Content Delivery Network

User Guide

Issue	04
Date	2025-01-14

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 Overview

After adding a domain name to CDN, if you need to stop acceleration or restart acceleration due to service changes, you can enable or disable CDN or delete domain names 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	**Disabling CDN**: You can disable CDN for a domain name in the **Enabled** state. **Enabling CDN**: You can enable CDN for a domain name in the **Disabled** 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

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 in the **Enabled** or **Error** state. CDN will no longer provide the acceleration service for this domain name, but the domain configuration will remain. To restore acceleration, enable CDN for it 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

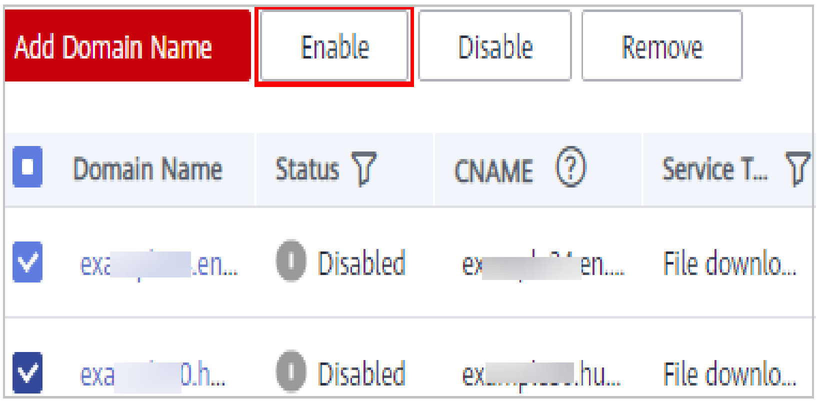
You can enable CDN for a domain name in the **Disabled** state.

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.



■	Domain Name	Status	CNAME	Service T...
☑	exa[redacted].en...	Disabled	ex[redacted]en....	File downlo...
☑	exa[redacted]0.h...	Disabled	ex[redacted].hu...	File downlo...

1.3 Deleting a Domain Name

If you no longer want to accelerate access to 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 use acceleration for the domain name again, re-add it to CDN.

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

What Is a Quota?

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 accounts. If an existing resource quota cannot meet your service requirements, submit a service ticket to increase the quota.

Table 1-2 CDN domain name quotas

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.

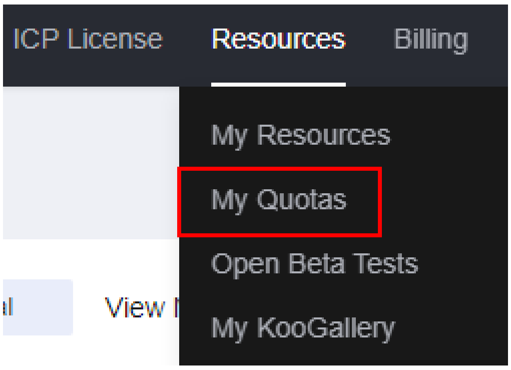
How Do I View My Quota?

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 upper right corner of the page, choose **Resources** > **My Quotas**. The **Service Quota** page is displayed.

   Figure 1-1 My Quotas

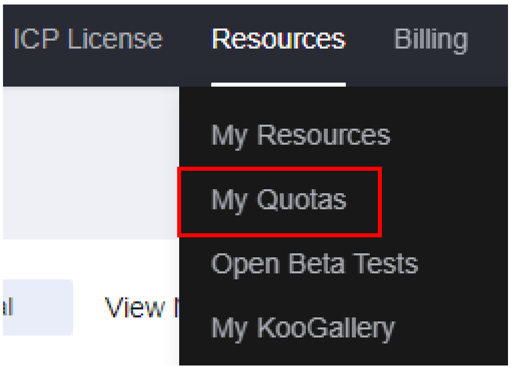
   

3. View the used and total quota of each type of CDN resources on the displayed page.

How Do I Apply for a Higher Quota?

1. Log in to Huawei Cloud console. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.
2. In the upper right corner of the page, choose **Resources** > **My Quotas**. The **Service Quota** page is displayed.

Figure 1-2 My Quotas



3. Click **Increase Quota**.
4. On the **Create Service Ticket** page, configure parameters as required.

   In the **Problem Description** area, fill in the content and describe why you need the adjustment.
5. After all mandatory parameters are configured, select **I have read and agree to the Tenant Authorization Letter and Privacy Statement** and click **Submit**.

   You can click **My Service Ticket** to view the service tickets you have submitted.

2 Custom Domain Name Configuration

2.1 Overview

After adding a domain name, you can customize the domain name to improve pull efficiency, website security, and cache hit ratio. Custom configuration items include OBS authorization, configuration replication, basic settings, origin settings, HTTPS settings, cache settings, access control, and advanced settings.

- IP addresses belong to carriers and change irregularly. Although Huawei Cloud periodically updates the IP address library, the update may be delayed. As a result, some **access control** functions may occasionally block or allow requests, or client requests may not be scheduled to the optimal PoP.

OBS Authorization

This item is mandatory when the origin server is an OBS private bucket.

Item	Description
OBS Authorization	If you use a Huawei Cloud OBS private bucket as the origin server, enable OBS authorization so that CDN can pull content from this bucket.

Basic Settings

You can configure the settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned by CDN.

Item	Description
Modifying 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.

Item	Description
Modifying the 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.
Modifying the 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.
Allowing Clients to Access CDN Using IPv6	To allow users to access CDN PoPs using IPv6, enable IPv6 on the CDN console.

Origin Settings

You can configure the settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned by CDN.

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.

Item	Description
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

You can configure the settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned by CDN.

Function	Description
Configuring an HTTPS Certificate	You can add a certificate for HTTPS acceleration.
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.
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

You can configure the settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned by CDN.

Item	Description
PoP Cache Rules	- 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

You can configure the settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned by CDN.

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.
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.

Advanced Settings

You can configure the settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned by CDN.

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.
WebSocket	If you have enabled whole site acceleration in scenarios such as on-screen commenting, collaborative session, market data broadcast, sports live update, online education, and IoT, you can configure WebSocket to implement long-term bidirectional data transmission.
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

You can configure the settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned by CDN.

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.

Constraints

By default, an account administrator has all permissions. You do not need to add permissions when configuring an agency as an account administrator. IAM users can enable OBS authorization only when they have the following permissions:

IAM permissions

- iam:agencies:listAgencies
- iam:agencies:createAgency
- iam:permissions:grantRoleToAgencyOnProject

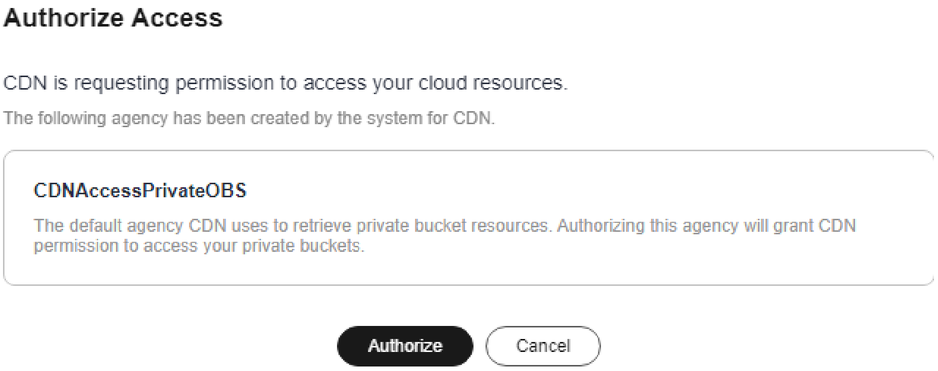
CDN permissions

- cdn:configuration:modifyChargeMode
- CDN ReadOnlyAccess

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.

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:cmk:get** and **kms:dek:crypto** policies to the CDNAccessPrivateOBS agency so that CDN can read and accelerate delivery of the encrypted files.

5. **(Optional)** Assign the **kms:cmk:get** and **kms:dek:crypto** policies 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. Click **Create Policy** in the upper right corner and set the parameters as follows:
      - **Policy Name**: Enter a custom name.
      - **Policy View**: Select **Visual editor**.

- **Policy Content**:
  - Select **Allow**.
  - Service: Select **Key Management Service**.
  - Actions: Select **kms:cmk:get** and **kms:dek:crypto**.
  - Resources: Select **All**.

e. Click **Next**.

f. Select the policy created in the previous step and click **Next**.

g. Set **Scope** to **Region-specific projects** and select the region based on the region of the OBS bucket.

h. Click **OK**.

2.3 Basic Settings

2.3.1 Overview

After adding domain name to CDN, you can modify its service area, service type, or origin server information under the **Basic Settings** tab to meet changing service requirements.

- You can modify basic settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned.

Item	Description
Modifying 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.
Modifying the 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.
Modifying the 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.
Allowing Clients to Access CDN Using IPv6	To allow users to access CDN PoPs using IPv6, enable IPv6 on the CDN console.

2.3.2 Modifying the 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.

Precautions

- 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.

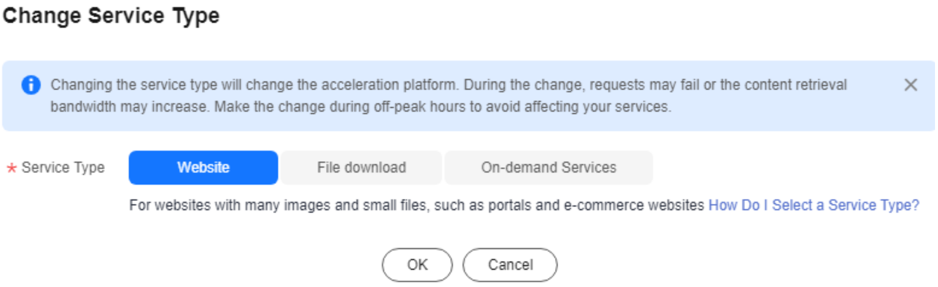
Procedure

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

Changing the service type will change the acceleration platform. During the change, requests may fail or the content retrieval bandwidth may increase. Make the change during off-peak hours to avoid affecting your services.

* Service Type: Website | File download | On-demand Services

For websites with many images and small files, such as portals and e-commerce websites How Do I Select a Service Type?

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

2.3.3 Modifying Origin Server Settings

An origin server hosts your website content. CDN accelerates delivery of such content. You can modify the origin server details, such as the IP address, domain name, and origin port, on the origin server settings page.

CDN Origin Pull Mechanism

- 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 high-priority IP addresses. If origin pull fails, the request is then forwarded to up to two low-priority IP addresses. If four attempts fail, the request fails.
  - Origin pull fails when the connection times out, the connection fails, or a 5*xx* error code is returned from the origin server.
- If an origin domain name resolves to multiple IP addresses, CDN attempts to pull content from up to two of these addresses. If both are unreachable, it will try other origin servers.

Precautions

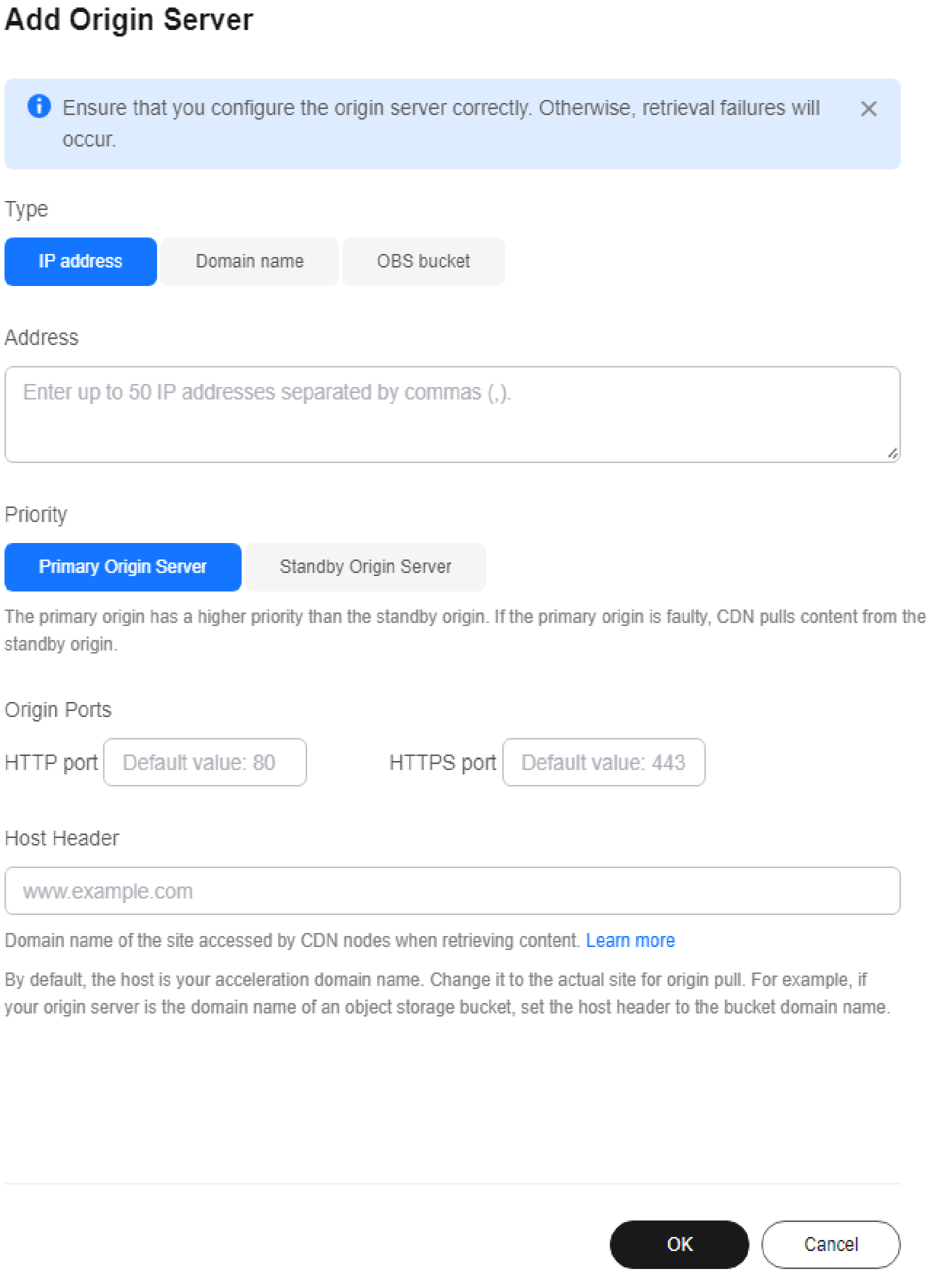
- Ensure that the origin server configuration is correct. Incorrect configuration of the origin server causes origin pull failures.
- If you have modified content on the origin server, refresh the CDN cache.
- When CDN pulls content, the origin server provider charges the bandwidth or traffic fees generated by the origin server. For example, the traffic generated when CDN pulls content from OBS is charged by OBS.

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

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

Type

Address

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

Priority

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: Default value: 80

HTTPS port: Default value: 443

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.

Table 2-1 Parameters

Parameter	Description
Type	**IP address** ● If an IP address is used as the origin address, CDN PoPs access the IP address directly to pull origin content. ● IPv4 is supported, but IPv6 is not supported. ● If multiple IP addresses are configured for the origin server, CDN uses the **load balancing mechanism** to pull content.

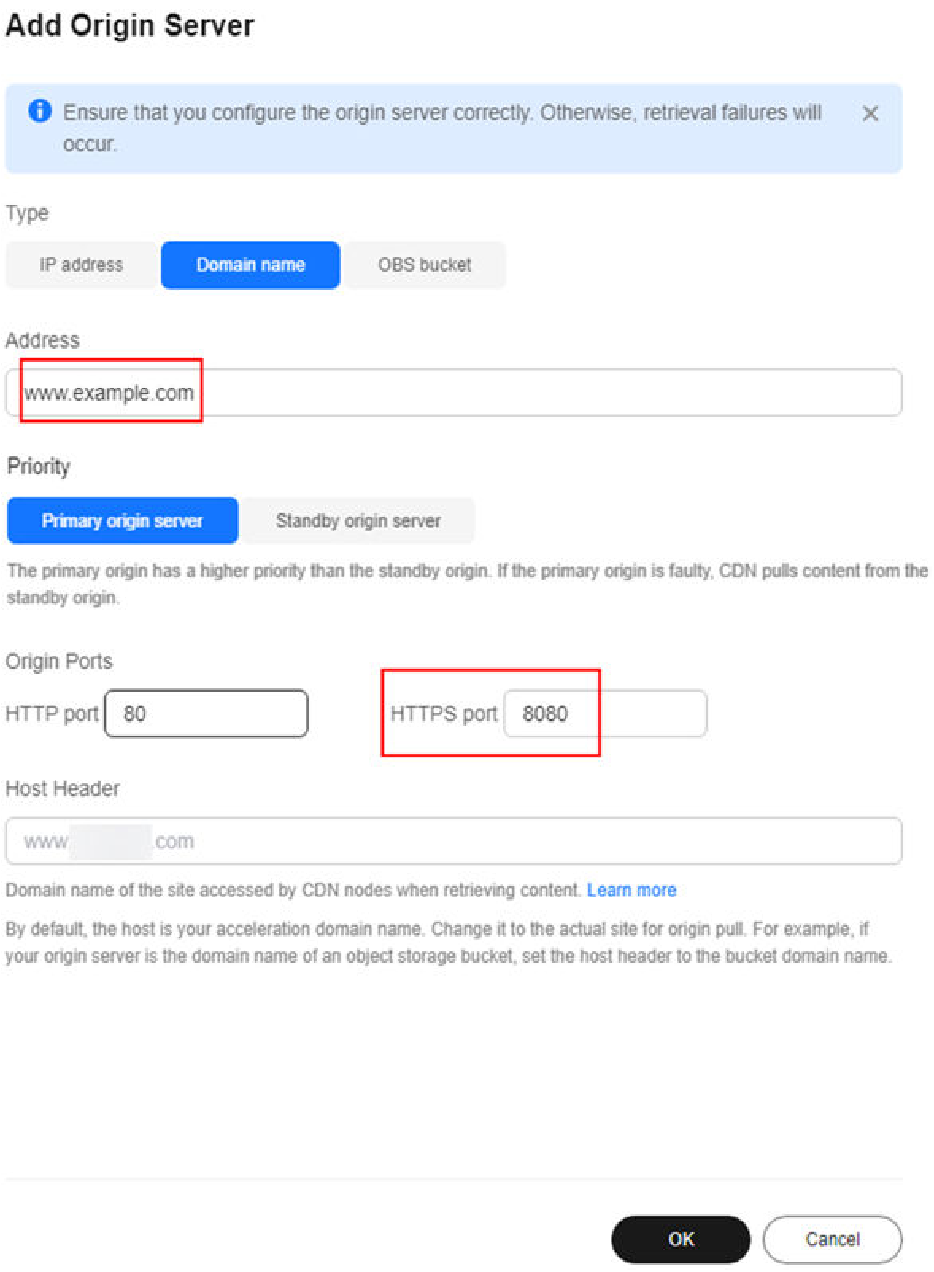
Parameter	Description
	Domain name ● The origin domain cannot be the same as the acceleration domain name. Otherwise, user requests will be repeatedly resolved to CDN PoPs, and CDN PoPs will not be able to obtain content from the origin server. ● An origin domain starts with a letter or digit and contains up to 255 characters, including letters, digits, hyphens (-), and periods (.). ● You can also enter the domain name of an object storage bucket in this field. **NOTE** ● **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 its billing standards.
	OBS bucket You can select the domain name of an OBS bucket under your account or customize one (OBS bucket under other Huawei Cloud accounts). **Important notes:** 1. If your OBS private bucket is unsuitable as an origin for your domain name, do not set the private bucket as the origin server. 2. If an OBS private bucket is configured as an origin server, enable **OBS authorization** and select the **Private bucket** option. Otherwise, origin pull will fail. 3. 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. 4. If OBS buckets are configured as origin servers for CDN, OBS charges the traffic for pulling content from the OBS buckets. 5. 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	This parameter is mandatory when **Type** is set to **OBS bucket**. ● **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	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. ● If only the primary and standby origin servers are configured: – CDN pulls content from the primary origin server first. When the primary server is faulty, CDN pulls content from the standby origin server. This helps reduce origin pull failures. – Configure at least one primary origin server. ● If you have configured a custom priority: – 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	The value ranges from 1 to 100. A larger value indicates a larger number of times that content is pulled from this origin server. ● If there are multiple origin servers with the same priority, the weight determines the proportion of content pulled from each origin server.
Origin Ports	Port numbers for CDN PoPs to pull content. By default, the HTTP port is 80 and the HTTPS port is 443. ● If **Type** is set to **OBS bucket**, the port numbers cannot be changed.
Host Header	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. 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: ● 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

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

Type: IP address | **Domain name** | OBS bucket

Address: www.example.com

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: 80

HTTPS port: 8080

Host Header: www.[redacted].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.

