domain configuration on the CDN console.

You can also click **Export** in the upper right corner of the **Domains** page and choose to export all data or selected data to an XLSX file.

Scenarios

The following table describes the functions.

Table 1-1 Scenarios

Item	Description
Enabling/ Disabling CDN for a Domain Name	Enable: You can enable a domain name in the Disabled state. Disable: You can disable a domain name in the Enabled state.
Deleting a Domain Name	You can remove a domain name in the Disabled, Error, or Rejected state. NOTE After a domain name is removed, the system automatically deletes the corresponding configuration of the domain name. If you want to use CDN for the removed domain name again, re-add and configure the domain name.
Domain Name Quota Management	Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas limit the number or amount of resources available to users. If the existing domain name quota cannot meet your service requirements, submit a service ticket to request a higher quota.

1.2 Enabling/Disabling CDN for a Domain Name

Scenarios

You can enable or disable CDN for your domain names on the **Domains** page in the CDN console.

Precautions

- Before disabling CDN for a domain name, have your domain requests resolved to the origin server or a CNAME record that is not allocated by Huawei Cloud CDN to prevent service interruptions.
- If a domain name has not been accessed for more than 180 days, CDN starts the domain name suspension process and disables CDN acceleration for the domain name after confirmation.
- Domain name settings are still retained. If the local DNS of a user has cached the resolution record or the user binds the domain name with a point of presence (PoP) in the **hosts** file to forcibly resolve requests, CDN will refuse to provide services for the user after receiving the requests. However, the corresponding traffic will be generated and charged.

Viewing Basic Domain Information

On the **Domains** page of the CDN console, click **Configure** in the row that contains the target domain name. On the **Basic Settings** tab, view the basic information about the domain name.

- Domain statuses include **Enabled**, **Disabled**, **Configuring**, **Error**, **Reviewing**, **Rejected**, and **Removing**.

Disabling CDN for Domain Names

You can disable CDN for a domain name whose status is **Enabled** or **Error**. After CDN is disabled, CDN will no longer provide acceleration services for your domain name, but the domain configurations will remain. To restore the acceleration service, enable CDN again.

Disabling CDN for a single domain name

1. On the **Domains** page of the CDN console, choose **More > Disable** in the **Operation** column of the row that contains the domain name for which CDN is to be disabled.
2. Confirm the information about the domain name and click **Yes**.

Disabling CDN for multiple domain names

On the **Domains** page of the CDN console, select the domain names for which CDN is to be disabled, and click **Disable** above the domain name list.

Enabling CDN for Domain Names

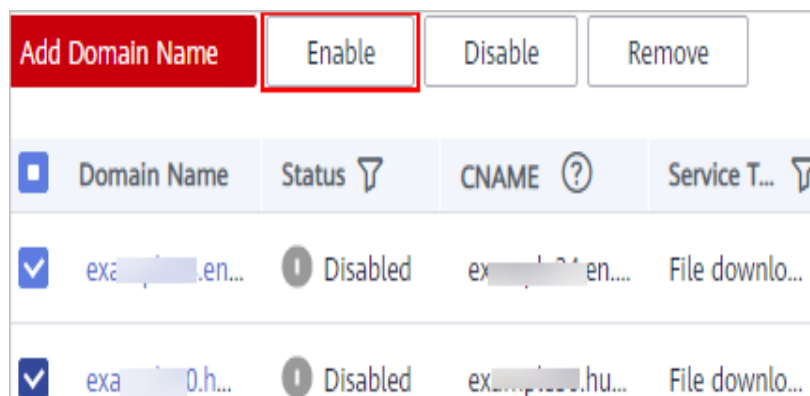
You can enable CDN for a domain name whose status is **Disabled**.

Enabling CDN for a single domain name

1. On the **Domains** page of the CDN console, choose **More > Enable** in the **Operation** column of the row that contains the domain name for which CDN is to be enabled.
2. Confirm the information about the domain name and click **Yes**.

Enabling CDN for multiple domain names

On the **Domains** page of the CDN console, select the domain names for which CDN is to be enabled, and click **Enable** above the domain name list.



1.3 Deleting a Domain Name

Scenarios

If you no longer want to accelerate a domain name, you can delete it from the **Domains** page of the CDN console. The system will automatically delete the corresponding configuration of the domain name. To enable CDN acceleration for the removed domain name, add and configure the domain name again.

Precautions

- You can only delete domain names in the **Disabled** or **Rejected** state.
- If a domain name has been in the **Disabled** or **Rejected** state for more than 120 days, CDN starts the domain name deletion process and deletes the domain name records after confirmation. If CDN acceleration is required for the domain name, add the domain name again.
- All settings of the domain name will be deleted from CDN PoPs and the domain name will no longer be charged by CDN.

Deleting a Single Domain Name

1. On the **Domains** page of the CDN console, choose **More > Delete** in the row that contains the domain name to delete.
2. Confirm the information about the domain name and click **Yes**.

Deleting Multiple Domain Names

On the **Domains** page of the CDN console, select the domain names to delete, and click **Delete** above the domain name list.

1.4 Domain Name Quota Management

Total Domain Name Quota

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas limit the quantity and capacity of resources available to users. If an existing resource quota cannot meet your service requirements, submit a service ticket to increase the quota. The following table lists the default quotas for CDN domain names.

Resource	Default Quota
Acceleration domain names	100
Files to be purged	2,000 per day
Directories to be purged	100 per day
URLs to be prefetched	1,000 per day

NOTE

If any domain name under your account is banned due to violation, you cannot add new acceleration domain names and perform cache purge or prefetch.

2 Domain Name Settings

2.1 Overview

After a domain name is added for acceleration, you can configure the domain name based on service requirements. Customized configuration items include basic settings, origin pull, HTTPS, cache, access control, and advanced settings.

Basic Settings

Ensure that the domain name is in the **Enabled** or **Configuring** state and is not locked or banned by CDN before configuring the settings.

Item	Description
Origin Server Settings	If the IP address or domain name of the origin server changes, origin server information is incorrect, or a standby origin server is needed, modify the origin server settings.
Host Header	If the domain name you want CDN to pull content is not your acceleration domain name, set a host header. CDN regards an acceleration domain name as the host by default.
Service Type	If the services of your domain name change and its service type cannot meet your requirements, you can change the service type on the CDN console.
IPv6	To allow users to access CDN PoPs using IPv6, enable IPv6 on the CDN console.

Origin Settings

Ensure that the domain name is in the **Enabled** or **Configuring** state and is not locked or banned by CDN before configuring the settings.

Item	Description
Origin Protocol	You can configure the request protocol used by CDN for origin pull.
Origin SNI	If your origin server IP address is bound to multiple domains and CDN visits the origin server using HTTPS, you can set the Server Name Indication (SNI) to specify the domain to be visited by CDN.
Origin URL Rewriting	If the URLs of origin pull requests do not match the origin server URLs, you can rewrite the request URLs to improve the origin pull hit ratio.
Advanced Origins	You can configure advanced origins to allow CDN to pull content from different origin servers based on different resource types or paths.
Range Requests	If you need to improve the distribution efficiency of large files, you can enable range requests.
Redirect from Origin	Assume that 302/301 redirect is performed for your origin server address. If you do not want CDN to directly send a 302/301 redirect address to users but to instead cache the requested content and then forward the content to users, you can enable redirect from origin.
ETag Verification	If your resources on the origin server remain unchanged and you do not want CDN to pull the resources after the cache expires, you can enable ETag verification.
Origin Request Headers	You can rewrite a header in an origin pull request on the CDN console.
Origin Response Timeout	You can adjust the origin response timeout based on the features and service scenarios of your origin server.

HTTPS Settings

Ensure that the domain name is in the **Enabled** or **Configuring** state and is not locked or banned by CDN before configuring the settings.

Function	Description
HTTPS Certificates	You can add a certificate for HTTPS acceleration.
HTTPS Certificate Requirements	Describes the combination and upload sequence of certificates issued by different authorities

Function	Description
HTTPS Certificate Format Conversion	You can convert certificates in other formats to the PEM format that CDN supports.
TLS Versions	You can enable or disable TLS versions as required.
Force Redirect	You can force redirect to HTTP or HTTPS.
HSTS	You can configure HSTS to force clients (such as browsers) to use HTTPS to access your server, improving access security.
HTTP/2	Describes the background and advantages of HTTP/2.
OCSP Stapling	If you enable this function, CDN will cache the status of online certificates in advance and return the status to browsers. Browsers do not need to query the status from CAs, accelerating the verification.
QUIC	You can configure the QUIC protocol to improve transmission security, reduce transmission and connection latency, and prevent network congestion.

Cache Settings

Ensure that the domain name is in the **Enabled** or **Configuring** state and is not locked or banned by CDN before configuring the settings.

Item	Description
Cache Rules	<ul style="list-style-type: none">You can set the time to live (TTL) and priority for different resources to increase the hit ratio and reduce the back-to-source rate.
Browser Cache TTL	You can set a browser cache TTL, during which users can obtain content directly from their browser cache (if available), reducing origin pulls.
Status Code Cache TTL	You can cache error status codes returned by the origin server to CDN PoPs, so CDN can return the error codes to users when they request resources. You can also set the status code cache TTL to reduce origin pull and pressure.

Access Control

Ensure that the domain name is in the **Enabled** or **Configuring** state and is not locked or banned by CDN before configuring the settings.

Item	Description
Referer Validation	Configure this item when you need to identify and filter visitors to restrict access.
IP ACL	Configure this item when you need to use IP address filtering to restrict access.
User-Agent ACL	Configure this item when you need to use User-Agent filtering to restrict access.
Token Authentication	Configure this item when you need to protect your website resources from being downloaded by malicious users.
Remote Authentication	Configure this item to allow CDN to forward user requests to a specific server for authentication, to prevent malicious resource download.

Advanced Settings

Ensure that the domain name is in the **Enabled** or **Configuring** state and is not locked or banned by CDN before configuring the settings.

Item	Description
HTTP Header Settings (Cross-origin Requests)	You can customize values of HTTP response headers for your website.
Custom Error Pages	You can customize error pages returned to user clients.
Smart Compression	You can compress static content on your websites by reducing file size. This speeds up file transfer and saves you a lot of bandwidth.
Request Rate Limiting	You can limit the user request rate within a specific range to reduce costs and the risk of burst bandwidth.

Video Settings

Ensure that the domain name is in the **Enabled** or **Configuring** state and is not locked or banned by CDN before configuring the settings.

Item	Description
Video Seek	Configure this item to allow users to seek to a certain position in a video without affecting the playback effect.

2.2 OBS Authorization

If you configure a Huawei Cloud OBS private bucket as the origin server, enable OBS authorization so that CDN can pull content from your private bucket.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the upper right corner of the **Domains** page, click **Enable OBS Authorization**.

Authorize Access

CDN is requesting permission to access your cloud resources.

The following agency has been created by the system for CDN.

CDNAccessPrivateOBS

The default agency CDN uses to retrieve private bucket resources. Authorizing this agency will grant CDN permission to access your private buckets.

Authorize

Cancel

4. Click **Authorize**. The system creates an agency named **CDNAccessPrivateOBS** for you on the IAM console. CDN now has the read-only permission to access your private OBS buckets.

NOTE

- Do not delete the **CDNAccessPrivateOBS** agency. Otherwise, CDN cannot pull resources from OBS private buckets.

If files in your OBS bucket are encrypted using KMS, assign the **KMS Administrator** permissions to the **CDNAccessPrivateOBS** agency so that CDN can read and accelerate the encrypted files.

5. **(Optional)** Assign the **KMS Administrator** permissions to the **CDNAccessPrivateOBS** agency.
 - a. Log in to [Huawei Cloud console](#). Choose **Service List > Management & Deployment > Identity and Access Management** to access the IAM console.
 - b. In the navigation pane, choose **Agencies**.
 - c. On the **Agencies** page, click **Authorize** in the **Operation** column of the row containing **CDNAccessPrivateOBS**.
The **Select Policy/Role** page is displayed.
 - d. In the upper right corner of the table, search for **KMS Administrator**, select this role, and click **Next**.

- e. Set **Scope** to **Region-specific projects** and select the region based on the region of the OBS bucket.
- f. Click **OK**.

2.3 Basic Settings

2.3.1 Service Type

If the services of your domain name change and its service type cannot meet your requirements, you can change the service type on the CDN console.

Important Notes

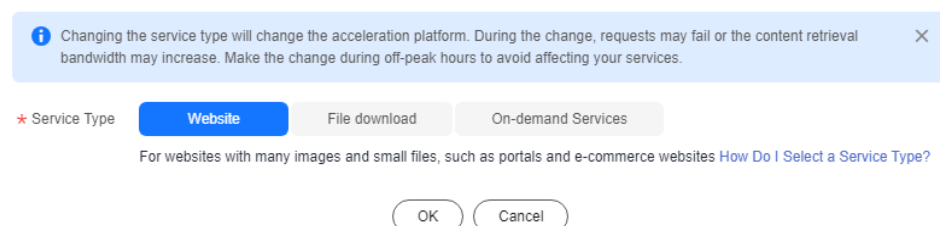
- Changing the service type will change the used acceleration platform. During the change, a small number of requests may fail or the origin pull bandwidth may increase. Change the service type during off-peak hours to avoid affecting your services.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain name list, click the domain name to modify or click **Configure** in the row containing the domain name.
4. On the **Basic Settings** tab, click **Edit** next to **Service Type**. The **Change Service Type** dialog box is displayed.

Figure 2-1 Changing the service type

Change Service Type



5. Select the new service type and click **OK**. The configuration takes about 5 minutes to complete.

2.3.2 Origin Server Settings

An origin server is a website server, that is the source of the data accelerated by CDN. If the origin server details, such as the IP address, domain name, and origin port, need to be modified, modify them on the origin server settings page.

Background

- When you add a domain name, CDN regards the configured origin server as the primary origin server by default. You can also add a standby origin server to reduce the origin pull failure rate.
- If the origin servers have multiple IP addresses, the following load balancing mechanism is used for origin pull.
 - An origin pull request can be forwarded to up to two IP addresses of the origin server with highest priority. If origin pull from both IP addresses fails, the request is forwarded to an origin server with a lower priority. The request can be forwarded to up to two IP addresses of the second origin server. If origin pull fails again, the request fails.
 - Origin pull fails when the connection times out, the connection fails, or a 5xx error code is returned from the origin server.

Precautions

- Ensure that the origin server configuration is correct. Incorrect configuration of the origin server causes origin pull failures.
- If you have modified content on the origin server, refresh the CDN cache.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Basic Settings** tab.
5. In the **Origin Server Settings** area, click **Edit**.
6. Click **Add** below the origin server list. The **Add Origin Server** drawer is displayed.

Figure 2-2 Adding an origin server

Add Origin Server

i Ensure that you configure the origin server correctly. Otherwise, retrieval failures will occur. X

Type

IP address

Domain name

OBS bucket

Address

Enter up to 50 IP addresses separated by commas (,).

Priority

Primary Origin Server

Standby Origin Server

The primary origin has a higher priority than the standby origin. If the primary origin is faulty, CDN pulls content from the standby origin.

Origin Ports

HTTP port

HTTPS port

Host Header

www.example.com

Domain name of the site accessed by CDN nodes when retrieving content. [Learn more](#)

By default, the host is your acceleration domain name. Change it to the actual site for origin pull. For example, if your origin server is the domain name of an object storage bucket, set the host header to the bucket domain name.

OK

Cancel

Table 2-1 Parameters

Parameter	Description
Type	<p>IP address</p> <ul style="list-style-type: none"> If an IP address is used as the origin address, CDN PoPs access the IP address directly to pull origin content. If multiple IP addresses are configured for the origin server, CDN uses the load balancing mechanism to pull content.

Parameter	Description
	<p>Domain name</p> <ul style="list-style-type: none"> The origin domain cannot be the same as the acceleration domain name. Otherwise, user requests will be repeatedly resolved to CDN PoPs, and CDN PoPs will not be able to obtain content from the origin server. You can also enter the domain name of an object storage bucket in this field. <p>NOTE</p> <ul style="list-style-type: none"> Private buckets cannot be used as origin servers. If you use an object storage bucket as your origin server, the object storage service will charge the CDN origin pull traffic based on the billing standard for outgoing Internet traffic. <p>OBS bucket</p> <p>Select an OBS bucket domain name under your account or customize one.</p> <p>Notes:</p> <ol style="list-style-type: none"> If your OBS private bucket is unsuitable as an origin for your domain name, do not set the private bucket as the origin server. If an OBS private bucket is configured as an origin server, enable OBS authorization and select the Private bucket checkbox. Otherwise, origin pull will fail. If you have enabled static website hosting for your OBS bucket, select the Static website hosting checkbox when adding a domain name. In this way, the list of all files in the bucket will not be displayed when users access the bucket. If OBS buckets are configured as origin servers for CDN, OBS charges the traffic for pulling content from the OBS buckets. When back-to-source by mirroring is configured on OBS and range requests are enabled on CDN, if the mirror origin server does not comply with the RFC Range Requests standard, the response to range requests is not 206 and CDN fails to pull content. In this case, submit a service ticket.
Address	Address accessed by CDN PoPs during origin pull.
Bucket	<p>This parameter is mandatory when Type is set to OBS bucket.</p> <ul style="list-style-type: none"> Public bucket: public read. All users can read objects in the bucket. Private bucket: Only users granted permissions by the ACL can access the bucket.

Parameter	Description
Priority	<p>Select Primary Origin Server, Standby Origin Server, or Custom. If you select Custom, enter an integer from 1 to 100. A larger value indicates a higher priority. The default priority of the primary origin server is 70, and that of the standby origin server is 30.</p> <ul style="list-style-type: none">• If only the primary and standby origin servers are configured:<ul style="list-style-type: none">- CDN pulls content from the primary origin server first. When the primary server is faulty, CDN pulls content from the standby origin server.- Configure at least one primary origin server.• If you have configured a custom priority:<ul style="list-style-type: none">- CDN pulls content from the origin server with the highest priority first. If such origin server is faulty, CDN pulls content from the origin server with a lower priority.
Weight	<p>The value ranges from 1 to 100. A larger value indicates a larger number of times that content is pulled from this IP address.</p> <ul style="list-style-type: none">• If there are multiple origin servers with the same priority, the weight determines the proportion of content pulled from each origin server.
Origin Port	<p>Port number for CDN PoPs to pull content. By default, the HTTP port is 80 and the HTTPS port is 443.</p> <ul style="list-style-type: none">• If Type is set to OBS bucket, the port numbers cannot be changed.
Host Header	<p>A host is specified in the HTTP request header. It is the domain name of the site accessed by CDN PoPs when CDN pulls content from the origin server. CDN obtains resources from the corresponding site based on the host details during origin pull.</p> <p>After a domain name is added, the default host will be the domain name. Change the host in a timely fashion if either of the following conditions is met:</p> <ul style="list-style-type: none">• If you set Type to Domain name and enter the domain name of an object storage bucket, set the host to the domain name of the bucket.• If you want CDN to pull content from a custom domain name, specify the host. For example, suppose an origin server is bound to two sites, www.origin01.com and www.origin02.com, and the domain name connected to CDN is www.example01.com. If you need CDN to pull content from www.origin02.com, you would need to set the host to www.origin02.com.

7. Set the parameters and click **OK**. Repeat **6** to add more origin servers. You can add up to 50 origin servers.

8. Click **Save** to add the origin server.
9. Click **Delete** or **Edit** in the origin server list to delete or edit an origin server.

Examples

Assume that you want to migrate resources of an acceleration domain name to a server whose domain name is `www.example.com` and HTTPS port number for origin pull is 8080. You can modify the origin server settings on CDN as follows:

Add Origin Server

i Ensure that you configure the origin server correctly. Otherwise, retrieval failures will occur. ×

Type

IP address Domain name OBS bucket

Address

Priority

Primary Origin Server Standby Origin Server

The primary origin has a higher priority than the standby origin. If the primary origin is faulty, CDN pulls content from the standby origin.

Origin Ports

HTTP port HTTPS port

Host Header

Domain name of the site accessed by CDN nodes when retrieving content. [Learn more](#)

By default, the host is your acceleration domain name. Change it to the actual site for origin pull. For example, if your origin server is the domain name of an object storage bucket, set the host header to the bucket domain name.

2.3.3 Host Header

A host is specified in HTTP request headers. It is the domain name of the site accessed by CDN during origin pull.

Background

The differences between the origin server and the host are as follows:

- The origin server decides the address to be accessed during origin pull.
- The host header decides the site that is associated with the requested content.

Assume that your origin server is an Nginx server. Its IP address is x.x.x.x, and its domain name is www.test.com. The following sites are deployed on the origin server.

```
server {  
    listen 80;  
    server_name www.a.com;  
  
    location / {  
        root html;  
    }  
}  
server {  
    listen 80;  
    server_name www.b.com;  
  
    location / {  
        root html;  
    }  
}
```

If you want CDN to pull content from this Nginx server, set the origin server address to **x.x.x.x** or **www.test.com** on CDN. Since there are multiple sites on the origin server, you need to specify the specific site to pull content. If you want CDN to obtain content from the **www.a.com** site, set the host to **www.a.com** on CDN. If you want CDN to obtain content from the **www.b.com** site, set the host to **www.b.com** on CDN.

Precautions

- After a domain name is added, CDN regards it as the host by default. If you do not want CDN to pull content from the acceleration domain name, set a host to specify the location of the requested content.
- If your origin server address is an IP address or a domain name, your host type is the acceleration domain name by default.
- If you set your origin server address as a domain name, and specify the domain name as that of an object storage bucket, set the host to the domain name of your object storage bucket. Otherwise, the origin pull fails.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. In the **Origin Server Settings** area, click **Edit** in the **Operation** column of the row containing the target origin server.

Figure 2-3 Editing the origin server

Edit Origin Server

i Ensure that you configure the origin server correctly. Otherwise, retrieval failures will occur. **X**

Type

IP address Domain name OBS bucket

Address

€

Priority

Primary Origin Server Standby Origin Server Custom

Default values: 70 for primary and 30 for standby. A larger value indicates a higher priority. If an origin server with a higher priority is faulty, CDN will pull content from an origin server with a lower priority.

Weight

50

Origin Ports

HTTP port 80 HTTPS port 443

Host Header

lxl juapi.com

Domain name of the site accessed by CDN nodes when retrieving content. [Learn more](#)

By default, the host is your acceleration domain name. Change it to the actual site for origin pull. For example, if your origin server is the domain name of an object storage bucket, set the host header to the bucket domain name.

OK Cancel

5. Enter the domain name of the host and click **OK**.
6. To edit host headers in a batch, click **Edit** above the origin server list.
 - In the **Host Header** column, modify the information and click **Save**.

NOTE

The configuration takes about 5 minutes.

Examples

Assume that you have an acceleration domain name **www.example.com**. Its origin server domain name is **www.origin.com**, and the host is **www.example01.com**.

Edit Origin Server

i Ensure that you configure the origin server correctly. Otherwise, retrieval failures will occur. ✕

Type

IP address Domain name OBS bucket

Address

www.origin.com

Priority

Primary Origin Server Standby Origin Server Custom

Default values: 70 for primary and 30 for standby. A larger value indicates a higher priority. If an origin server with a higher priority is faulty, CDN will pull content from an origin server with a lower priority.

Weight

50

Origin Ports

HTTP port HTTPS port

Host Header

www.example01.com

Domain name of the site accessed by CDN nodes when retrieving content. [Learn more](#)

By default, the host is your acceleration domain name. Change it to the actual site for origin pull. For example, if your origin server is the domain name of an object storage bucket, set the host header to the bucket domain name.

When a user requests the **http://www.example.com/test.jpg** file, the file is not cached on CDN, and CDN pulls that file from the origin server **www.origin.com** whose IP address is 192.168.1.1. The file is found in the **www.example01.com** site of the origin server. CDN then returns the file to the user, and caches the file on PoPs.

2.3.4 IPv6

You can enable IPv6 to allow clients to access CDN PoPs using the IPv6 protocol and allow CDN to carry IPv6 client IP addresses to access your origin server.

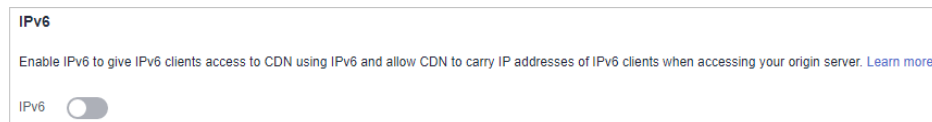
Precautions

- Most CDN PoPs support IPv6. After IPv6 is enabled, if a user uses IPv6 to access CDN but the optimal PoP does not support IPv6, the user can still use IPv4 to access the PoP.
- IPv6 cannot be enabled for domain names with special configurations.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain name list, click the domain name or click **Configure** in the row containing the domain name.

Figure 2-4 IPv6



NOTE

After IPv6 is enabled on the CDN console, if the origin server does not support IPv6, IPv4 will be used for origin pull.

4. Switch on **IPv6**.

2.4 Origin Settings

2.4.1 Overview

When a user requests content on an acceleration domain name, and the content is not cached on CDN PoPs, CDN PoPs will pull the content from the origin server. You can set origin parameters based on your needs to speed up access.

The following table describes the origin settings.

Function	Description
Origin Protocol	You can configure the request protocol used by CDN for origin pull.
Origin SNI	If your origin server IP address is bound to multiple domains and CDN visits the origin server using HTTPS, you can set the SNI to specify the domain to be visited by CDN.

Function	Description
Origin URL Rewriting	If the URLs of origin pull requests do not match the origin server URLs, you can rewrite the request URLs to improve the origin pull hit ratio.
Advanced Origins	You can configure advanced origins to allow CDN to pull content from different origin servers based on different resource types or paths.
Range Requests	You can allow CDN to pull large files from the origin server by range and return ranges to users, speeding up distribution and reducing bandwidth consumption.
Redirect from Origin	If your origin server uses a 301/302 redirect, you can enable redirect from origin to cache the redirected resources on CDN PoPs for accelerated distribution.
ETag Verification	If your resources on the origin server remain unchanged and you do not want CDN to pull the resources after the cache expires, you can enable ETag verification.
Origin Response Timeout	You can adjust the origin response timeout based on the features and service scenarios of your origin server.
Origin Request Headers	You can rewrite headers in users' request URLs for origin pull.

2.4.2 Origin Protocol

You can configure the protocol used for origin pull.