2.3.4 Modifying the 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.
- The actual host of a wildcard domain name is the domain name accessed by users, even though the default host is listed as the wildcard domain name itself.
- Do not set the host to a wildcard domain name for an acceleration domain that is not a wildcard domain name, as this will result in an invalid host.
- When a Huawei Cloud OBS bucket is used as an origin server, the bucket's domain name is used as the host by default. To use a custom host, ensure that the host has been added as a **user domain name** of the bucket. Or, bucket access will fail.

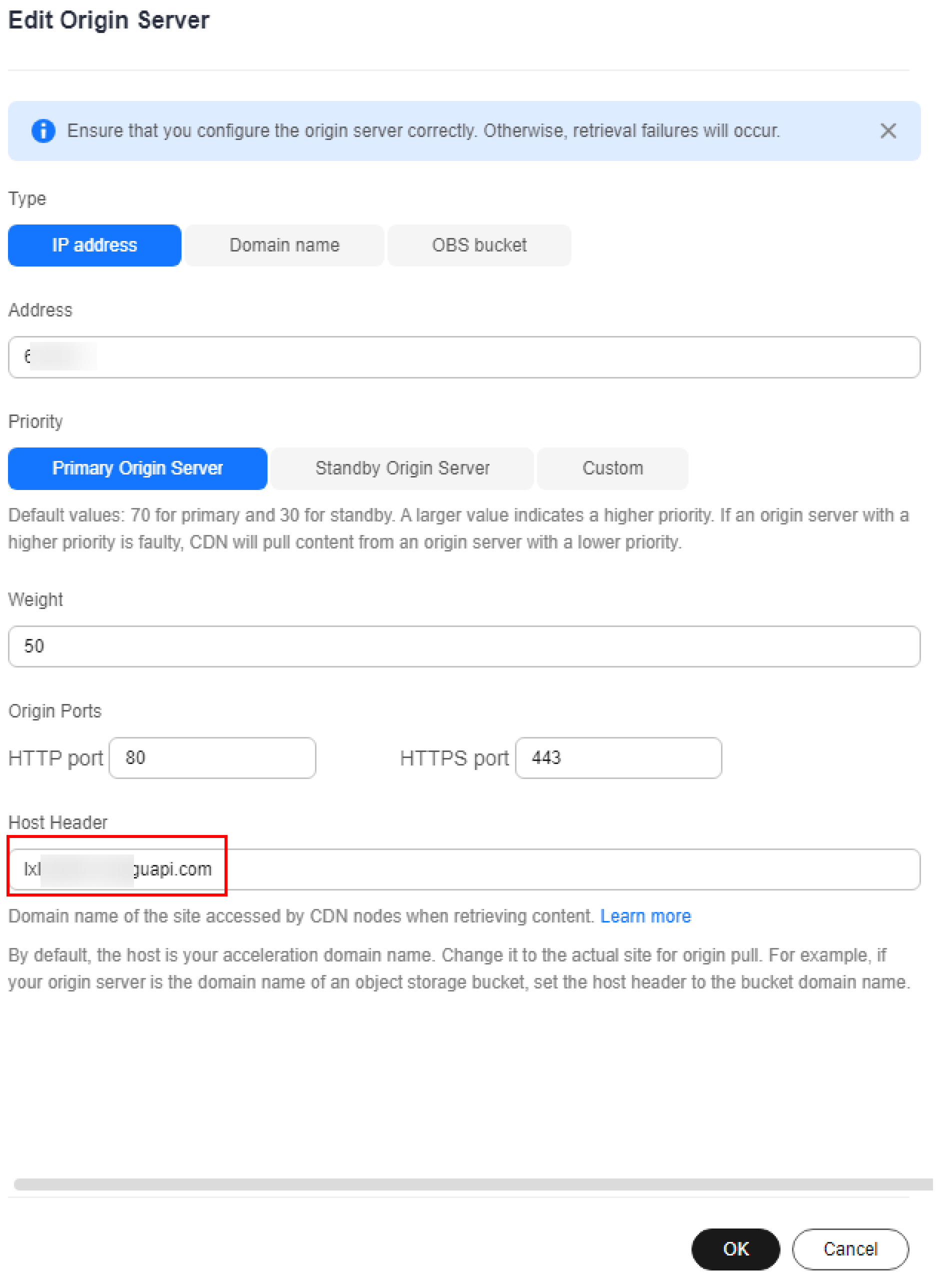
- If you set your origin server address as a domain name, and specify the domain name as that of an object storage bucket, set the host to the domain name of your object storage bucket. Otherwise, the origin pull fails.

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

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

Type: IP address (selected) | Domain name | OBS bucket

Address: 6[redacted]

Priority: Primary Origin Server (selected) | 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[redacted]guapi.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.

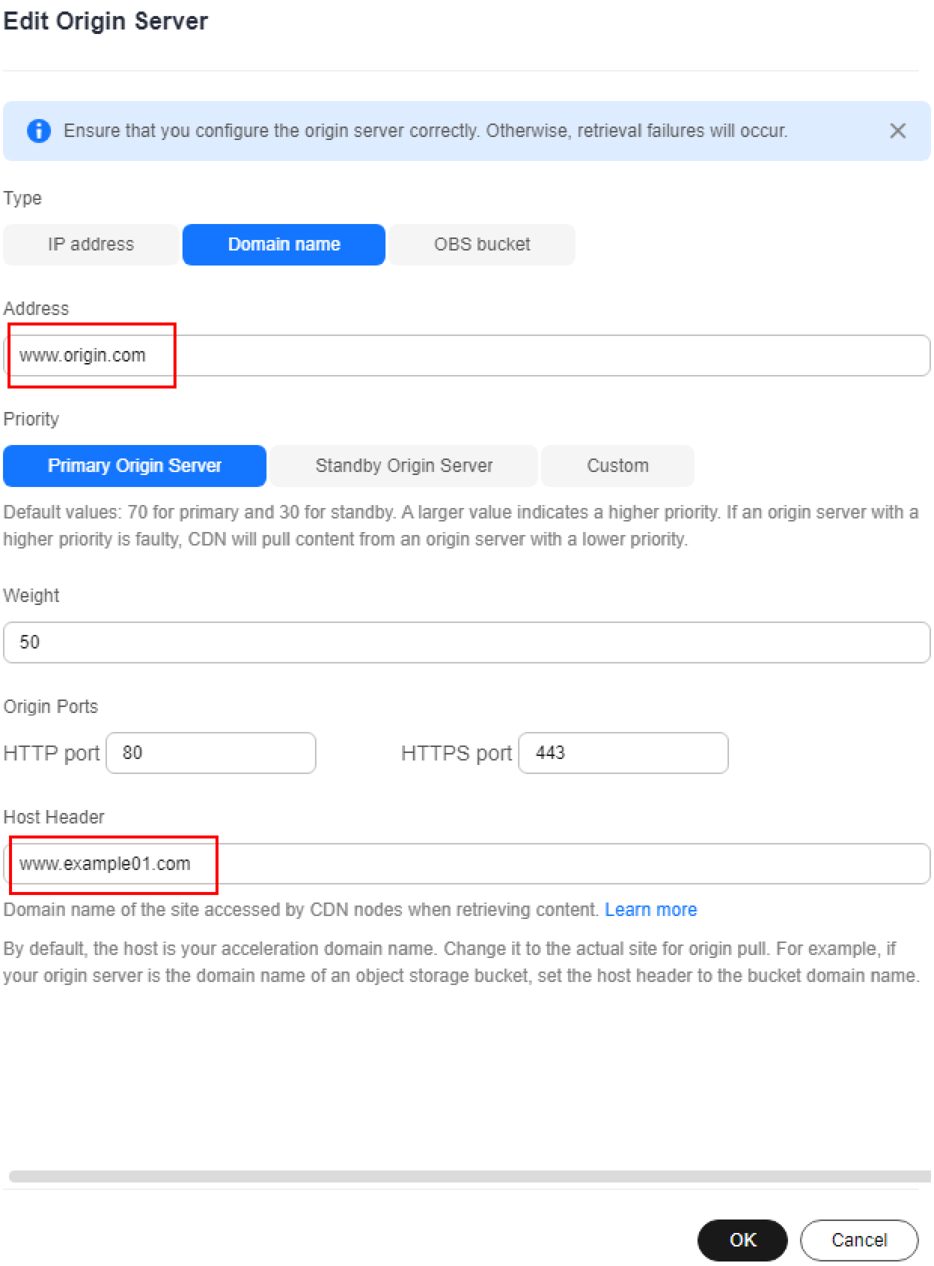
5. Enter the domain name of the host and click **OK**.
6. To edit host headers in a batch, click **Edit** above the origin server list.
   - In the **Host Header** column, modify the information and click **Save**.

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

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: 80 HTTPS port: 443

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.

2.3.5 Allowing Clients to Access CDN Using IPv6

You can enable IPv6 to allow clients to access CDN PoPs using the IPv6 protocol. 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.

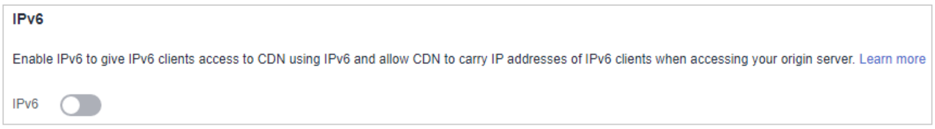
Procedure

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

   IPv6

   Enable IPv6 to give IPv6 clients access to CDN using IPv6 and allow CDN to carry IP addresses of IPv6 clients when accessing your origin server. Learn more

   IPv6

   NOTE

   After IPv6 is enabled on the CDN console, if the origin server does not support IPv6 access, CDN pulls content using IPv4.

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.

CDN Origin Pull Principle

1. An end user initiates a request when visiting a website. DNS resolution points the URL requested by the client (such as a browser) to the acceleration domain name.
2. The CDN PoP searches the cache. If the resource has been cached on the CDN PoP, the PoP returns the resource to the client.
3. **The CDN PoP initiates a pull request** to the origin server based on the origin pull policy of the domain name if the requested resource is not cached on the PoP.
4. **The origin server returns the requested resource** to the PoP based on the requested URL and parameters.
5. The PoP returns the resource to the client. It also caches the resource for future requests from clients.

Supported Configuration Items

- You can modify origin settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned.

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 during origin pull.
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.
Dynamic Content Pull Mode	By default, CDN pulls dynamic content from the origin server with the best performance. You can choose to pull content from origin servers based on their weights.

2.4.2 Origin Protocol

You can configure the protocol used for origin pull.

Precautions

- By default, CDN uses HTTP for origin pulls.
- 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.

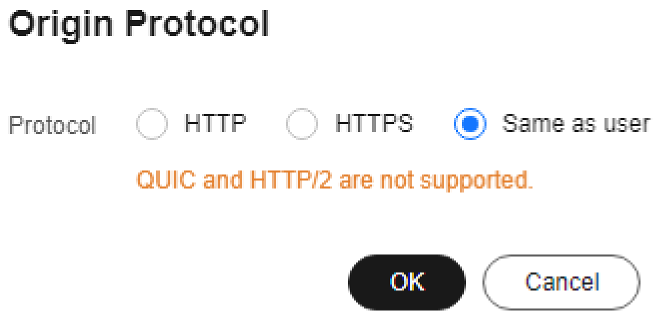
Procedure

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.

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 during origin pull.

Constraints

- 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 whole site acceleration.

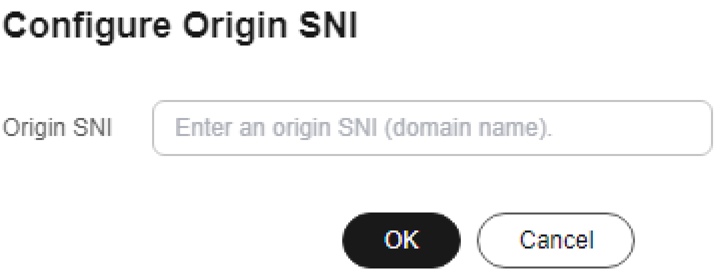
- The origin SNI cannot be set for domain names with special configurations.
- By default, CDN PoPs carry the SNI information when they pull origin content using HTTPS. If no origin SNI is configured, the host is used.

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 **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: Enter an origin SNI (domain name).

   Table 2-3 Parameters

Parameter	Description
Origin SNI	Origin domain name to be accessed by CDN during origin pull, for example, **test.example.com**. ● Wildcard domains are not supported. ● The value contains up to 75 characters, including letters, digits, hyphens (-), and periods (.). It cannot start with a hyphen (-) or period (.).

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 origin server URLs, 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.

Constraints

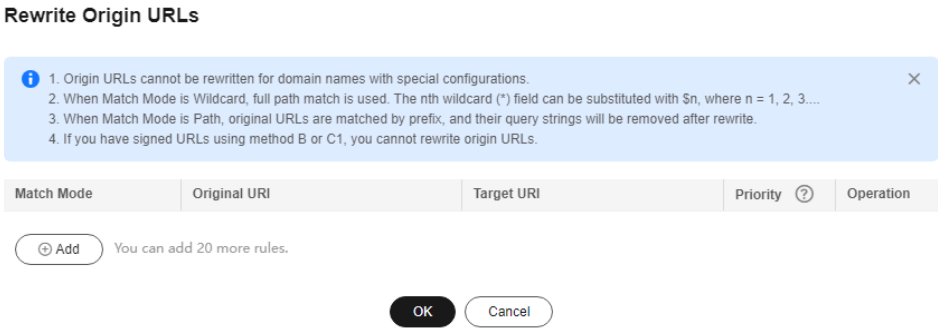
- You can add up to 20 URL rewrite rules.
- This function is not available if you have signed URLs using method B or C1.
- If the service type of your domain name is whole site acceleration, this function takes effect only for static resources.

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 URL Rewrite** area, click **Edit**.

Figure 2-7 Rewriting origin URLs



Rewrite Origin URLs

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

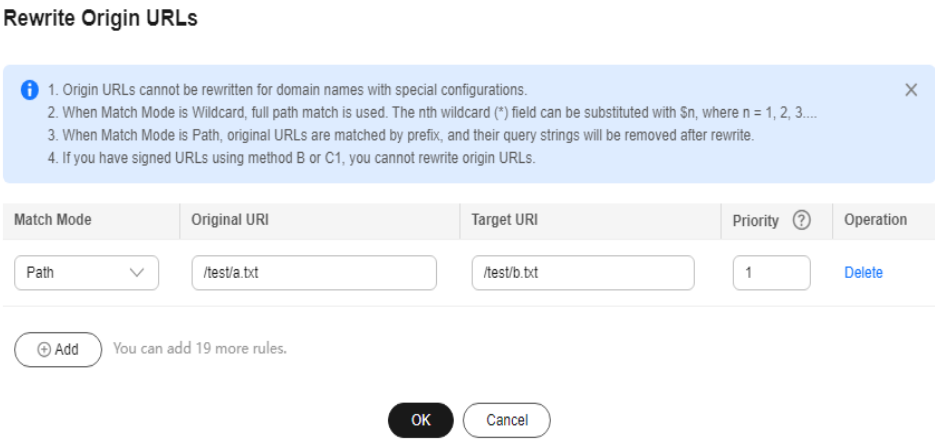
Table 2-4 Parameter description

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**.

Parameter	Description
	Full path: Rewrites the entire URL. The original URI must be a specific path, for example, **/test/01/abc.mp4**.
Original URI	URI to be rewritten. ● 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.
Target URI	URI after rewrite. ● 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 *n*th wildcard (*) field can be substituted by $*n*, where n = 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 $*n*.
Priority	Priority of a URL rewrite rule. ● 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

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.

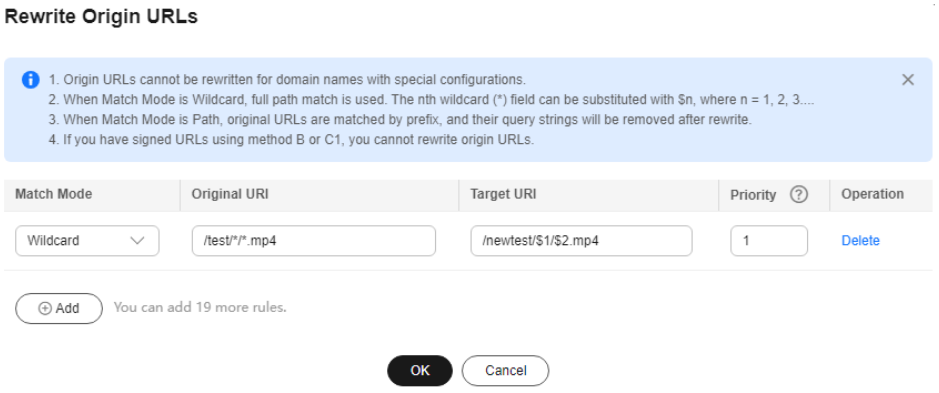
Match Mode	Original URI	Target URI	Priority	Operation
Path	/test/a.txt	/test/b.txt	1	Delete

You can add 19 more rules.

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

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.

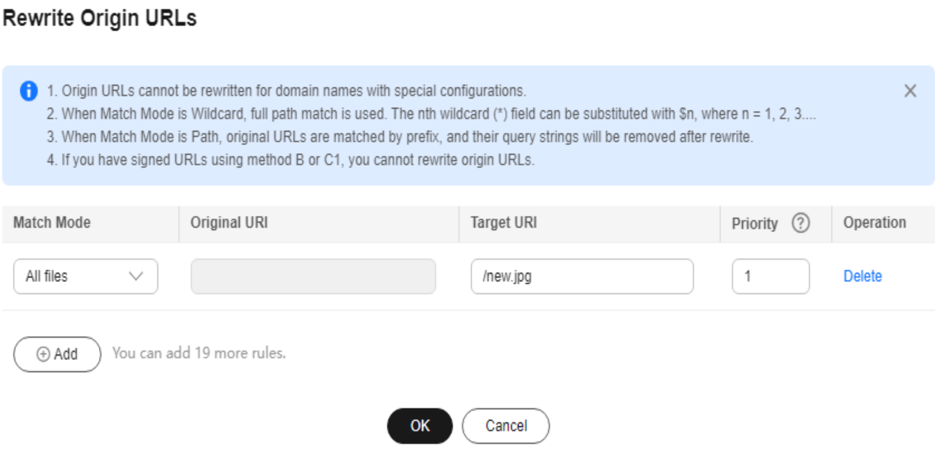
Match Mode	Original URI	Target URI	Priority	Operation
Wildcard	/test/*/*.mp4	/newtest/$1/$2.mp4	1	Delete

You can add 19 more rules.

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

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.

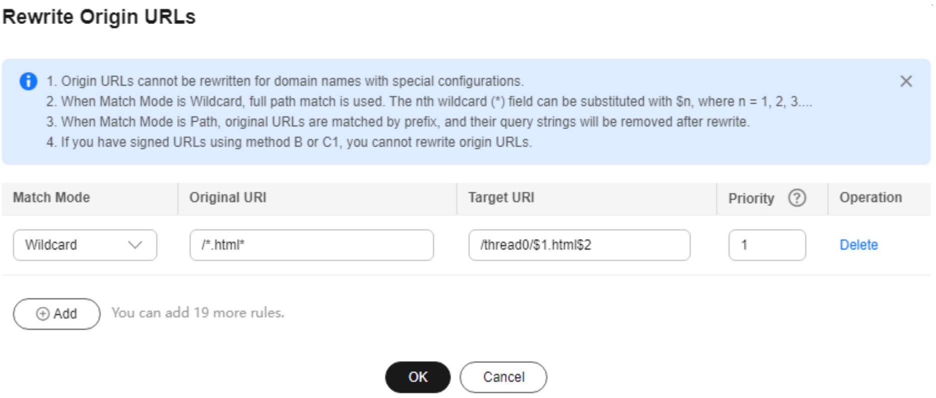
Match Mode	Original URI	Target URI	Priority	Operation
All files		/new.jpg	1	Delete

You can add 19 more rules.

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

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

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

Basic origin: origin server configured when you add a domain name to CDN. It is the default address of origin pulls for user requests.

Advanced origin: origin server from which CDN pulls content when a user request URL matches the resource type or path rule of this server.

Constraints

- You can configure up to 20 rules.
- Domain names whose service type is whole site acceleration do not support this function.

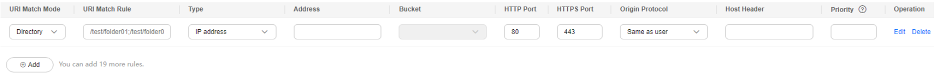
Procedure

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 **Advanced Origin** area, click **Edit**.

6. Click **Add** to add an advanced origin rule

Figure 2-8 Advanced origins



URI Match Mode	URI Match Rule	Type	Address	Bucket	HTTP Port	HTTPS Port	Origin Protocol	Host Header	Priority	Operation
Directory	/test/folder01;/test/folder0	IP address			80	443	Same as user			Edit Delete

Table 2-5 Parameter description

Parameter	Description
URI Match Mode	URIs can be matched by **All files**, **File name extension**, and **Directory**.
URI Match Rule	● **All files**: All requested resources are pulled from the configured advanced origin server. Exercise caution when selecting this option. ● **File name extension** – All file types are supported. – Start with a period (.) and separate multiple extensions by 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 (;). Spaces are not allowed. Enter up to 20 directories and up to 512 characters. Example: **/test/folder01;/test/folder02** **NOTE** If you have signed URLs using method B or C1, URIs cannot be matched by **Directory**.
Type	Select **IP address**, **Domain name**, or **OBS bucket**.

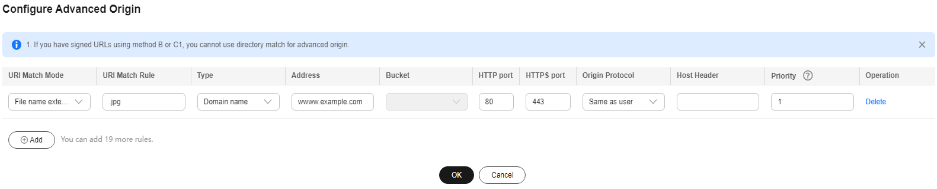
Parameter	Description
Address	**IP address** - Enter an IPv4 address. **Domain name** - Start with a letter or digit. Enter up to 255 characters, including letters, digits, hyphens (-), and periods (.). - Third-party public object storage buckets can be accessed using their domain names. **OBS bucket** - 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**. NOTE - You cannot add an OBS bucket if the domain name has special configuration.
HTTP Port	Port number for origin pull using HTTP. - 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.
HTTPS Port	Port number for origin pull using HTTPS. - 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	Protocol used by CDN PoPs to pull content from the origin server. **HTTP**: CDN uses HTTP for origin pull. **HTTPS**: CDN uses HTTPS for origin pull. (Ensure that the origin server supports HTTPS access.) **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.
Host Header	Host information of the advanced origin. For details, see **Modifying the Host Header**. - 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.

Parameter	Description
Bucket	This parameter is mandatory when **Type** is set to **OBS bucket**. ● **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	The priority value ranges from 1 to 100. The larger the value, the higher the priority.
Operation	**Delete**: Delete the rule.

7. Configure parameters and click **OK**.

Example

Example: Assume that you have configured an advanced origin for domain name wwww.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	wwww.example.com		80	443	Same as user		1	Delete

You can add 19 more rules.

Configuration result: When a user requests an uncached JPG resource, CDN pulls the resource from the origin server wwww.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.

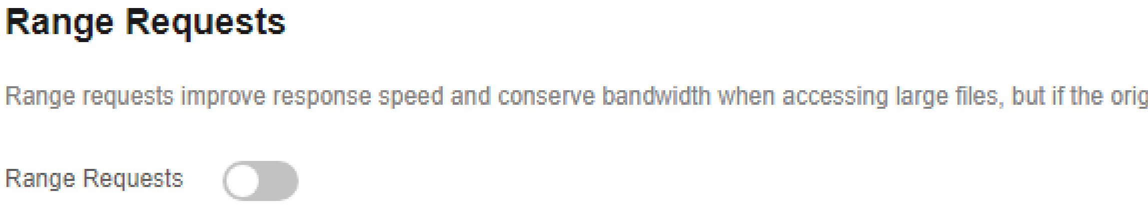
- By default, range requests are enabled for file download acceleration and on-demand service acceleration.
- If an origin server resource exceeds 1 GB and range requests are not enabled, origin pull for such resource will fail.
- If the service type of your domain name is whole site acceleration, this function takes effect only for static resources.

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 orig

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

  The 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

  The 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.

Precautions

If the service type of your domain name is whole site acceleration, this function takes effect only for static resources.

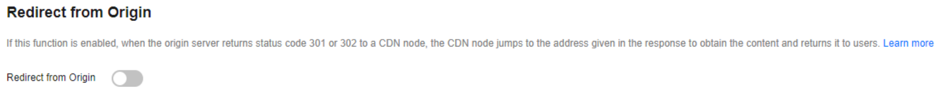
Procedure

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 **Redirect from Origin**.

   Figure 2-10 Configuring redirect from origin

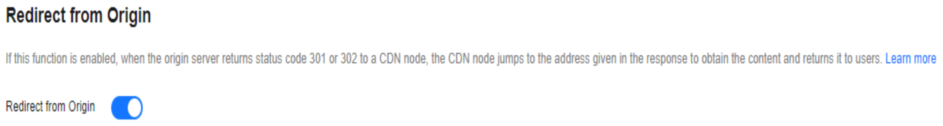
   Redirect from Origin

   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

   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

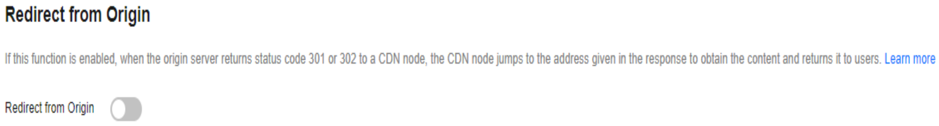
  Redirect from Origin ●

  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.

  a. The PoP directly sends a request to the redirect address.
  b. After obtaining the requested content, the PoP returns the content to the user and caches the content.

c. 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

Redirect from Origin ○

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.

a. 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.

b. 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.

c. 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.
- If range requests are enabled for an acceleration domain name, when the **Last-Modified** values of different segments of an origin resource pulled by CDN PoPs are different, CDN determines that the resource has changed. To avoid returning incorrect resources to clients, CDN interrupts the connection and client access. If similar problems occur, take the following measures:

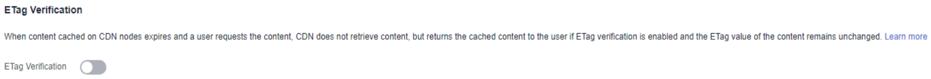
   a. Disable **range requests**.
   b. If resource segments are stored on different origin servers, move them to the same origin server.
   c. Submit a service ticket to disable the verification of the **Last-Modified** value during origin pull.
- If the service type of your domain name is whole site acceleration, this function takes effect only for static resources.

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



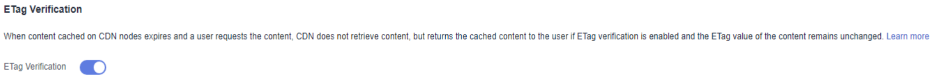
ETag Verification

When content cached on CDN nodes expires and a user requests the content, CDN does not retrieve content, but returns the cached content to the user if ETag verification is enabled and the ETag value of the content remains unchanged. Learn more

ETag Verification ○

Examples

Assume that you have enabled ETag verification for domain name www.example.com.



ETag Verification

When content cached on CDN nodes expires and a user requests the content, CDN does not retrieve content, but returns the cached content to the user if ETag verification is enabled and the ETag value of the content remains unchanged. Learn more

ETag Verification ●

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.

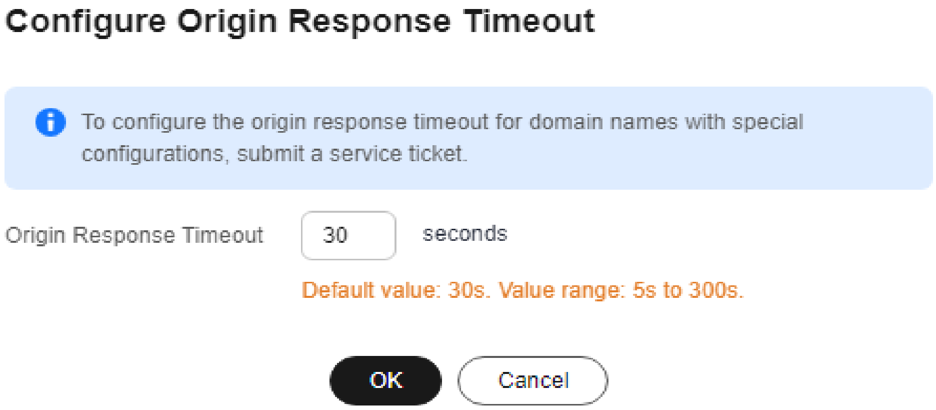
Procedure

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

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

Origin Response Timeout 30 seconds

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

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

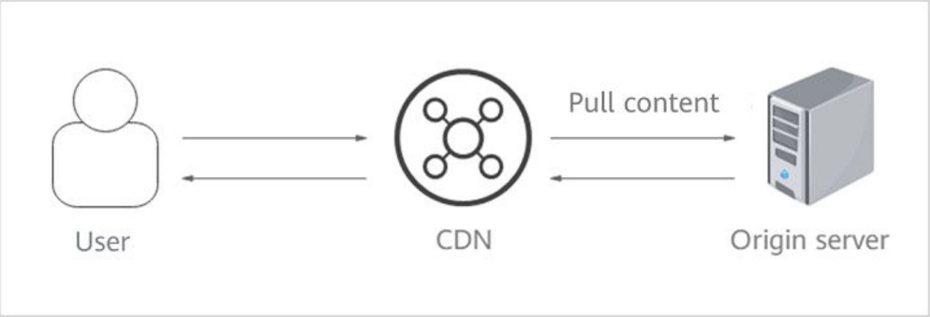
2.4.10 Origin Request Headers

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

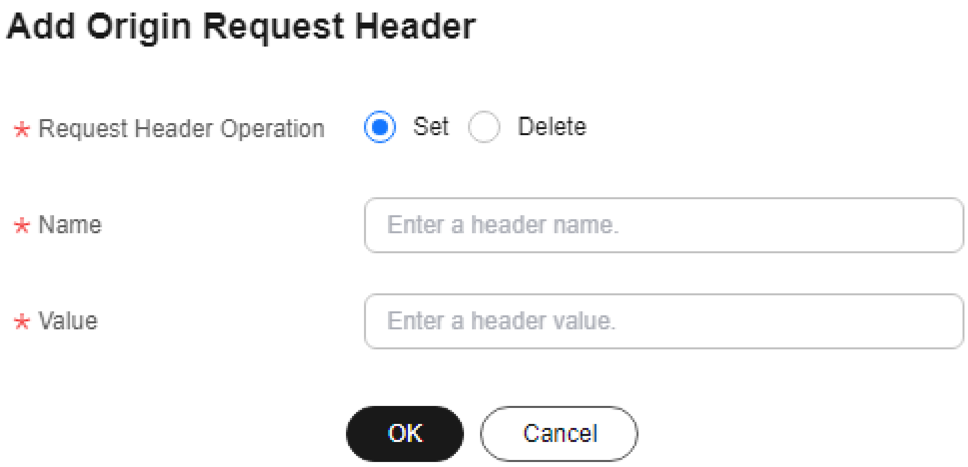
- This setting only modifies HTTP messages for origin pull through CDN. It does not modify those in an HTTP message that CDN PoPs return to users.
- A request header cannot have two different values at the same time.
- If your domain name has special configurations, the origin request headers cannot be configured.
- You can add up to 10 headers.

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: Enter a header name.

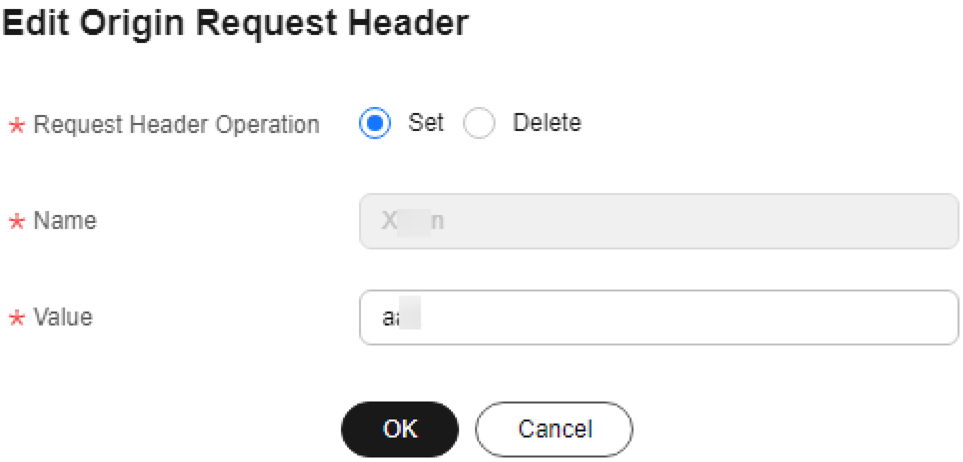
* Value: Enter a header value.

Table 2-6 Parameter description

Parameter	Example	Description
Request Header Operation	Set	Add a specific header to an HTTP request of origin pull. ● 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. ● If a request URL contains the **X-test** header, it will be deleted during origin pull.
Name	X-test	● Enter 1 to 100 characters. ● Start with a letter and use only letters, digits, or hyphens (-).
Value	aaa	● Enter 1 to 1,000 characters. ● Enter letters, digits, and the following special characters: .-_*#!&+|^~'"/:;,=@?<> ● Variables, such as *$client_ip* and *$remote_port*, 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[redacted]n

* Value a[redacted]

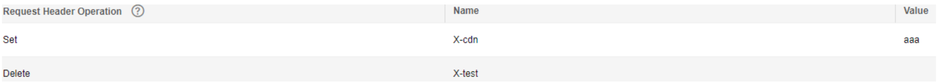
Parameter	Example	Description
Request Header Operation	Set	Add a specific header to an HTTP request of origin pull. ● If a request URL contains the **X-test** header and its value is **111**, CDN will set **X-test** to **aaa** during origin pull. ● If a request URL does not contain the **X-test** header, 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. ● 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	● Enter 1 to 1,000 characters. ● Enter letters, digits, and the following special characters: .-_*#!&+|^~'"/:;,=@?<> ● Variables, such as *$client_ip* and *$remote_port*, 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 that is not cached on CDN, 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.

Constraints

- If your domain name has special configurations, **Content-Type**, **Cache-Control**, and **Expires** cannot be configured.
- The following request headers can only be modified. You cannot set **Request Header Operation** to **Delete** for them.