Precautions

- By default, HTTP is used.
- If you have enabled [HTTP/2](#) and set the origin protocol to **Same as user**, CDN uses HTTPS/1.1 for origin pull.
- When CDN uses HTTPS for origin pull, TLS 1.3 is not supported.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. Click **Edit** next to **Origin Protocol**. The **Origin Protocol** dialog box is displayed.

Figure 2-5 Origin protocol

Origin Protocol

Protocol HTTP HTTPS Same as user

QUIC and HTTP/2 are not supported.

OK

Cancel

Table 2-2 Parameter description

Origin Protocol	Description
Same as user	The origin protocol is the same as the client access protocol. For example, if a client accesses CDN using HTTP, CDN also uses HTTP for origin pull.
HTTP	CDN uses HTTP for origin pull.
HTTPS	CDN uses HTTPS for origin pull.

6. Select an origin protocol and click **OK**.

2.4.3 Origin SNI

If your origin server IP address is bound to multiple domains and CDN visits the origin server using HTTPS, you can set the SNI to specify the domain to be visited by CDN.

Precautions

- You can set the origin SNI only when the origin protocol is HTTPS or same as that in user requests.
- The origin SNI cannot be set for domain names with special configurations.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. Switch on **Origin SNI** and enter the origin SNI.

Figure 2-6 Origin SNI

Configure Origin SNI

Origin SNI

Table 2-3 Parameters

Parameter	Description
Configure Origin SNI	<p>Origin domain name to be accessed when CDN pulls origin content, for example, test.example.com.</p> <ul style="list-style-type: none"> • Wildcard domains are not supported. • The value can contain letters, digits, hyphens (-), and periods (.).

6. Click **OK**.

2.4.4 Origin URL Rewriting

If the URLs of origin pull requests do not match the origin server URLs, origin pull fails. You can rewrite origin URLs to those that match the origin server, improving the origin pull hit ratio.

Scenarios

Assume that you have changed the storage path of a video file on the origin server from **/test/** to **/video/**. Users may fail to obtain the correct file if they use the original access URL. In this case, you can use this function to rewrite URLs for CDN to pull the file, so users can obtain the correct file without changing the access URL.

Precautions

- You can add up to 20 URL rewrite rules.
- This function is not available if you have signed URLs using method B or C1.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.

- In the **Origin URL Rewrite** area, click **Edit**.

Figure 2-7 Rewriting origin URLs

Rewrite Origin URLs

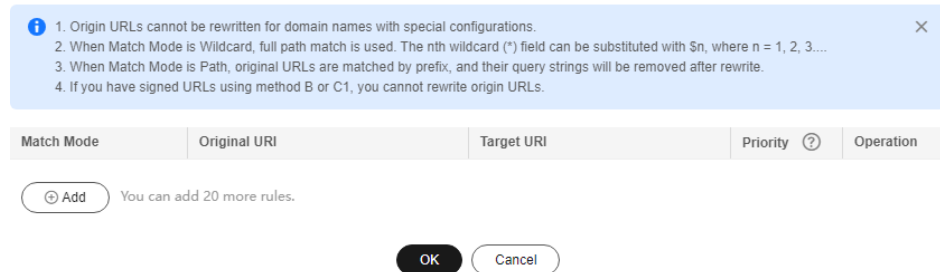


Table 2-4 Parameter description

Parameter	Description
Match Mode	All files: Rewrites URLs of pulling all files under this domain name from the origin server.
	Path: Rewrites URLs of pulling files under a specific path from the origin server. Prefix match is used. For example, if the original URI is /test , all files whose prefix is /test (such as /test , /test01 , and /test**) will be matched.
	Wildcard: Wildcard characters (*) are supported. Files are matched by full path. The original URI must be a specific path, for example, /test/*/*.mp4 .
	Full path: Rewrites the entire URL. The original URI must be a specific path, for example, /test/01/abc.mp4 .
Original URI	<p>URI to be rewritten.</p> <ul style="list-style-type: none"> A URI starts with a slash (/) and does not contain http://, https://, or the domain name. A URI contains up to 512 characters. Wildcards (*) are supported, for example, /test/*/*.mp4. When Match Mode is Path or Full path, no parameters can be specified. When Match Mode is Wildcard and a slash (/) is entered, the root directory is matched.

Parameter	Description
Target URI	<p>URI after rewrite.</p> <ul style="list-style-type: none"> A URI starts with a slash (/) and does not contain http://, https://, or the domain name. A URI contains up to 256 characters. When Match Mode is set to Wildcard, the <i>n</i>th wildcard (*) field can be substituted by \$<i>n</i>, where <i>n</i> = 1, 2, 3... Assume that the source URI is /test/*/*.mp4 and the target URI is /newtest/\$1/\$2.mp4. When a user requests /test/11/22.mp4, \$1 captures 11 and \$2 captures 22, and the actual URI for origin pull is /newtest/11/22.mp4. Other match modes do not support \$<i>n</i>.
Priority	<p>Priority of a URL rewrite rule.</p> <ul style="list-style-type: none"> The priority of a rule is mandatory and must be unique. The rule with the highest priority will be used for matching first. The priority is an integer ranging from 1 to 100. A greater number indicates a higher priority.

Examples

Example 1: Assume that you have configured the following rewrite rule for domain name www.example.com.

Rewrite Origin URLs

i 1. Origin URLs cannot be rewritten for domain names with special configurations. X

2. When Match Mode is Wildcard, full path match is used. The nth wildcard (*) field can be substituted with \$n, where n = 1, 2, 3...

3. When Match Mode is Path, original URLs are matched by prefix, and their query strings will be removed after rewrite.

4. If you have signed URLs using method B or C1, you cannot rewrite origin URLs.

Match Mode	Original URI	Target URI	Priority ?	Operation
Path v	<input type="text" value="/test/a.txt"/>	<input type="text" value="/test/b.txt"/>	<input type="text" value="1"/>	Delete

+ Add You can add 19 more rules.

OK
Cancel

Original origin pull request: **https://www.example.com/test/a.txt**

Rewritten origin pull request: **https://www.example.com/test/b.txt**

Example 2: Assume that you have configured the following rewrite rule for domain name www.example.com.

Rewrite Origin URLs

i 1. Origin URLs cannot be rewritten for domain names with special configurations. ✕

2. When Match Mode is Wildcard, full path match is used. The nth wildcard (*) field can be substituted with \$n, where n = 1, 2, 3....

3. When Match Mode is Path, original URLs are matched by prefix, and their query strings will be removed after rewrite.

4. If you have signed URLs using method B or C1, you cannot rewrite origin URLs.

Match Mode	Original URI	Target URI	Priority ?	Operation
Wildcard ▼	/test/**.mp4	/newtest/\$1/\$2.mp4	1	Delete

+ Add You can add 19 more rules.

OK
Cancel

Original origin pull request: <https://www.example.com/test/aaa/bbb.mp4>

Rewritten origin pull request: <https://www.example.com/newtest/aaa/bbb.mp4>

Example 3: Assume that you have configured the following rewrite rule for domain name www.example.com.

Rewrite Origin URLs

i 1. Origin URLs cannot be rewritten for domain names with special configurations. ✕

2. When Match Mode is Wildcard, full path match is used. The nth wildcard (*) field can be substituted with \$n, where n = 1, 2, 3....

3. When Match Mode is Path, original URLs are matched by prefix, and their query strings will be removed after rewrite.

4. If you have signed URLs using method B or C1, you cannot rewrite origin URLs.

Match Mode	Original URI	Target URI	Priority ?	Operation
All files ▼		/new.jpg	1	Delete

+ Add You can add 19 more rules.

OK
Cancel

Original origin pull request: <https://www.example.com/test/aaa/bbb.txt>

Rewritten origin pull request: <https://www.example.com/new.jpg>

Example 4: Assume that you have configured the following rewrite rule for domain name www.example.com.

Rewrite Origin URLs

i 1. Origin URLs cannot be rewritten for domain names with special configurations. ✕

2. When Match Mode is Wildcard, full path match is used. The nth wildcard (*) field can be substituted with \$n, where n = 1, 2, 3....

3. When Match Mode is Path, original URLs are matched by prefix, and their query strings will be removed after rewrite.

4. If you have signed URLs using method B or C1, you cannot rewrite origin URLs.

Match Mode	Original URI	Target URI	Priority ?	Operation
Wildcard ▼	/*.html*	/thread0/\$1.html\$2	1	Delete

+ Add You can add 19 more rules.

OK
Cancel

Original origin pull request: <https://www.example.com/123.html?id=3>

Rewritten origin pull request: <https://www.example.com/thread0/123.html?id=3>

2.4.5 Advanced Origins

You can configure advanced origins to allow CDN to pull content from different origin servers based on different URL paths.

Differences Between Advanced and Basic Origin Servers

The basic origin server is the default address of origin pulls. CDN pulls content from the advanced origin server only when a user request URL matches the rule of the advanced origin server.

Precautions

- You can configure up to 20 rules.

Procedure

- Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
- In the navigation pane, choose **Domains**.
- In the domain list, click the target domain name or click **Configure** in the **Operation** column.
- Click the **Origin Settings** tab.
- Click **Edit** next to **Advanced Origin**.

Figure 2-8 Advanced origins

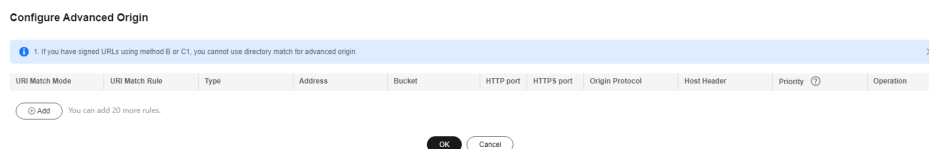


Table 2-5 Parameter description

Parameter	Description
URI Match Mode	URIs can be matched by All files , File name extension , and Directory .

Parameter	Description
URI Match Rule	<ul style="list-style-type: none"> ● All files: All requested resources are pulled from the configured advanced origin server. Exercise caution when selecting this option. ● File name extension <ul style="list-style-type: none"> – All file types are supported. – Start each file name extension with a period (.), and separate file name extensions with semicolons (;). – Enter up to 20 file name extensions. – Enter up to 512 characters. – File name extensions are case sensitive. Example: .JPG;.zip;.exe ● Directory: Start with a slash (/) and separate multiple directories by semicolons (;). Enter up to 20 directories and up to 512 characters. Example: /test/folder01;/test/folder02 <p>NOTE If you have signed URLs using method B or C1, URIs cannot be matched by Directory.</p>
Type	Select IP address , Domain name , or OBS bucket .
Address	<p>IP address</p> <ul style="list-style-type: none"> ● Enter an IPv4 address. <p>Domain name</p> <ul style="list-style-type: none"> ● Enter up to 250 characters. ● Third-party object storage buckets (public buckets) can be accessed using origin server domain names. <p>OBS bucket</p> <ul style="list-style-type: none"> ● Enter up to 250 characters. ● Only OBS buckets of the current account can be accessed. ● To access OBS private buckets, allow CDN to read OBS private buckets. For details, see OBS Authorization. <p>NOTE</p> <ul style="list-style-type: none"> ● You cannot add an OBS bucket if the domain name has special configuration.
HTTP Port	<p>Port number for origin pull using HTTP.</p> <ul style="list-style-type: none"> ● The port number ranges from 1 to 65535. The default port is 80. ● If Type is set to OBS bucket, this parameter cannot be modified.

Parameter	Description
HTTPS Port	<p>Port number for origin pull using HTTPS.</p> <ul style="list-style-type: none"> The port number ranges from 1 to 65535. The default port is 443. If Type is set to OBS bucket, this parameter cannot be modified.
Origin Protocol	<p>Protocol used by CDN PoPs to pull content from the origin server.</p> <p>HTTP</p> <p>HTTPS: CDN uses HTTPS for origin pull. (Ensure that the origin server supports HTTPS access.)</p> <p>Same as user: The origin protocol is the same as the client access protocol. For example, if a client accesses CDN using HTTP, CDN also uses HTTP for origin pull.</p>
Host Header	<p>Host information of the advanced origin. For details, see Host Header.</p> <ul style="list-style-type: none"> If Type is set to IP address or Domain name, the host is the acceleration domain name by default. If Type is set to OBS bucket, the host is the OBS bucket domain name by default.
Bucket	<p>This parameter is mandatory when Type is set to OBS bucket.</p> <ul style="list-style-type: none"> Public bucket: Select this option when the OBS bucket policy is public read or public read and write. Private bucket: Select this option when the OBS bucket policy is private.
Priority	<p>The priority value ranges from 1 to 65,535. The larger the value, the higher the priority.</p>
Operation	<p>Delete: Delete the rule.</p>

6. Configure parameters and click **OK**.

Example

Example: Assume that you have configured advanced origins for domain name www.example01.com.

Configure Advanced Origin

1. If you have signed URLs using method B or C1, you cannot use directory match for advanced origin.

URI Match Mode	URI Match Rule	Type	Address	Bucket	HTTP port	HTTPS port	Origin Protocol	Host Header	Priority	Operation
File name exte...	jpg	Domain name	www.example.com		80	443	Same as user		1	Delete

+ Add You can add 19 more rules.

OK **Cancel**

Configuration result: When a user requests an uncached JPG resource, CDN pulls the resource from the origin server `www.example.com`. CDN pulls other uncached resources from the basic origin server.

2.4.6 Range Requests

A range request allows the origin server to send data of a specific range to a CDN PoP based on the range information in the HTTP request header.

Background

- Range information specifies the positions of the first and last bytes for the data to be returned. For example, **Range: bytes=0-100** indicates that the first 101 bytes of the file are required.
- If this function is enabled, when a client requests a resource that is not cached or has expired, CDN PoPs initiate a range request to pull the required resource from the origin server by segment and cache the resource.
- Range requests shorten the distribution time of large files, improve origin pull efficiency, and reduce resource consumption.

Precautions

- To enable range requests for origin pull, the origin server must support range requests, that is, requests with the **Range** field in the headers. Otherwise, origin pull may fail.
- By default, range requests are enabled for file download acceleration and on-demand service acceleration.
- If an origin server resource exceeds 1 GB and range requests are not enabled, origin pull for such resource will fail.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. In the **Range Requests** area, switch on or off **Range Requests** based on service requirements.

Figure 2-9 Range requests

Range Requests

Range requests improve response speed and conserve bandwidth when accessing large files, but if the origin server does not support range requests, origin pull may fail.

Range Requests

Example

Assume that you have enabled range requests for domain name `www.example.com`.

- If user A requests `www.example.com/cdn.mp4`, and CDN PoPs do not cache the content or the cached content on the CDN PoPs has expired, the optimal CDN PoP initiates a range request to pull ranges of the content from the origin server. Ranges of the content are then cached on the PoP.
- When user A's requested content is being cached, if user B sends a range request to this PoP, and the cache on the PoP already contains the range of the content requested by user B, the PoP immediately returns the requested range.

2.4.7 Redirect from Origin

Background

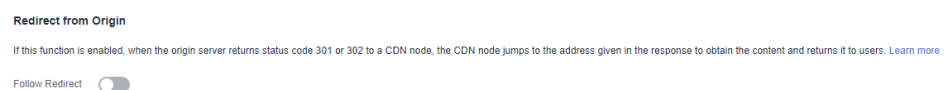
If an origin server uses a 301/302 redirect, when a CDN PoP sends a request to pull content requested by a user from the origin server, a 301/302 status code is returned. CDN then takes action based on whether redirect from origin is enabled.

- **Disabled**
A CDN PoP returns the redirect address to the user and leaves the user to finish the request process. If the domain name of the redirect address is not added to CDN, the subsequent request process will not be accelerated by CDN.
- **Enabled**
A CDN PoP pulls content from the redirect address and caches the content, which is then returned to the user. When another user requests the same content, the cache is returned directly.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. In the **Redirect from Origin** area, switch on or off **Follow Redirect**.

Figure 2-10 Configuring redirect from origin



Examples

- Assume that redirect from origin is **enabled** for domain name `www.example.com`.

Redirect from Origin

If this function is enabled, when the origin server returns status code 301 or 302 to a CDN node, the CDN node jumps to the address given in the response to obtain the content and returns it to users. [Learn more](#)

Follow Redirect

If a user requests the `www.example.com/cdn.jpg` file and the CDN PoP does not cache the content, the PoP pulls the content from the origin server. The origin server returns the HTTP status code 301 or 302 and the redirect address `www.example.com/test/cdn.jpg`.

- The PoP directly sends a request to the redirect address.
 - After obtaining the requested content, the PoP returns the content to the user and caches the content.
 - When another user requests the same file, the PoP directly returns the cached content.
- Assume that redirect from origin is **disabled** for domain name `www.example.com`.

Redirect from Origin

If this function is enabled, when the origin server returns status code 301 or 302 to a CDN node, the CDN node jumps to the address given in the response to obtain the content and returns it to users. [Learn more](#)

Follow Redirect

If a user requests the `www.example.com/cdn.jpg` file and the CDN PoP does not cache the content, the PoP pulls the content from the origin server. The origin server returns the HTTP status code 301 or 302 and the redirect address `www.example.com/test/cdn.jpg`.

- The PoP directly returns the HTTP status code 301 or 302 to the user client. The user client sends a request to the redirect address.
- If the domain name of the redirect address is not added to CDN, CDN PoPs do not cache the requested content and the subsequent request process will not be accelerated.
- If another user requests the same file, the preceding process is repeated.

2.4.8 ETag Verification

Background

An entity tag (ETag) of a URL is used to indicate whether the URL object is changed.

After a domain name is connected to CDN for acceleration, when a user request content for the first time, CDN PoPs pull content from the origin server, return content to the user, and cache the content to CDN PoPs. Within the configured cache TTL, when a user requests the content again, CDN does not need to pull content from the origin server. It returns the cached content to the user. When the content cached on CDN PoPs expires and a user requests the content:

- If ETag verification is enabled, CDN verifies the **ETag** value. If the values of **ETag**, **Last-Modified**, and **Content-Length** do not change, CDN returns the

cached content to the user, reducing the origin pull ratio and relieving the pressure on the origin server. If the value of **ETag**, **Last-Modified**, or **Content-Length** changes, CDN pulls content from the origin server.

- If ETag verification is disabled, CDN does not verify the **ETag** value. If the values of **Last-Modified** and **Content-Length** do not change, CDN returns the cached content to the user. If the value of **Last-Modified** or **Content-Length** changes, CDN pulls the resource from the origin server.

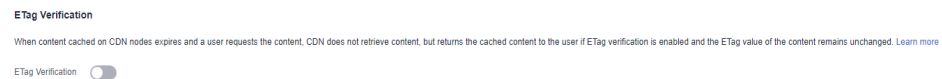
Precautions

- By default, ETag verification is enabled.

Procedure

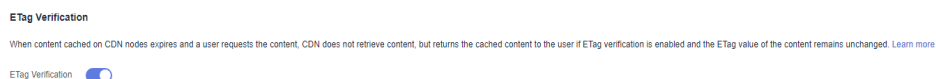
1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. Configure **ETag Verification** as required.

Figure 2-11 ETag verification



Examples

Assume that you have enabled ETag verification for domain name [www.example.com](#).



After the cache of a resource under the domain name expires, when a user requests the resource, CDN verifies the ETag. If the ETag value remains unchanged, CDN directly returns the cached resource to the user and recalculates the cache expiration time. If the ETag value changes, CDN pulls the latest resource from the origin server, returns it to the user, and caches the resource.

2.4.9 Origin Response Timeout

If the content requested by a user is not cached on CDN PoPs, CDN pulls the content from the origin server. If the origin pull times out, origin pull fails. The default timeout interval is 30s.

- The origin response timeout in this document refers to the timeout interval for loading data after a TCP connection is set up, excluding the connection setup time.

If the timeout interval is too short, origin pull may fail frequently due to unstable network connections. If the timeout interval is too long, failed requests may still occupy connections for a long time when the maximum number of connections to the origin server is reached. As a result, normal requests fail. You can adjust the timeout interval based on the service features and network status of your origin server to ensure normal origin pull.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. In the **Origin Response Timeout** area, click **Edit**.

Figure 2-12 Origin response timeout

Configure Origin Response Timeout

i To configure the origin response timeout for domain names with special configurations, submit a service ticket.

Origin Response Timeout seconds

Default value: 30s. Value range: 5s to 300s.

OK **Cancel**

6. Enter the timeout interval and click **OK**.

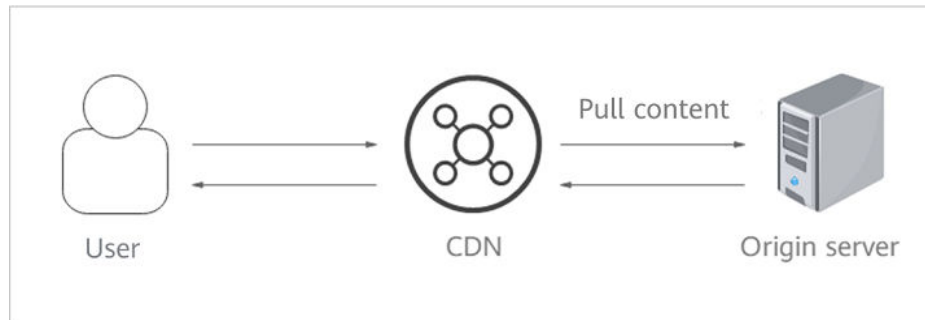
2.4.10 Origin Request Headers

You can configure HTTP headers in origin pull URLs.

Background

If the requested content is not cached on CDN PoPs, CDN PoPs pull that content from an origin server. You can configure HTTP headers on the CDN console to rewrite header details in origin pull URLs.

HTTP headers are part of an HTTP request or response message that define the operating parameters of an HTTP transaction.



Precautions

- This setting only modifies HTTP messages for origin pull through CDN. It does not modify those in an HTTP message that CDN PoPs return to users.
- A request header cannot have two different values at the same time.
- If your domain name has special configurations, the origin request headers cannot be configured.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. In the **Origin Request Headers** area, click **Add**.
6. Configure the header details.
 - **Add**: Add a header to CDN to rewrite HTTP headers in user request URLs.

Figure 2-13 Adding an origin request header

Add Origin Request Header

★ Request Header Operation Set Delete

★ Name

★ Value

Table 2-6 Parameter description

Parameter	Example	Description
Request Header Operation	Set	Add a specific header to an HTTP request of origin pull. <ul style="list-style-type: none"> If a request URL contains the X-test header and its value is 111, CDN will set X-test to aaa during origin pull. If a request URL does not contain the X-test header, CDN will add X-test and set its value to aaa during origin pull.
	Delete	Delete the HTTP header that exists in a user request URL. <ul style="list-style-type: none"> If a request URL contains the X-test header, it will be deleted during origin pull.
Name	X-test	<ul style="list-style-type: none"> Enter 1 to 64 characters. Enter only letters, digits, or hyphens (-).
Value	aaa	<ul style="list-style-type: none"> Enter 1 to 1,000 characters. When the header is Content-Disposition or Content-Language, the value contains up to 128 characters Enter letters, digits, and the following special characters: <code>._*#!&+ ^~"/;,:=@?<></code> Variables, such as <code>\$client_ip</code> and <code>\$remote_port</code>, are not allowed.

- **Edit:** Modify the value or operation of a header during origin pull. Click **Edit** in the **Operation** column next to a header.

Figure 2-14 Editing an origin request header

Edit Origin Request Header

★ Request Header Operation Set Delete

★ Name

X-test

★ Value

aaa

OK

Cancel

Parameter	Example	Description
Request Header Operation	Set	<p>Add a specific header to an HTTP request of origin pull.</p> <ul style="list-style-type: none"> If a request URL contains the X-test header and its value is 111, CDN will set X-test to aaa during origin pull. If a request URL does not contain the X-test header, CDN will add X-test and set its value to aaa during origin pull.
	Delete	<p>Delete the HTTP header that exists in a user request URL.</p> <ul style="list-style-type: none"> If a request URL contains the X-test header, it will be deleted during origin pull.
Name	X-test	This parameter cannot be modified.
Value	aaa	<ul style="list-style-type: none"> Enter 1 to 1,000 characters. When the header is Content-Disposition or Content-Language, the value contains up to 128 characters Enter letters, digits, and the following special characters: <code>.-_ *#!&+ ^~"/;,:=@?<></code> Variables, such as <code>\$client_ip</code> and <code>\$remote_port</code>, are not allowed.

- **Delete:** Delete the header settings. Click **Delete** in the **Operation** column of the request header to be deleted. In the displayed dialog box, select other domain names with the same header to be deleted and click **OK**.

7. Click **OK**.

Example

Assume that you have configured the following origin request headers for domain name `www.example.com`:

Request Header Operation	Name	Value
Set	X-cdn	aaa
Delete	X-test	

When a user requests the `http://www.example.com/abc.jpg` file, the file is not cached on CDN, and CDN pulls that file from the origin server. The **X-cdn** header will be added and the **X-test** header will be deleted during origin pull.

Restrictions

- If your domain name has special configurations, **Content-Type**, **Cache-Control**, and **Expires** cannot be configured.

- The following request headers can be modified but cannot be deleted.

Content-Base	Content-Disposition
Server	Content-Language
Cache-Control	Expires
Content-Type	-

- The following standard headers cannot be added, deleted, or modified.