Expires	Content-Disposition

Content-Type	Content-Language
Cache-Control	-

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

a_dynamic	cross-origin-embedder-policy	origin	strict-transport-security
accept	cross-origin-opener-policy	ping-from	te
accept-ch	cross-origin-resource-policy	ping-to	timing-allow-origin
accept-charset	date	pragma	tk
accept-ch-lifetime	device-memory	proxy-authenticate	trailer
accept-push-policy	dnt	proxy-authorization	transfer-encoding
accept-ranges	dpr	public-key-pins	upgrade
accept-signature	early-data	public-key-pins-report-only	upgrade-insecure-requests
access-control-allow-credentials	etag	push-policy	vary
access-control-allow-headers	expect	range	via
access-control-allow-methods	expect-ct	referer-policy	viewport-width
access-control-allow-origin	feature-policy	report-to	warning
access-control-expose-headers	forwarded	retry-after	width
access-control-max-age	from	save-data	www-authenticate
access-control-request-headers	host	sec-fetch-dest	x-client-ip
access-control-request-method	if-match	sec-fetch-mode	x-content-type-options
age	if-modified-since	sec-fetch-site	x-dns-prefetch-control
allow	if-none-match	sec-fetch-user	x-download-options

alt-svc	if-range	sec-websocket-accept	x-firefox-spdy
authorization	if-unmodified-since	sec-websocket-extensions	x-forwarded-for
clear-site-data	keep-alive	sec-websocket-key	x-forwarded-host
connection	large-allocation	sec-websocket-protocol	x-frame-options(xfo)
content-dpr	last-event-id	sec-websocket-version	x-permitted-cross-domain-policies
content-encoding	last-modified	server	x-pingback
content-length	link	server-timing	x-powered-by
content-location	location	service-worker-allowed	x-requested-with
content-range	max-age	signature	x-robots-tag
content-security-policy	max-forwards	signed-headers	x-ua-compatible
content-security-policy-report-only	nel	sourcemap	x-xss-protection

2.4.11 Dynamic Content Pull Mode

This mode is used by CDN whole site acceleration to pull dynamic content from the origin server. CDN calculates the optimal route based on intelligent and real-time dynamic routing, improving network transmission stability and rate. You can choose to pull content from origin servers based on their weights.

Precautions

The default pull mode for dynamic content is **By performance**.

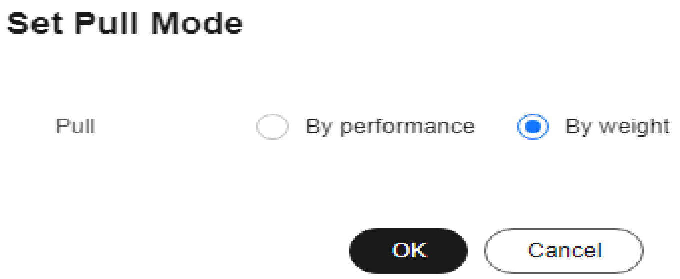
Procedure

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 **Dynamic Content Pull Mode** area, click **Edit**.

Figure 2-15 Dynamic content pull mode



Set Pull Mode

Pull ○ By performance ● By weight

Table 2-7 Parameters

Pull Mode	Description
By performance	Default mode. CDN pulls content from the origin server with the shortest latency calculated through dynamic routing. This improves user experience, but cannot implement load balancing.
By weight	CDN pulls content from all origin servers weighted as configured, ensuring load balancing.

6. Select a pull mode and click **OK**.

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.

- You can configure a domain name certificate for CDN PoPs. Then clients can use HTTPS to access CDN PoPs. If you want CDN to use HTTPS for origin pull, configure an HTTPS certificate for your origin server.
- You can modify certificate settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned.

Function	Description
SCM Authorization	An SCM agency is required for SCM certificate configuration, so that you can directly obtain the certificate content when configuring SCM certifications in CDN.
Configuring an HTTPS Certificate	You can add a certificate on CDN PoPs to allow clients to access PoPs using HTTPS.
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 Transport Layer Security (TLS) versions as required.
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 configure force redirect to HTTP or HTTPS for requests from clients to CDN PoPs.
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 SCM Authorization

If your certificate has been uploaded to **Cloud Certificate Manager (CCM)** of Huawei Cloud, you can enable SCM authorization so that you can directly obtain the certificate content when configuring certificates on CDN.

Constraints

1. IAM users can enable SCM authorization only when they have the following permissions.

Associated Cloud Service	Permission
IAM	● iam:roles:listRoles ● iam:roles:createRole ● iam:agencies:listAgencies ● iam:agencies:createAgency ● iam:permissions:grantRoleToAgencyOnDomain
CDN	● cdn:configuration:modifyChargeMode ● CDN ReadOnlyAccess
SCM	scm:cert:list

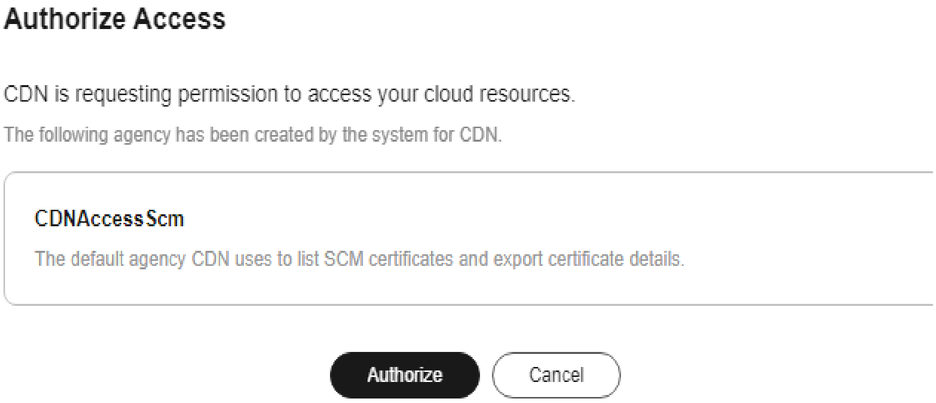
2. After creating an agency, IAM users can configure certificates for domain names when they have the following permissions.
   - cdn:configuration:modifyHttpsConf
   - cdn:configuration:modifyOriginConfInfo

Enabling SCM Authorization

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 page, click **Enable SCM Authorization**.

   Figure 2-16 Cloud resource authorization

   Authorize Access

   CDN is requesting permission to access your cloud resources.

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

   CDNAccessScm

   The default agency CDN uses to list SCM certificates and export certificate details.

4. Click **OK**. The system creates an agency named **CDNAccessScm** for you on the IAM console. CDN now has the permission to list your SCM certificates and export certificate details.

   NOTE

   - Do not delete this agency. Otherwise, CDN cannot obtain certificate content when you configure an HTTPS certificate.

2.5.3 Configuring an HTTPS Certificate

Background

CDN supports HTTPS acceleration. You can configure an HTTPS certificate for an acceleration domain name on the CDN console. Then clients can use HTTPS to access CDN PoPs. The differences between HTTP and HTTPS are as follows:

- **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.

Constraints

- CDN supports your own certificates or SSL Certificate Manager (SCM) certificates. The format of your own certificates must meet the requirements described in **HTTPS Certificate Requirements**.
- 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**.

Precautions

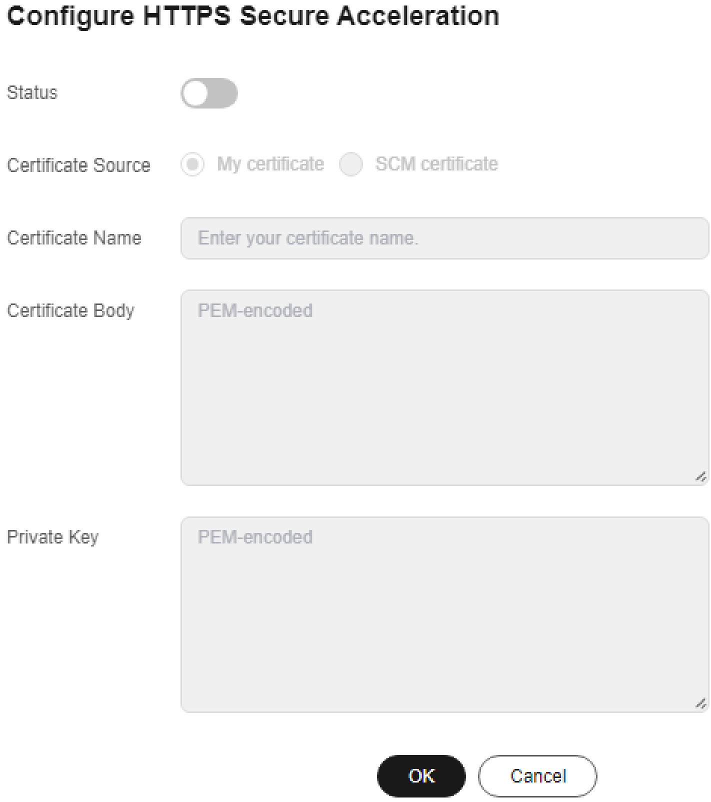
- An acceleration domain name has its associated certificate. They must match. If your domain name is a wildcard domain, configure a certificate for it by referring to
- Certificate settings will be automatically deleted once HTTPS acceleration is disabled. To enable HTTPS acceleration again, you need to re-configure the certificate.
- 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 an HTTPS Certificate

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 2-17 Configuring HTTPS secure acceleration



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

Table 2-8 Parameters of an international certificate

Parameter	Description
Certificate Source	Select **My certificate** or **SCM certificate**.
Certificate Name	● **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	● **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. **NOTE** The certificate body cannot contain spaces or blank lines. Otherwise, a message is displayed indicating that certificate parameters are incorrect.

Parameter	Description
Private Key	- **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. Click **OK**.
9. 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.

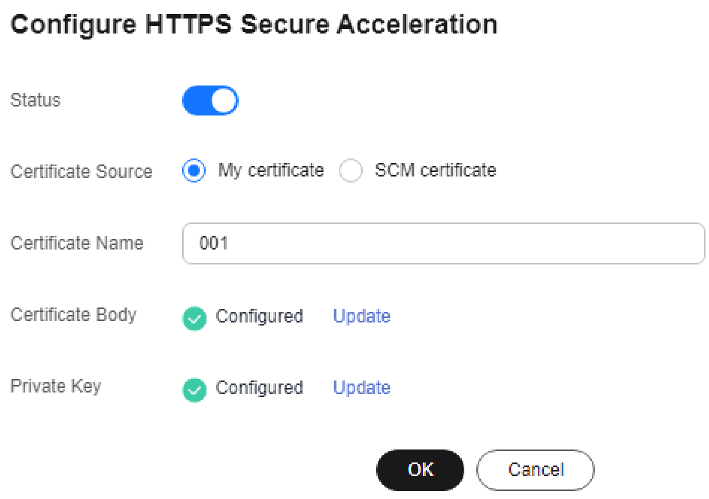
Updating an HTTPS Certificate

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 2-18 Updating a certificate



Configure HTTPS Secure Acceleration

Status: on

Certificate Source: ● My certificate ○ SCM certificate

Certificate Name: 001

Certificate Body: ✓ Configured Update

Private Key: ✓ Configured Update

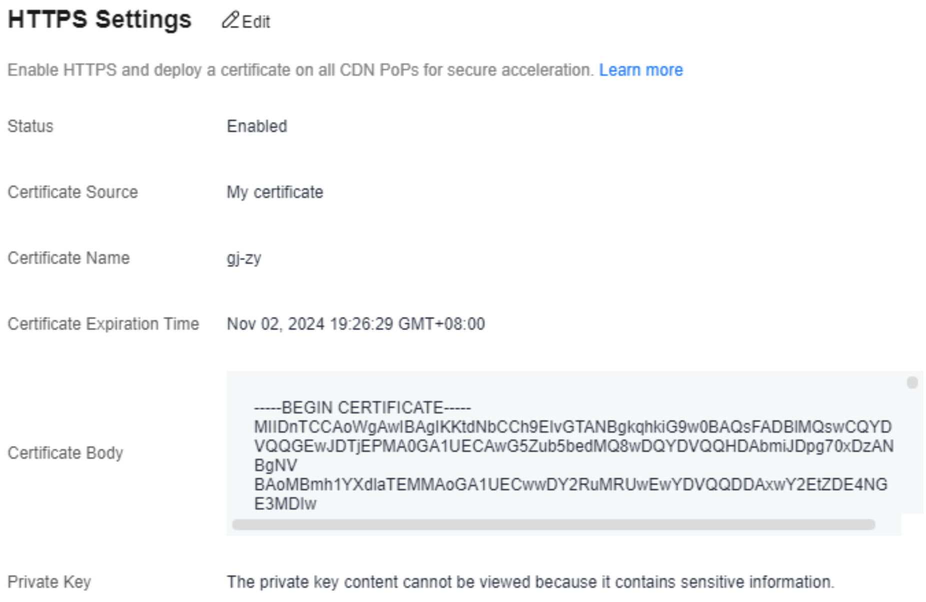
6. Click **Update** to update the configured certificate and private key. It takes approximately 5 to 10 minutes for the update to take effect.

Viewing HTTPS Certificate Information

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

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 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

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
VQQGEwJDTjEPMA0GA1UECAwG5Zub5bedMQ8wDQYDVQQHDAbmiJDpg70xDzAN
BgNV
BAoMBmh1YXdlaTEMMAoGA1UECwwDY2RuMRUwEwYDVQQDDAxwY2EtZDE4NG
E3MDIw
```

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

Disabling a Certificate

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 **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.

2.5.4 HTTPS Certificate Requirements

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

Certificates Issued by Root CA

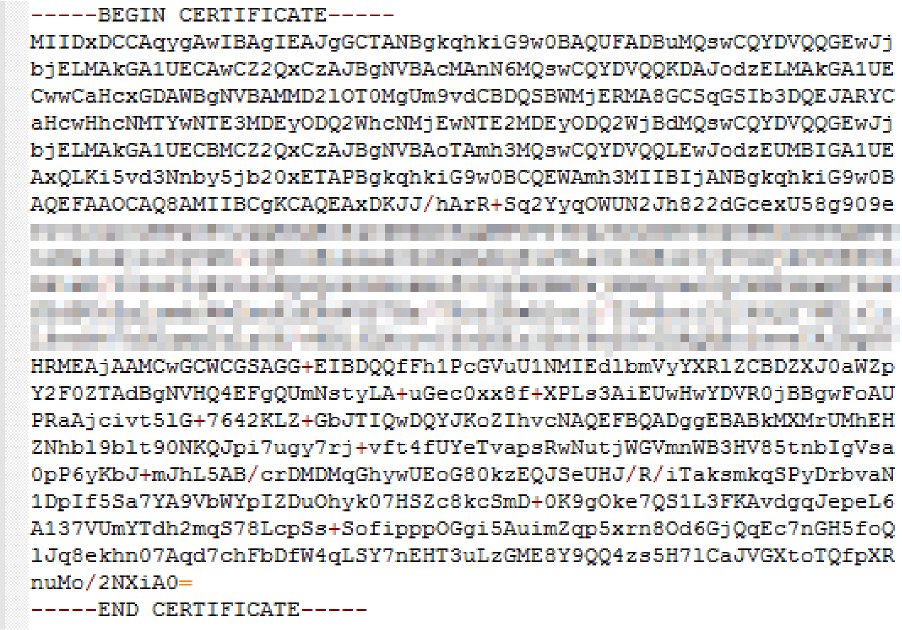
A certificate issued by Root CA is a complete certificate. When configuring HTTPS, you only need to upload the certificate.

Use a text editor to open the certificate. The certificate content should be something similar to what is in **Figure 2-19**.

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 2-19 PEM certificate



```
-----BEGIN CERTIFICATE-----
MIIDxDCCAqygAwIBAgIEAJgGCTANBgkqhkiG9w0BAQUFADBuMQswCQYDVQQGEwJj
bjELMAkGA1UECAwCZ2QxCzAJBgNVBAcMAnN6MQswCQYDVQQKDAJodzELMAkGA1UE
CwwCaHcxGDAWBgNVBAMMD21OT0MgUm9vdCBDQSBWMjERMA8GCSqGSIb3DQEJARYC
aHcwHhcNMTYwNTE3MDEyODQ2WhcNMjEwNTE2MDEyODQ2WjBdMQswCQYDVQQGEwJj
bjELMAkGA1UECBMCZ2QxCzAJBgNVBAoTAmh3MQswCQYDVQQLEwJodzEUMBIGA1UE
AxQLKi5vd3Nnby5jb20xETAPBgkqhkiG9w0BCQEWAmh3MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909e
[redacted]
HRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZp
Y2F0ZTAdBgNVHQ4EFgQUmNstyLA+uGec0xx8f+XPLs3AiEUwHwYDVR0jBBgwFoAU
PRaAjcivt51G+7642KLZ+GbJTIQwDQYJKoZIhvcNAQEFBQADggEBABkMXMrUMhEH
ZNhbl9blt90NKQJpi7ugy7rj+vft4fUYeTvapsRwNutjWGVmnWB3HV85tnbIgVsa
0pP6yKbJ+mJhL5AB/crDMDMqGhywUEoG80kzEQJSeUHJ/R/iTaksmkqSPyDrbvaN
1DpIf5Sa7YA9VbWYpIZDuOhyk07HSZc8kcSmD+0K9gOke7QS1L3FKAvdgqJepeL6
A137VUmYTdh2mqS78LcpSs+SofipppOGgi5AuimZqp5xrn8Od6GjQqEc7nGH5foQ
lJq8ekhn07Aqd7chFbDfW4qLSY7nEHT3uLzGME8Y9QQ4zs5H7lCaJVGXtoTQfpXR
nuMo/2NXiA0=
-----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 acceleration. A combined certificate is shown as **Figure 2-20**.