Origin	accept-ch	clear-site-data	push-policy
WsTag	Tcp-Retrans	access-control-allow-methods	access-control-max-age
vary	Date	X-Forward-Type	width
Age	ETag	Purge-Extra	X-Cacheable
access-control-allow-headers	Front-End-Https	ping-to	content-range
cross-origin-opener-policy	Location	viewport-width	Mime-Version
Proxy-Support	X-Resp-Time	If-Range	sec-fetch-dest
device-memory	X-Mem-Url	Cdn-Src-Ip	ping-from
Allow	X-Url-Blackwhite-List	early-data	Sec-WebSocket-Extensions
if-unmodified-since	X-Forward-Uri	Conf-File	x-download-options
X-Error-Status	Negotiate	x-permitted-cross-domain-policies	service-worker-allowed
X-Appa	x-firefox-spdy	content-dpr	X-Miss-Times-Limit
X-Bwctrl-Limit	X-Bwctrl-Para	X-Max-Conns	nel
public-key-pins-report-only	X-MAA-Alias	Sec-WebSocket-Location	X-Cache-2
Authorization	Expect	last-event-id	Sec-WebSocket-Key
X-Refresh-Pattern	forwarded	X-Local-Ip	Sec-WebSocket-Protocol
feature-policy	cross-origin-resource-policy	Request-Range	Conf-Other

strict-transport-security	signed-headers	Cdn-Server-Ip	Sec-WebSocket-Version
accept	X-Black-List	content-location	sourcemap
Partition-Block-Size	Proxy-Authentication-Info	cross-origin-embedder-policy	X-Request-Id
x-dns-prefetch-control	if-none-match	If-Non-Match	Public
X-White-List	x-ua-compatible	Keep-Alive	Transfer-Encoding
alt-svc	max-age	Last-Modified	x-xss-protection
Sec-WebSocket-Nonce	dnt	Link	x-robots-tag
Key	expect-ct	sec-fetch-site	access-control-request-headers
X-Error-URL	X-Log-Url	content-encoding	X-Times-Limit
X-Appa-Origin	X-Miss-Rate-Limit	X-IP-Region	Dynamic
X-Squid-Error	From	accept-ch-lifetime	X-MAA-Auth
Connection	X-Via-CDN	Max-Forwards	Upgrade
sec-fetch-user	content-security-policy-report-only	Pragma	save-data
X-Client-Ip	Cdn-Qos	x-powered-by	X-Forward-Measured
accept-push-policy	server	large-allocation	X-Request-Uri
X-Forward-Ip	Host	Proxy-Authenticate	X-Request-Url
X-Cache-Lookup	Conf-Option	X-Forward-Host	upgrade-insecure-requests
X-Accelerator-Vary	signature	X-Ip-Blackwhite-List	X-Cdn-Src-Port
Sec-WebSocket-Draft	Sec-WebSocket-Origin	X-IP-Region-CN	public-key-pins
Ws-Hdr	If-Match	Proxy-Authorization	X-Rate-Limit
sec-fetch-mode	trailer	X-Rewrite-Url	Via
X-Cache	X-Mgr-Traffic	accept-signature	Warning

dpr	If-Modified-Since	Authentication-Info	access-control-request-method
Content-Length	x-frame-options(xfo)	Range	A_Dynamic
te	x-forwarded-host	Title	WWW-Authenticate
tk	X-Query-Key	accept-charset	access-control-allow-origin
accept-ranges	report-to	access-control-expose-headers	x-content-type-options
Proxy-Connection	server-timing	Retry-After	x-requested-with
X-No-Referer	X-Forward-Peer	Sec-WebSocket-Accept	X-Forwarded-For
Conf-Err-Host	Sec-WebSocket-Key2	access-control-allow-credentials	X-Denyattack-Dynconf
referrer-policy	Sec-WebSocket-Key1	content-security-policy	timing-allow-origin
X-DNS-Time	Conf-File-List	X-expireURL	x-pingback
Purge-Domain	x-forwarded-proto	-	-

2.4.11 FAQ

In What Scenarios Does CDN Pull Content from an Origin Server?

- The desired content is not cached on the CDN PoPs.
- The cached content on CDN PoPs has expired.

What Is the Difference Between a Host and an Origin Server?

- The origin server decides the address to be accessed during origin pull.
- The host decides the site that is associated with the requested content.

Assume that your origin server is an Nginx server. Its IP address is x.x.x.x, and its domain name is www.test.com. The following sites are deployed on the origin server:

```
server {
    listen 80;
    server_name www.a.com;

    location / {
        root html;
    }
}
server {
    listen 80;
    server_name www.b.com;
```

```
location / {  
    root html;  
}
```

If you want CDN to pull content from this Nginx server, set the origin server address to **x.x.x.x** or **www.test.com** on CDN. Since there are multiple sites on the origin server, you need to specify the specific site to pull content. If you want CDN to obtain content from the **www.a.com** site, set the host to **www.a.com** on CDN. If you want CDN to obtain content from the **www.b.com** site, set the host to **www.b.com** on CDN.

Does Huawei Cloud CDN Support Direct Origin Pull Through Crawler Access?

No.

Huawei Cloud CDN cannot distinguish normal user access from crawler access. If the crawler records the IP address of a PoP, the crawler can directly access that IP address next time. If the PoP is malfunctioning or undergoing routine maintenance, the crawler will be unable to pull content from that IP address.

How Do I Configure the Origin Server If a Non-Huawei Object Storage Bucket Serves as an Origin Server?

1. Obtain the domain name of the object storage bucket (private buckets are not supported).

When adding a domain name on the CDN console, select **Domain name** for **Type** and enter the domain name of the object storage bucket in the text box.

2. Modify origin settings.

By default, the host is your acceleration domain name. If you configure an object storage bucket as your origin server, change the host to the domain name of that object storage bucket. Otherwise, origin pull fails.

2.5 HTTPS Settings

2.5.1 Overview

HTTPS ensures secure transmission through encryption and identity authentication. It is widely used in security-sensitive communications on the World Wide Web, such as online payment.

The following table describes the HTTPS settings:

Function	Description
HTTPS Certificates	You can add a certificate for HTTPS acceleration.
TLS Versions	You can enable or disable TLS versions as required.

Function	Description
HTTPS Certificate Requirements	Describes the combination and upload sequence of certificates issued by different authorities
HTTPS Certificate Format Conversion	You can convert certificates in other formats to the PEM format that CDN supports.
OCSP Stapling	You can allow CDN to cache the status of online certificates in advance and return the status to browsers. Browsers do not need to query the status from certificate authorities (CAs), accelerating the verification.
Force Redirect	You can force redirect to HTTP or HTTPS.
HSTS	You can configure HSTS to force clients (such as browsers) to use HTTPS to access your server, improving access security.
HTTP/2	Describes the background and advantages of HTTP/2.
QUIC	You can configure the QUIC protocol to improve transmission security, reduce transmission and connection latency, and prevent network congestion.

2.5.2 HTTPS Certificates

You can configure an HTTPS certificate for an acceleration domain name on the CDN console to enable HTTPS acceleration.

Background

- **HTTP**
HTTP transfers content in plaintext without any data encryption. If an attacker intercepts packets transmitted between browsers and website servers, the transmitted content can be read directly.
- **HTTPS**
Based on HTTP, HTTPS uses Secure Sockets Layer (SSL) to encrypt data transmission. With SSL, servers are authenticated using certificates, and communications between browsers and servers are encrypted.

Prerequisites

CDN supports your own certificates. The format of your own certificates must meet the requirements described in [HTTPS Certificate Requirements](#).

Precautions

- Only certificates and private keys in PEM format are supported. If a certificate is not in PEM format, convert the certificate by referring to [HTTPS Certificate Requirements](#).
- An acceleration domain name has its associated certificate. They must match. If your domain name is a wildcard domain, configure a certificate for it by referring to
- Certificate settings will be automatically deleted once HTTPS secure acceleration is disabled. You need to re-configure the certificate if HTTPS secure acceleration is enabled again.
- If your certificate has changed, update certificate information on the CDN console in a timely manner.
- To use HTTPS for all links, the origin protocol should be HTTPS (and the origin server must support HTTPS). For details, see [Origin Protocol](#).

Configuring HTTPS Certificates

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **HTTPS Settings** tab.
5. On the **HTTPS Settings** tab page, click **Edit**. The **Configure HTTPS Secure Acceleration** dialog box is displayed.

Figure 2-15 Configuring HTTPS secure acceleration
Configure HTTPS Secure Acceleration

The screenshot shows a configuration interface for HTTPS secure acceleration. It includes a 'Status' toggle switch, a 'Certificate Source' section with radio buttons for 'My certificate' and 'SCM certificate', a 'Certificate Name' text input field, and two large text areas for 'Certificate Body' and 'Private Key', both containing the placeholder text 'PEM-encoded'. At the bottom are 'OK' and 'Cancel' buttons.

6. Switch on **Status** to enable this configuration item.
7. Set related parameters.

Table 2-7 Parameters of an international certificate

Parameter	Description
Certificate Source	Select My certificate or SCM certificate .
Certificate Name	<ul style="list-style-type: none"> • My certificate: Enter the certificate name containing 3 to 64 characters. • SCM certificate: CDN automatically obtains SSL certificates uploaded to the CCM console. You only need to select the desired one from the drop-down list.
Certificate Body	<ul style="list-style-type: none"> • My certificate: Use a local text editor to open the certificate and copy the content to the text box. • SCM certificate: The certificate body is automatically filled in. <p>NOTE The certificate body cannot contain spaces or blank lines. Otherwise, a message is displayed indicating that certificate parameters are incorrect.</p>

Parameter	Description
Private Key	<ul style="list-style-type: none"> • My certificate: Use a local text editor to open the private key and copy the content to the text box. • SCM certificate: The private key is automatically filled in.

8. (Optional) To set another certificate, click **Add Certificate** at the bottom and set related parameters.
 - Standards of the two certificates must be different. For example, if you have set an international certificate, you can add a Chinese (SM2) certificate.

9. Click **OK**.

10. Check whether the HTTPS certificate has taken effect.

If the certificate has taken effect, you can access website resources of the acceleration domain name through HTTPS and view the website authentication information by clicking the lock icon in the address box of the browser.

Updating the HTTPS Certificate

If your domain name certificate is updated, you need to update the certificate details in the HTTPS configuration item.

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**. The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **HTTPS Settings** tab.
5. On the **HTTPS Settings** tab, click **Edit**. The **Configure HTTPS Secure Acceleration** dialog box is displayed.

Figure 2-16 Updating a certificate

Configure HTTPS Secure Acceleration

Status

Certificate Source My certificate SCM certificate

Certificate Name

Certificate Body Configured [Update](#)

Private Key Configured [Update](#)

- Click **Update** to update the configured certificate and private key. It takes approximately 5 to 10 minutes for the update to take effect.

Viewing HTTPS Certificate Information

On the HTTPS certificate configuration page, you can view details about the HTTPS certificate configured for the acceleration domain names.

- Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
- In the navigation pane, choose **Domains**.
- In the domain list, click the target domain name or click **Configure** in the **Operation** column.
- Click the **HTTPS Settings** tab.
- On the page displayed, you can view details about the HTTPS certificate configured for the domain name, such as the certificate expiration time. You can also view the certificate content. However, the private key content cannot be viewed, for security reasons.

HTTPS Settings [Edit](#)

Enable HTTPS and deploy a certificate on all CDN PoPs for secure acceleration. [Learn more](#)

Status	Enabled
Certificate Source	My certificate
Certificate Name	gj-zy
Certificate Expiration Time	Nov 02, 2024 19:26:29 GMT+08:00

Certificate Body

```
-----BEGIN CERTIFICATE-----  
MIIDnTCCAoWgAwIBAgIKKtdNbCCh9ElvGTANBgkqhkiG9w0BAQsFADBIMQswCQYD  
VQQGEwJDTJEPMA0GA1UECAwG5Zub5bedMQ8wDQYDVQQHDAAbmiJDpg70xDzAN  
BgNV  
BAoMBmh1YXdlaTEMMMAoGA1UECwwDY2RuMRUwEwYDVQQDDAxxwY2EiZDE4NG  
E3MDIw
```

Private Key

The private key content cannot be viewed because it contains sensitive information.

Disabling the Certificate

- Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > CDN**.
The CDN console is displayed.
- In the navigation pane, choose **Domains**.
- In the domain list, click the target domain name or click **Configure** in the **Operation** column.
- Click the **HTTPS Settings** tab.
- Click **Edit** next to **HTTPS Settings**.
The **Configure HTTPS Secure Acceleration** dialog box is displayed.

6. Disable the **Status** switch and click **OK**.
 - Disable QUIC before disabling the certificate.

Certificate Expiration Time

The expiration time of a certificate chain is the same as that of the certificate that first expires in the chain.

2.5.3 HTTPS Certificate Requirements

The HTTPS configuration only supports certificates or private keys in PEM format. For different certificate issuing agencies, there are different upload requirements.

Certificates Issued by Root CA

A certificate issued by Root CA is a complete certificate. When configuring HTTPS, you only need to upload the certificate.

Use a text editor to open the certificate. The certificate content should be something similar to what is in [Figure 2-17](#).

A PEM certificate:

- The certificate starts with the -----BEGIN CERTIFICATE----- statement and ends with the -----END CERTIFICATE----- statement.
- Each line of the certificate is 64 characters long, but the last line can be shorter.
- No spaces are allowed in the certificate content.

Figure 2-17 PEM certificate

```
-----BEGIN CERTIFICATE-----
MIIDxCCAqygAwIBAgIEAJGCTANBgkqhkiG9w0BAQUFADBUMQswCQYDVQQLGwJj
bjELMAkGA1UECAwCZ2ZxZCZAJBgNVBAMcN6MqswCQYDVQQLKDAJodzeELMAkGA1UE
CwwCaHcxGDAwBGNVBAAMD21OT0MgUm9vdCBDQSBWMjERMAsGCSqGSIb3DQEJARYC
aHcwHhcNMTYwNTE3MDEyODQ2WhcNMjEwNTE2MDEyODQ2WjBdMQswCQYDVQQLGwJj
bjELMAkGA1UECBMCZ2ZxZCZAJBgNVBAoTAmh3MqswCQYDVQQLLEwJodzeEUMBGA1UE
AxQLKi5vd3Nnby5jb20xETAPBgkqhkiG9w0BCQEWAmh3MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAXDKJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909e
-----END CERTIFICATE-----
```

Certificates Issued by Intermediate Agencies

A certificate file issued by an intermediate agency contains several certificates. You need to combine the certificates into a single, complete certificate for upload

when configuring HTTPS security acceleration. A combined certificate is shown as [Figure 2-18](#).

Use a text editor to open all of the certificates. Start with the server certificate and append the content of the intermediate certificates to the file. Generally, an instruction will be issued together with the certificate. Be aware of the rules in the instruction. The general rules are as follows:

- There are no empty lines between certificates.
- The formats of certificate chains are as follows:

```
-----BEGIN CERTIFICATE-----  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
-----END CERTIFICATE-----
```


In the following examples, the name of certificates before conversion is **old_certificate** by default, and that of private keys before conversion is **old_key** by default. The new certificate and private key names are **new_certificate** and **new_key** respectively.

- **Converting DER to PEM**

```
openssl x509 -inform der -in old_certificate.cer -out new_certificate.pem  
openssl rsa -inform DER -outform pem -in old_key.der -out new_key.key
```

- **Converting P7B to PEM**

```
openssl pkcs7 -print_certs -in old_certificate.p7b -out new_certificate.cer
```

- **Converting PFX to PEM**

```
openssl pkcs12 -in old_certificate.pfx -nokeys -out new_certificate.pem  
openssl pkcs12 -in old_certificate.pfx -nocerts -out new_key.key
```

You can also use an online third-party certificate conversion tool to convert certificates into different formats.

2.5.5 TLS Versions

You can configure TLS versions as required.

Background

Transport Layer Security (TLS) is a security protocol used to ensure security and data integrity for Internet communication. The most typical application is HTTPS. TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3 are available. A later version is more secure, but is less compatible with browsers of earlier versions.

Table 2-8 TLS versions supported by mainstream browsers

TLS Version	Mainstream Browser
TLS 1.0	<ul style="list-style-type: none">• Chrome 1• Firefox 2+
TLS 1.1	<ul style="list-style-type: none">• Chrome 22+• Firefox 24+• Safari 7+
TLS 1.2	<ul style="list-style-type: none">• Chrome 30+• Firefox 27+• Safari 7+
TLS 1.3	<ul style="list-style-type: none">• Chrome 70+• Firefox 63+• Safari 14+

Constraints

- An HTTPS certificate has been configured. For details, see [HTTPS Certificates](#).
- You can enable a single version or consecutive versions. For example, you cannot enable TLS 1.0 and TLS 1.2 but disable TLS 1.1.

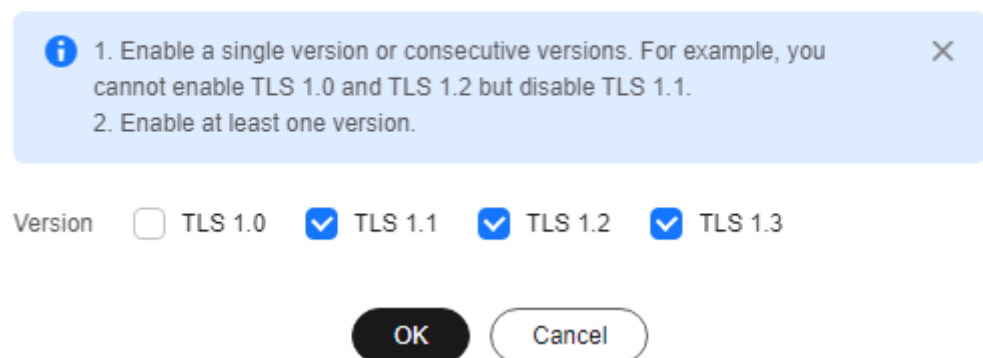
- You need to enable at least one version.
- By default, TLS 1.1, TLS 1.2, and TLS 1.3 are enabled.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **HTTPS Settings** tab.
5. In the **TLS Version** area, click **Edit**.

Figure 2-20 Configuring the TLS versions

Configure TLS Version



6. Select one or more TLS versions and click **OK**.

2.5.6 Force Redirect

Requests from clients to CDN PoPs can be forcibly redirected to HTTP or HTTPS.

Scenarios

Force redirect to HTTP: If you do not have high security requirements, use 301 or 302 to forcibly redirect all client requests to HTTP.

Force redirect to HTTPS: If you have set a certificate for your domain name on CDN and you pay more attention to business security, use 301 or 302 to forcibly redirect all client requests to HTTPS.

Precautions

- To redirect requests to HTTPS, [configure an HTTPS certificate](#) for your domain name first.
- If you enable HTTP/2, force redirect to HTTP does not take effect.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **HTTPS Settings** tab.
5. Click **Edit** next to **Force Redirect**. The **Force Redirect** dialog box is displayed.

Figure 2-21 Force redirect

Force Redirect

Status

Protocol HTTP HTTPS

Redirect Mode 301 302

Table 2-9 Parameter description

Parameter	Description
Status	Whether to enable this function. Enabled: Specify whether to redirect requests from clients to HTTP or HTTPS. Disabled: Both HTTP and HTTPS requests from clients are supported.
Protocol	HTTP : Requests from clients to CDN PoPs are forcibly redirected to HTTP. HTTPS : Requests from clients to CDN PoPs are forcibly redirected to HTTPS.
Redirect Mode	301 302

6. Select a protocol and click **OK**.

2.5.7 HSTS

HTTP Strict Transport Security (HSTS) is a web security protocol promoted by Internet Engineering Task Force (IETF). HSTS forces clients (such as browsers) to use HTTPS to access your server, improving access security.

Working Principles

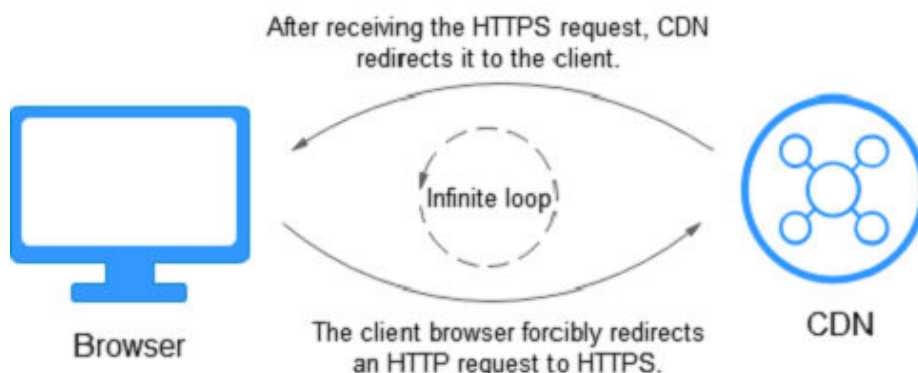
If HSTS is configured on CDN, when a client (such as a browser) uses HTTPS to access a CDN PoP for the first time, the PoP responds to the browser with the **Strict-Transport-Security** header. The browser caches this header if it supports HSTS and uses HTTPS to access CDN PoPs until the cache expires.

Prerequisites

You have [configured an HTTPS certificate](#).

Precautions

- Use [force redirect](#) to redirect the first HTTP client request to HTTPS.
- To disable the HTTPS certificate, disable HSTS as well.
- When HSTS is enabled and a browser caches the **Strict-Transport-Security** header, force redirect to HTTP will lead to an infinite loop. As a result, the domain name cannot be accessed.



- To enable HSTS for domain names with special configuration, submit a service ticket.
- HSTS takes effect on clients. After HSTS is disabled, you need to refresh the browser cache. In this way, the next HTTP request from a client will not be automatically redirected to HTTPS.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.

4. Click the **HTTPS Settings** tab.
5. In the **HSTS** area, click **Edit**.
6. Turn on the **Status** switch and set parameters.

Figure 2-22 HSTS

HSTS

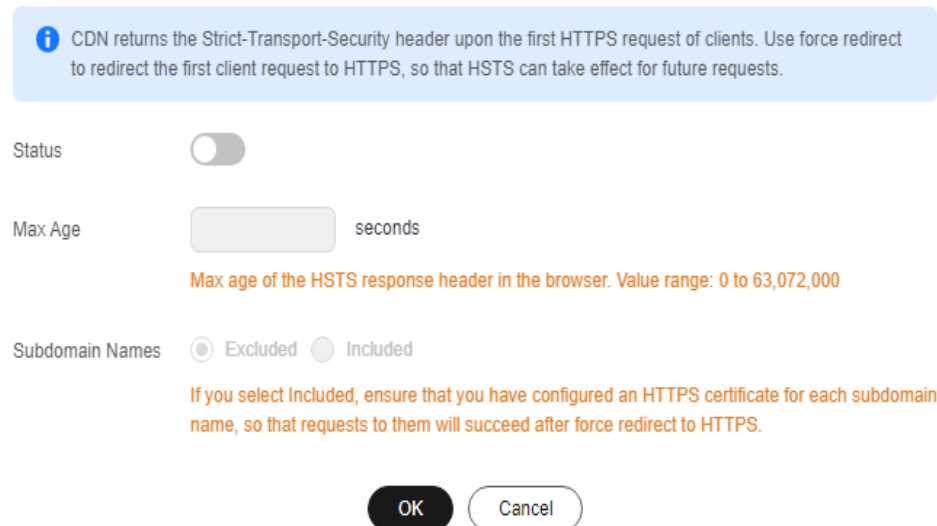


Table 2-10 Parameters

Parameter	Description
Max Age	<p>TTL of the response header Strict-Transport-Security on clients.</p> <ul style="list-style-type: none"> • The value ranges from 0 to 63,072,000, in seconds. • If the TTL is too short, the client cache frequently expires, affecting HSTS. If the TTL is too long and the HTTPS certificate is canceled within the TTL, the domain name cannot be accessed, affecting businesses. The recommended TTL is 5,184,000 seconds, that is, 60 days.
Subdomain Names	<p>Whether to enable HSTS for subdomain names.</p> <ul style="list-style-type: none"> • Excluded: HSTS is disabled for subdomain names. • Included: HSTS is enabled for subdomain names. Check whether HTTPS certificates have been configured for all subdomain names. Otherwise, subdomain names cannot be accessed.

7. Click **OK**.

Example

Assume that you have configured the following HSTS settings for the domain name www.example.com.

HSTS [Edit](#)

When HSTS is enabled, CDN adds the Strict-Transport-Security header to responses to clients. After caching the header, clients will automatically use HTTPS to send requests to CDN nodes, improving access security. [Learn more](#)

Status Enabled

Max Age 518,400 seconds

Subdomain Names Included

Configuration effect:

1. When a client uses HTTPS to access the domain name for the first time, the CDN PoP returns the requested content with the **Strict-Transport-Security** header.
2. If the client does not support HSTS, the protocol of client requests to CDN PoPs is not changed.
3. If the client supports HSTS, the client caches the **Strict-Transport-Security** header. When the client accesses the domain name again, the browser automatically converts the HTTP request to an HTTPS request and sends the request to CDN.
4. After the browser TTL expires, step **1** is performed again.

2.5.8 HTTP/2

Background

HTTP/2 is a next-generation hypertext transfer protocol. It reduces the TCP handshake delay, reduces the packet header transmission volume, and improves transmission efficiency. Addresses in the format of **http://url** can use only the HTTP/1.x protocol, and those in the format of **https://url** support HTTP/2.

Prerequisites

An HTTPS certificate has been configured. For details, see [HTTPS Certificates](#).

- Disabling the HTTPS certificate will disable HTTP/2.
- After configuring the HTTPS certificate, wait about 5 minutes for the configuration to complete and then enable HTTP/2.

Protocol Advantages

HTTP/2 outperforms HTTP/1.1 and keeps the syntax of HTTP/1.1.

HTTP/2 outperforms HTTP/1.1 in the following aspects:

- Binary framing
HTTP/2 uses binary format to transfer data, while HTTP/1.1 is a text-based protocol. Binary format is more advantageous in resolving and optimizing the protocol, and it raises the efficiency of data transfer.
- Header field compression
HTTP/2 compresses and transfers message headers using HPACK. These headers are traced and stored in a header table. Once a message header has been sent for once, it is cached and can be obtained by other identical message headers automatically.

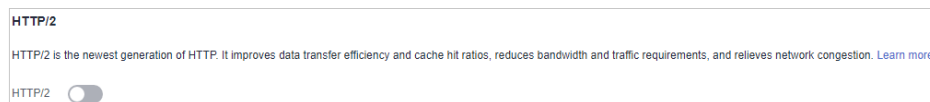
Requests using HTTP/1.1 carry a large amount of redundant header information, which causes waste to bandwidth. With header field compression, HTTP/2 saves the bandwidth and traffic.

- **Multiplexing**

HTTP/2 multiplexes multiple requests or responses over a single TCP connection. While HTTP/1.1 establishes a TCP connection for each request or response in order. By sending requests concurrently, HTTP/2 lessens the pressure on server connection and alleviates the network blocking problem.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **HTTPS Settings** tab.
5. Switch on **HTTP/2**.



2.5.9 OCSP Stapling

When Online Certificate Status Protocol (OCSP) stapling is enabled, CDN queries and caches the status of online certificates in advance and returns the status to a browser when establishing a TLS connection with the browser. This means that the browser does not need to query the status from certificate authorities (CAs), accelerating the verification.

Working Principles

CAs provide OCSP information for clients to check validity of certificates in real time.

- **When OCSP stapling is disabled**, each visitor to the website sends a query for OCSP, affecting page loading on browsers. A large number of concurrent requests bring great pressure to CA servers.
- **When OCSP stapling is enabled**, CDN queries and caches verification results of online certificates in advance. Users do not need to send requests to CAs. They only need to verify the validity of the cached results. This improves the TLS handshake efficiency and reduces the verification time.

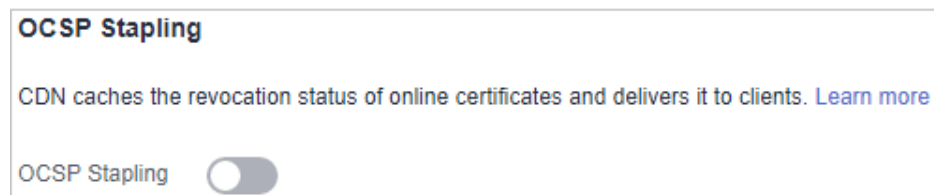
Constraints

- An HTTPS certificate has been configured. For details, see [HTTPS Certificates](#).
 - Disabling the HTTPS certificate will disable OCSP stapling.
 - After configuring the HTTPS certificate, wait about 5 minutes for the configuration to complete and then enable OCSP stapling.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **HTTPS Settings** tab.

Figure 2-23 OCSP stapling



NOTE

By default, OCSP stapling is disabled.

5. Switch on **OCSP Stapling**.

2.5.10 QUIC

This chapter describes what is QUIC and how to configure QUIC.

What Is QUIC?

Quick UDP Internet Connections (QUIC) is a UDP-based transport protocol. It has the following features:

- It has excellent performance in weak networks and can provide available services in the case of packet loss and severe network delay.
- All QUIC traffic is encrypted, improving transmission security.
- It reduces the transmission and connection delay and prevents network congestion.

Supported Version

IETF-v1 (H3)

Prerequisites

An international HTTPS certificate has been configured. For details, see [HTTPS Certificates](#).

- Disabling the HTTPS certificate will disable QUIC.
- After configuring the HTTPS certificate, wait about 5 minutes for the configuration to complete and then enable QUIC.

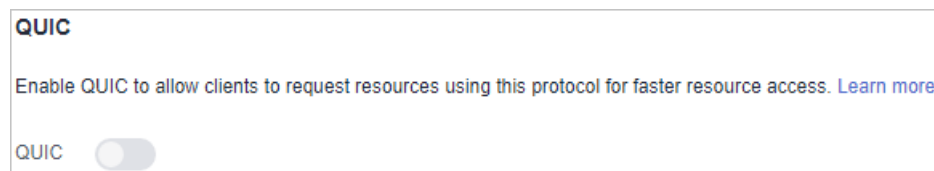
Precautions

- QUIC cannot be used for origin pull.
- This function is in OBT and is available for free trial.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **HTTPS Settings** tab.
5. In the **QUIC** area, switch on **QUIC**.

Figure 2-24 QUIC



2.5.11 FAQ

How Do I Fix It If "Incomplete certificate chain" Is Displayed?

This is maybe because:

- Invalid certificate format
- Certificates are filled in wrong.
- Certificates are installed in the wrong order.

Sort the certificates with the root certificate at the end. For example, if you have three certificates, A, B, and C; and the root certificate, the order should be: certificate C - certificate B - certificate A - root certificate.

For details about how to get the certificate chain right, see [HTTPS Certificate Requirements](#).

Alternatively, use an online certificate chain tool to fix the incomplete certificate chain.

How Do I Fix It If the System Displays a Message Indicating that the Certificate Format Is Incorrect?

HTTPS configuration only supports certificates and private keys in the PEM format. Different certificate authorities have different requirements on the upload of the certificate body. For details about the format requirements, see [HTTPS Certificate Requirements](#). If your certificate format is not PEM, use an online third-party tool to convert the certificate before uploading it.

2.6 Cache Settings

2.6.1 Overview

CDN caches origin content on PoPs across the globe so that users can obtain content from nearby PoPs. You can modify cache settings to change the cache status of resources on CDN PoPs.

The following table describes the cache settings.

Function	Description
Cache Rules	You can set the cache TTL and priority for different resources to increase the hit ratio and reduce the back-to-source rate.
Browser Cache TTL	You can set a browser cache TTL, during which users can obtain content directly from their browser cache (if available), reducing origin pulls.
Status Code Cache TTL	You can cache error codes returned by the origin server to CDN PoPs in a specific duration, so that CDN returns the error codes to users when they request content. This can reduce origin pulls and relieve the pressure on the origin server.

NOTE

- If you have modified the cache rules and origin cache control settings, pay attention to the following:
 - The new rule does not apply to content that has been cached but only applies to new content.

2.6.2 Cache Rules

You can configure the TTL for one or more cached resources on CDN PoPs. If the TTL of a file cached on CDN PoPs has reached, CDN requests the most recent content of the file from the origin server when a user requests the file. CDN returns the content to the user and caches it on CDN PoPs. You can cache all files and the homepage, or cache desired content by directory, file type, and full path.

Background

Cache policies on CDN PoPs comply with HTTP. You can control cache aging by configuring the **Cache-Control: max-age** field in an HTTP response header. By leveraging cache rules, you can optimize cache periods for different services. Appropriate cache policies can increase the hit ratio and reduce the origin pull rate, which reduces bandwidth utilization.

After receiving a request, a CDN PoP will check whether the requested content has expired in the cache. If the requested content is valid in the cache, it will be

returned directly from that CDN PoP to the user, speeding up site response. If the requested content in the cache has expired, the CDN PoP will send a request to obtain new content from an origin server so it can update its local cache and serve new content to the user.

Precautions

- Up to 60 cache rules can be added to each domain name.
- The cache TTL affects the origin pull rate directly. If the TTL is short, cached content on CDN PoPs becomes invalid in a short time, resulting in frequent origin pulls, which increases the origin server load and prolong the access latency. However, if the TTL is too long, cached content may be outdated as a result.
- If the TTL is set to 0, CDN pulls content from the origin server for all user requests, which may interrupt the acceleration service.
- Resources cached on PoPs may be deleted due to infrequent access.
- If you have modified the cache rule,
 - The new rule does not apply to content that has been cached but only applies to new content.
 - You can refresh the cache to make the modification immediately take effect for new content and the content that has been cached.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Cache Settings** tab.
5. In the **Cache Rules** area, click **Edit**. The **Configure Cache Rule** dialog box is displayed.
6. Click **Add** to add cache rules. See [Figure 2-25](#). [Table 2-11](#) describes the parameters. You can click **Suggested Rules** to view the recommended configuration.

Figure 2-25 Configuring a cache rule

Configure Cache Rule

ⓘ Your modifications are effective in minutes for new content cached. For existing cache, refresh to apply them. ×

Type	Content	Priority ?	TTL ?	Query Parameters	URL Parameters	Origin Cache Control	Operation
File type <input type="text"/>	<input type="text" value=".php;.jsp;.asp;.aspx"/>	<input type="text" value="2"/>	<input type="text" value="0"/> <input type="text" value="seconds"/>	<input type="text" value="Retain all"/>	<input type="text"/>	<input type="checkbox"/>	Delete
All files <input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="30"/> <input type="text" value="days"/>	<input type="text" value="Retain all"/>	<input type="text"/>	<input type="checkbox"/>	Delete

[Suggested Rules](#) ^

Table 2-11 Cache rule parameters

Parameter	Description	Configuration Rule
All files	All cached resources on CDN PoPs	By default, CDN has a rule for every new domain name. The rule specifies that the TTL for All files is 30 days. You can modify but cannot delete this rule.
File type	Files of a specific type If the service type of a new domain name is Website , File download , or On-demand service and its origin server is a private one, CDN adds a rule to it by default. The rule specifies that the TTL is 0 for common dynamic files, such as .php .jsp .asp, and .aspx files. CDN pulls such files from the origin server for every request. You can modify and delete this rule.	<ul style="list-style-type: none"> • All file types are supported. • Start each file name extension with a period (.), and separate file name extensions with semicolons (;). • Enter up to 50 file name extensions. • Enter up to 1,000 characters. • File name extensions are case-insensitive. <p>Example: .JPG;.zip;.exe</p>

Parameter	Description	Configuration Rule
Directory	Files in a directory	<p>Directories are matched by prefix. Start a directory with a slash (/), and separate multiple directories with semicolons (;). Enter a maximum of 20 directories with a maximum of 255 characters in total. Example: /test/folder01;/test/folder02</p> <ul style="list-style-type: none"> • Wildcard matching is supported. Rules for using wildcards (*): <ul style="list-style-type: none"> - Only one directory with one wildcard can be set for each rule. Example: /test/* - CDN uses prefix match. For example, when the path of a cache rule is /test/*, /test/abc and /test/abc/001 also use this rule. - Wildcards cannot be set for domain names with special configurations. - Wildcards cannot match slashes (/). For example, /test*/abc cannot match /test/folder01/folder02/abc. - A wildcard can match one or more characters but cannot match zero characters. For example, /test* cannot match /test. - /* cannot be set as a path.

Parameter	Description	Configuration Rule
Full path	A specific file	A full path must start with a slash (/) and cannot end with a wildcard (*). A file in the specified directory or file with the wildcard (*) can be matched. Enter only one full path. Examples: /test/index.html or /test/*.jpg
Homepage	Root directory	The root directory of a website is the top-level directory of the website folder, which contains all subfolders of the website. For example, for abc/file01/2.png , abc/ is the root directory, and a cache rule is configured for abc/ .
Priority	Priority of a cache rule Each cache rule must have a unique priority. If a resource is specified in multiple cache rules, the rule with the highest priority is applied.	Enter an integer ranging from 1 to 100. A greater number indicates a higher priority.
TTL	Duration that a file can be cached. If the TTL of the file has reached, CDN requests the most recent content of the file from the origin server when a user requests the file from a CDN PoP. In addition, the CDN caches that content on the CDN PoP.	The TTL of a cached file cannot exceed 365 days. You are advised to set the time according to the following rules: <ul style="list-style-type: none"> • For static files (such as .jpg and .zip files) that are not frequently updated, set the TTL to more than one month. • For static files (such as .js and .css files) that are frequently updated, set the TTL based on service requirements. • For dynamic files (such as .php, .jsp, and .asp files), set the TTL to 0 seconds.

Parameter	Description	Configuration Rule
Query Parameters	<p>Most web page requests carry URL parameters starting with a question mark (?). If parameters do not contain important information (such as version), you can ignore them to improve the cache hit ratio and speed up delivery.</p> <p>Configuration rules:</p> <ul style="list-style-type: none"> • If resources do not change with URL parameters, ignore query parameters. • If resources change with URL parameters, do not ignore query parameters. • If you have enabled video seek, set Query Parameters to Ignore all for your video resources. 	<ul style="list-style-type: none"> • Retain all: CDN retains all parameters following the question mark (?). • Ignore all: CDN ignores all parameters following the question mark (?) in request URLs, improving the cache hit ratio. • Ignore specific: CDN ignores the specified parameters in request URLs but retains other parameters. • Retain specific: CDN retains the specified parameters in request URLs but ignores other parameters.
URL Parameters	<p>Parameters to be ignored or retained. Leave this parameter blank when Query Parameters is set to Retain all or Ignore all.</p>	<ul style="list-style-type: none"> • Enter up to 10 parameter names separated by semicolons (;). • Only letters, digits, periods (.), underscores (_), and tildes (~) are supported.
Origin Cache Control	<p>If Cache-Control: max-age or Expires has been configured for the origin server and you want the cache TTL on the CDN side to be the same as that configured on the origin server, you can switch on Origin Cache Control. Then Cache-Control: max-age or Expires determines how long content is cached on CDN PoPs.</p> <p>NOTE</p> <ul style="list-style-type: none"> • If both Cache-Control and Expires are configured on the origin server, Cache-Control is preferentially used. • If origin cache control is enabled on CDN but neither Cache-Control nor Expires is configured on the origin server, CDN PoPs use the cache rules configured on CDN. 	<p>By default, this function is disabled.</p>

Parameter	Description	Configuration Rule
Forcible Cache	<p>Whether CDN PoP cache ignores the no-cache, private, and no-store fields in the Cache-Control response header sent from the origin server. Forcible cache supplements origin cache control. The default rules are as follows:</p> <ol style="list-style-type: none"> When origin cache control is enabled, forcible cache is disabled. <ul style="list-style-type: none"> If no-cache, private, or no-store is set in the Cache-Control response header, CDN PoPs do not cache resources. If other response headers are set, the priority is s-maxage > max-age > expires. For example, if Cache-Control: max-age=500, s-maxage=400 is set on the origin server, the cache TTL on CDN PoPs is 400s. If the preceding response headers are not set, the cache TTL configured on the CDN console is used. When origin cache control is disabled, forcible cache is enabled. <ul style="list-style-type: none"> CDN ignores response headers from the origin server and uses the cache TTL configured on the CDN console. 	Enabled

Parameter	Description	Configuration Rule
	<p>NOTE</p> <ul style="list-style-type: none"> This parameter is a special configuration parameter and is for display only. You cannot modify it. If necessary, submit a service ticket to modify it. When both origin cache control and forcible cache are disabled, there are two cases: <ol style="list-style-type: none"> If no-cache, private, or no-store is set in the Cache-Control response header sent from the origin server, CDN PoPs do not cache resources. If no-cache, private, or no-store is not set, CDN uses the cache TTL configured on the CDN console. 	

- (Optional) Delete a cache rule if you no longer use it.
- Click **OK**.

Examples

Scenario 1: Assume that you have configured CDN acceleration for the domain name `www.example.com`. The following figure shows the cache rule configuration.

Type	Content	Priority	TTL	Query Parameters
Homepage		2	0 day	Retain all
All files		1	30 days	Ignore all

The homepage of the website is not cached, and URL parameters are not ignored in requests for all pages.

Scenario 2: Assume that you do not want to cache files of a specific type.

- You have configured CDN acceleration for the domain name `www.example.com`. Due to service requirements, files in `.do` format do not need to be cached, and URL parameters should be ignored in requests for all files.

You can add a cache rule for your website on the CDN console, with **Type** set to **File type**, **Content** to `.do`, and **TTL** to **0**.

Type	Content	Priority	TTL	Query Parameters
File type	<code>.do</code>	3	0 day	Retain all
All files		1	30 days	Ignore all

NOTE

The new rule only applies to new content. After the new rule is added, refresh the cached URL or directory where the `.do` file is located on the CDN console so that the new rule can take effect for all `.do` files.

2. You have configured CDN acceleration for your website, the login page of your website is displayed cyclically, and your customers cannot log in to the website. After CDN acceleration is disabled, customers can log in to the website.

This is because CDN PoPs have cached the login page. To resolve the issue, add a cache rule for your website on the CDN console and set the cache TTL of the login page to 0 in the rule. Take the login page of the Huawei Cloud console as an example. The login page of the Huawei Cloud console is <https://auth.huaweicloud.com/authui/login.html#/login>. You can add a cache rule on the CDN console, with **Type** set to **Full path**, **Content** to **/authui/login.html#/login**, and **TTL** to **0**.

Type	Content	Priority	TTL	Query Parameters
Full path	/authui/login.html#/login	4	0 day	Retain all
All files		1	30 days	Ignore all

Scenario 3: Assume that you have configured the following cache rules for your acceleration domain name www.example.com but do not know which rule takes effect.

Type	Content	Priority	TTL
Full path	/test/*.jpg	8	3 days
Directory	/test/folder01	6	5 days
File type	.jpg	2	1 day
All files		1	30 days

When a user requests www.example.com/test/cdn.jpg, rules of the **All files**, **File type**, and **Full path** type are all matched. The priority of the **Full path** rule is 8, which is the highest among the three rules. Therefore, the rule of the **Full path** type (**/test/*.jpg**) is used.

2.6.3 Browser Cache TTL

Customize the cache time to live (TTL) of client browsers to reduce the pull rate. When a user requests a resource, if the resource is cached in their browser, the resource is directly returned. Otherwise, the browser will request resource from a CDN PoP.

Precautions

- Add up to 10 rules for each domain name.
- Add only one rule for all files or homepage for each domain name.

Procedure

1. Log in to . Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the domain name you want to modify or click **Configure** in the **Operation** column.
4. Click the **Cache Settings** tab.
5. In the **Browser Cache TTL** area, click **Edit**.

- In the displayed dialog box, click **Add** and set the browser cache policy as required.

Figure 2-26 Browser cache TTL

Configure Browser Cache TTL

Table 2-12 Parameters

Parameter	Description
Type	<ul style="list-style-type: none"> • All files • File type: files with the specified extension names • Directory: files under the specified directory • Full path: file of the complete path • Homepage

Parameter	Description
Content	<p>When Type is set to All files, leave this parameter blank.</p> <p>When Type is set to File type:</p> <ul style="list-style-type: none"> • Start with a period (.) and separate file name extensions by commas (,). Do not end with a comma (,) or enter consecutive commas (,,). • Enter up to 20 file name extensions. • Enter up to 255 characters. • File name extensions are case-insensitive. • Example: .JPG,.zip,.exe <p>When Type is set to Directory:</p> <ul style="list-style-type: none"> • Start with a slash (/) and separate directories by commas (,). Do not end with a comma (,) or enter consecutive commas (,,). • Enter up to 20 directories. • Enter up to 255 characters. • Do not enter wildcards (*). • Example: /test/folder01,/test/folder02 <p>When Type is set to Full path:</p> <ul style="list-style-type: none"> • Start with a slash (/). • A wildcard (*) can only follow the last slash (/). • Enter only one full path. • Enter up to 255 characters. The following special characters are not allowed: ; :"\ • Examples: /test/index.html or /test/*.jpg <p>When Type is set to Homepage, the root directory of a website is used. It is the top-level directory of the website folder, which contains all subfolders of the website. For example, for www.example.com/abc/file01/2.png, abc/ is the root directory.</p>
Priority	<p>Priority of the rule. Enter an integer ranging from 1 to 100. A greater number indicates a higher priority.</p> <p>Each rule must have a unique priority.</p>
Cache Mode	<ul style="list-style-type: none"> • Honor origin Cache-Control: Comply with the cache policy of the origin server, that is, the setting of the Cache-Control header. • Cache: Comply with the TTL set in this rule. • No cache: Browsers do not cache the resources.
TTL	<p>When the configured TTL arrives and a user requests the resources again, the browser requests the resources from CDN.</p>

7. Click **OK**.

2.6.4 Status Code Cache TTL

When a CDN PoP pulls a resource from the origin server, the origin server returns a status code. You can set the cache time to live (TTL) of the status code on the CDN console. When a client requests the resource again, origin pull will not be triggered, reducing the origin pull ratio and the pressure on the origin server.

Scenarios

This function applies to the scenario where the origin server returns an abnormal status code. When the origin server is running properly, CDN caches an origin resource on PoPs based on cache rules you configure. When a user accesses the resource, origin pull will not be triggered. If the origin server responds abnormally and you do not want the origin server to respond to all requests, you can set the status code cache TTL to reduce the pressure on the origin server.

- **Application:** If users are continuously accessing image **abc.jpg** that is not cached on CDN PoPs and that has been deleted from the origin server, CDN PoPs will pull the image for each user request and the origin server will return a 4xx status code, increasing the pressure on the origin server. In this case, if you configure the cache TTL for the status code 4xx on CDN, CDN PoPs will directly return the status code 4xx when users request the image, and origin pull is not required.

Precautions

- If a resource is not cached on CDN PoPs, the status code generated when a client requests the resource cannot be cached even if a cache TTL has been set for this status code.
- The status code cache TTL cannot be configured for domain names with special configurations.
- By default, CDN caches status codes 404, 500, 502, and 504 for 3 seconds and does not cache other status codes.
 - The header settings determine whether the 404 status code is cached by default. If the **X-HTTP-Method-Override**, **X-HTTP-Method**, or **X-Method-Override** header is carried, the 404 status code is not cached by default. If not, the 404 status code is cached for 3 seconds.
- When **Query Parameters** is set to **Ignore all** for a resource, and a status code (for example, 400) returned for a client request is cached, the status code (400 in this example) will be returned for all requests for the resource within the cache TTL.
- You can modify the cache TTL of the following status codes:
 - 4XX: 400, 403, 404, 405, and 414
 - 5XX: 500, 501, 502, 503, and 504
 - 3XX: 301 and 302

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Cache Settings** tab.
5. Click **Add** under **Status Code Cache TTL**.

Figure 2-27 Adding a status code cache TTL

Add Cache Rule

* Status Code

* Cache TTL

Table 2-13 Parameters

Parameter	Description	Example
Status Code	Status code to be cached.	404
Cache TTL	Duration for caching the status codes on CDN PoPs. <ul style="list-style-type: none"> • If it is set to 0, the status code is not cached. • The maximum value is 365 days. • The 3XX status codes can be cached for 0 to 20 seconds. 	3 days

6. Configure the parameters and click **OK**.

Example

Assume that you have configured the following status code cache rules for the domain name [www.example.com](#).

Status Code	Cache TTL
404	30 days

Result: When a user accesses a resource that is not cached on a CDN PoP, the CDN PoP pulls the resources from the origin server. However, the origin server has

deleted the resource and returns a status code 404. CDN transparently transmits the status code to the user and caches the status code on the CDN PoP. Within the cache TTL (30 days), when a user accesses the resource again, CDN directly returns the status code 404 to the user and does not need to pull content from the origin server, reducing the pressure on the origin server.

2.7 Access Control

2.7.1 Overview

You can configure referer validation, IP address access control lists (ACLs), User-Agent access control lists (ACLs), and token authentication to identify and filter out unauthorized users and improve CDN security.

Function	Description
Referer Validation	This section describes how to configure a referer blacklist or whitelist. Users are identified and filtered according to the configured filter policies, in order to control access sources.
IP ACL	This section describes how to configure a policy for filtering out requests from specific IP addresses to restrict access.
User-Agent ACL	This section describes how to configure User-Agent filtering to restrict access.
Token Authentication	This section describes how to configure token authentication to protect website resources from being downloaded by malicious users.
Remote Authentication	This section describes how to configure remote authentication, so CDN can forward user requests to a specific server for authentication to prevent malicious resource download.

2.7.2 Referer Validation

This topic describes how to configure a referer blacklist or whitelist. Users are identified and filtered according to the configured filter policies, controlling access sources.

Background

The referer field in an HTTP request header identifies the address of the web page from which the resource has been requested. CDN PoPs can use the referer field to trace and identify the source.

When receiving access requests from users, the CDN PoPs identify and check users against the referer blacklist or whitelist. Only users meeting blacklist and whitelist

requirements can access the content. Unqualified users will receive a 403 error response.

Precautions

- This function is disabled by default.
- Either a referer blacklist or whitelist can be configured.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab.
5. In the **Referer Validation** area, click **Edit**. The **Configure Referer Validation** dialog box is displayed.

Figure 2-28 Configuring referer validation

Configure Referer Validation

Status

* Type Referer blacklist Referer whitelist

Include blank referer ?

* Rule

OK Cancel

6. Switch on **Status** to enable this configuration item.
7. Select a value for **Type** and set referer parameters based on service requirements. The following table describes the parameters.

Table 2-14 Parameters

Parameter	Description	Filling Rule
Include blank referer	<p>A blank referer is when the referer field in an HTTP request is left blank or when an HTTP request does not contain the referer field. If this option is selected, such requests will also be filtered out based on configured whitelists and blacklists.</p> <p>NOTE A blank referer indicates that the referer field is left blank or is not included in an HTTP request. The referer field with value null is not a blank referer.</p>	/
Referer whitelist	<ul style="list-style-type: none"> • If the referer field of an access request matches the whitelist rules, the requester can access the requested content. Otherwise, CDN returns a 403 error response code, indicating that access is forbidden. • If Include blank referer is selected and an access request contains a blank referer, the requester can access the requested content. 	<ul style="list-style-type: none"> • Enter domain names or IP addresses separated by semicolons (;). • Wildcard domain names are supported. • Enter up to two asterisks (*). They cannot be consecutive or at the end. • Domain names and IP addresses with ports are supported. The maximum port number is 65535. • Enter up to 400 domain names and IP addresses. Example: www.example.com:443 ;*.test.com;192.168.0.0 <p>NOTE Domain names with special configurations support only one asterisk (*).</p>

Parameter	Description	Filling Rule
Referer blacklist	<ul style="list-style-type: none"> If the referer field in an access request matches the blacklist rules, the requester cannot access the requested content, and 403 Forbidden will be returned. Otherwise, the requester can access the requested content. If Include blank referer is selected and an access request contains a blank referer, the access request will be rejected, and 403 Forbidden will be returned. 	<ul style="list-style-type: none"> Enter domain names or IP addresses separated by semicolons (;). Wildcard domain names are supported. Enter up to two asterisks (*). They cannot be consecutive or at the end. Domain names and IP addresses with ports are supported. The maximum port number is 65535. Enter up to 400 domain names and IP addresses. Example: www.example.com:443 ;*.test.com;192.168.0.0 <p>NOTE Domain names with special configurations support only one asterisk (*).</p>

8. In the **Rule** text box, enter the domain names.
9. Click **OK**.
10. (Optional) Disable referer validation.
 - Switch off **Status** to disable referer validation and clear all referer validation settings. You need to set related parameters when enabling this function again.

Examples

1. Assume that a referer whitelist **www.test.com** is configured for the domain name **www.example.com** and **Include blank referer** is selected.

Status	Enabled
Type	Referer whitelist
Rule	<code>www.test.com</code>

Blank Referer Contained

- If user 1 requests the URL **https://www.example.com/file.html** and the value of the referer field in the request is blank, CDN returns the content.
 - If user 2 requests the URL **https://www.example.com/file.html** and the value of the referer field in the request is **www.test.com**, CDN returns the content.
 - If user 3 requests the URL **https://www.example.com/file.html** and the value of the referer field in the request is **www.abc.com**, CDN returns a 403 error response code.
2. Assume that a referer blacklist **www.test01.com** is configured for the domain name **www.example01.com** and **Include blank referer** is selected.

Status	Enabled
Type	Referer blacklist
Rule	<code>www.test01.com</code>

Blank Referer Contained

- If user 1 requests the URL **https://www.example01.com/file.html** and the value of the referer field in the request is blank, CDN returns a 403 error response code.
- If user 2 requests the URL **https://www.example01.com/file.html** and the value of the referer field in the request is **www.test01.com**, CDN returns a 403 error response code.
- If user 3 requests the URL **https://www.example01.com/file.html** and the value of the referer field in the request is **www.bcd.com**, CDN returns the content.