Use a text editor to open all of the PEM 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:

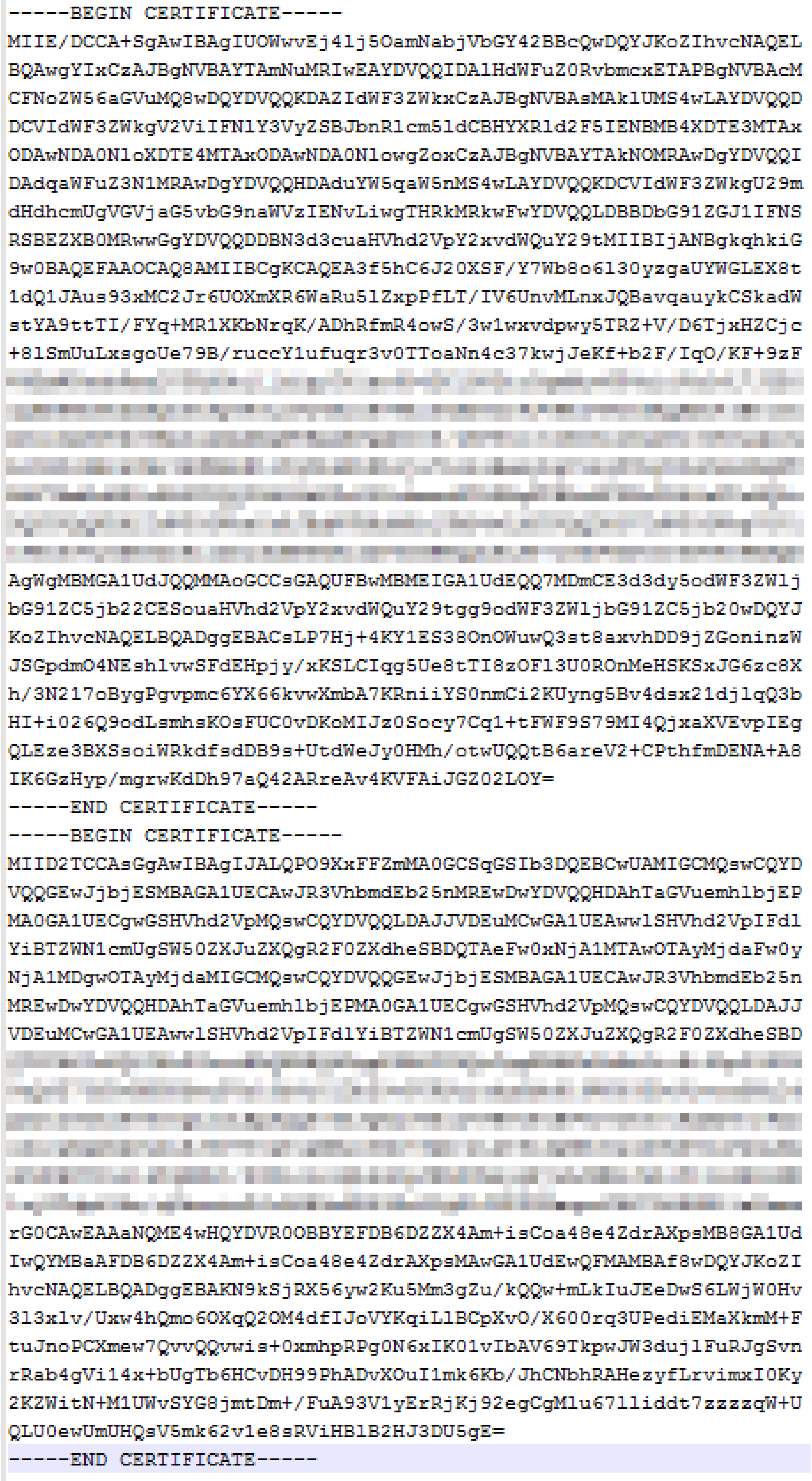
  -----BEGIN CERTIFICATE-----

  -----END CERTIFICATE-----

  -----BEGIN CERTIFICATE-----

  -----END CERTIFICATE-----

Figure 2-20 Combined certificate



```
-----BEGIN CERTIFICATE-----
MIIE/DCCA+SgAwIBAgIUOWwvEj4lj5OamNabjVbGY42BBcQwDQYJKoZIhvcNAQEL
BQAwgYIxCzAJBgNVBAYTAmNuMRIwEAYDVQQIDAlHdWFuZ0RvbmcxETAPBgNVBAcM
CFNoZW56aGVuMQ8wDQYDVQQKDAZIdWF3ZWkxCzAJBgNVBAsMAklUMS4wLAYDVQQD
DCVIdWF3ZWkgV2ViIFNlY3VyZSBJbnRlcm5ldCBHYXRld2F5IENBMB4XDTE3MTAx
ODAwNDA0NloXDTE4MTAxODAwNDA0NlowgZoxCzAJBgNVBAYTAkNOMRAwDgYDVQQI
DAdqaWFuZ3N1MRAwDgYDVQQHDAduYW5qaW5nMS4wLAYDVQQKDCVIdWF3ZWkgU29m
dHdhcmUgVGVjaG5vbG9naWVzIENvLiwgTHRkMRkwFwYDVQQLDBBDbG91ZGJ1IFNS
RSBEZXB0MRwwGgYDVQQDDBN3d3cuaHVhd2VpY2xvdWQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3f5hC6J20XSF/Y7Wb8o6l30yzgaUYWGLEX8t
1dQ1JAus93xMC2Jr6UOXmXR6WaRu5lZxpPfLT/IV6UnvMLnxJQBavqauykCSkadW
stYA9ttTI/FYq+MR1XKbNrqK/ADhRfmR4owS/3w1wxvdpwy5TRZ+V/D6TjxHZCjc
+8lSmUuLxsgoUe79B/ruccY1ufuqr3v0TToaNn4c37kwjJeKf+b2F/IqO/KF+9zF
[redacted]
AgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMEIGA1UdEQQ7MDmCE3d3dy5odWF3ZW1j
bG91ZC5jb22CESouaHVhd2VpY2xvdWQuY29tgg9odWF3ZW1jbG91ZC5jb20wDQYJ
KoZIhvcNAQELBQADggEBACsLP7Hj+4KY1ES38OnOWuwQ3st8axvhDD9jZGoninzW
JSGpdmO4NEshlvwSFdEHpjy/xKSLCIqg5Ue8tTI8zOFl3U0ROnMeHSKSxJG6zc8X
h/3N217oBygPgvpmc6YX66kvwXmbA7KRniiYS0nmCi2KUyng5Bv4dsx21djlqQ3b
HI+i026Q9odLsmhsKOsFUC0vDKoMIJz0Socy7Cq1+tFWF9S79MI4QjxaXVEvpIEg
QLEze3BXSsoiWRkdfsdDB9s+UtdWeJy0HMh/otwUQQtB6areV2+CPthfmDENA+A8
IK6GzHyp/mgrwKdDh97aQ42ARreAv4KVFAiJGZ02LOY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID2TCCAsGgAwIBAgIJALQPO9XxFFZmMA0GCSqGSIb3DQEBCwUAMIGCMQswCQYD
VQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25nMREwDwYDVQQHDAhTaGVuemhlbjEP
MA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAJJVDEuMCwGA1UEAwwlSHVhd2VpIFdl
YiBTZWN1cmUgSW50ZXJuZXQgR2F0ZXdheSBDQTAeFw0xNjA1MTAwOTAyMjdaFw0y
NjA1MDgwOTAyMjdaMIGCMQswCQYDVQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25n
MREwDwYDVQQHDAhTaGVuemhlbjEPMA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAJJ
VDEuMCwGA1UEAwwlSHVhd2VpIFdlYiBTZWN1cmUgSW50ZXJuZXQgR2F0ZXdheSBD
[redacted]
rG0CAwEAAaNQME4wHQYDVR0OBBYEFDB6DZZX4Am+isCoa48e4ZdrAXpsMB8GA1Ud
IwQYMBaAFDB6DZZX4Am+isCoa48e4ZdrAXpsMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAKN9kSjRX56yw2Ku5Mm3gZu/kQQw+mLkIuJEeDwS6LWjW0Hv
3l3xlv/Uxw4hQmo6OXqQ2OM4dfIJoVYKqiLlBCpXvO/X600rq3UPediEMaXkmM+F
tuJnoPCXmew7QvvQQvwis+0xmhpRPg0N6xIK01vIbAV69TkpwJW3dujlFuRJgSvn
rRab4gVi14x+bUgTb6HCvDH99PhADvXOuI1mk6Kb/JhCNbhRAHezyfLrvimxI0Ky
2KZWitN+M1UWvSYG8jmtDm+/FuA93V1yErRjKj92egCgMlu67lliddt7zzzzqW+U
QLU0ewUmUHQsV5mk62v1e8sRViHBlB2HJ3DU5gE=
-----END CERTIFICATE-----
```

RSA Private Key

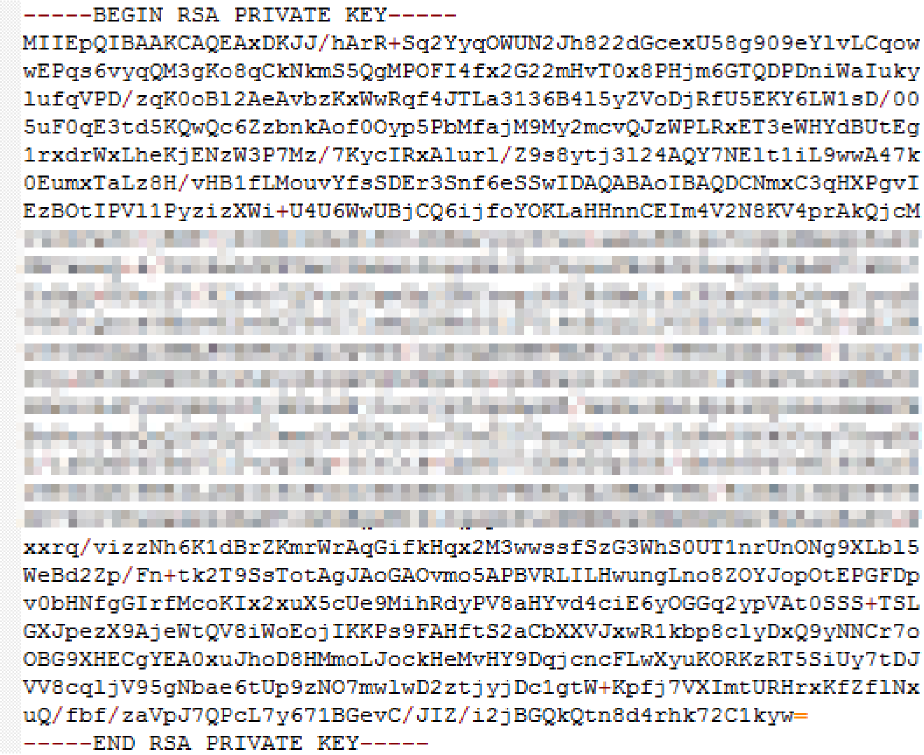
PEM files can contain certificates or private keys. If a PEM file contains only private keys, the file suffix may be replaced by KEY.

Use a text editor to open the private key file in the PEM or KEY format. Then you can view the private key content, as shown in **Figure 2-21**.

Content of an RSA private key:

- The private key starts with the **-----BEGIN RSA PRIVATE KEY-----** statement and ends with the **-----END RSA PRIVATE KEY-----** statement.
- Each line of the private key is 64 characters long, but the last line can be shorter.
- No spaces are allowed in the private key content.

Figure 2-21 RSA private key



```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909eYlvLCqow
wEPqs6vyqQM3gKo8qCkNkmS5QgMPOFI4fx2G22mHvT0x8PHjm6GTQDPDniWaIuky
lufqVPD/zqK0oBl2AeAvbzKxWwRqf4JTLa3136B415yZVoDjRfU5EKY6LW1sD/00
5uF0qE3td5KQwQc6ZzbnkAof0Oyp5PbMfajM9My2mcvQJzWPLRxET3eWHYdBUtEg
1rxdrWxLheKjENzW3P7Mz/7KycIRxAlurl/Z9s8ytj3124AQY7NElt1iL9wwA47k
0EumxTaLz8H/vHB1fLMouvYfsSDEr3Snf6eSSwIDAQABAoIBAQDCNmxC3qHXPgvI
EzBOtIPV11PyzizXWi+U4U6WwUBjCQ6ijfoYOKLaHHnnCEIm4V2N8KV4prAkQjcM
[redacted]
xxrq/vizzNh6K1dBrZKmrWrAqGifkHqx2M3wwssfSzG3WhSOUT1nrUnONg9XLbl5
WeBd2Zp/Fn+tk2T9SsTotAgJAoGAOvmo5APBVRLILHwungLno8ZOYJopOtEPGFDp
v0bHNfgGIrfMcoKIx2xuX5cUe9MihRdyPV8aHYvd4ciE6yOGGq2ypVAt0SSS+TSL
GXJpezX9AjeWtQV8iWoEojIKKPs9FAHftS2aCbXXVJxwR1kbp8clyDxQ9yNNCr7o
OBG9XHECgYEA0xuJhoD8HMmoLJockHeMvHY9DqjcncFLwXyuKORKzRT5SiUy7tDJ
VV8cqljV95gNbae6tUp9zNO7mwlwD2ztjyjDc1gtW+Kpfj7VXImtURHrxKfZflNx
uQ/fbf/zaVpJ7QPcL7y671BGevC/JIZ/i2jBGQkQtn8d4rhk72C1kyw=
-----END RSA PRIVATE KEY-----
```

If the certificate chain of a private key file contains the following information: **-----BEGIN PRIVATE KEY-----** and **-----END PRIVATE KEY-----**, or **-----BEGIN ENCRYPTED PRIVATE KEY-----** and **-----END ENCRYPTED PRIVATE KEY-----**, you need to use the OpenSSL tool to run the following command to convert the format:

```
openssl rsa -in old_key.key -out new_key.key
```

2.5.5 HTTPS Certificate Format Conversion

CDN only supports certificates or private keys in PEM format. The following examples illustrate some popular conversion methods.

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.

2.5.6 TLS Versions

You can configure TLS versions as required.

Background

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 2-9 TLS versions supported by mainstream browsers

TLS Version	Mainstream Browser
TLS 1.0	● Chrome 1 ● Firefox 2+
TLS 1.1	● Chrome 22+ ● Firefox 24+ ● Safari 7+
TLS 1.2	● Chrome 30+ ● Firefox 27+ ● Safari 7+
TLS 1.3	● Chrome 70+ ● Firefox 63+ ● Safari 14+

Constraints

- Before configuring the TLS versions, configure an HTTPS certificate first. For details, see **Configuring an HTTPS Certificate**.
- 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.

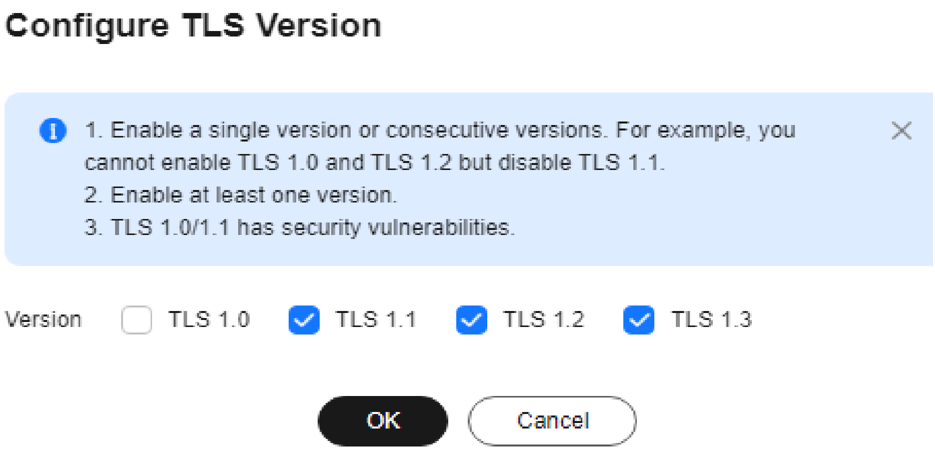
- You need to enable at least one version.
- By default, TLS 1.1, TLS 1.2, and TLS 1.3 are enabled.

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 2-22 Configuring the TLS versions



Configure TLS Version

1. Enable a single version or consecutive versions. For example, you cannot enable TLS 1.0 and TLS 1.2 but disable TLS 1.1.
2. Enable at least one version.
3. TLS 1.0/1.1 has security vulnerabilities.

Version □ TLS 1.0 ☑ TLS 1.1 ☑ TLS 1.2 ☑ TLS 1.3

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

2.5.7 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 301/302/307 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 security, use 301/302/307 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 have configured force redirect to HTTPS, disabling the certificate will also disable force redirect to HTTPS.

- If you have enabled HTTP/2, force redirect to HTTP does not take effect.

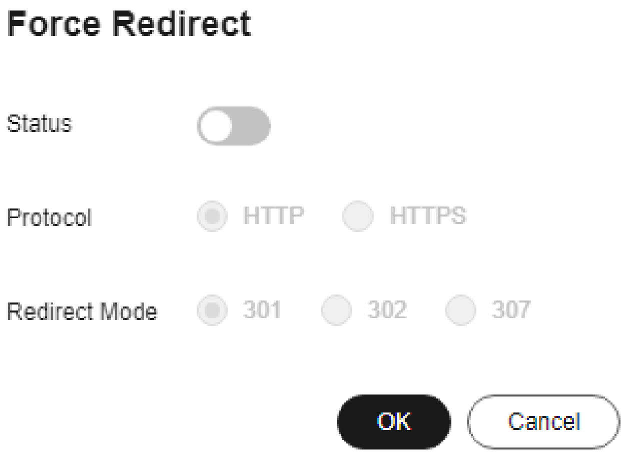
Procedure

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 2-23 Force redirect



Force Redirect

Status

Protocol ● HTTP ○ HTTPS

Redirect Mode ● 301 ○ 302 ○ 307

Table 2-10 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	301 302 307

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

2.5.8 HSTS

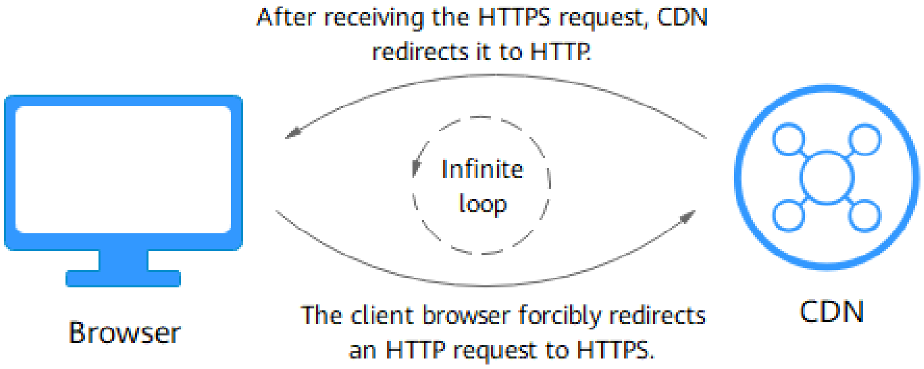
HTTP Strict Transport Security (HSTS) is a web security protocol promoted by Internet Engineering Task Force (IETF). HSTS forces clients (such as browsers) to use HTTPS to access your server, improving access security.

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.

Precautions

- HSTS is valid when an international HTTPS certificate is configured.
- 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.