2.7.3 IP ACL

This topic describes how to configure an access control list (ACL) of IP addresses. You can set a filtering policy to filter out requests from specific IP addresses to restrict access and prevent content theft and attacks.

Precautions

- This function is disabled by default.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab.
5. In the **IP ACL** area, click **Edit**. The **Configure IP ACL** dialog box is displayed.

Figure 2-29 Configuring an IP ACL

Configure IP ACL

Configure IP ACL

Information:

1. Up to 500 blacklisted or whitelisted IP addresses and subnets are supported. Enter one IP address or subnet on each row.
2. The IP address portion of the subnet must be the first IP address on that block.
3. Duplicate IP addresses and IP address segments will be removed.
4. Wildcards are not supported.
5. IPv6 is supported.

Status:

Type: IP address blacklist IP address whitelist

Rule:

Buttons:

6. Switch on **Status** to enable this configuration item.
7. Select a type and enter rules.

Parameter	Description
Type	<ul style="list-style-type: none">● IP address blacklist: If the IP address of a user is included in the IP address blacklist, status code 403 will be returned when the user accesses a CDN PoP.● IP address whitelist: If the IP address of a user is not included in the IP address whitelist, status code 403 will be returned when the user accesses a CDN PoP. NOTE <ul style="list-style-type: none">● Either an IP address blacklist or IP address whitelist can be configured.
Rule	<ul style="list-style-type: none">● Up to 500 IP addresses or subnets are supported. Enter one IP address or subnet on each row.● The IP address portion of the subnet must be the first IP address on that block.● Duplicate IP addresses and IP address segments will be removed.● Wildcards are not supported, for example, 192.168.0.*.● IPv6 is supported. NOTE <p>An IP address segment cannot include an IP address you specify.</p> <ul style="list-style-type: none">● Example: You cannot enter 10.62.53.75 and 10.62.53.0/24 in the same rule.

8. Click **OK**.
9. (Optional) Disable the IP ACL.
 - Switch off **Status** to disable the IP ACL and clear all IP ACL settings. You need to set related parameters when enabling this function again.

Examples

Assume that you have configured the following ACL for domain name **www.example.com**:

Status Enabled

Type IP address blacklist

Rule 192.168.1.1

- A user requests **http://www.example.com/abc.jpg**. The user client IP address 192.168.1.1 is included in the blacklist, so error code 403 is returned.
- A user requests **http://www.example.com/abc.jpg**. The user client IP address 192.168.1.3 is not included in the blacklist, so the requested content is returned.

2.7.4 User-Agent ACL

You can configure a User-Agent access control list (ACL) for your domain name to identify and filter visitors and enhance domain name security.

Background

You can configure a User-Agent blacklist or whitelist to filter requests to your domain name based on the User-Agent field.

- Blacklist: Requests including fields in the blacklist cannot access the content and 403 will be returned.
- Whitelist: Only requests including fields in the whitelist can access the content. Other requests will fail and 403 will be returned.

Precautions

- This function is disabled by default.
- Either a User-Agent blacklist or whitelist can be configured.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab.
5. In the **User-Agent Access Control** area, click **Edit**. The **Configure User-Agent Access Control** dialog box is displayed.

Figure 2-30 Configuring a User-Agent ACL
Configure User-Agent ACL

Status

* Type Blacklist Whitelist

You can configure either a blacklist or whitelist for your domain name.

* Rule

Only wildcard characters (*) can be used for regular expression matching. If no wildcard character is specified, exact matching will be performed. Enter up to 10 rules and enter them on separate rows.

OK Cancel

6. Switch on **Status** to enable this configuration item.
7. Select a type and enter rules.

Parameter	Description
Type	<ul style="list-style-type: none"> • Blacklist: Requests including fields in the blacklist cannot access the content. 403 is returned. • Whitelist: Only requests including fields in the whitelist can access the content. Other requests will fail and 403 will be returned.
Rule	<ul style="list-style-type: none"> • Enter letters, digits, spaces, and the following special characters: <code>*.-_() ;/!@\$^&+=~?''[]</code> • Only wildcard characters (*) can be used for regular expression matching. If no wildcard character is included, exact matching will be used. • Enter up to 100 characters for a rule. • Enter up to 10 rules, and enter them at separate rows.

8. Click **OK**.
9. (Optional) Disable the User-Agent ACL.
 - Switch off **Status** to disable the User-Agent ACL and clear all settings of the blacklist or whitelist. You need to set related parameters when enabling this function again.

Example

Assume that you have configured the following User-Agent blacklist for domain name **www.example.com**:

Status Enabled

Type Blacklist

Rule 

Trident

Chrome

If **User-Agent** in the header of an HTTP request is one of the following:

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
```

Trident or **Chrome** is included in the blacklist, so 403 is returned.

2.7.5 Token Authentication

2.7.5.1 Signing Method A

By default, public resources are distributed by CDN. Token authentication protects these resources from being downloaded and stolen by malicious users. Huawei Cloud CDN provides four URL signing methods. This topic describes the signing method A.

NOTE

- Token authentication is disabled by default.
- If your domain name has special configurations, token authentication cannot be configured for this domain name on the CDN console.
- When token authentication is configured, user requests will include authentication parameters. If **Ignore specific parameters** is not configured:
 - Origin pull will become frequent.
 - If your origin server is an OBS bucket, fees for bucket outbound traffic will incur.

How It Works

An example signed URL looks like:

```
http://DomainName/Filename?auth_key=timestamp-rand-uid-md5hash  
http://DomainName/Filename?auth_key=timestamp-rand-uid-sha256
```

The following table describes the parameters in a signed URL.

Table 2-15 Parameter description

Parameter	Description
DomainName	Acceleration domain name.
timestamp	Time when the authentication server generates a signed URL, that is, the authentication start time. The value is a decimal integer, indicating the total number of seconds that have elapsed since 00:00:00 January 1, 1970.
Validity Period	How long a signed URL remains effective. The value ranges from 0s to 31,536,000s. Example: If the validity period is set to 1,800s, users can access CDN within 1,800s since the time indicated by timestamp . Authentication fails and the URL is inaccessible if users access CDN 1,800s later.
rand	Random number. The recommended value is a UUID, which cannot contain hyphens (-), for example, 202cb962ac59075b964b07152d234b70 .
uid	User ID. This parameter is not used now. You can set it to 0 .
md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of digits (0 to 9) and lowercase letters.
sha256	A string of 64 characters calculated using the SHA256 algorithm. The string consists of digits and lowercase letters.

Parameter	Description
Filename	Back-to-origin URL. Its value must start with a slash (/) and does not include the parameters following the question mark (?).
PrivateKey	Signing key, which is used to generate a signed URL, for example, huaweicloud12345 . Enter 16 to 32 characters. The password can only and must contain both letters and digits.
Authentication Parameter	Authentication parameter carried in a URL. The default value is auth_key .

Verification Method

After receiving a request, a CDN server verifies the request as follows:

1. Checks whether authentication parameters are included in the request. If not, the request is considered invalid and an HTTP 403 error code is returned.
2. Checks whether the current system time is within the range [timestamp, timestamp+valid period]. If the current system time exceeds the range, the CDN server considers that the request expires and returns an HTTP 403 error code. If the current system time is within the range, the next step proceeds.
3. Constructs a character string, calculates **HashValue** with the string using the MD5 and SHA256 algorithm, and compares **HashValue** with the **md5hash** or **sha256** value in the request. If the **md5hash** or **sha256** value is the same as **HashValue**, the authentication is successful and a file is returned. Otherwise, the authentication fails and an HTTP 403 error code is returned. **HashValue** is calculated as follows:

```
sstring = "Filename-Timestamp-rand-uid-PrivateKey"  
HashValue = md5sum(sstring)
```

Or

```
sstring = "Filename-Timestamp-rand-uid-PrivateKey"  
HashValue = sha256sum(sstring)
```

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab and click **Configure** under **Token Authentication**.

Figure 2-31 Configuring token authentication
Configure Token Authentication

Status


Signing Method Method A Method B Method C1 Method C2


Signed URL example:
http://hwcdn.example.com/test/1.jpg?auth_key=1498752000-0-0-40e64d69aac7d15edfc6ec8a080042cb [Learn more](#)

Authentication Scope All files Specific files Specific files excluded

Inheritance M3U8 MPD
Add authentication parameters to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds.

Start Time Same as user request Current time

Signing Key 
Enter 16 to 32 characters, containing letters and digits. [Automatically Generate](#)

Secondary Key 
Enter 16 to 32 characters, containing letters and digits. [Automatically Generate](#)

5. Turn on the **Status** switch.
6. Set the parameters according to the following table and click **OK**.

Table 2-16 Parameter description

Parameter	Description
Signing Method	Select Method A .
Authentication Scope	Files to be authenticated. Select All files , Specific files , or Specific files excluded .

Parameter	Description
Inheritance	<p>Add authentication parameters to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds.</p> <p>NOTE</p> <ul style="list-style-type: none"> • If there are multi-layer M3U8/MPD files, only the first-layer M3U8/MPD files are parsed, and the TS/MP4 streams of M3U8/MPD files in other layers are not expanded. • The standard M3U8 format is supported. M3U8 files are parsed by line. If the parsing fails, responses from the origin server are returned to users. URIs starting with the #EXT-X-MAP tag and URLs/URIs not starting with the pound key (#) are supported. • The standard MPD format is supported. MPD files are parsed by line. If the parsing fails, responses from the origin server are returned to users. The URI between tags <BaseURL> and </BaseURL> is identified. The SegmentTemplate tag is not supported. • If your M3U8/MPD index files contain special characters, CDN does not automatically transcode the characters during authentication calculation. If clients have the logic for automatically transcoding special characters, the access may fail due to the authentication failure. • If the origin server returns resources compressed using gzip or Brotli to CDN PoPs, the authentication inheritance settings become invalid.
Start Time	<ul style="list-style-type: none"> • Same as user request: time when a user accesses the M3U8/MPD file. • Current time: current time of the authentication server.
File Name Extension	<p>Set this parameter when you select Specific files or Specific files excluded for Authentication Scope. Only requests for files with the specified file name extensions are authenticated or not authenticated.</p> <ul style="list-style-type: none"> • Only lowercase letters and digits are supported. Use semicolons (;) to separate multiple file name extensions.
Signing Key	<p>Authentication password. Enter 16 to 32 characters. The password can only and must contain both letters and digits.</p>
Secondary Key	<p>(Optional) Secondary password for authentication. If you want the old and new keys to take effect, you can set the old key as the secondary key. Users can access content only after CDN verifies the primary or secondary key.</p> <ul style="list-style-type: none"> • Enter 16 to 32 characters. The password can only and must contain both letters and digits.
Parameter	<p>Authentication parameter carried in a URL. The default value is auth_key.</p> <ul style="list-style-type: none"> • Enter up to 100 characters. • Enter letters, digits, and underscores (_). Do not start with a digit.

Parameter	Description
Encryption Algorithm	MD5 or SHA256 .
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s.

Authentication Calculator

Using the authentication calculator, you can generate a signed URL for users. Set parameters according to [Table 2-16](#) and [Table 2-17](#), and click **Generate** to generate a signed URL that will expire at a specific time.

NOTE

Escape special characters in the signed URL if any.

Table 2-17 Parameter description

Parameter	Description
Signing Key	Authentication password. Enter 16 to 32 characters. The password can only and must contain both letters and digits. The value must be the same as the signing key specified in the token authentication configuration.
Access Path	Path of the content, which starts with a slash (/) and does not carry a query string.
Encryption Algorithm	MD5 or SHA256 .
Start Time	Time when the signed URL will take effect.
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s. If this value is greater than the validity period set in the token authentication configuration, the latter will be used. Example: If you set this parameter to 2,000s, but the validity period set in the token authentication configuration is 1,800s, the validity period of signed URLs will be 1,800s.

Disabling Token Authentication

Switch off **Status** to disable token authentication and clear all token authentication settings. You need to set related parameters when enabling this function again.

Example

The following uses the MD5 algorithm as an example:

1. Assume the back-to-origin URL is as follows:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`
2. Set **PrivateKey** to **huaweicloud12345**.
3. The authentication takes effect since 00:00:00 on June 30, 2017. **Timestamp** is **1498752000**. Set the validity period to 1,800s.
4. The CDN server constructs a string for calculating **HashValue**.
`/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3-1498752000-0-0-huaweicloud12345`
5. The CDN server calculates **HashValue** according to the signed character string.
`HashValue = md5sum("/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3-1498752000-0-0-huaweicloud12345") =4143ae4a8034c637fd256dfd3542bafc`
6. The request URL is as follows:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3?auth_key=1498752000-0-0-4143ae4a8034c637fd256dfd3542bafc`

If the request is within the validity period (from 00:00:00 on June 30, 2017 to 00:30:00 on June 30, 2017) and the calculated **HashValue** is the same as the **md5hash** value (**4143ae4a8034c637fd256dfd3542bafc**) carried in the request, the authentication is successful.

2.7.5.2 Signing Method B

By default, public resources are distributed by CDN. Token authentication protects these resources from being downloaded and stolen by malicious users. Huawei Cloud CDN provides four URL signing methods. This topic describes the signing method B.

NOTE

- Token authentication is disabled by default.
- If your domain name has special configurations, token authentication cannot be configured for this domain name on the CDN console.
- When token authentication is configured, user requests will include authentication parameters. If **Ignore specific parameters** is not configured:
 - Origin pull will become frequent.
 - If your origin server is an OBS bucket, fees for bucket outbound traffic will incur.

How It Works

An example signed URL looks like:

```
http://DomainName/timestamp/sha256/FileName
```

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

If the authentication is successful, the back-to-origin URL is:

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

The following table describes the parameters in a signed URL.

Table 2-18 Parameter description

Parameter	Description
DomainName	Acceleration domain name.
timestamp	Time when the authentication server generates a signed URL, that is, the authentication start time. The UTC+08:00 time of the authentication server is used. The format is YYYYMMDDHHMMSS, for example, 20170630100000.
Validity Period	How long a signed URL remains effective. The value ranges from 0s to 31,536,000s. Example: If the validity period is set to 1,800s and timestamp is 201706301000 , the URL expires at 10:30:00 a.m. on June 30, 2017.
md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of digits (0 to 9) and lowercase letters.
sha256	A string of 64 characters calculated using the SHA256 algorithm. The string consists of digits and lowercase letters.
Filename	Back-to-origin URL. Its value must start with a slash (/) and does not include the parameters following the question mark (?).
PrivateKey	Signing key, which is used to generate a signed URL, for example, huaweicloud12345 . Enter 16 to 32 characters. The password can only and must contain both letters and digits.

Verification Method

After receiving a request, a CDN server verifies the request as follows:

1. Checks whether authentication parameters are included in the request. If not, the request is considered invalid and an HTTP 403 error code is returned.
2. Checks whether the current system time is within the range [timestamp, timestamp+valid period]. If the current system time exceeds the range, the CDN server considers that the request expires and returns an HTTP 403 error code. If the current system time is within the range, the next step proceeds.
3. Constructs a character string, calculates **HashValue** with the string using the MD5 and SHA256 algorithm, and compares **HashValue** with the **md5hash** or **sha256** value in the request. If the **md5hash** or **sha256** value is the same as **HashValue**, the authentication is successful and a file is returned. Otherwise, the authentication fails and an HTTP 403 error code is returned. **HashValue** is calculated as follows:

```
sstring = "PrivateKeytimestampFilename"  
HashValue = sha256sum(sstring)
```

Or

```
sstring = "PrivateKeytimestampFilename"  
HashValue = md5sum(sstring)
```

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab and click **Configure** under **Token Authentication**.

Figure 2-32 Configuring token authentication
Configure Token Authentication

Status

Signing Method Method A Method B Method C1 Method C2

Signed URL example:
http://hwcdn.example.com/test/1.jpg?auth_key=1498752000-0-0-40e64d69aac7d15edfc6ec8a080042cb [Learn more](#)

Authentication Scope All files Specific files Specific files excluded

Inheritance M3U8 MPD

Add authentication parameters to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds.

Start Time Same as user request Current time

Signing Key [Automatically Generate](#)

Secondary Key [Automatically Generate](#)

Parameters

OK Cancel

5. Turn on the **Status** switch.
6. Set the parameters according to the following table and click **OK**.

Table 2-19 Parameter description

Parameter	Description
Signing Method	Select Method B .
Authentication Scope	Files to be authenticated. Select All files , Specific files , or Specific files excluded .

Parameter	Description
Inheritance	<p>Add authentication parameters to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds.</p> <p>NOTE</p> <ul style="list-style-type: none"> • If there are multi-layer M3U8/MPD files, only the first-layer M3U8/MPD files are parsed, and the TS/MP4 streams of M3U8/MPD files in other layers are not expanded. • The standard M3U8 format is supported. M3U8 files are parsed by line. If the parsing fails, responses from the origin server are returned to users. URIs starting with the #EXT-X-MAP tag and URLs/URIs not starting with the pound key (#) are supported. • The standard MPD format is supported. MPD files are parsed by line. If the parsing fails, responses from the origin server are returned to users. The URI between tags <BaseURL> and </BaseURL> is identified. The SegmentTemplate tag is not supported. • If your M3U8/MPD index files contain special characters, CDN does not automatically transcode the characters during authentication calculation. If clients have the logic for automatically transcoding special characters, the access may fail due to the authentication failure. • If the origin server returns resources compressed using gzip or Brotli to CDN PoPs, the authentication inheritance settings become invalid.
Start Time	<ul style="list-style-type: none"> • Same as user request: time when a user accesses the M3U8/MPD file. • Current time: current time of the authentication server.
File Name Extension	<p>Set this parameter when you select Specific files or Specific files excluded for Authentication Scope. Only requests for files with the specified file name extensions are authenticated or not authenticated.</p> <ul style="list-style-type: none"> • Only lowercase letters and digits are supported. Use semicolons (;) to separate multiple file name extensions.
Signing Key	<p>Authentication password. Enter 16 to 32 characters. The password can only and must contain both letters and digits.</p>
Secondary Key	<p>(Optional) Secondary password for authentication. If you want the old and new keys to take effect, you can set the old key as the secondary key. Users can access content only after CDN verifies the primary or secondary key.</p> <ul style="list-style-type: none"> • Enter 16 to 32 characters. The password can only and must contain both letters and digits.
Encryption Algorithm	<p>MD5 or SHA256.</p>
Validity Period	<p>How long a signed URL remains effective. The value ranges from 0s to 31,536,000s.</p>

Authentication Calculator

Using the authentication calculator, you can generate a signed URL for users. Set parameters according to [Table 2-19](#) and [Table 2-20](#), and click **Generate** to generate a signed URL that will expire at a specific time.

Table 2-20 Parameter description

Parameter	Description
Signing Key	Authentication password. Enter 16 to 32 characters. The password can only and must contain both letters and digits. The value must be the same as the signing key specified in the token authentication configuration.
Access Path	Path of the content, which starts with a slash (/) and does not carry a query string.
Encryption Algorithm	MD5 or SHA256 .
Start Time	Time when the signed URL will take effect.
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s. If this value is greater than the validity period set in the token authentication configuration, the latter will be used. Example: If you set this parameter to 2,000s, but the validity period set in the token authentication configuration is 1,800s, the validity period of signed URLs will be 1,800s.

NOTE

Escape special characters in the signed URL if any.

Disabling Token Authentication

Switch off **Status** to disable token authentication and clear all token authentication settings. You need to set related parameters when enabling this function again.

Example

The following uses the MD5 algorithm as an example:

1. Assume that the back-to-origin URL is as follows:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`
2. Set **PrivateKey** to **huaweicloud12345**.
3. **timestamp** is **201706301000**.
4. The CDN server constructs a string for calculating **md5hash**.
`huaweicloud12345201706301000/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`
5. The CDN server calculates **md5hash** according to the signed character string.


```
md5hash = md5sum("huaweicloud12345201706301000/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3")  
=668f28d134ec6446a8ae83a43d0a554b
```

6. The request URL is:

```
http://hwcdn.example.com/201706301000/668f28d134ec6446a8ae83a43d0a554b/T128_2_1_0_sdk/  
0210/M00/82/3E/test.mp3
```

If the request is within the validity period (from 10:00:00 on June 30, 2017 to 10:30:00 on June 30, 2017) and the calculated **md5hash** is the same as the **md5hash** value (**668f28d134ec6446a8ae83a43d0a554b**) carried in the request, the authentication is successful.

2.7.5.3 Signing Method C1

By default, public resources are distributed by CDN. Token authentication protects these resources from being downloaded and stolen by malicious users. Huawei Cloud CDN provides four URL signing methods. This topic describes the signing method C1.

NOTE

- Token authentication is disabled by default.
- If your domain name has special configurations, token authentication cannot be configured for this domain name on the CDN console.
- When token authentication is configured, user requests will include authentication parameters. If **Ignore specific parameters** is not configured:
 - Origin pull will become frequent.
 - If your origin server is an OBS bucket, fees for bucket outbound traffic will incur.

How It Works

An example signed URL looks like:

```
http://DomainName/{<sha256>/<timestamp>}/FileName  
http://DomainName/{<md5hash>/<timestamp>}/FileName
```

The following table describes the parameters in a signed URL.

Table 2-21 Parameter description

Parameter	Description
DomainName	Acceleration domain name.
timestamp	Time when the authentication server generates a signed URL, that is, the authentication start time. The value is a hexadecimal integer, indicating the total number of seconds that have elapsed since 00:00:00 January 1, 1970.
Validity Period	How long a signed URL remains effective. The value ranges from 0s to 31,536,000s. Example: If the validity period is set to 1,800s, users can access CDN within 1,800s since the time indicated by timestamp . Authentication fails and the URL is inaccessible if users access CDN 1,800s later.

Parameter	Description
md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of digits (0 to 9) and lowercase letters.
sha256	A string of 64 characters calculated using the SHA256 algorithm. The string consists of digits and lowercase letters.
Filename	Back-to-origin URL. Its value must start with a slash (/) and does not include the parameters following the question mark (?).
PrivateKey	Signing key, which is used to generate a signed URL, for example, huaweicloud12345 . Enter 16 to 32 characters. The password can only and must contain both letters and digits.

Verification Method

After receiving a request, a CDN server verifies the request as follows:

1. Checks whether authentication parameters are included in the request. If not, the request is considered invalid and an HTTP 403 error code is returned.
2. Checks whether the current system time is within the range [timestamp, timestamp+valid period]. If the current system time exceeds the range, the CDN server considers that the request expires and returns an HTTP 403 error code. If the current system time is within the range, the next step proceeds.
3. Constructs a character string, calculates **HashValue** with the string using the MD5 and SHA256 algorithm, and compares **HashValue** with the **md5hash** or **sha256** value in the request. If the **md5hash** or **sha256** value is the same as **HashValue**, the authentication is successful and a file is returned. Otherwise, the authentication fails and an HTTP 403 error code is returned. **HashValue** is calculated as follows:

```
sstring = "PrivateKeyFilenameTimestamp"  
HashValue = md5sum(sstring)
```

Or

```
sstring = "PrivateKeyFilenameTimestamp"  
HashValue = sha256sum(sstring)
```

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab and click **Configure** under **Token Authentication**.

Figure 2-33 Configuring token authentication
Configure Token Authentication

Status

Signing Method Method A Method B Method C1 Method C2

Signed URL example:
http://hwcdn.example.com/test/1.jpg?auth_key=1498752000-0-0-40e64d69aac7d15edfc6ec8a080042cb [Learn more](#)

Authentication Scope All files Specific files Specific files excluded

Inheritance M3U8 MPD

Add authentication parameters to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds.

Start Time Same as user request Current time

Signing Key

Enter 16 to 32 characters, containing letters and digits. [Automatically Generate](#)

Secondary Key

Enter 16 to 32 characters, containing letters and digits. [Automatically Generate](#)

- Turn on the **Status** switch.
- Set the parameters according to the following table and click **OK**.

Table 2-22 Parameter description

Parameter	Description
Signing Method	Select Method C1 .
Authentication Scope	Files to be authenticated. Select All files , Specific files , or Specific files excluded .

Parameter	Description
Inheritance	<p>Add authentication parameters to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds.</p> <p>NOTE</p> <ul style="list-style-type: none">• If there are multi-layer M3U8/MPD files, only the first-layer M3U8/MPD files are parsed, and the TS/MP4 streams of M3U8/MPD files in other layers are not expanded.• The standard M3U8 format is supported. M3U8 files are parsed by line. If the parsing fails, responses from the origin server are returned to users. URIs starting with the #EXT-X-MAP tag and URLs/URIs not starting with the pound key (#) are supported.• The standard MPD format is supported. MPD files are parsed by line. If the parsing fails, responses from the origin server are returned to users. The URI between tags <BaseURL> and </BaseURL> is identified. The SegmentTemplate tag is not supported.• If your M3U8/MPD index files contain special characters, CDN does not automatically transcode the characters during authentication calculation. If clients have the logic for automatically transcoding special characters, the access may fail due to the authentication failure.• If the origin server returns resources compressed using gzip or Brotli to CDN PoPs, the authentication inheritance settings become invalid.
Start Time	<ul style="list-style-type: none">• Same as user request: time when a user accesses the M3U8/MPD file.• Current time: current time of the authentication server.
File Name Extension	<p>Set this parameter when you select Specific files or Specific files excluded for Authentication Scope. Only requests for files with the specified file name extensions are authenticated or not authenticated.</p> <ul style="list-style-type: none">• Only lowercase letters and digits are supported. Use semicolons (;) to separate multiple file name extensions.
Signing Key	Authentication password. Enter 16 to 32 characters. The password can only and must contain both letters and digits.
Secondary Key	<p>(Optional) Secondary password for authentication. If you want the old and new keys to take effect, you can set the old key as the secondary key. Users can access content only after CDN verifies the primary or secondary key.</p> <ul style="list-style-type: none">• Enter 16 to 32 characters. The password can only and must contain both letters and digits.
Encryption Algorithm	MD5 or SHA256 .
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s.

Authentication Calculator

Using the authentication calculator, you can generate a signed URL for users. Set parameters according to [Table 2-22](#) and [Table 2-23](#), and click **Generate** to generate a signed URL that will expire at a specific time.

NOTE

Escape special characters in the signed URL if any.

Table 2-23 Parameter description

Parameter	Description
Signing Key	Authentication password. Enter 16 to 32 characters. The password can only and must contain both letters and digits. The value must be the same as the signing key specified in the token authentication configuration.
Access Path	Path of the content, which starts with a slash (/) and does not carry a query string.
Encryption Algorithm	MD5 or SHA256 .
Start Time	Time when the signed URL will take effect.
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s. If this value is greater than the validity period set in the token authentication configuration, the latter will be used. Example: If you set this parameter to 2,000s, but the validity period set in the token authentication configuration is 1,800s, the validity period of signed URLs will be 1,800s.

Disabling Token Authentication

Switch off **Status** to disable token authentication and clear all token authentication settings. You need to set related parameters when enabling this function again.

Example

The following uses the MD5 algorithm as an example:

1. Assume that the back-to-origin URL is as follows:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`
2. Set **PrivateKey** to **huaweicloud12345**.
3. The authentication takes effect since 10:00:00 on June 30, 2017. **Timestamp** is **5955b0a0**. Set the validity period to 1,800s.
4. The CDN server constructs a string for calculating **md5hash**.
`huaweicloud12345/T128_2_1_0_sdk/0210/M00/82/3E/test.mp35955b0a0`
5. The CDN server calculates **md5hash** according to the signed character string.
`md5hash = md5sum(huaweicloud12345/T128_2_1_0_sdk/0210/M00/82/3E/test.mp35955b0a0) = 8540f43a2416fd4a432fe4f92d2ea089`

6. The request URL is:
`http://hwcdn.example.com/8540f43a2416fd4a432fe4f92d2ea089/5955b0a0/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`

If the request is within the validity period (from 10:00:00 on June 30, 2017 to 10:30:00 on June 30, 2017) and the calculated **md5hash** is the same as the **md5hash** value (**8540f43a2416fd4a432fe4f92d2ea089**) carried in the request, the authentication is successful.

2.7.5.4 Signing Method C2

By default, public resources are distributed by CDN. Token authentication protects these resources from being downloaded and stolen by malicious users. Huawei Cloud CDN provides four URL signing methods. This topic describes the signing method C2.

NOTE

- Token authentication is disabled by default.
- If your domain name has special configurations, token authentication cannot be configured for this domain name on the CDN console.
- When token authentication is configured, user requests will include authentication parameters. If **Ignore specific parameters** is not configured:
 - Origin pull will become frequent.
 - If your origin server is an OBS bucket, fees for bucket outbound traffic will incur.

How It Works

An example signed URL looks like:

```
http://DomainName/FileName?auth_key=<sha256>&timestamp=<timestamp>  
http://DomainName/FileName?auth_key=<md5hash>&timestamp=<timestamp>
```

The following table describes the parameters in a signed URL.

Table 2-24 Parameter description

Parameter	Description
DomainName	Acceleration domain name.
timestamp	Time when the authentication server generates a signed URL, that is, the authentication start time. The value is the total number of seconds that have elapsed since 00:00:00 January 1, 1970. It is a decimal or hexadecimal integer.
Validity Period	How long a signed URL remains effective. The value ranges from 0s to 31,536,000s. Example: If the validity period is set to 1,800s, users can access CDN within 1,800s since the time indicated by timestamp . Authentication fails and the URL is inaccessible if users access CDN 1,800s later.
md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of digits (0 to 9) and lowercase letters.

Parameter	Description
sha256	A string of 64 characters calculated using the SHA256 algorithm. The string consists of digits and lowercase letters.
Filename	Back-to-origin URL. Its value must start with a slash (/) and does not include the parameters following the question mark (?).
PrivateKey	Signing key, which is used to generate a signed URL, for example, huaweicloud12345 . Enter 16 to 32 characters. The password can only and must contain both letters and digits.
Authentication Parameter	Authentication parameter carried in a URL. The default value is auth_key .
Timestamp	Timestamp parameter name carried in the request URL.

Verification Method

After receiving a request, a CDN server verifies the request as follows:

1. Checks whether authentication parameters are included in the request. If not, the request is considered invalid and an HTTP 403 error code is returned.
2. Checks whether the current system time is within the range [timestamp, timestamp+valid period]. If the current system time exceeds the range, the CDN server considers that the request expires and returns an HTTP 403 error code. If the current system time is within the range, the next step proceeds.
3. Constructs a character string, calculates **HashValue** with the string using the MD5 and SHA256 algorithm, and compares **HashValue** with the **md5hash** or **sha256** value in the request. If the **md5hash** or **sha256** value is the same as **HashValue**, the authentication is successful and a file is returned. Otherwise, the authentication fails and an HTTP 403 error code is returned. **HashValue** is calculated as follows:

```
sstring = "PrivateKeyFilenameTimestamp"  
HashValue = md5sum(sstring)
```

Or

```
sstring = "PrivateKeyFilenameTimestamp"  
HashValue = sha256sum(sstring)
```

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab and click **Configure** under **Token Authentication**.

Figure 2-34 Configuring token authentication
Configure Token Authentication

Status


Signing Method Method A Method B Method C1 Method C2


Signed URL example:
http://hwcdn.example.com/test/1.jpg?auth_key=1498752000-0-0-40e64d69aac7d15edfc6ec8a080042cb [Learn more](#)

Authentication Scope All files Specific files Specific files excluded

Inheritance M3U8 MPD
Add authentication parameters to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds.

Start Time Same as user request Current time

Signing Key 
Enter 16 to 32 characters, containing letters and digits. [Automatically Generate](#)

Secondary Key 
Enter 16 to 32 characters, containing letters and digits. [Automatically Generate](#)

5. Turn on the **Status** switch.
6. Set the parameters according to the following table and click **OK**.

Table 2-25 Parameter description

Parameter	Description
Signing Method	Select Method C2 .
Authentication Scope	Files to be authenticated. Select All files , Specific files , or Specific files excluded .

Parameter	Description
Inheritance	<p>Add authentication parameters to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds.</p> <p>NOTE</p> <ul style="list-style-type: none">• If there are multi-layer M3U8/MPD files, only the first-layer M3U8/MPD files are parsed, and the TS/MP4 streams of M3U8/MPD files in other layers are not expanded.• The standard M3U8 format is supported. M3U8 files are parsed by line. If the parsing fails, responses from the origin server are returned to users. URIs starting with the #EXT-X-MAP tag and URLs/URIs not starting with the pound key (#) are supported.• The standard MPD format is supported. MPD files are parsed by line. If the parsing fails, responses from the origin server are returned to users. The URI between tags <BaseURL> and </BaseURL> is identified. The SegmentTemplate tag is not supported.• If your M3U8/MPD index files contain special characters, CDN does not automatically transcode the characters during authentication calculation. If clients have the logic for automatically transcoding special characters, the access may fail due to the authentication failure.• If the origin server returns resources compressed using gzip or Brotli to CDN PoPs, the authentication inheritance settings become invalid.
Start Time	<ul style="list-style-type: none">• Same as user request: time when a user accesses the M3U8/MPD file.• Current time: current time of the authentication server.
File Name Extension	<p>Set this parameter when you select Specific files or Specific files excluded for Authentication Scope. Only requests for files with the specified file name extensions are authenticated or not authenticated.</p> <ul style="list-style-type: none">• Only lowercase letters and digits are supported. Use semicolons (;) to separate multiple file name extensions.
Signing Key	Authentication password. Enter 16 to 32 characters. The password can only and must contain both letters and digits.
Secondary Key	<p>(Optional) Secondary password for authentication. If you want the old and new keys to take effect, you can set the old key as the secondary key. Users can access content only after CDN verifies the primary or secondary key.</p> <ul style="list-style-type: none">• Enter 16 to 32 characters. The password can only and must contain both letters and digits.
Parameter	<p>Authentication parameter carried in a URL. The default value is auth_key.</p> <ul style="list-style-type: none">• Enter up to 100 characters.• Enter letters, digits, and underscores (_). Do not start with a digit.

Parameter	Description
Time Format	Format of the time in the signed URL.
Encryption Algorithm	MD5 or SHA256 .
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s.

Authentication Calculator

Using the authentication calculator, you can generate a signed URL for users. Set parameters according to [Table 2-25](#) and [Table 2-26](#), and click **Generate** to generate a signed URL that will expire at a specific time.

NOTE

Escape special characters in the signed URL if any.

Table 2-26 Parameter description

Parameter	Description
Signing Key	Authentication password. Enter 16 to 32 characters. The password can only and must contain both letters and digits. The value must be the same as the signing key specified in the token authentication configuration.
Access Path	Path of the content, which starts with a slash (/) and does not carry a query string.
Encryption Algorithm	MD5 or SHA256 .
Start Time	Time when the signed URL will take effect.
Time Format	Format of the time in the signed URL. Time format of the signed URL, which must be the same as that specified in the URL signing configuration.
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s. If this value is greater than the validity period set in the token authentication configuration, the latter will be used. Example: If you set this parameter to 2,000s, but the validity period set in the token authentication configuration is 1,800s, the validity period of signed URLs will be 1,800s.

Disabling Token Authentication

Switch off **Status** to disable token authentication and clear all token authentication settings. You need to set related parameters when enabling this function again.

Example

The following uses the MD5 algorithm as an example:

1. Assume that the back-to-origin URL is as follows:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`
2. Set **PrivateKey** to **huaweicloud12345**.
3. The authentication takes effect since 10:00:00 on June 30, 2017. **Timestamp** is **5955b0a0**. Set the validity period to 1,800s.
4. The CDN server constructs a string for calculating **md5hash**.
`huaweicloud12345/T128_2_1_0_sdk/0210/M00/82/3E/test.mp35955b0a0`
5. The CDN server calculates **md5hash** according to the signed character string.
`md5hash = md5sum(huaweicloud12345/T128_2_1_0_sdk/0210/M00/82/3E/test.mp35955b0a0) = 8540f43a2416fd4a432fe4f92d2ea089`
6. The request URL is:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3?auth_key=8540f43a2416fd4a432fe4f92d2ea089×tamp=5955b0a0`

If the request is within the validity period (from 10:00:00 on June 30, 2017 to 10:30:00 on June 30, 2017) and the calculated **md5hash** is the same as the **md5hash** value (**8540f43a2416fd4a432fe4f92d2ea089**) carried in the request, the authentication is successful.

2.7.6 Remote Authentication

Huawei Cloud CDN supports remote authentication. When a user requests a resource from a CDN PoP, CDN forwards the user request to a specific authentication server and determines whether to return the resource to the user based on the result returned by the authentication server.

Background

Remote authentication is similar to token authentication. Differences are as follows:

- Token authentication: Authentication is performed by CDN PoPs.
- Remote authentication: CDN PoPs forward user requests to a specific authentication server for authentication.

The remote authentication process is as follows.

Figure 2-35 Remote authentication process

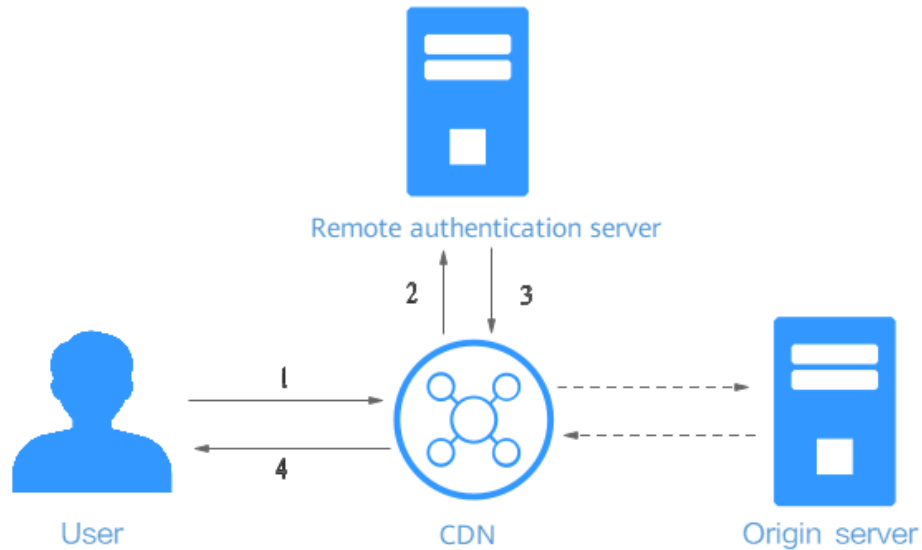


Table 2-27 Process description

Step	Description
1	A user carries authentication parameters to access a CDN PoP.
2	CDN forwards the request to a remote authentication server.
3	The remote authentication server verifies the request and returns a status code to the CDN PoP.
4	The CDN PoP determines whether to return the requested resource to the user based on the received status code.

Precautions

- Remote authentication is disabled by default.

Procedure

- Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
- In the navigation pane, choose **Domains**.
- In the domain list, click the target domain name or click **Configure** in the **Operation** column.
- Click the **Access Control** tab and click **Remote Authentication**.

Figure 2-36 Configuring remote authentication

Configure Remote Authentication

Status

* Authentication Server Address

* Request Method GET POST HEAD

* File Type All Specific file types

URL Parameters

* Parameters to Retain All Specific None

Custom URL Parameters	Type	Parameter	Value	Operation
+ Add				

Header Parameters

* Request Headers to Retain All Specific None

Table 2-28 Parameter description

Parameter	Description	Example
Authentication Server Address	<p>IP address of a reachable server.</p> <ul style="list-style-type: none"> The address must include http:// or https://. The address cannot be a local address such as localhost or 127.0.0.1. The address cannot be an acceleration domain name added on CDN. The default ports of the remote authentication server are 80 and 443. To change them, submit a service ticket. 	https:// example.com/auth
Request Method	Request method supported by the authentication server. GET, POST, and HEAD are supported.	GET

Parameter	Description	Example
File Type	<ul style="list-style-type: none"> • All: Requests for all files are authenticated. • Specific file types: Requests for files of specified types are authenticated. Separate types by vertical bars (), for example, jpg MP4. <ul style="list-style-type: none"> - Enter up to 512 characters, including letters and digits. • File types are case insensitive. For example, jpg and JPG indicate the same file type. 	All
Parameters to Retain	<p>Parameters that need to be authenticated in user requests. You can retain or ignore all URL parameters or retain specific URL parameters.</p> <ul style="list-style-type: none"> • Parameters are case insensitive. Use vertical bars () to separate them. 	All
Custom URL Parameters	<p>Parameters to be added when CDN PoPs forward user requests to the remote authentication server. You can select preset parameters or customize parameters (parameters and values are case insensitive).</p> <ul style="list-style-type: none"> • Customize a parameter, which does not support variables. • Select a preset or customized parameter, which supports variables. 	Select http_host . Value: \$http_host .
Request Headers to Retain	<p>Headers to be authenticated in user requests. You can retain or ignore all request headers or retain specific request headers.</p> <p>Headers are case insensitive. Use vertical bars () to separate them.</p>	All

Parameter	Description	Example
Custom Request Header Parameters	<p>Request headers to be added when CDN PoPs forward user requests to the remote authentication server. You can select preset request headers or customize request headers (headers and values are case insensitive).</p> <ul style="list-style-type: none">• Customize a parameter, which does not support variables.• Select a preset or customized parameter, which supports preset variables.	<p>Select http_referer. Value: \$http_referer.</p>
Success Status Code	<p>Status code returned by the remote authentication server to CDN PoPs when authentication is successful.</p> <ul style="list-style-type: none">• Value range: 2xx and 3xx.	200
Failure Status Code	<p>Status code returned by the remote authentication server to CDN PoPs when authentication fails.</p> <ul style="list-style-type: none">• Value range: 4xx and 5xx.	403
Custom Response Status Code	<p>Status code returned by CDN PoPs to users when authentication fails.</p> <ul style="list-style-type: none">• Value range: 2xx, 3xx, 4xx, and 5xx.	403
Timeout Interval	<p>Duration from the time when a CDN PoP forwards an authentication request to the time when the CDN PoP receives the result returned by the remote authentication server. Enter 0 or a value ranging from 50 to 3,000. The unit is millisecond.</p>	60
Action After Timeout	<p>How CDN PoPs process a user request after authentication times out.</p> <ul style="list-style-type: none">• Accept: The user request will be accepted and the requested resource will be returned.• Reject: The user request will be rejected and the configured custom response status code will be returned.	Reject

Table 2-29 Preset parameters

Variable	Description	Remarks
\$http_host	Host value in the request header.	These values can be obtained only when client requests carry them.
\$http_user_agent	User-Agent value in the request header.	
\$http_referer	Referer value in the request header.	
\$http_x_forwarded_for	X-Forwarded-For value in the request header.	
\$http_content_type	Content-Type value in the request header.	
\$remote_addr	IP address of the client.	-
\$scheme	Protocol type of the request.	-
\$server_protocol	Protocol version of the request.	-
\$request_uri	Content of uri + ? + args	-
\$uri	Original URI of the request.	-
\$args	Query string of the request, excluding the question mark (?).	-
\$request_method	Request method.	-

5. Configure parameters as prompted and click **OK**.
6. (Optional) Disable remote authentication.
 - Switch off **Status** to disable remote authentication and clear all remote authentication settings. You need to set related parameters when enabling this function again.

2.7.7 IP Access Frequency

You can restrict the number of times that a single IP address requests a URL from a PoP per second to defend against CC attacks and malicious theft.

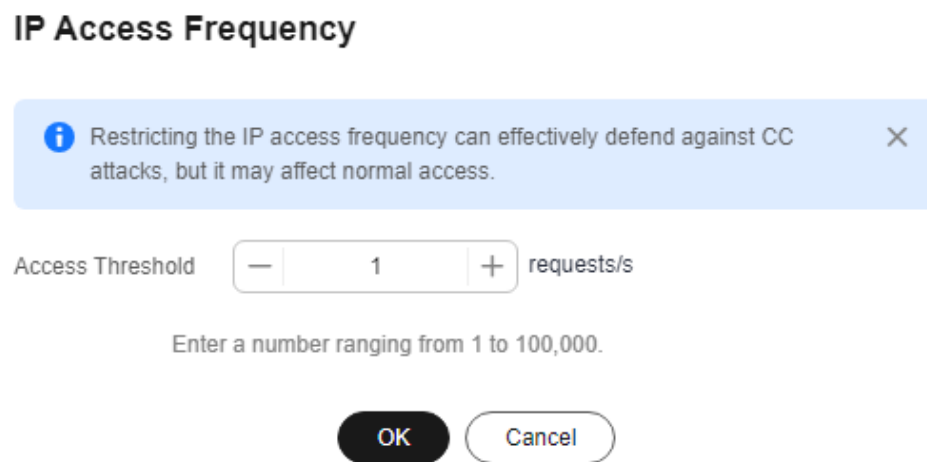
Precautions

- Restricting the IP access frequency can effectively defend against CC attacks, but it may affect normal access.
- When the threshold is reached, CDN returns status code 403. The restriction is removed 10 minutes later.
- By default, this function is disabled.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab and turn on the **IP Access Frequency** switch.

Figure 2-37 IP access frequency



5. Set **Access Threshold** and click **OK**.
 - When the number of times that a single IP address accesses a single URL via a PoP per second reaches the threshold, CDN returns status code 403 to the client. The restriction is removed 10 minutes later.
 - If you change **Access Threshold** within the restriction duration, the change takes effect after the restriction is removed.
6. Turn off the **IP Access Frequency** switch to disable it.

Example

Configuration: You have restricted the IP access frequency of domain name [www.example.com](#) to 10,000 times/second.

Condition for triggering IP access frequency restriction: The number of times that an IP address requests a URL from a PoP per second reaches 10,000.

Example: A client's IP address is 0.0.0.0. This client accesses <https://www.example.com/abc.jpg> for 10,000 times within 1 second, triggering the access frequency restriction. When the client accesses this URL again, the request is blocked and status code 403 is returned. The restriction is removed 10 minutes later.

2.8 Advanced Settings

2.8.1 HTTP Header Settings (Cross-origin Requests)

HTTP headers are part of an HTTP request or response message that define the operating parameters of an HTTP transaction.


Cross-origin resource sharing (CORS) is a mechanism that allows cross-origin access. When website A accesses resources on website B, a cross-origin request is sent. If website B does not allow website A to access the resources, a cross-domain problem occurs. In this case, you can configure HTTP header settings and add custom headers in response messages returned to the requester to implement functions such as CORS.

Precautions

- Some headers cannot be set or deleted. For details, see [Constraints](#).
- You can add up to 10 HTTP response header configurations.
- HTTP header configuration is domain name-specific. When the configuration takes effect, the specified headers will be added to or removed from response messages for any resources under the entire domain. However, HTTP header configuration only affects the response behavior of the clients (browsers). They do not affect the cache behavior of CDN PoPs.

Supported Response Headers

Huawei Cloud CDN lets you customize the following different HTTP response headers:

- **Content-Disposition**
The Content-Disposition header can start a download on the client side and specify the name of the file to be downloaded.
When a server sends a file to a browser, as long as the file format is supported (for instance TXT or JPG), the file is opened using the browser by default. If the file needs to be treated as an attachment and saved with a specific file name, you can use the Content-Disposition header field to specify this requirement.
- **Content-Language**
The Content-Language header specifies the preferred language or language combination of the browser. Content can be customized for different users.
- **Access-Control-Allow-Origin**
The Access-Control-Allow-Origin header carries the domain names that are allowed for CORS after server authentication. For a simple CORS request, the browser determines whether to return the requested resource content to the client based on this message header. For a pre-check request, the browser determines whether to initiate an actual CORS request to the server based on this message header.
 **NOTE**
To prevent cross-domain errors caused by browser cache, clear browser cache after configuring Access-Control-Allow-Origin.
- **Access-Control-Allow-Methods**
The Access-Control-Allow-Methods header carries the methods that are allowed for CORS after server authentication. For a simple CORS request, the

browser determines whether to return the requested resource content to the client based on this message header. For a pre-check request, the browser determines whether to initiate an actual CORS request to the server based on this message header.

- **Access-Control-Max-Age**

The Access-Control-Max-Age header determines how long the pre-check results for CORS requests allowed by the server can be cached. The browser determines the TTL for pre-check request results based on this message header. As long as the period defined by this header has not expired, the browser can determine whether to initiate a CORS request to the server based on the results. Once this period expires, the browser needs to send another pre-check request to the server.

- **Access-Control-Expose-Headers**

Access-Control-Expose-Headers specify the response headers that the browser can expose to the client. You can use this field to define the response headers visible to the client. The following response headers are visible to the client by default: Cache-Control, Content-Language, Content-Type, Expires, Last-Modified, and Pragma.

- **Custom**

If the preceding response headers cannot meet your needs, you can create response headers. A custom response header can contain 1 to 100 characters, starting with a letter and consisting of letters, digits, and hyphens (-).

Procedure

1. Log in to the [Huawei Cloud console](#).
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Advanced Settings** tab.
5. In the **HTTP Headers** area, click **Edit**. The **Configure HTTP Headers** dialog box is displayed.

Figure 2-38 Configuring HTTP headers

Configure HTTP Headers

After HTTP header configuration takes effect, all responses for content under this domain name will include the configured message headers.

Response Head...	Parameter	Value	Operation
+ Add			
OK Cancel			

6. Click **Add** and select a response header operation from the drop-down list.

Response Header Operation	Description
Set	<ul style="list-style-type: none"> • If the header already exists in the response, the header value you configure will overwrite the original one. • If the header does not exist in the response, the header will be added to the response.
Delete	The header will be deleted from the response.

7. Set the header parameter and value.

Parameter	Description	Example Value
Content-disposition	<p>Starts a download on the client side and specifies the name of the file to be downloaded.</p> <p>Value requirements: For a typical configuration, see the example on the right.</p>	attachment;filename=FileName.xls
Content-Language	<p>Specifies the language of the response page of the client.</p> <p>Value requirements: For a typical configuration, see the example on the right.</p>	zh-CN en-US

Parameter	Description	Example Value
Access-Control-Allow-Origin	<p>Specifies the foreign domain URLs (request sources) that are allowed to access the resource in cross-origin resource sharing (CORS).</p> <p>Value requirements:</p> <ul style="list-style-type: none"> • Enter a URL or up to 66 URLs. • Wildcard domain names are supported. • Enter up to 1,000 characters. • Separate URLs with commas (,). • Start with http:// or https://. • If this is set to *, no URLs are allowed after the wildcard (*). • Domain names with port numbers are supported. • The value can be null, which is case-insensitive. 	<p>Example 1: https:// www.example.com</p> <p>Example 2: *</p> <p>Example 3: https:// www.example.com, https:// www.example01.co m,https://*.abc.com</p>
Access-Control-Allow-Methods	<p>Specifies the HTTP request methods that can be used in a CORS request.</p> <p>Value requirements: Multiple methods can be configured at the same time. Separate them with commas (,).</p>	GET,POST,HEAD
Access-Control-Max-Age	<p>Specifies how long to cache the pre-check results of CORS requests on specific resources.</p> <p>Value requirements: This value is expressed in seconds and ranges from 0 to 1,000,000,000.</p>	86400

Parameter	Description	Example Value
Access-Control-Expose-Headers	<p>Specifies the response header information visible to the client for a CORS request.</p> <p>Value requirements: Enter 1 to 256 characters. Multiple headers can be configured at the same time. Separate them by commas (,).</p>	Content-Length,Content-Encoding
Access-control-allow-headers	<p>Specifies the fields that can be carried in a cross-domain request.</p> <p>Value requirements: Enter 1 to 1,000 characters. Multiple fields can be configured at the same time. Separate them by commas (,).</p>	X- Custom-Header
Custom	<p>Specifies the custom response header for a CORS request.</p> <p>Value requirements: Enter 1 to 1,000 characters, which can contain letters, digits, spaces, and the following special characters: .-_*#!&+ ^~"/;,:=@?<></p> <p>NOTE</p> <ul style="list-style-type: none"> If the custom parameter is Cache-Control, the value can be public, private, no-cache, no-store, no-transform, only-if-cached, proxy-revalidate, must-revalidate, immutable, max-age=***, stale-while-revalidate=***, s-maxage=***, stale-if-error=***, or min-fresh=*** (***) is a number). Multiple values are separated by commas (,). The value of the Cache-Control header may affect the PoP cache. 	x-testcdn

8. Click **OK**.

Constraints

- If your domain name has special configurations, **Content-Type**, **Expires**, or **Cache-Control** cannot be configured.
- The following response headers can be modified but cannot be deleted.

Content-Base	Content-Disposition
Server	Content-Language
Cache-Control	Expires
Content-Type	-

- CDN does not support the following response headers:

A_Dynamic	If-None-Match	Sec-WebSocket-Origin	X-Forward-Peer
Accept-Ranges	If-Range	Sec-WebSocket-Protocol	X-Forward-Type
X-Forward-Ip	Keep-Alive	Sec-WebSocket-Version	X-Forward-Uri
Allow	Key	Set-Cookie	X-Forwarded-For
Authentication-Info	Last-Modified	Tcp-Retrans	X-IP-Region
Authorization	Link	Title	X-IP-Region-CN
X-Forward-Measured	Location	Transfer-Encoding	X-Ip-Blackwhite-List
Cdn-Qos	Max-Forwards	Upgrade	X-Local-Ip
Cdn-Server-Ip	Meter	Vary	X-Log-Url
Cdn-Src-Ip	Mime-Version	Via	X-MAA-Alias
Conf-Err-Host	Negotiate	WWW-Authenticate	X-MAA-Auth
Conf-File	Origin	Warning	X-Max-Conns
Conf-File-List	Partition-Block-Size	Ws-Hdr	X-Mem-Url
Conf-Option	Pragma	WsTag	X-Mgr-Traffic
Conf-Other	Proxy-Authenticate	X-Accelerator-Vary	X-Miss-Rate-Limit

Connection	Proxy-Authentication-Info	X-Appa	X-Miss-Times-Limit
Content-Encoding	Proxy-Authorization	X-Appa-Origin	X-No-Referer
Content-Length	Proxy-Connection	X-Black-List	X-Query-Key
Content-Location	Proxy-Support	X-Bwctrl-Limit	X-Rate-Limit
Content-MD5	Public	X-Bwctrl-Para	X-Refresh-Pattern
Content-Range	Purge-Domain	X-Cache	X-Request-Id
Sec-WebSocket-Nonce	Purge-Extra	X-Cache-2	X-Request-Uri
Date	Range	X-Cache-Lookup	X-Request-Url
Dynamic	Request-Range	X-Cacheable	X-Resp-Time
ETag	Retry-After	X-Cdn-Src-Port	X-Rewrite-Url
Error	Sec-WebSocket-Accept	X-Client-Ip	X-Squid-Error
Expect	Sec-WebSocket-Draft	X-DNS-Time	X-Times-Limit
If-Modified-Since	Sec-WebSocket-Extensions	X-Denyattack-Dynconf	X-Url-Blackwhite-List
From	Sec-WebSocket-Key	X-Error-Status	X-Via-CDN
Front-End-Https	Sec-WebSocket-Key1	X-Error-URL	X-White-List
Host	Sec-WebSocket-Key2	X-Forward-Host	-
If-Match	Sec-WebSocket-Location	-	-

2.8.2 Custom Error Pages

When an error is reported during user access, an error page is displayed on the user client. You can customize the error page on the CDN console to optimize user experience.

Precautions

- You can customize error pages for status codes 4xx and 5xx.

- If CDN acceleration is enabled for the custom error pages, you will be billed by CDN.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Advanced Settings** tab.
5. In the **Custom Error Pages** area, click **Add**.

Figure 2-39 Customizing an error page

Customize Error Page

✱ Error Code

✱ Redirect Mode 301 302

✱ Destination URL

Table 2-30 Parameter description

Parameter	Description	Example
Error Code	Error code (4xx or 5xx) whose error page needs to be customized.	404
Redirect Mode	Mode of redirecting the error code page to a new page. The options are 301 and 302 .	301
Destination URL	New page to which the error code page is redirected. The value must start with http:// or https://.	https://example.com/error404.html

6. Configure the parameters and click **OK**.

Example

Image **abc.jpg** has been deleted from the origin server and the cache on CDN PoPs has expired. When a user accesses <https://example.com/abc.jpg>, a status

code 404 is returned. Assume that you configure the following settings on the CDN console:

Error Code	Redirect Mode	Destination URL
404	301	https://example.com/error404.html

Result: When another user accesses <https://example.com/abc.jpg>, the user will be redirected to <https://example.com/error404.html>.

2.8.3 Smart Compression

Background

If smart compression is enabled, CDN automatically compresses your static files. This can save you a lot of bandwidth by reducing file size and speed up file transfer. Smart compression includes gzip compression and Brotli compression. The performance of Brotli compression is 15% to 25% higher than that of gzip compression.

Precautions

- Smart compression applies to JS, HTML, CSS, XML, JSON, SHTML, and HTM files.
- Do not enable this function if MD5 verification has been configured for your origin server. When CDN compresses static files, the MD5 value is changed. As a result, the MD5 value of the compressed file is different from that of the file on the origin server.
- You cannot enable smart compression for domain names with special configurations.
- If both gzip and Brotli compression are enabled, Brotli compression is preferentially performed.
- General image files (such as PNG, JPG, and JPEG) and video files (such as MP4, AVI, and WMV) have already been compressed. Therefore, you do not need to enable smart compression (gzip or Brotli) for these files.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Advanced Settings** tab.
5. Click **Edit** next to **Smart Compression**.

Figure 2-40 Smart compression

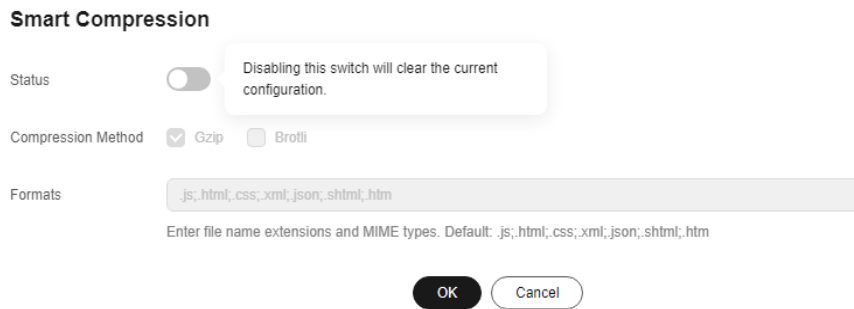


Table 2-31 Parameter description

Parameter	Description
Status	Turn on or off the switch.
Compression Mode	Gzip or Brotli compression. If both are selected, Brotli compression is used.
Format	Enter file name extensions and multipurpose internet mail extensions (MIME). <ul style="list-style-type: none"> • A single extension contains up to 50 characters and all extensions contain up to 2,000 characters. Separate extensions by semicolon (;). • If this parameter is left empty, the default value <code>.js;.html;.css;.xml;.json;.shtml;.htm</code> is used.

6. Select a compression method and click **OK**.

2.8.4 Request Rate Limiting

Limit the user request rate within a specific range to reduce costs and the risk of burst bandwidth.

Precautions

- Rate limiting takes effect for all user requests to the domain name, which affects the acceleration effect and user experience.
- You can configure up to 60 rate limiting rules.
- You can configure only one rate limiting rule for **All files**.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.

4. Click the **Advanced Settings** tab.
5. In the **Request Rate Limiting** area, click **Edit**.

Figure 2-41 Configuring request rate limiting

Configure Request Rate Limiting

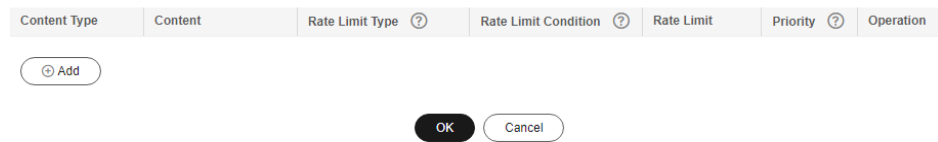


Table 2-32 Parameters

Parameter	Description
Content Type	<ul style="list-style-type: none"> ● All files ● Directory: files in a specific directory
Content	<ul style="list-style-type: none"> ● This parameter is left blank when Content Type is set to All files. ● when Content Type is set to Directory, specify this parameter. <ol style="list-style-type: none"> 1. Start with a slash (/), for example, /test/folder. 2. Do not end with a slash (/). 3. Each rule corresponds to a directory. Multiple directories cannot be configured for a rule.
Rate Limit Type	Rate limiting by transmission traffic is supported. That is, when the traffic of a single HTTP request reaches the specified value, the access speed is limited. The access speed of subsequent requests cannot exceed the specified rate limit.
Rate Limit Condition	Volume of the transmitted traffic that triggers rate limiting. <ul style="list-style-type: none"> ● The unit is byte. The maximum value is 1 GB, that is, 1,073,741,824 bytes.
Rate Limit	Maximum access speed when rate limiting starts. <ul style="list-style-type: none"> ● The maximum value is 100 Mbit/s.
Priority	Priority of a rate limiting rule. Each cache rule must have a unique priority. If multiple rate limiting rules are configured for a resource, CDN uses the rate limiting rule with the highest priority. <ul style="list-style-type: none"> ● Enter an integer ranging from 1 to 100. A greater number indicates a higher priority.

6. Toggle on the **Status** switch, configure required parameters, and click **OK**.

2.9 Video Settings

2.9.1 Video Seek

Background

Video seek is mainly used in VOD scenarios. It allows users to seek to a certain position in a video without affecting the playback effect.

- If video seek is configured, a user client sends a request similar to the following to the server when the user drags the progress bar during video playback:

```
http://www.example.com/test.flv?start=50
```

Data starting from the 50th byte is returned to the client. If the video has been cached on a CDN PoP, the CDN PoP directly returns the data to the user.

- Video seek is valid only when URL parameter filtering is set to **Ignore URL Parameters** for MP4 and FLV files. For details, see [Cache Rules](#).
- Video seek is valid only when your origin server supports Range requests.
- Only MP4 and FLV videos are supported.

Table 2-33 File formats

File Format	Meta Information	Start Parameter	Example
MP4	The meta information of the video on the origin server must be contained in the header of the file.	The start parameter indicates a time. CDN automatically locates the key frame before the time specified by the start parameter if the specified time is not a key frame. The unit is second and decimal places are supported. For example, start=1.01 indicates that the start time is 1.01 seconds.	<pre>http://www.example.com/test.mp4?start=50</pre> The playback starts from the 50th second.
FLV	The video on the origin server must contain meta information.	The start parameter indicates a byte. CDN automatically locates the key frame before the byte specified by the start parameter if the specified byte is not a key frame.	<pre>http://www.example.com/test.flv?start=500</pre> The playback starts from the 500th byte.

Precautions

- You have configured a cache rule for FLV and MP4 files and .

Procedure

- Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
- In the navigation pane, choose **Domains**.
- In the domain list, click the target domain name or click **Configure** in the **Operation** column.
- Click the **Video Settings** tab.
- Click **Edit** next to **Video Seek**.

Figure 2-42 Configuring video seek

Configure Video Seek

i 1. Configure a cache rule for FLV and MP4 files and set [URL parameter filtering](#) to Ignore all.
2. Time-based FLV seek is valid only when Video Seek is enabled.

Video Seek

Time-based FLV Seek

Custom Parameters **?** Start End

OK **Cancel**

- (Optional) Enable time-based FLV seek.
Switch on **Time-based FLV Seek**, so FLV videos can be sought by time.

NOTE

If you enable **Time-based FLV Seek**, it is valid only when **Video Seek** is enabled.

- (Optional) Configure the start and end parameters.
 - By default, the start parameter is **start** and the end parameter is **end**.
 - A parameter can contain up to 64 characters, including letters, digits, and underscores (_).
- Click **OK**.

2.10 Tag Management

You can use tags to customize resource categories, add tags to domain names, and manage resources with ease.

Scenarios

Tags help you identify your cloud resources. When you have many cloud resources of the same type, you can use tags to classify them by dimension (for example,

use, owner, or environment). You can quickly search for specific cloud resources based on the tags added to them. For example, you can define a set of tags for cloud resources in an account to track the owner and usage of each cloud resource, making resource management easier.

Restrictions

- You can add up to 20 tags to each domain name.

Adding a Tag on the Configuration Page

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column. Click the **Tags** tab and click **Edit Tag**.

Figure 2-43 Editing tags

Edit Tag

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) 

+ [Add Tag](#)

You can add 20 more tags.

Cancel

OK

Table 2-34 Parameter description

Parameter	Description	Example
Tag key	<ul style="list-style-type: none"> Enter 1 to 128 characters Enter letters, digits, spaces, and special characters (_ . : = + - @). Do not start or end with a space. Do not start with _sys_. 	Protocol

Parameter	Description	Example
Tag value	<ul style="list-style-type: none">• Enter 1 to 255 characters.• Enter letters, digits, spaces, and special characters (_ . : = + - @ /). Do not start or end with a space.	HTTPS

4. Click **Add Tag**, enter a tag key and value, and click **OK**.

Deleting a Tag

- On the domain name configuration page
 - a. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
 - b. In the navigation pane, choose **Domains**.
 - c. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
 - d. Click the **Tags** tab.
 - e. Click **Edit Tag**.
 - f. Click **Delete** next to the tag to be deleted and click **OK**.

Searching for Resources by Tag

You can use tags to search for resources.

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. Enter one or more tag key-value pairs into the text box and press **Enter** to search for domain names with the specified tags.

3 Cache Purge and Prefetch

3.1 Overview

CDN can purge and prefetch content.

- **Cache Purge** forces cached content on CDN PoPs to expire. If a user requests that content, CDN has to pull fresh content from the origin server and then cache that new content.
- **Cache Prefetch** allows the origin server to proactively send the most current content to a CDN PoP. If a user requests the content, the CDN PoP immediately returns the cached content. It does not need to pull any new content.

Prerequisites

Cache purge and prefetch can only be configured for domain names in the **Enabled** or **Configuring** state. For more information about the domain status, see [Viewing Basic Domain Information](#).

3.2 Cache Prefetch

Background

CDN simulates user requests and caches resources to CDN PoPs, so that users can obtain the latest resources from the nearest CDN PoP.

Typical Scenarios

Initial access: When you connect a domain name to CDN for the first time, you can prefetch large files including videos to improve user experience.

Installation package release: Before releasing a software installation package or upgrade package, you can prefetch the content to the globally distributed CDN PoPs. After the software or upgrade is launched, the CDN PoPs directly respond to the download requests of a large number of users, which improves the download speed and greatly reduces the pressure on your origin server.

Promotional activity: Before releasing a promotional campaign, you can prefetch the static content involved on the activity page to CDN PoPs. After the activity starts, the CDN PoPs respond to user requests for accessing all static content, which ensures service availability and improves user experience.

Precautions

- Cache prefetch can be performed only for unbanned domain names in **Enabled** or **Configuring** state. For more information about the domain status, see [Viewing Basic Domain Information](#).
- The time required to complete a prefetch task depends on the number and size of target files, and on network conditions.
- If the cache prefetch status of a URL is **Completed**, the prefetch is complete.
- Prefetching a large number of files may fully occupy the bandwidth resources of the origin server. Therefore, you are advised to prefetch files in batches.
- Dynamic files, such as ASP, JSP, and PHP files, cannot be prefetched.
- If you have set **cache-control** to **s-maxage=0**, **max-age=0**, **private**, **no-cache**, or **no-store** on the origin server and enabled **Origin Cache Control** on the CDN console, the origin server does not allow caching. As a result, cache prefetch fails.
- If **Origin Cache Control** is not enabled and the cache TTL of the content to be prefetched is set to **0**, CDN cannot cache the resource and the prefetch fails.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Prefetch & Purge**.
3. Click the **Prefetch** tab and enter URLs to be prefetched.

Figure 3-1 Cache prefetch

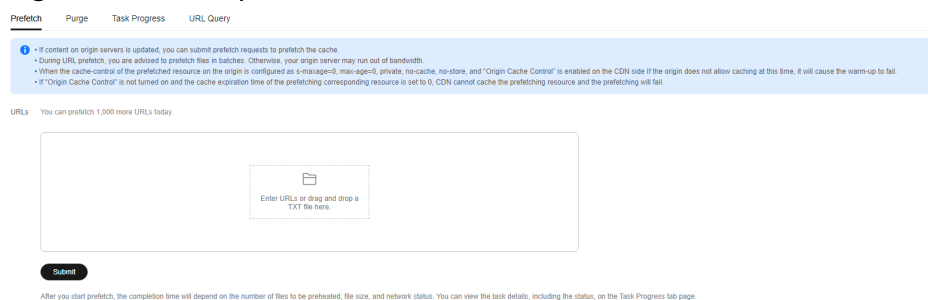


Table 3-1 Parameter description

Type	Description
URL prefetch <ul style="list-style-type: none">• CDN prefetches a specific file.	The format of a URL in the text box or in the TXT file must meet the following requirements: <ul style="list-style-type: none">• http:// or https:// must be included.• Enter one URL per row.• Each account can prefetch a maximum of 1,000 URLs per day or per task. Example: http://www.example.com/file01.html http://www.example.com/file02.html https://example.huawei.com/download/app/abc.apk

4. Click **Submit**.

After a prefetch task is submitted, you can view the status of the task on the **Task Progress** tab.

3.3 Cache Purge

Background

After resources on the origin server are updated, if the old resources cached on CDN PoPs do not expire, CDN still returns the old resources to users. You can use cache purge to forcibly expire resources cached on CDN PoPs. When a user accesses a resource, CDN pulls the latest resource from the origin server, returns it to the user, and caches it on CDN PoPs.

Typical Scenarios

New content release: After new content overwrites old content with the same name on origin servers, to enable all users to access the latest content, you can submit requests to refresh corresponding URLs or directories of the content, forcing the cached content on the PoPs to expire.

Non-compliant content clearing: When non-compliant content is detected and deleted from origin servers, the cached content on PoPs can still be accessed. You can refresh URLs to delete the cached content.

Precautions

- Cache purge can be performed only for unbanned domain names in **Enabled** or **Configuring** state. For more information about the domain status, see [Viewing Basic Domain Information](#).
- If a URL is rewritten, you must use the actual resource path of the new URL for cache purge.
- Some resources may be cached in browsers. Refresh the browser cache after the PoP cache is refreshed.

- It takes about 5 minutes for a cache purge task to take effect.
- By default, cache of TS/MP4 files under M3U8/MPD index files is not refreshed.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Prefetch & Purge**.
3. Click the **Purge** tab, select the content type, and enter the URLs or directories to be refreshed.

Figure 3-2 Cache purge

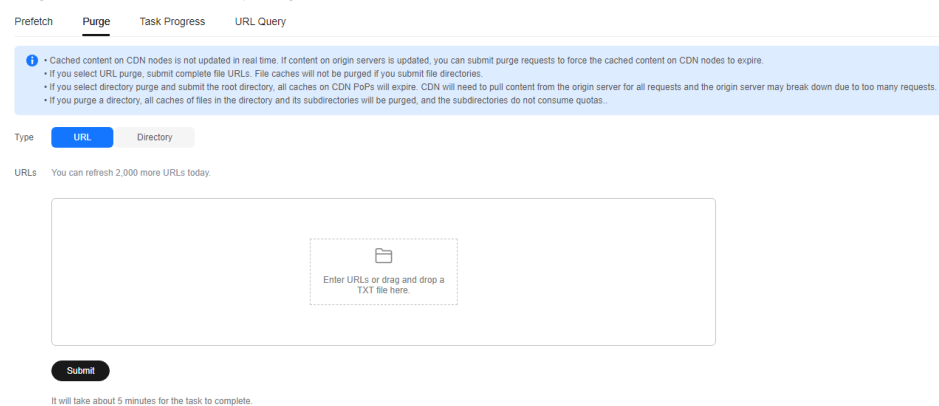


Table 3-2 Parameter description

Type	Description
<p>URL</p> <ul style="list-style-type: none"> • CDN refreshes a specific file. 	<p>The format of a URL in the text box or in the TXT file must meet the following requirements:</p> <ul style="list-style-type: none"> • Each account can refresh a maximum of 2,000 URLs per day and a maximum of 1,000 URLs per task. • The http:// or https:// part of the URL must be included. • Enter one URL per row. <p>Examples:</p> <p>http://www.example.com/file01.html http://www.example.com/file02.html https://example.huawei.com/download/app/abc.apk</p> <p>NOTE</p> <ul style="list-style-type: none"> • Submit complete file URLs. If you submit a directory, URL refreshing does not take effect. • If a URL contains spaces, escape spaces in the URL and disable URL Encode.

Type	Description
<p>Directory</p> <ul style="list-style-type: none"> • CDN refreshes all files in a directory. 	<p>Refreshing modes:</p> <ul style="list-style-type: none"> • Refresh updated resources: Refresh resources that have been updated in a directory (including subdirectories). • Refresh all resources: Refresh all resources in a directory, including resources in subdirectories. <p>Configuration rules:</p> <ul style="list-style-type: none"> • Each account can refresh a maximum of 100 directories per day at a time. • A URL must contain http or https and end with a slash (/). • Enter one URL per row. <p>Examples:</p> <p>http://www.example01.com/folder01/ http://www.example01.com/folder02/</p> <p>NOTE</p> <ul style="list-style-type: none"> • URLs in the text box or in the TXT file have the same format requirements. • If you select Refresh all resources when refreshing the root directory, the cache of all resources will expire. As a result, CDN pulls content for all requests from the origin server. If the access traffic is too heavy, the origin server may break down. • If you select Refresh all resources when refreshing a directory, all resources in the directory, including subdirectories will be refreshed. Only one directory is counted against the directory refreshing quota.

4. Click **Submit**.

After a purge task is submitted, you can view the status of the task on the **Task Progress** tab.

3.4 Viewing Task Progresses

After a cache purge or prefetch task is submitted, you can view the task status on the **Task Progress** tab page.

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Prefetch & Purge**.
3. Select the **Task Progress** tab to check the task status.
 - You can view the failure cause of a failed task.

Prefetch Purge **Task Progress** URL Query

You can query the progress of purge and prefetch tasks over the past 15 days.

Type	Status	Task ID	File type	URLs	Running	Successful	Failed	Created
<input checked="" type="radio"/> Prefetch	Completed	2268470000	URL	1	0	0	1	Oct 19, 2023 14:31:46 GMT+08:00
<input type="radio"/> Purge	Completed	2268462603	URL	1	0	1	0	Oct 19, 2023 14:27:54 GMT+08:00

Total Records: 2

Selected: 2268470000 (Task ID)

URL	Status	Cause
https://rh.../smtest.jpg	Failed	Origin error: Troubleshooting

NOTE

- On the **Task Progress** tab page, you can view the status of cache purge and prefetch tasks over the last 15 days.
- You can also query the cache purge and prefetch records of the last 15 days on the **URL Query** tab page.

3.5 FAQ

What Are the Differences Between Cache Purge and Prefetch?

The differences between cache purge and prefetch are:

- **Cache purge**
After you submit a cache purge request, cached content on CDN PoPs will be forcibly expired. If a user requests that content, CDN will have to request fresh content from the origin server and then cache that new content.
- **Cache prefetch**
After you submit a cache prefetch request, the origin server proactively sends the most current content to a CDN PoP to be cached. If a user requests the content, the CDN PoP immediately returns the cached content. It does not need to pull any new content.

Is There a Sequence Between CDN Cache Purge and Prefetch?

If you want to update cached content on CDN PoPs after your origin content is updated, pay attention to the following:

- You must purge the cache first. It takes about 5 minutes for a cache purge task to take effect. Then, prefetch the cache.
- If you skip cache purge and directly perform cache prefetch, the cached content on CDN PoPs will not be updated.
- If you access CDN for the first time and no content is cached on CDN PoPs, you can directly perform cache prefetch to cache content to CDN PoPs.

Does Cache Purge Refresh Content Cached on All PoPs?

Yes.

Why Is a Particular Prefetch Task in the Being Processed Status for Such a Long Time?

Possible causes include:

- The task was submitted during a peak hour, so it is still in the queue.
- You are prefetching a large number of files. Prefetch will pull content from the origin server, so pulling a large number of files may consume all of the bandwidth available for your origin server. You are advised to:
 - Divide files to be prefetched into batches.
 - Prefetch files during off-peak hours, for example, at night.
 - Increase your origin server bandwidth.
- The task has been completed but the status is not refreshed on the console. Refresh the console page and check again.

How Do I Purge the CDN Cache Where the Domain Name Includes a Wildcard?

When purging the cache for a domain name that includes a wildcard, enter the URLs or directories of the level-2 domain names to be refreshed. Do not enter a URL containing a wildcard, such as **https://*.example.com/file01.html** or **https://*.example.com/file02/**.

Example:

- An acceleration domain name is ***.example.com**.
- The level-2 domain name housing the content to be refreshed is **abc.example.com**.
 - a. Enter the URL to be refreshed: **https://abc.example.com/file01.html**.
 - b. Enter the directory to be refreshed: **https://abc.example.com/file02/**.

Why Is It That Even After I Prefetched or Purged the Cache, the Content Has Not Updated?

The interval between cache purge and prefetch may be too short. As a result, the purge fails. If a cache has just been purged or prefetched, it is recommended that you wait at least 5 minutes before repeating this action.

What Do I Do If a Cache Prefetch Operation Fails?

It is possible that:

- A large number of files are being prefetched at the same time, and this operation has occupied all of the origin server's bandwidth. In this case, you are advised to perform prefetch operations in batches. You can also increase the bandwidth of the origin server to improve the efficiency.
- The cache TTL of your requested content is 0. In this case, change the cache TTL.
- **Cache-Control** is **private**, **no-cache**, or **no-store**. If **Cache-Control** is not configured, the default value **private** is used.

- You requested to prefetch directories, dynamic content, or URLs whose cache TTL is set to 0.

Do I Need to Prefetch or Purge HTTP and HTTPS URLs Separately?

No. You only need to prefetch or purge either HTTP or HTTPS URLs.

Can I Prefetch M3U8 Files?

Yes.

Why Does the System Report an Error Indicating that I Have No Permission to Purge the Cache?

It is possible that your acceleration domain name has been disabled. Enable CDN for the domain name again. If your account is in arrears, CDN may have been disabled for your acceleration domain name.

Are Cache Purge and Prefetch Mandatory?

It depends.

- If a file is updated on an origin server, the file needs to be updated on CDN PoPs as well.
- It is recommended that large files, especially video files, be prefetched to improve user experience.
- Prefetch is not recommended for small files.

Currently, CDN does not support automatic purge or prefetch. You need to manually perform these operations.

4 Statistical Analysis

4.1 Statistics Description

Table 4-1 displays reports provided by CDN. You can learn:

Table 4-1 Statistics description

Indicator	Description
Utilization Statistics	You can query the used traffic/bandwidth.
Access Statistics	You can query the total requests and queries per second for all your domain names.
Origin Server Statistics	You can query the traffic, bandwidth, and failure rate of origin pulls for all your domain names.
Region & Carrier Statistics	You can query the traffic/bandwidth usage and total requests for all domain names by region or carrier.
Status Codes	You can query the status codes of requests to all domain names.

 **NOTE**

- CDN allows you to query statistics about deleted domain names.
- If you have enabled the enterprise project function, statistics of deleted domain names cannot be queried.

4.2 Utilization Statistics

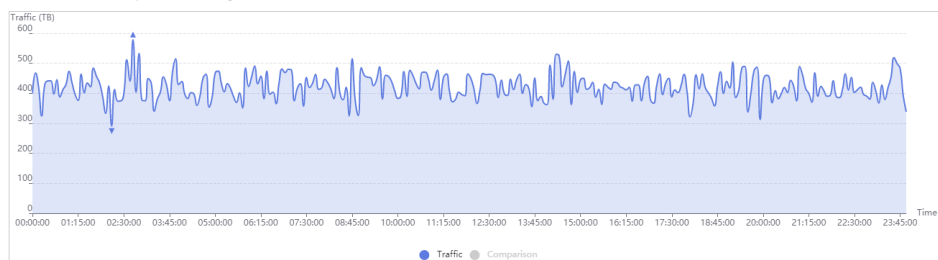
You can view the traffic/bandwidth of all domain names (excluding those deleted if you have enabled the enterprise project function).

- Data of the past 90 days can be queried, and each query can include data of up to 7 days.

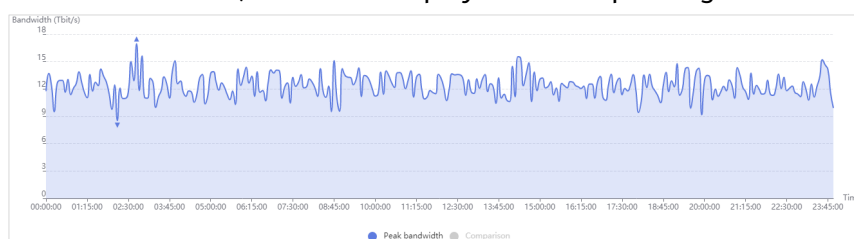
- If no data is available within the queried time range, no data is displayed on the traffic/bandwidth trend chart or in the domain name traffic/bandwidth utilization list.
- The minimum granularity is 5 minutes.
- The logged traffic statistics are displayed. However, the billable traffic is 10% higher than the logged statistics because TCP/IP packet headers and TCP retransmissions also consume traffic.
- There is a delay of about one hour for data displayed on the **Traffic** page.
- You can compare data.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Statistical Analysis > Utilization Statistics**.
3. Set search criteria to query the following data:
 - **Traffic Monitoring**: displays the traffic of specific domain names over time. You can click legend entries, for example, Traffic , to hide or display the corresponding statistics.



- **Peak Bandwidth Monitoring**: displays the peak bandwidth of specific domain names over time. You can click legend entries, for example, Peak bandwidth , to hide or display the corresponding statistics.



- **Domain Name Traffic/Bandwidth Utilization**: displays the traffic and bandwidth of specific domain names.

You can click **Traffic** or **Peak Bandwidth** on the table heading to view the statistics in either descending or ascending order.

4.3 Access Statistics

You can view the total number of requests and queries per second of all your domain names (excluding those deleted if you have enabled the enterprise project function).

- Data of the past 90 days can be queried, and each query can include data of up to 7 days.
- The access information is displayed based on the log statistics. The data is updated once an hour.
- If no data is available within the queried time range, no data is displayed on the total requests and queries per second trend charts or in the domain name access details list.
- The minimum granularity is 5 minutes.

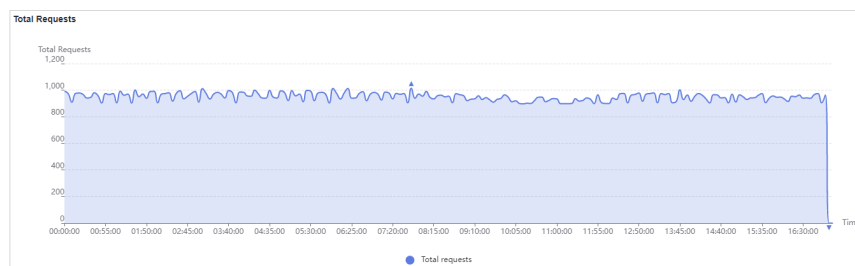
Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.

The CDN console is displayed.

2. In the navigation pane, choose **Statistical Analysis > Access Statistics**.
3. Set search criteria to query the following data:

- **Total Requests:** displays the number of requests to specific domain names over time.



- **Queries per Second:** displays the queries per second of specific domain names over time.

Queries per second is a common measure of the number of queries that domain names receive during one second.



- **Domain Name Access:** displays the number of requests to specific domain names, cache hit ratio, and queries per second.

You can click **Total Requests** or **Queries per Second** on the table heading to view the statistics in either descending or ascending order.

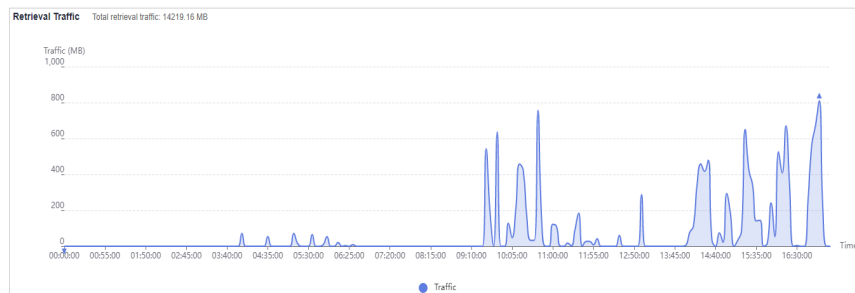
4.4 Origin Server Statistics

You can view the traffic, bandwidth, and failure rate of origin pulls for all your domain names (excluding those deleted if you have enabled the enterprise project function).

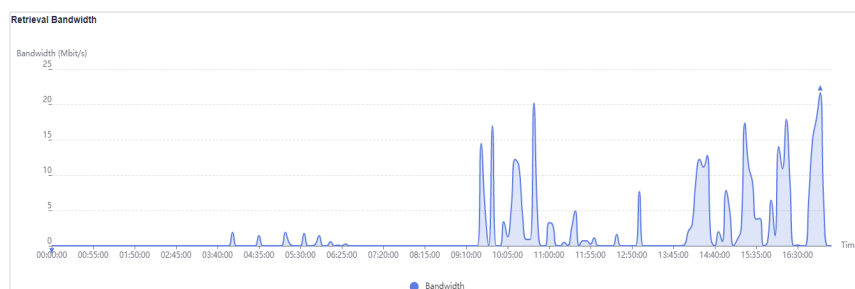
- Data of the past 90 days can be queried, and each query can include data of up to 7 days.
- If no data is available within the queried time range, no data is displayed on the retrieval traffic/bandwidth and retrieval failure rate trend charts or in the domain name retrieval details list.
- The minimum granularity is 5 minutes.

Procedure

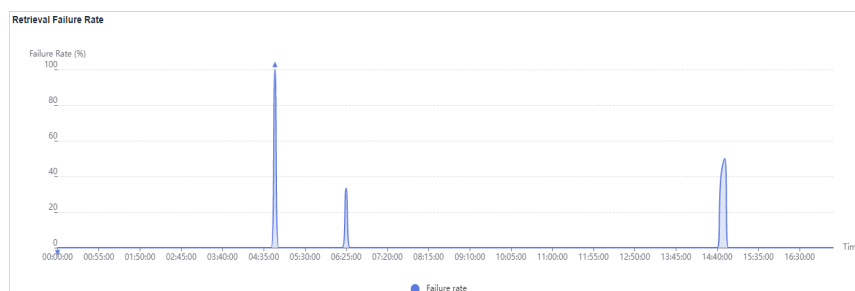
1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Statistical Analysis > Origin Server Statistics**.
3. Set search criteria to query the following data:
 - **Retrieval Traffic:** displays the origin pull traffic of specific domain names over time.



- **Retrieval Bandwidth:** displays the origin pull bandwidth of specific domain names over time.



- **Retrieval Failure Rate:** displays the origin pull failure rate over time.
Retrieval failure rate = $\frac{\text{Number of failed origin pull requests}}{\text{Number of total origin pull requests}}$



 NOTE

- Origin pull failures may be caused by host configuration errors, disconnection between CDN and the host, HTTP incompatibility, and host errors.
 - If the last status code of an origin pull request is 2xx, 3xx, 404, or 416, the request is successful. Other status codes indicate that the request fails.
- **Domain Name Retrieval Details:** displays the traffic, bandwidth, and failure rates of origin pull from specific domain names.

You can click **Retrieval Traffic**, **Retrieval Bandwidth**, or **Retrieval Failure Rate** on the table heading to view the statistics in either descending or ascending order.

Domain Name	Retrieval Traffic 	Retrieval Bandwidth 	Retrieval Failure Rate 
brc-2.com	1.87 GB	2.61 Mbit/s	0.00 %
ww-1.site	6.84 KB	0.04 kbit/s	76.47 %

4.5 Data Analysis

You can view domain name rankings, **region/carrier rankings**, popular URLs, popular referers, and popular user agents to learn about the domain status and promptly adjust businesses.

Precautions

- Data of the past 90 days can be queried, and each query can include data of up to 7 days.
- The minimum statistical granularity is day.
- The statistical latency and algorithm error may cause the difference between the statistical data and the logged data. The logged data is used.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Analytics > Data Analysis**.
3. View domain name rankings, **region/carrier rankings**, popular URLs, popular referers, and popular user agents.
 - **Domain Rankings:** displays the rankings of all domain names under your account. By default, domain names are sorted by traffic in descending order.
 - **Regions & Carriers:** displays data about regions and carriers of users who access your domain names. This report is displayed by default and does not need to be customized.
 - **Popular URLs:** top 100 URLs sorted by traffic or number of requests
 - **Popular Referers:** top 100 referers sorted by traffic or number of requests
 - **Popular User Agents:** top 100 user agents sorted by traffic or number of requests

4.6 Region & Carrier Statistics

You can query the traffic/bandwidth usage, number of requests, and visitor distribution of all domain names (excluding those deleted if you have enabled the enterprise project function) by region or carrier.

- Data of the past 90 days can be queried, and each query can include data of up to 7 days.
- If no data is available within the queried time range, no data is displayed in the list of carrier index statistical details.
- The minimum granularity is 5 minutes.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.

The CDN console is displayed.

2. In the navigation pane, choose **Statistical Analysis**.
3. Under **Statistical Analysis**, choose **Region & Carrier Statistics**.
4. Select a tab and set search criteria to query the following data:

- **Visitor Region:** displays the region where visitors are located.

Visitor Region	Traffic (Percentage) ↓	Peak Bandwidth ↓	Total Requests (Percentage) ↓
China	1.02 MB (100.00%)	0.05 kbit/s	1,066,000 (100.00%)

- **Carriers: SFR**

- i. **Carrier Index Distribution:** displays the proportion each carrier occupies in different index statistics.



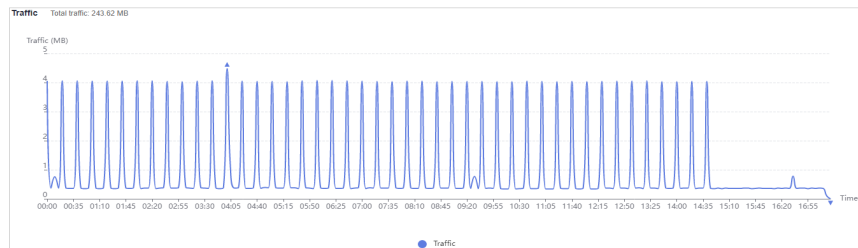
- ii. **Carrier Index Statistical Details:** displays the traffic, peak bandwidth, and number of requests by carrier. You can click **Traffic**, **Peak Bandwidth** or **Total Requests** in the table heading of **Carrier Index Statistical Details** to see the data in ascending or descending order.

Carrier Index Statistical Details

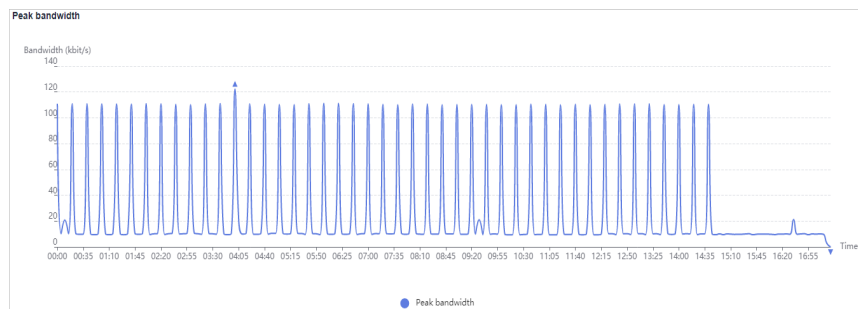
Carrier	Traffic (Percentage)	Peak Bandwidth (Percentage)	Total Requests (Percentage)
Other	110.64 MB (93.75%)	85.04 kbit/s (98.35%)	228 (1.19%)
China Mobile	7.03 MB (5.96%)	1.26 kbit/s (1.46%)	18,035 (94.12%)
China Mobile Tietong	349.32 KB (0.29%)	0.07 kbit/s (0.08%)	893 (4.66%)
China Telecom	5.07 KB (0.00%)	0.07 kbit/s (0.08%)	5 (0.03%)
China Unicom	0.75 KB (0.00%)	0.02 kbit/s (0.02%)	1 (0.01%)

– **Utilization (Regions)**

- i. **Traffic:** displays the traffic of specific domain names by country/region or carriers.



- ii. **Peak bandwidth:** displays the peak bandwidth of specific domain names by country/region or carriers.

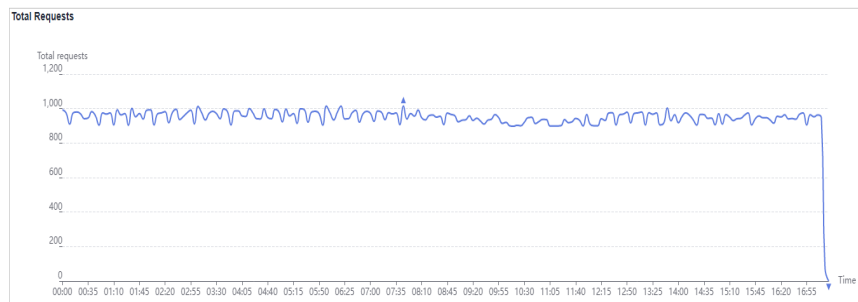


- iii. **Domain Name Traffic/Bandwidth Utilization:** displays the traffic and bandwidth of specific domain names.

Domain Name	Traffic	Peak Bandwidth
1m...t.com	1.02 MB	0.05 kbit/s

– **Visits (Regions)**

- i. **Total Requests:** displays the number of requests to the domain name in the specified region.



- ii. **Domain Name Access:** displays access details about the domain name in the specified region.

Domain Name	Total Requests
1m...st.com	106.80 Ten Thousands

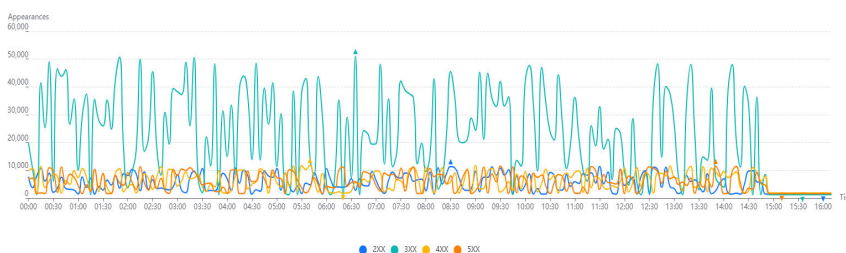
4.7 Status Codes

You can view status codes returned to requests to all domain names (excluding those deleted if you have enabled the enterprise project function).

- Data of the past 90 days can be queried, and each query can include data of up to 7 days.
- If no data is available within the queried time range, no data is displayed in the list of status codes.
- The minimum granularity is 5 minutes.

Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.
The CDN console is displayed.
2. In the navigation pane, choose **Statistical Analysis > Status Codes**.
3. Set search criteria to query the following data:
 - **Status Codes Overview**: displays the number of each status code over time.



You can click legend entries, for example, 2XX, to hide or display the statistics of specific codes. Statistics are collected on status codes, including 2XX, 3XX, 4XX, and 5XX.

Status Code	Description
2XX	Success. A request has been accepted and processed by the server.
3XX	Redirection. The client needs to perform further operations to complete the request.
4XX	Client error. There was an error on the client side, including but not limited to syntax errors or failure to complete the request.
5XX	Server error. There was an error when the server was processing the request.

- **Status Code Statistics**: displays the number and proportion of different status codes for specific domain names.

You can click **Appearances** or **Percentage** in the table heading of the statistics details list to view the corresponding data in ascending or descending order.

Status Code 	Appearances 	Percentage 
20X	1,054,003	13.53%
50X	1,109,929	14.35%
40X	1,171,917	15.16%
30X	4,396,207	56.86%

5 Resource Package Management

CDN provides you with traffic packages. You can purchase them to save money. You can also view the basic package information and manage them on the **Resource Packages** page.

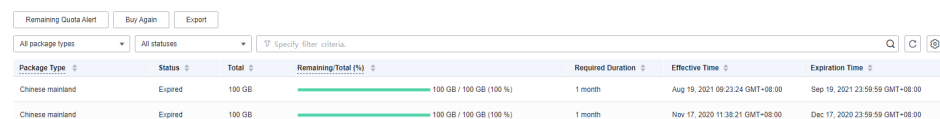
Procedure

1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.

The CDN console is displayed.

2. In the navigation pane, choose **Resource Packages**.

Figure 5-1 Managing resource packages



Package Type	Status	Total	Remaining/Total (%)	Required Duration	Effective Time	Expiration Time
Chinese mainland	Expired	100 GB	100 GB / 100 GB (100 %)	1 month	Aug 19, 2021 09:23:24 GMT+08:00	Sep 19, 2021 23:59:59 GMT+08:00
Chinese mainland	Expired	100 GB	100 GB / 100 GB (100 %)	1 month	Nov 17, 2020 11:38:21 GMT+08:00	Dec 17, 2020 23:59:59 GMT+08:00

3. You can perform the following operations:
 - Viewing basic information about a package: Learn about your package consumption at any time.
 - Searching for resource packages: Filter traffic packages by region, status, required duration, and effective time. Different dimensions have the AND relationship, and similar dimensions have the OR relationship.
 - Setting the remaining quota alert: Click **Remaining Quota Alert** to set an alert for remaining quotas of valid packages. Purchase a new package or top up your account in a timely manner to avoid service loss caused by arrears.
 - Buying packages again: Click **Buy Again** and buy packages based on your service requirements.
 - Exporting package information: Click **Export** to export the information of resource packages on the current page to an Excel file.
 - Buying packages: Click **Buy Package** and buy packages based on your service requirements.

6 Log Management

CDN records the requests to all domain names including those deleted. If you have enabled the enterprise project function, log management is not available for these deleted domain names. You can download logs for a specific period over the past 30 days. Then you can analyze the access to your service resources in detail.

Log Description

Most logs are generated in 24 hours. Download them after they are generated.

The log naming rules are as follows: *Start time of the query period-Domain name-Service area.gz*. So a typical log name might be, **2018021123-[www.example01.com-ov.gz](#)**.

By default, a log file is generated for each domain name every hour, and 24 log files are generated every day. The size of a log file is limited. If a log file generated within an hour is too large, it will be divided into multiple files. In this case, a segment flag is added to the name of each log file.

Example of log file content