After receiving the HTTPS request, CDN redirects it to HTTP.
Infinite loop
Browser
The client browser forcibly redirects an HTTP request to HTTPS.
CDN

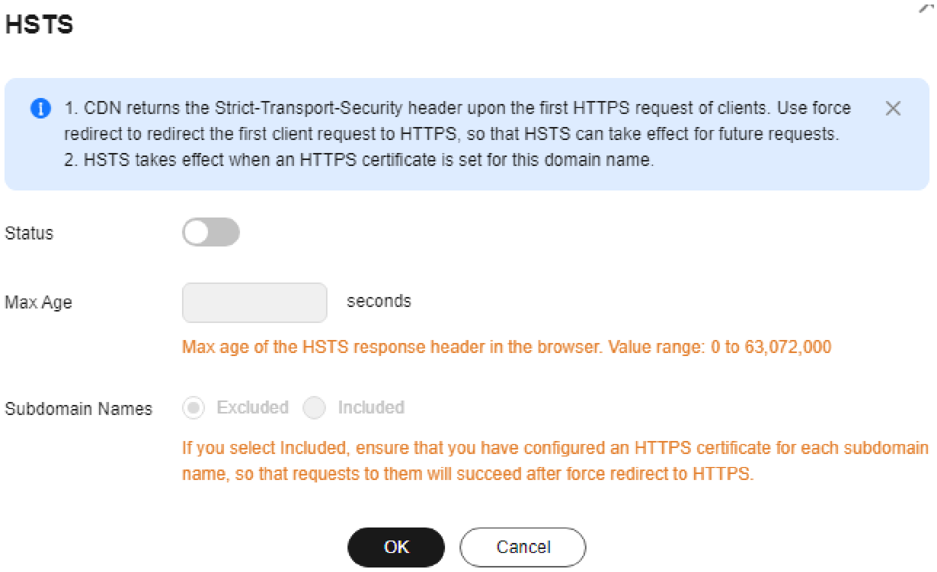
- To enable HSTS for domain names with special configuration, submit a service ticket.
- HSTS takes effect on clients. After HSTS is disabled, you need to refresh the browser cache. In this way, the next HTTP request from a client will not be automatically redirected to HTTPS.

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 2-24 HSTS



HSTS

1. CDN returns the Strict-Transport-Security header upon the first HTTPS request of clients. Use force redirect to redirect the first client request to HTTPS, so that HSTS can take effect for future requests.
2. HSTS takes effect when an HTTPS certificate is set for this domain name.

Status

Max Age seconds

Max age of the HSTS response header in the browser. Value range: 0 to 63,072,000

Subdomain Names ● Excluded ○ Included

If you select Included, ensure that you have configured an HTTPS certificate for each subdomain name, so that requests to them will succeed after force redirect to HTTPS.

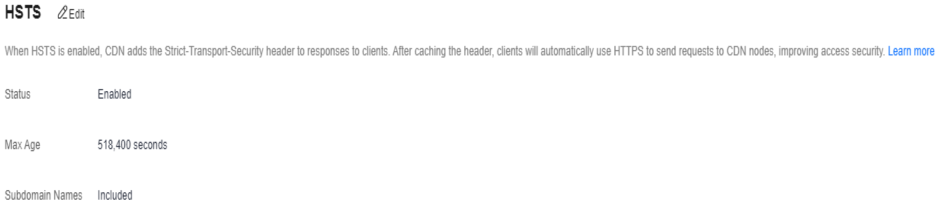
Table 2-11 Parameters

Parameter	Description
Max Age	TTL of the response header **Strict-Transport-Security** on clients. ● 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	Whether to enable HSTS for subdomain names. ● **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. Subdomain names without a certificate cannot be accessed.

7. Click **OK**.

Example

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



HSTS

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

Result:

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.

2.5.9 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 starting with **http://** can use only the HTTP/1.x protocol, and those starting with **https://** support HTTP/2.

Prerequisites

An HTTPS certificate has been configured. For details, see **Configuring an HTTPS Certificate**.

- 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/1.1 is the current mainstream protocol used on the Internet. 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.

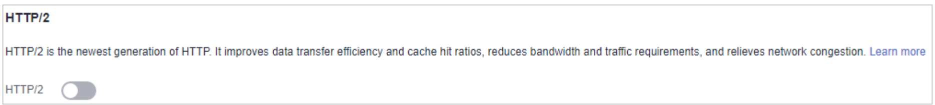
- Multiplexing

  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**.



HTTP/2

HTTP/2 is the newest generation of HTTP. It improves data transfer efficiency and cache hit ratios, reduces bandwidth and traffic requirements, and relieves network congestion. Learn more

HTTP/2 ○

2.5.10 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 **Configuring an HTTPS Certificate**.

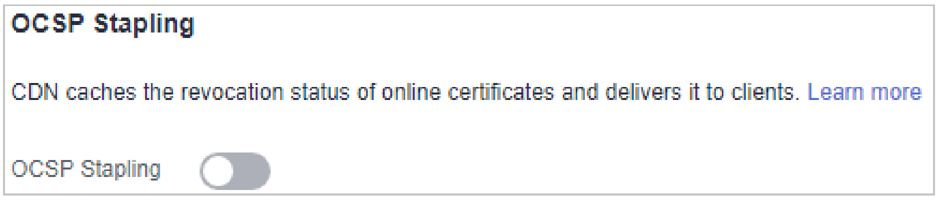
- Disabling the HTTPS certificate will disable OCSP stapling.
- After configuring the HTTPS certificate, wait about 5 minutes for the configuration to complete and then enable OCSP stapling.

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 2-25 OCSP stapling

   OCSP Stapling

   CDN caches the revocation status of online certificates and delivers it to clients. Learn more

   OCSP Stapling

   NOTE

   By default, OCSP stapling is disabled.
5. Switch on **OCSP Stapling**.

2.5.11 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 **Configuring an HTTPS Certificate**.

- 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

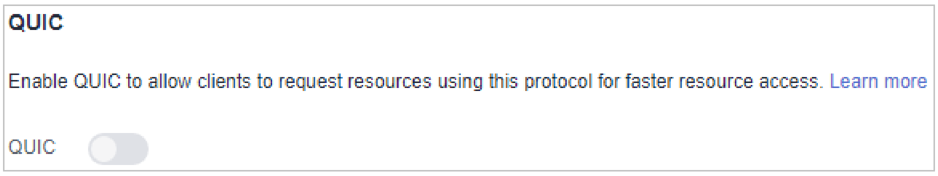
- QUIC cannot be used for origin pull.
- This function is in OBT and is available for free trial.

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 2-26 QUIC



QUIC

Enable QUIC to allow clients to request resources using this protocol for faster resource access. Learn more

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 rules and relevant settings of caches on CDN PoPs.

- You can modify cache settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned.

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.

Function	Description
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,
  - Your modifications are effective for new content cached.
  - You can **purge** to apply modifications to the existing cache.

2.6.2 PoP Cache Rules

You can configure the TTL for one or more cached resources on CDN PoPs. If the TTL of a file 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 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 periods 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 prolongs 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,

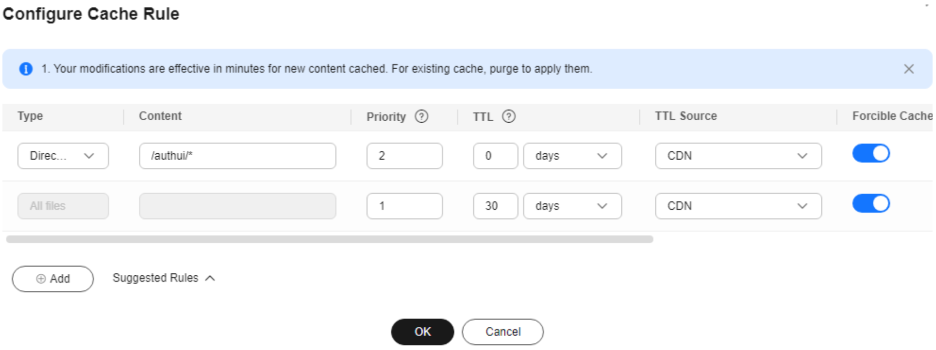
- Your modifications are effective for new content cached.
- You can purge to apply modifications to all resources (including the existing PoP cache).

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 **Cache Settings** tab.
5. In the **Cache Rules** area, click **Edit**. The **Configure Cache Rule** dialog box is displayed.
6. Click **Add** to add a cache rule. **Table 2-12** describes the parameters. You can click **Suggested Rules** to view the recommended configuration.

Figure 2-27 Configuring a cache rule



Configure Cache Rule

1. Your modifications are effective in minutes for new content cached. For existing cache, purge to apply them.

Type	Content	Priority	TTL		TTL Source	Forcible Cache
Direc...	/authui/*	2	0	days	CDN	●
All files		1	30	days	CDN	●

Table 2-12 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.

Parameter	Description	Configuration Rule
File type	Files of specific types. If the service type of a new domain name is **Website**, **File download**, or **On-demand services** and its origin server type is **IP address** or **Domain name**, 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.	- All file types are supported. - Start each file name extension with a period (.), and separate file name extensions with semicolons (;). - Enter up to file name extensions. - Enter up to 1,000 characters. - File name extensions are case-insensitive. Example: **.JPG;.zip;.exe**

Parameter	Description	Configuration Rule
Directory	Files in a directory	Directories are matched by prefix. Start a directory with a slash (/), and separate multiple directories with semicolons (;). Enter up to 20 directories with up to 255 characters in total. Example: **/test/folder01;/test/folder02** ● Wildcard matching is supported. Rules for using wildcards (*): – Only one directory with one wildcard can be set for each rule. Example: **/test/*** – CDN uses prefix match. For example, when the path in 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. ● You can configure only one cache rule for the homepage.
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 has reached, CDN pulls the most recent content of the file from the origin server when a user requests the file from a CDN PoP. Then, CDN caches that content on the PoP and serves it to the user.	The TTL of a cached file cannot exceed 365 days. You are advised to set the time according to the following rules: ● 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 content (such as .php, .jsp, and .asp files and dynamic APIs), set the TTL to 0 seconds.

Parameter	Description	Configuration Rule
Query Parameters	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. **Configuration rules:** ● If resources do not change with URL parameters, ignore query parameters. ● If resources change with URL parameters, retain query parameters. ● If you have enabled video seek, set **Query Parameters** to **Ignore all** for your video resources.	● **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	Parameters to be ignored or retained. Leave this parameter blank when **Query Parameters** is set to **Retain all** or **Ignore all**.	● Enter up to 10 parameter names separated by semicolons (;). ● Only letters, digits, periods (.), underscores (_), and tildes (~) are supported.

Parameter	Description	Configuration Rule
TTL Source, that is, the original **Origin Cache Control** field	If **Cache-Control: max-age** or **Expires** has been configured on the origin server, you can set **TTL Source** on CDN to synchronize the cache TTL from the origin server to CDN or force CDN to use the shorter TTL between the cache TTL in the cache rule and that on the origin server. By default, the cache TTL in the CDN cache rule is used. **TTL Source** values include: ● **Origin server**: CDN PoPs use the cache TTL set on the origin server. ● **CDN**: CDN PoPs use the cache TTL set in the cache rule. ● **Whichever is shorter**: CDN PoPs use the shorter TTL between the cache TTL in the cache rule and that on the origin server. **NOTE** ● If both **Cache-Control** and **Expires** are configured on the origin server, **Cache-Control** is preferentially used. ● If **TTL Source** is set to **Origin server**, but **Cache-Control** and **Expires** are not configured on the origin server, CDN PoPs use the cache rule configured on CDN.	The default TTL source is CDN.

Parameter	Description	Configuration Rule
Forcible Cache	Whether to ignore the **no-cache**, **private**, and **no-store** fields in the **Cache-Control** response header of the origin server. When this function is enabled, these fields are ignored. Forcible cache supplements TTL source. The rules are as follows: 1. When **TTL Source** is set to **Origin server** and **Forcible Cache** is disabled: ● 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. 2. When **TTL Source** is set to **Origin server** and **Forcible Cache** is enabled: ● If cache directives are set in the response header of the origin server, 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.	By default, this function is enabled.

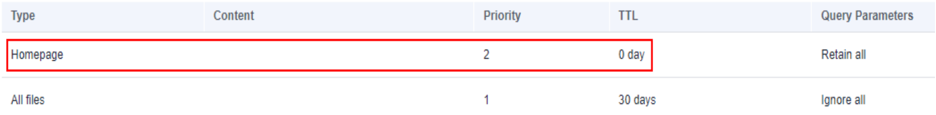
Parameter	Description	Configuration Rule
	3. When **TTL Source** is set to **CDN** and **Forcible Cache** is enabled: ● CDN ignores response headers from the origin server and uses the cache TTL configured on the CDN console. 4. When **TTL Source** is set to **CDN** and **Forcible Cache** is disabled: a. 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. b. If **no-cache**, **private**, or **no-store** is not set, CDN uses the cache TTL configured on the CDN console. 5. When **TTL Source** is set to **Whichever is shorter** and **Forcible Cache** is disabled: ● If the cache TTL set on CDN is shorter, the rule **6.d** is used. ● If the cache TTL set on the origin server is shorter, the rule **6.a** is used. 6. When **TTL Source** is set to **Whichever is shorter** and **Forcible Cache** is enabled: ● If the cache TTL set on CDN is shorter, the rule **6.c** is used. ● If the cache TTL set on the origin server is shorter, the rule **6.b** is used.	

Parameter	Description	Configuration Rule
SWR	If you have set **Cache-Control** to **stale-while-revalidate=***** (specific duration) on your origin server, you can enable SWR on CDN. This allows clients to use stale resources cached on CDN PoPs, as long as the specified SWR duration has not elapsed. At the same time, CDN pulls and caches the latest resources from the origin server to serve future user requests.	-

7. (Optional) Delete a cache rule if you no long use it.
8. 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.



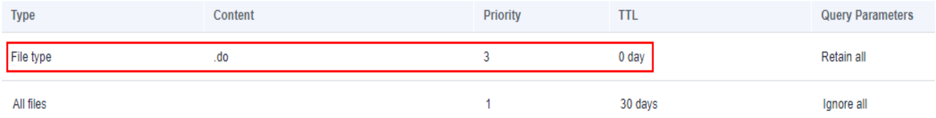
Type	Content	Priority	TTL	Query Parameters
Homepage		2	0 day	Retain all
All files		1	30 days	Ignore all

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.

1. 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**.

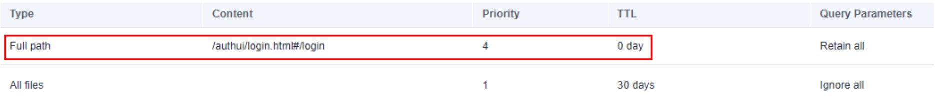
Type	Content	Priority	TTL	Query Parameters
File type	.do	3	0 day	Retain all
All files		1	30 days	Ignore all

   NOTE

   The new rule only applies to new content. After the new rule is added, purge 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.

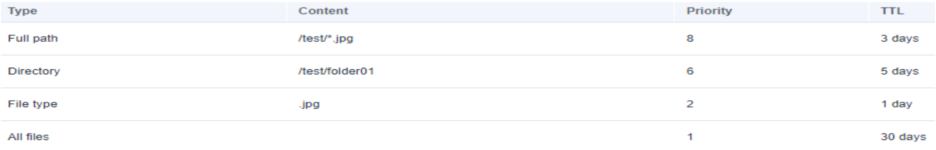
2. You have configured CDN acceleration for your website, the login page of your website is displayed cyclically, and your customers cannot log in to the website. After CDN acceleration is disabled, customers can log in to the website.

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

You can 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 the 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.

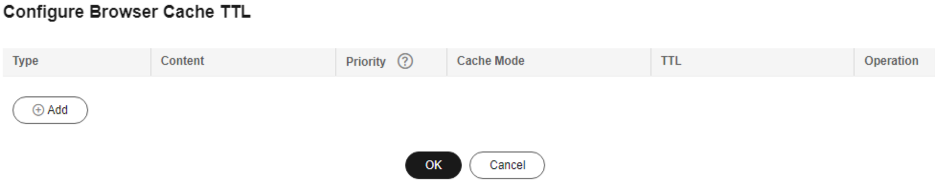
Procedure

1. Log in to **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 **Browser Cache TTL** area, click **Edit**.
6. In the displayed dialog box, click **Add** and set the browser cache policy as required.

Figure 2-28 Browser cache TTL


Configure Browser Cache TTL

Type	Content	Priority ?	Cache Mode	TTL	Operation

Table 2-13 Parameters

Parameter	Description
Type	● **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	When **Type** is set to **All files**, you do not need to set this parameter. When **Type** is set to **File type**: ● 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** When **Type** is set to **Directory**: ● 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** When **Type** is set to **Full path**: ● 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** 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.
Priority	Priority of the rule. Enter an integer ranging from 1 to 100. A greater number indicates a higher priority. ● Each rule must have a unique priority.

Parameter	Description
Cache Mode	● **Honor origin Cache-Control**: Comply with the cache policy of the origin server, that is, the setting of the **Cache-Control** header. ● **Cache**: The browser caching behavior depends on the value of the **Cache-Control** header of the origin server. 1. If the value of the **Cache-Control** header on the origin server is **no-cache**, **no-store**, or **private**, browsers do not cache the resources. 2. For other values, browsers use the TTL set in this rule. ● **No cache**: Browsers do not cache the resources.
TTL	When the configured TTL arrives and a user requests the resources again, the browser requests the resources from CDN. ● The value ranges from 0 to 365 days.

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 image **abc.jpg** has been deleted from the origin server and is not cached on CDN PoPs, CDN pulls it for each request, but the origin server returns a 4*xx* status code each time. This increases the pressure on the origin server. In this case, if you configure the cache TTL for the status code 4*xx* on CDN, CDN PoPs will directly return the status code 4*xx* 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.

- If the service type of your domain name is whole site acceleration, this function takes effect only for static resources.
- 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:
  - 4*XX*: 400, 401, 403, 404, 405, 407, 414, 416, and 451
  - 5*XX*: 500, 501, 502, 503, 504, 509, and 514
  - 3*XX*: 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 2-29 Adding a status code cache TTL

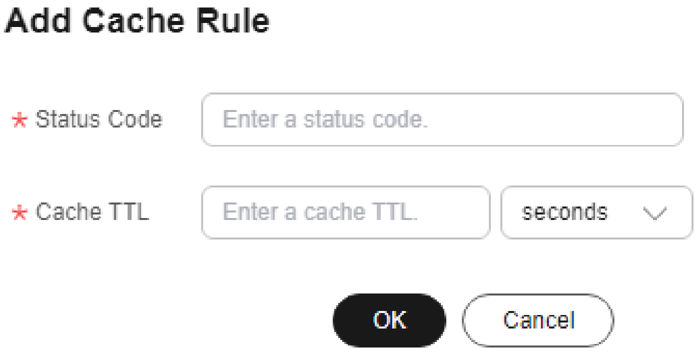


Table 2-14 Parameters

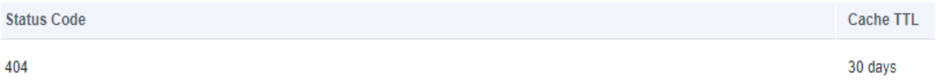
Parameter	Description	Example
Status Code	Status code to be cached.	404

Parameter	Description	Example
Cache TTL	Duration for caching the status codes on CDN PoPs. ● If it is set to **0**, the status code is not cached. ● The value ranges from 0 to 365 days. **NOTE** Status codes 3*XX* and 416 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 ACLs, token authentication, remote authentication, and IP access frequency to identify and filter out unauthorized users and improve CDN security.

- You can modify access control settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned by CDN.
- IP addresses belong to carriers and change irregularly. Although Huawei Cloud periodically updates the IP address library, the update may be delayed. As a result, some access control functions may occasionally block or allow requests, or client requests may not be scheduled to the optimal PoP.

Function	Description
Referer Validation	You can configure a referer blacklist or whitelist to identify and filter out users from specific access sources.

Function	Description
IP ACL	You can filter out requests from specific IP addresses.
User-Agent ACL	You can filter out requests from specific user agents.
Token Authentication	You can protect your website resources from being downloaded by malicious users.
Remote Authentication	You can allow CDN to forward user requests to a specific server for authentication to prevent malicious resource download.
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.

2.7.2 Referer Validation

You can set a referer blacklist or whitelist to identify and filter out values of the **Referer** header in HTTP requests, controlling access sources.

Background

The **Referer** header identifies the address of the web page from which the resource has been requested. CDN PoPs can use this header 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.

Constraints

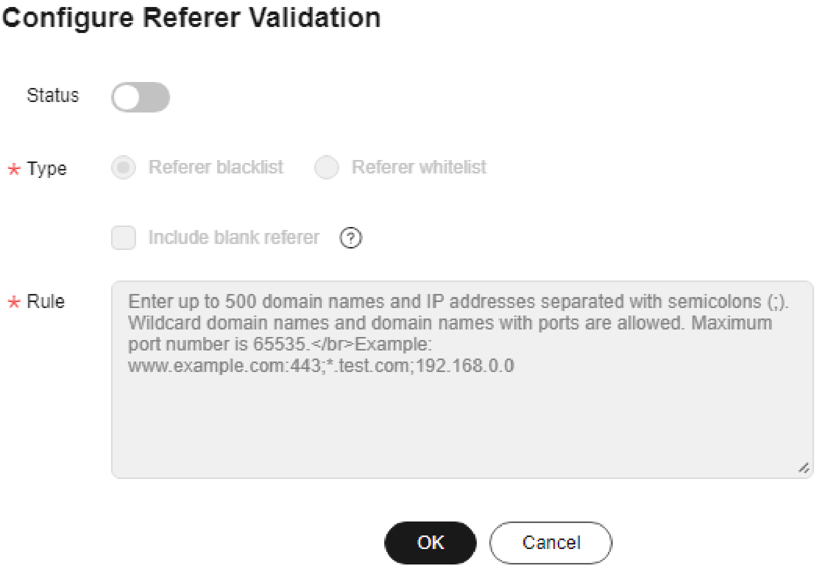
- This function is disabled by default.
- Either a referer blacklist or whitelist can be configured.

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 2-30 Configuring referer validation



Configure Referer Validation

Status

* Type ● Referer blacklist ○ Referer whitelist

□ Include blank referer ?

* Rule

Enter up to 500 domain names and IP addresses separated with semicolons (;). Wildcard domain names and domain names with ports are allowed. Maximum port number is 65535.</br>Example: www.example.com:443;*.test.com;192.168.0.0

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 2-15 Parameters

Parameter	Description	Filling Rule
Include blank referer	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 accepted (whitelist) or rejected (blacklist). **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.	/

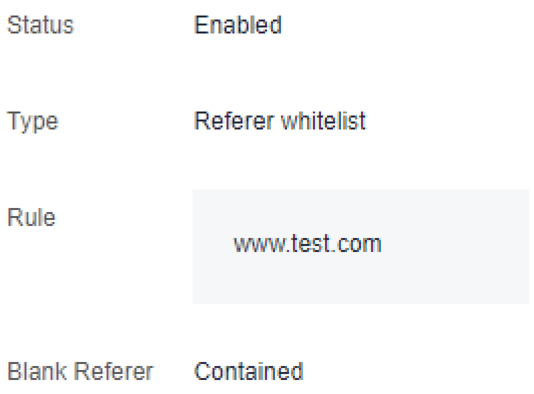
Parameter	Description	Filling Rule
Referer whitelist	● If the referer field of an access request matches the whitelist rules, the requester can access the requested content. Otherwise, CDN returns a 403 error response code, indicating that access is forbidden. ● If **Include blank referer** is selected and an access request contains a blank referer, the requester can access the requested content.	● 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 500 domain names and IP addresses. Example: **www.example.com:443;*.test.com;192.168.0.0** **NOTE** Domain names with special configurations support only one asterisk (*).

Parameter	Description	Filling Rule
Referer blacklist	● 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.	● 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 500 domain names and IP addresses. Example: **www.example.com:443;*.test.com;192.168.0.0** **NOTE** Domain names with special configurations support only one asterisk (*).

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

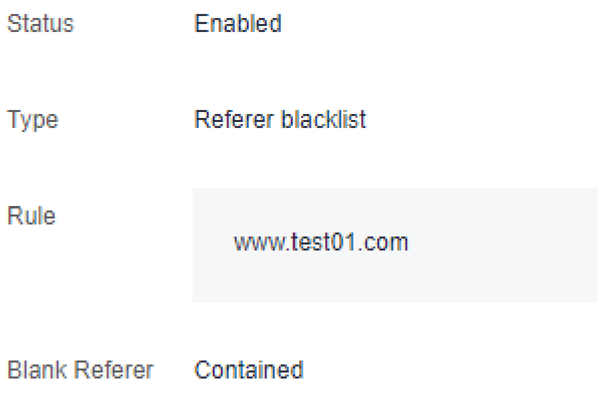
1. Assume that a referer whitelist **www.test.com** is configured for the domain name **www.example.com** and **Include blank referer** is selected.



Status	Enabled
Type	Referer whitelist
Rule	www.test.com
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	www.test01.com
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

You can filter out requests from specific IP addresses to restrict access and prevent content theft and attacks.

Precautions

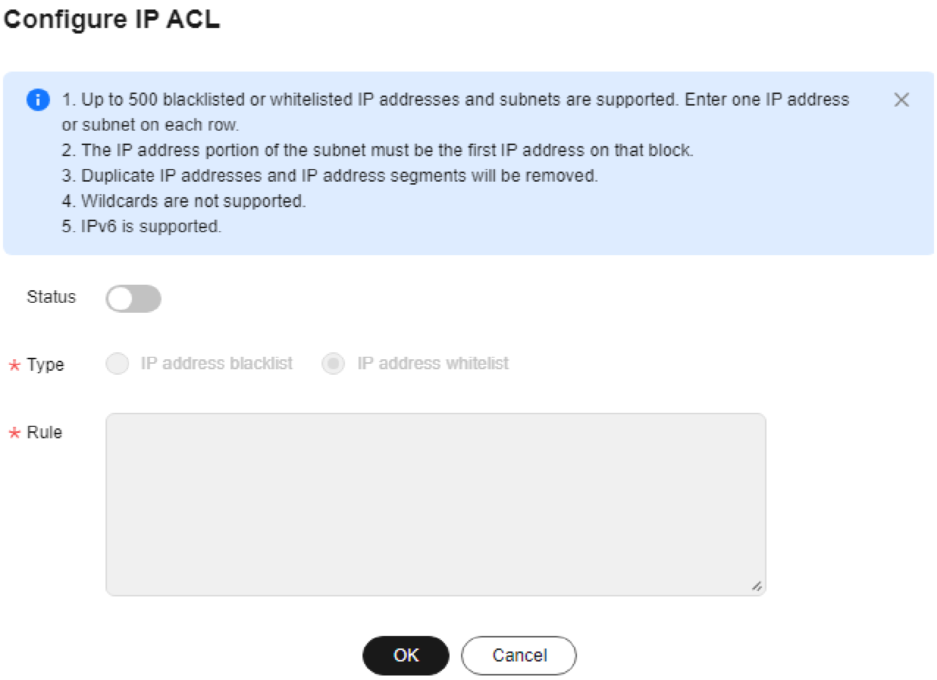
- This function is disabled by default.
- Either an IP address blacklist or IP address whitelist can be configured.

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 **IP ACL** area, click **Edit**. The **Configure IP ACL** dialog box is displayed.

Figure 2-31 Configuring an IP ACL



Configure IP ACL

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.

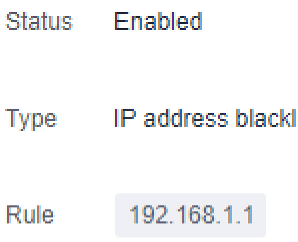
6. Switch on **Status** to enable this configuration item.
7. Select a type and enter rules.

Parameter	Description
Type	● **IP address blacklist**: If the IP address of a user is included in the 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 whitelist, status code 403 will be returned when the user accesses a CDN PoP. **NOTE** ● Either an IP address blacklist or IP address whitelist can be configured.
Rule	● 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** An IP address segment cannot include an IP address you specify. ● 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 ACL for your domain name to identify and filter visitors and enhance domain name security.

Background

You can 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

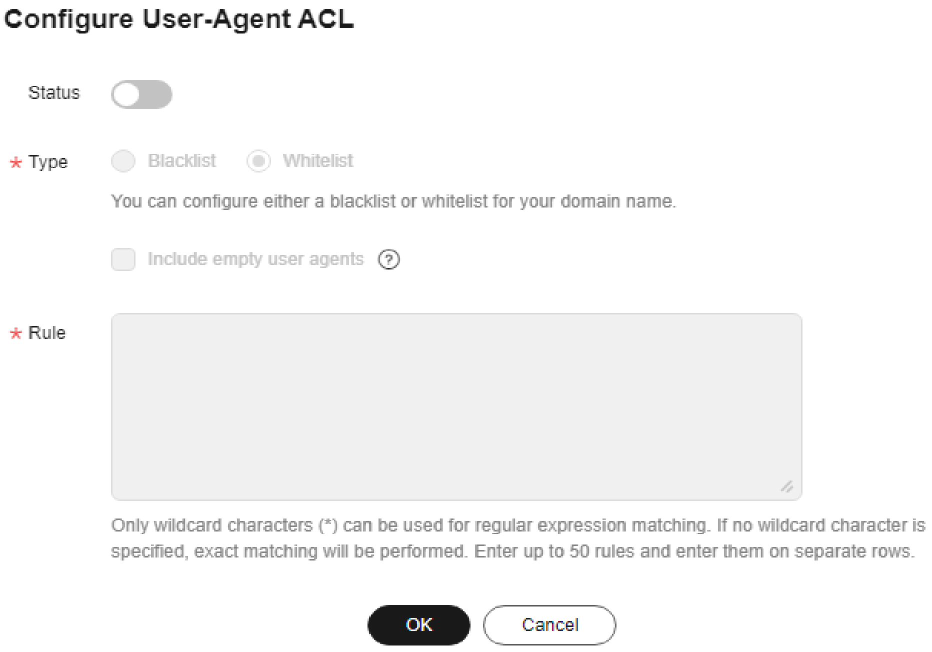
- This function is disabled by default.
- Either a User-Agent blacklist or whitelist can be configured.

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 ACL** area, click **Edit**. The **Configure User-Agent ACL** dialog box is displayed.

Figure 2-32 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.

□ Include empty user agents ?

* 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 50 rules and enter them on separate rows.

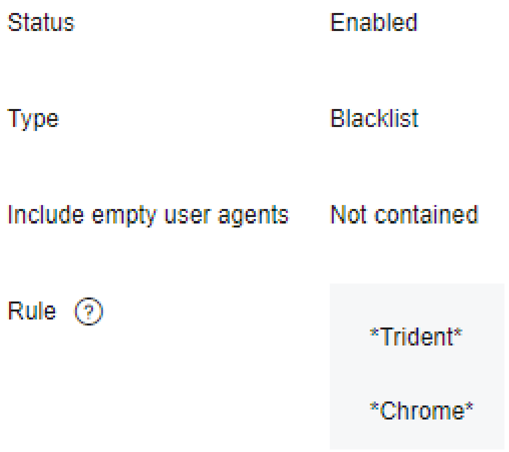
6. Switch on **Status** to enable this configuration item.
7. Select a type and enter rules.

Parameter	Description
Type	● **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.
Include empty user agents	An empty user agent indicates that the User-Agent field is left blank or is not included in an HTTP request. If this option is selected, such requests will also be accepted (whitelist) or rejected (blacklist). **NOTE** The **User-Agent** field with value **null** is not an empty user agent.
Rule	● Enter letters, digits, spaces, and the following special characters: *.-_();,/'#!@$^&+=~?"[]{}\:% **NOTE** For domain names with special configurations, (), {}, or [] must be both entered. ● 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 50 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
Include empty user agents	Not contained
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, the content distributed by CDN is public resources. 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.
- You cannot configure this function for domain names with special configurations 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

Example signed URLs look 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 2-16 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 the 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 only when the current time is earlier than or equal to **timestamp** + 1,800s. Or, the signed URL is considered invalid.
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 lowercase letters and digits.
sha256	A string of 64 characters calculated using the SHA256 algorithm. The string consists of lowercase letters and digits.
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**. A key contains 6 to 32 characters, including 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 the authentication parameter is included in the request. If not, the request is considered invalid and an HTTP 403 error code is returned.
2. Checks whether the value of **timestamp** plus the validity period specified in the signed URL is later than the current time.
   - If not, the signed URL is considered invalid and the HTTP 403 error is returned.
   - If yes, the time verification passes and CDN goes to step **3**.
3. Constructs **sstring**, calculates **HashValue** using this string and the MD5 or 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 the requested file is returned. Or, 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

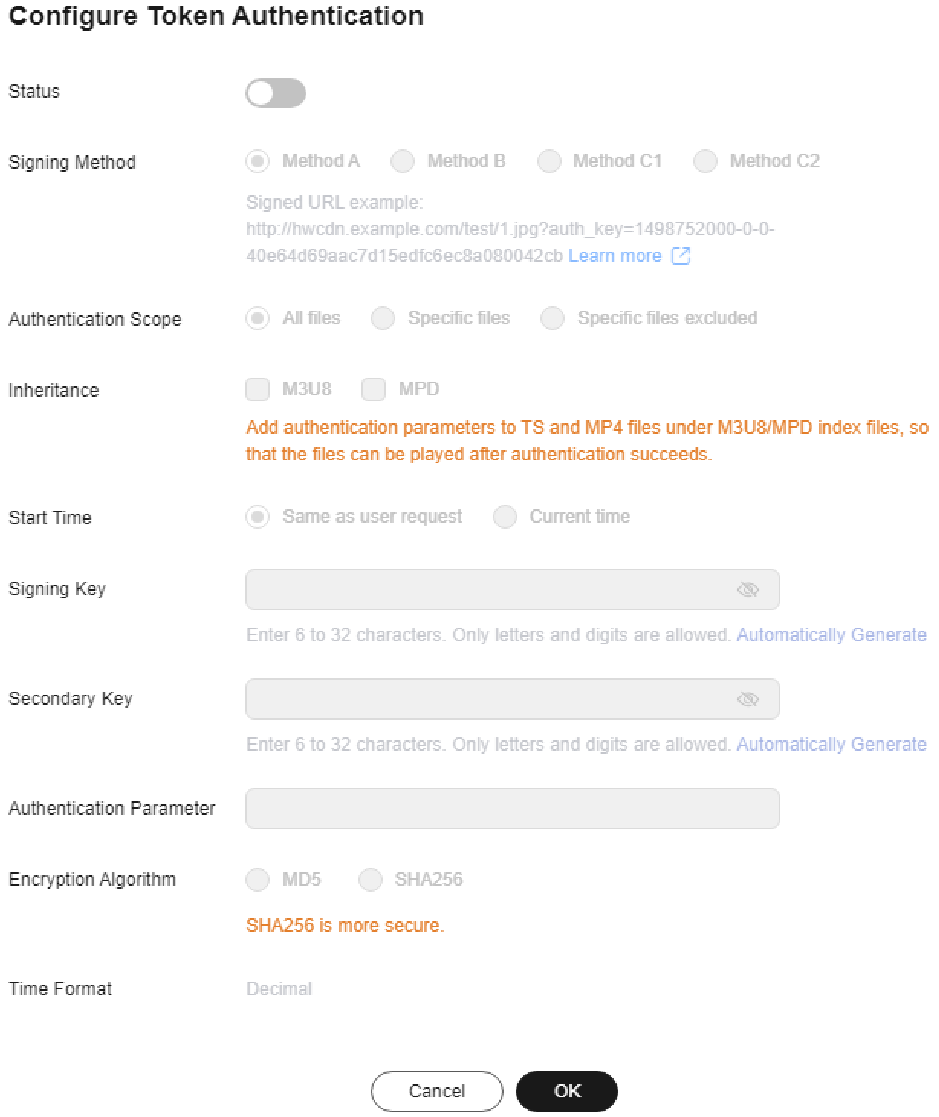
```
sstring = "Filename-Timestamp-rand-uid-PrivateKey"
HashValue = sha256sum(sstring)
```

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 2-33 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 6 to 32 characters. Only letters and digits are allowed. Automatically Generate

Secondary Key

Enter 6 to 32 characters. Only letters and digits are allowed. Automatically Generate

Authentication Parameter

Encryption Algorithm ○ MD5 ○ SHA256

SHA256 is more secure.

Time Format Decimal

5. Turn on the **Status** switch.

6. Set the parameters according to the following table and click **OK**.

Table 2-17 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	Add the authentication parameter to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds. **NOTE** ● 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	● **Same as user request**: time when a user accesses the M3U8/MPD file. ● **Current time**: current time of the authentication server.
File Name Extensions	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. ● Only lowercase letters and digits are supported. Use semicolons (;) to separate multiple file name extensions.
Signing Key	Authentication password. The value contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.
Secondary Key	(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. ● A key contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.

Parameter	Description
Authentication Parameter	Authentication parameter carried in a URL. The default value is **auth_key**. ● Enter up to 100 characters. ● Start with a letter. Enter letters, digits, and underscores (_).
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 2-17** and **Table 2-18**, 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 2-18 Parameter description

Parameter	Description
Signing Key	Authentication password. Enter 6 to 32 characters, including 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 settings, the latter will be used. Example: If you set this parameter to 2,000s, but the validity period set in the token authentication settings 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. The back-to-origin URL is as follows:
```
http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3
```
2. The signing key is **huaweicloud12345** (customizable).
3. The authentication takes effect since 00:00:00 on June 30, 2017. Therefore, **timestamp** is **1498752000**. The validity period is 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 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 a request is within the validity period (earlier than or equal to 00:30:00 on June 30, 2017) and the **md5hash** value in the request is the same as the calculated **HashValue** (**4143ae4a8034c637fd256dfd3542bafc**), the authentication is successful.