```
[05/Feb/2018:07:54:52 +0800] x.x.x.x 1 "-" "HTTP/1.1" "GET" "www.test.com" "/test/1234.apk" 206 720 HIT  
"Mozilla/5.0 (Linux; U; Android 6.0; zh-cn; EVA-AL10 Build/HUAWEIEVA-AL10) AppleWebKit/533.1 (KHTML,  
like Gecko) Mobile Safari/533.1" "bytes=-256" x.x.x.x
```

Table 6-1 describes each field (from left to right) in the log.

Table 6-1 Description of a CDN log file

No	Field Description	Example
1	Log generation time	[05/Feb/2018:07:54:52 +0800]
2	Access IP address	x.x.x.x
3	Time to last byte (ms)	1
4	Referer information	-
5	HTTP protocol identifier	HTTP/1.1

No	Field Description	Example
6	HTTP request method	GET
7	Acceleration domain name	www.test.com
8	Requested path (excluding URL parameters)	/test/1234.apk
9	HTTP status code	206
10	Response size (bytes)	720
11	Cache hit status	HIT
12	User-Agent information, which helps servers recognize the OS, OS version, CPU, browser, and browser's version information	Mozilla/5.0 (Linux; U; Android 6.0; en-us; EVA-AL10 Build/HUAWEIEVA-AL10) AppleWebKit/533.1 (KHTML, like Gecko) Mobile Safari/533.1
13	Range information. It specifies the positions of the first and last bytes for the data to be returned. bytes can be expressed by the following three methods: <ul style="list-style-type: none">• bytes=x-y: requesting content from the xth to yth byte.• bytes=-y: requesting content from the last y bytes.• bytes=x-: requesting content from the xth to the last byte.	bytes=-256
14	Server IP address (available from late May 2024), that is, the IP address used by the CDN server to send responses	x.x.x.x

Downloading Logs

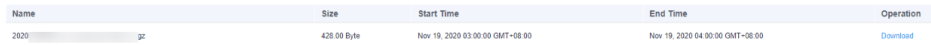
1. Log in to [Huawei Cloud console](#). Choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**.

The CDN console is displayed.

2. In the navigation pane, choose **Logs**.
3. Select the acceleration domain name and specify the time range for the query.

All logs of the specified time range are displayed in the log list. If no requests are received within the period queried, no logs are generated and no data is displayed on the page.

Figure 6-1 Log management



Name	Size	Start Time	End Time	Operation
2020-11-19-03-00-00-04-00-00	428.00 Byte	Nov 19, 2020 03:00:00 GMT+08:00	Nov 19, 2020 04:00:00 GMT+08:00	Download

4. Click **Download** in the row of the desired log to download the log file to a local computer.

7 Permissions Management

7.1 Creating a User and Granting CDN Permissions

This chapter describes how to use to implement fine-grained permissions control for your CDN resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing CDN resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust an account or cloud service to perform professional and efficient O&M on your CDN resources.

If your account does not require individual IAM users, skip this chapter.

This section describes the procedure for granting permissions.

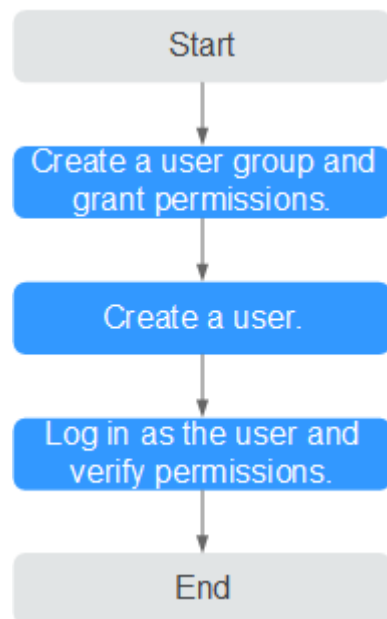
Prerequisites

Learn about the permissions (see .) supported by CDN and choose policies or roles according to your requirements.

Process Flow

[Figure 7-1](#) shows the process of granting CDN permissions.

Figure 7-1 Process of granting CDN permissions



1. Create a user group and assign permissions.
Create a user group on the IAM console, and assign the **CDN DomainReadOnlyAccess** policy to the group.
2. Create an IAM user and add it to the user group.
Create a user on the IAM console and add the user to the group created in 1.
3. Log in as the IAM user and verify permissions.
Log in to the CDN console as the created user, and verify that it only has read permissions for CDN domain names.
 - Enable or disable an acceleration domain name. If a message appears indicating that you have insufficient permissions to perform the operation, the **CDN DomainReadOnlyAccess** policy has already taken effect.
 - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **CDN DomainReadOnlyAccess** policy has already taken effect.

7.2 Creating a Custom Policy

Custom policies can be created to supplement the system-defined policies of CDN.

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions without the need to know policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

This section provides examples of common custom CCE policies.

Example Custom Policies

- Example 1: Allowing users to create acceleration domain names

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cdn:configuration:createDomains"
      ]
    }
  ]
}
```

- Example 2: Allowing users to set an IP blacklist

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "cdn:configuration:modifyIpAcl"
      ],
      "Effect": "Allow"
    }
  ]
}
```

- Example 3: Denying users to delete acceleration domain names.

A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

The following method can be used if you need to assign permissions of the **CDN Admin** policy to a user but also forbid the user from deleting acceleration domain names. Create a custom policy for denying acceleration domain name deletion, and assign both policies to the group the user belongs to. Then the user can perform all operations on CDN except deleting acceleration domain names. The following is an example deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "cdn:configuration:deleteDomains"
      ],
      "Effect": "Deny"
    }
  ]
}
```

8 Enterprise Projects

Enterprise Management allows unified cloud resource management by enterprise project. You can manage resources and personnel in enterprise projects, and assign one or more user groups to manage enterprise projects. You can create CDN enterprise projects on the Enterprise Management console to manage your domain resources in a centralized manner.

Creating an Enterprise Project

To create a CDN enterprise project:

1. On the Enterprise Management console, create an enterprise project based on your enterprise's requirements. For example, you can create enterprise projects based on the service types of the CDN acceleration domain names.
2. After an enterprise project is created, you can migrate your domain name resources to a specified enterprise project.

NOTE

- An enterprise project named **default** is created by default. This project is used to manage any resources that are not allocated to a specific enterprise project.
- Migrating an acceleration domain name between enterprise projects does not affect the acceleration service.

A Change History

Released On	Description
2024-04-26	This issue is the fifth official release. <ul style="list-style-type: none">Added sections "Origin SNI", "Advanced Origins", "ETag Verification", "HSTS", "QUIC", "Browser Cache TTL", "Remote Authentication", "IP Access Frequency", "Request Rate Limiting", "Video Seek", and "Tag Management."
2024-04-16	This issue is the fourth official release. <ul style="list-style-type: none">Added sections "Smart Compression" and "IPv6."
2024-01-10	This issue is the third official release. <ul style="list-style-type: none">Added the OBS private bucket access function.
2023-11-28	This issue is the second official release. <ul style="list-style-type: none">Added the traffic package management function.
2023-03-30	This issue is the first official release.