2.7.5.2 Signing Method B

By default, the content distributed by CDN is public resources. 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.
- You cannot configure this function for domain names with special configurations 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

Example signed URLs look 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 2-19 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 YYYYMMDDHHMM, for example, 201706301000.
Validity period	How long the 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 only when the current time is earlier than or equal to **timestamp** + 1,800s. Or, the signed URL is considered invalid.
md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of lowercase letters and digits.
sha256	A string of 64 characters calculated using the SHA256 algorithm. The string consists of lowercase letters and digits.
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**. A key contains 6 to 32 characters, including letters and digits.

Verification Method

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

1. Checks whether the authentication parameter is included in the request. If not, the request is considered invalid and an HTTP 403 error code is returned.
2. Checks whether the value of **timestamp** plus the validity period specified in the signed URL is later than the current time.
   - If not, the signed URL is considered invalid and the HTTP 403 error is returned.
   - If yes, the time verification passes and CDN goes to step **3**.
3. Constructs **sstring**, calculates **HashValue** using this string and the MD5 or 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 the requested file is returned. Or, 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)
```

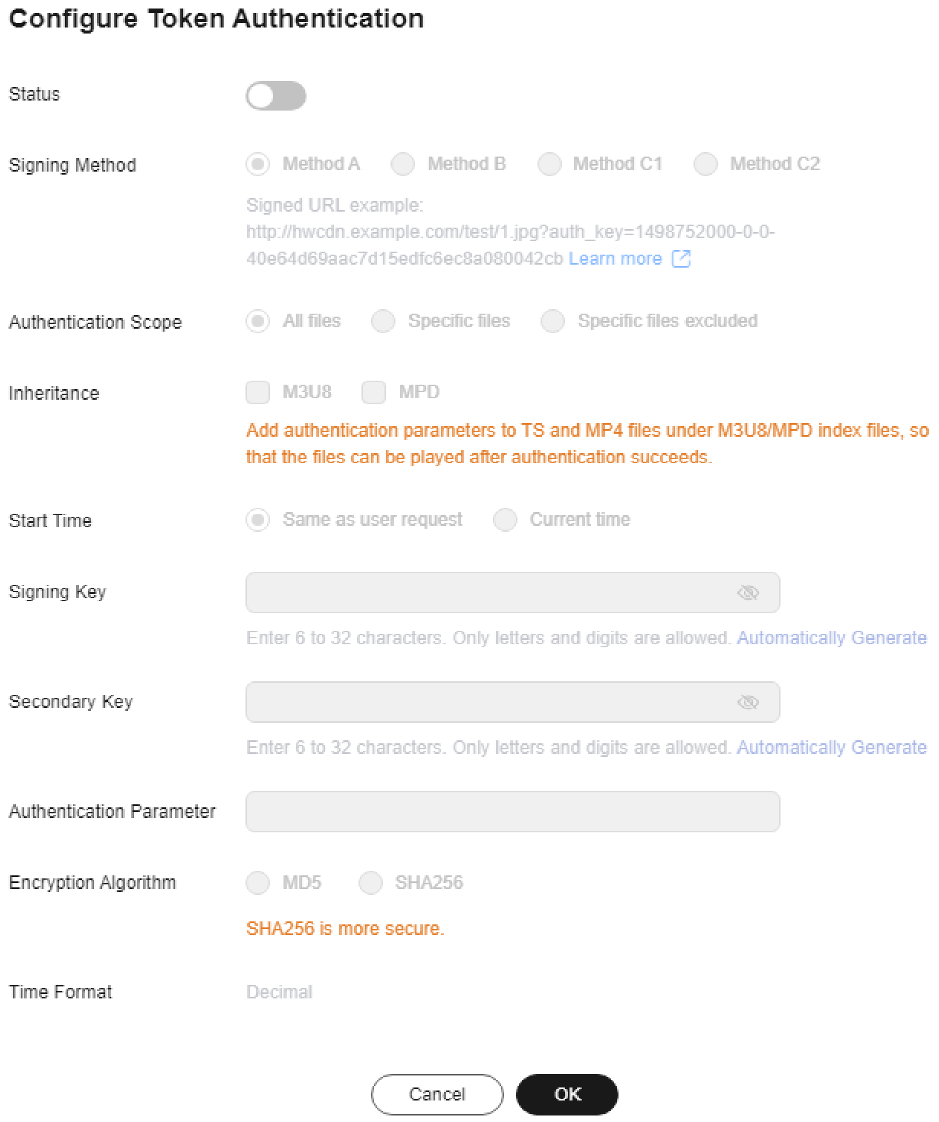
Procedure

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 2-34 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 6 to 32 characters. Only letters and digits are allowed. Automatically Generate

Secondary Key

Enter 6 to 32 characters. Only letters and digits are allowed. Automatically Generate

Authentication Parameter

Encryption Algorithm ○ MD5 ○ SHA256

SHA256 is more secure.

Time Format Decimal

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

Table 2-20 Parameter description

Parameter	Description
Signing Method	Select **Method B**.
Authentication Scope	Files to be authenticated. Select **All files**, **Specific files**, or **Specific files excluded**.
Inheritance	Add the authentication parameter to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds. **NOTE** ● 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	● **Same as user request**: time when a user accesses the M3U8/MPD file. ● **Current time**: current time of the authentication server.
File Name Extensions	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. ● Only lowercase letters and digits are supported. Use semicolons (;) to separate multiple file name extensions.
Signing Key	Authentication password. The value contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.

Parameter	Description
Secondary Key	(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. ● A key contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.
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 2-20** and **Table 2-21**, and click **Generate** to generate a signed URL that will expire at a specific time.

Table 2-21 Parameter description

Parameter	Description
Signing Key	Authentication password. Enter 6 to 32 characters, including 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 settings, the latter will be used. Example: If you set this parameter to 2,000s, but the validity period set in the token authentication settings 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. The back-to-origin URL is as follows:
   ```
   http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3
   ```
2. The signing key is **huaweicloud12345** (customizable).
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 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 a request is within the validity period (earlier than or equal to 10:30:00 on June 30, 2017) and the **md5hash** value in the request is the same as the calculated **md5hash** value (**668f28d134ec6446a8ae83a43d0a554b**), the authentication is successful.

2.7.5.3 Signing Method C1

By default, the content distributed by CDN is public resources. 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.
- You cannot configure this function for domain names with special configurations 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

Example signed URLs look like:

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

The following table describes the parameters in a signed URL.

Table 2-22 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 only when the current time is earlier than or equal to **timestamp** + 1,800s. Or, the signed URL is considered invalid.
md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of lowercase letters and digits.
sha256	A string of 64 characters calculated using the SHA256 algorithm. The string consists of lowercase letters and digits.
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**. A key contains 6 to 32 characters, including letters and digits.

Verification Method

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

1. Checks whether the authentication parameter is included in the request. If not, the request is considered invalid and an HTTP 403 error code is returned.
2. Checks whether the value of **timestamp** plus the validity period specified in the signed URL is later than the current time.
   - If not, the signed URL is considered invalid and the HTTP 403 error is returned.
   - If yes, the time verification passes and CDN goes to step 3.
3. Constructs **sstring**, calculates **HashValue** using this string and the MD5 or 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 the requested file is returned. Or, 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)
```

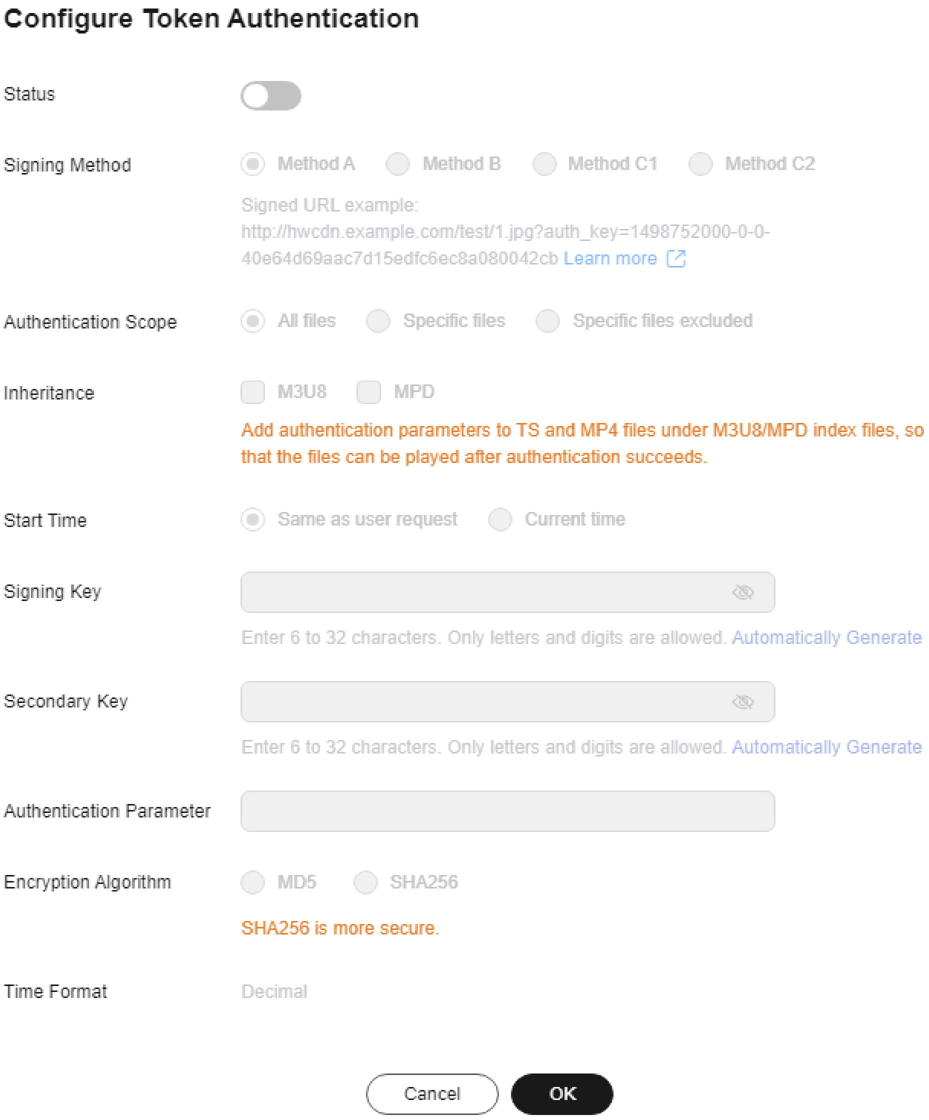
Procedure

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 2-35 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 6 to 32 characters. Only letters and digits are allowed. Automatically Generate

   Secondary Key

   Enter 6 to 32 characters. Only letters and digits are allowed. Automatically Generate

   Authentication Parameter

   Encryption Algorithm ○ MD5 ○ SHA256

   SHA256 is more secure.

   Time Format Decimal

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

Table 2-23 Parameter description

Parameter	Description
Signing Method	Select **Method C1**.
Authentication Scope	Files to be authenticated. Select **All files**, **Specific files**, or **Specific files excluded**.
Inheritance	Add the authentication parameter to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds. **NOTE** ● 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	● **Same as user request**: time when a user accesses the M3U8/MPD file. ● **Current time**: current time of the authentication server.
File Name Extensions	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. ● Only lowercase letters and digits are supported. Use semicolons (;) to separate multiple file name extensions.
Signing Key	Authentication password. The value contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.

Parameter	Description
Secondary Key	(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. ● A key contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.
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 2-23** and **Table 2-24**, 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 2-24 Parameter description

Parameter	Description
Signing Key	Authentication password. Enter 6 to 32 characters, including 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 settings, the latter will be used. Example: If you set this parameter to 2,000s, but the validity period set in the token authentication settings 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. The back-to-origin URL is as follows:
```
http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3
```
2. The signing key is **huaweicloud12345** (customizable).
3. The authentication takes effect since 10:00:00 on June 30, 2017. Therefore, **timestamp** is **5955b0a0**. The validity period is 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 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 a request is within the validity period (earlier than or equal to 10:30:00 on June 30, 2017) and the **md5hash** value in the request is the same as the calculated **md5hash** value (**8540f43a2416fd4a432fe4f92d2ea089**), the authentication is successful.

2.7.5.4 Signing Method C2

By default, the content distributed by CDN is public resources. 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.
- You cannot configure this function for domain names with special configurations 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

Example signed URLs look 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 2-25 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 only when the current time is earlier than or equal to **timestamp** + 1,800s. Or, the signed URL is considered invalid.
md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of lowercase letters and digits.
sha256	A string of 64 characters calculated using the SHA256 algorithm. The string consists of lowercase letters and digits.
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**. A key contains 6 to 32 characters, including letters and digits.
Authentication parameter	Authentication parameter carried in a URL. The default value is **auth_key**.
Time parameter	Name of the timestamp parameter carried in the request URL.

Verification Method

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

1. Checks whether the authentication parameter is included in the request. If not, the request is considered invalid and an HTTP 403 error code is returned.
2. Checks whether the value of **timestamp** plus the validity period specified in the signed URL is later than the current time.
   - If not, the signed URL is considered invalid and the HTTP 403 error is returned.
   - If yes, the time verification passes and CDN goes to step 3.
3. Constructs **sstring**, calculates **HashValue** using this string and the MD5 or 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 the requested file is returned.

Or, 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)
```

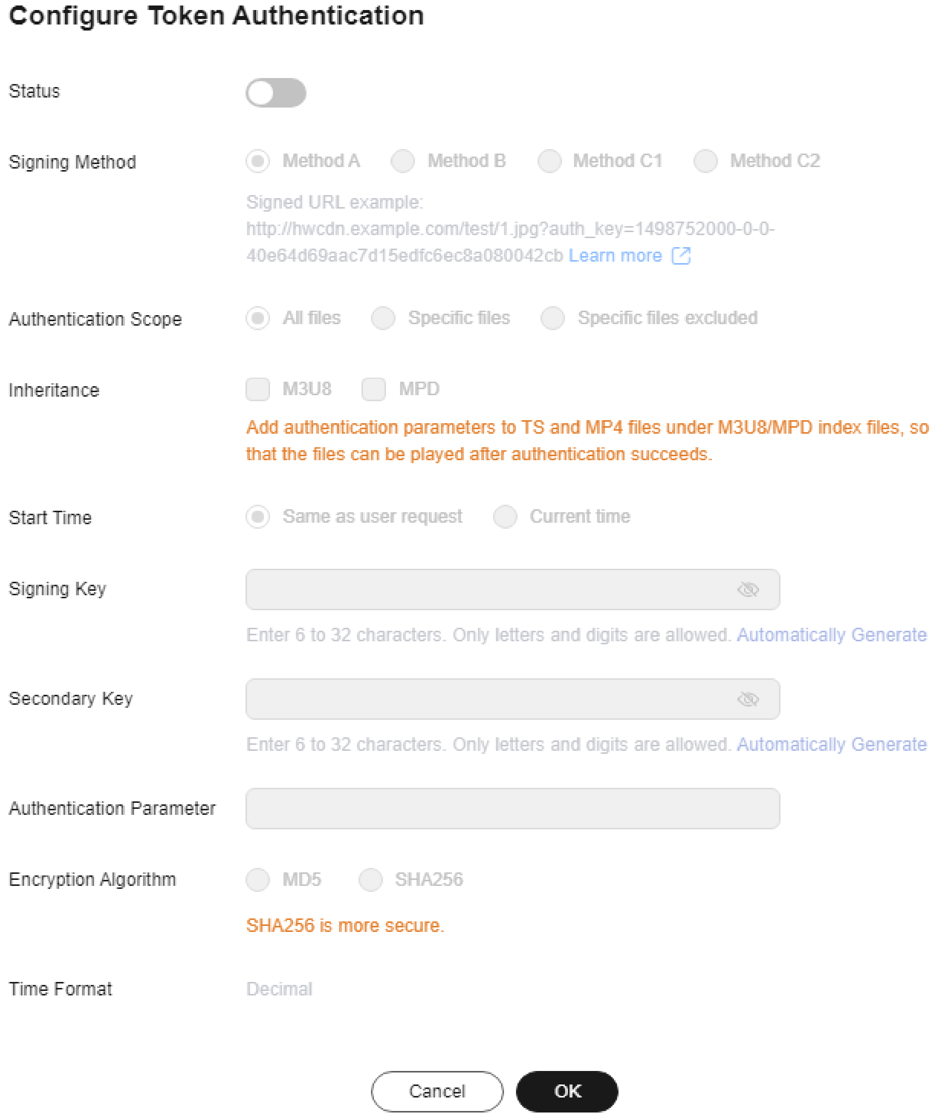
Procedure

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 2-36 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 6 to 32 characters. Only letters and digits are allowed. Automatically Generate

Secondary Key

Enter 6 to 32 characters. Only letters and digits are allowed. Automatically Generate

Authentication Parameter

Encryption Algorithm ○ MD5 ○ SHA256

SHA256 is more secure.

Time Format Decimal

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

Table 2-26 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	Add the authentication parameter to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds. **NOTE** - 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	- **Same as user request**: time when a user accesses the M3U8/MPD file. - **Current time**: current time of the authentication server.
File Name Extensions	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. - Only lowercase letters and digits are supported. Use semicolons (;) to separate multiple file name extensions.
Signing Key	Authentication password. The value contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.
Secondary Key	(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. - A key contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.

Parameter	Description
Authentication Parameter	Authentication parameter carried in a URL. The default value is **auth_key**. ● Enter up to 100 characters. ● Start with a letter. Enter letters, digits, and underscores (_).
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 2-26** and **Table 2-27**, 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 2-27 Parameter description

Parameter	Description
Signing Key	Authentication password. Enter 6 to 32 characters, including 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 token authentication settings.
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 settings, the latter will be used. Example: If you set this parameter to 2,000s, but the validity period set in the token authentication settings 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. The back-to-origin URL is as follows:
   ```
   http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3
   ```
2. The signing key is **huaweicloud12345** (customizable).
3. The authentication takes effect since 10:00:00 on June 30, 2017. Therefore, **timestamp** is **5955b0a0**. The validity period is 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 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&timestamp=5955b0a0
   ```

If a request is within the validity period (earlier than or equal to 10:30:00 on June 30, 2017) and the **md5hash** value in the request is the same as the calculated **md5hash** value (**8540f43a2416fd4a432fe4f92d2ea089**), 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 server you specify for authentication.

The remote authentication process is as follows.

Figure 2-37 Remote authentication process

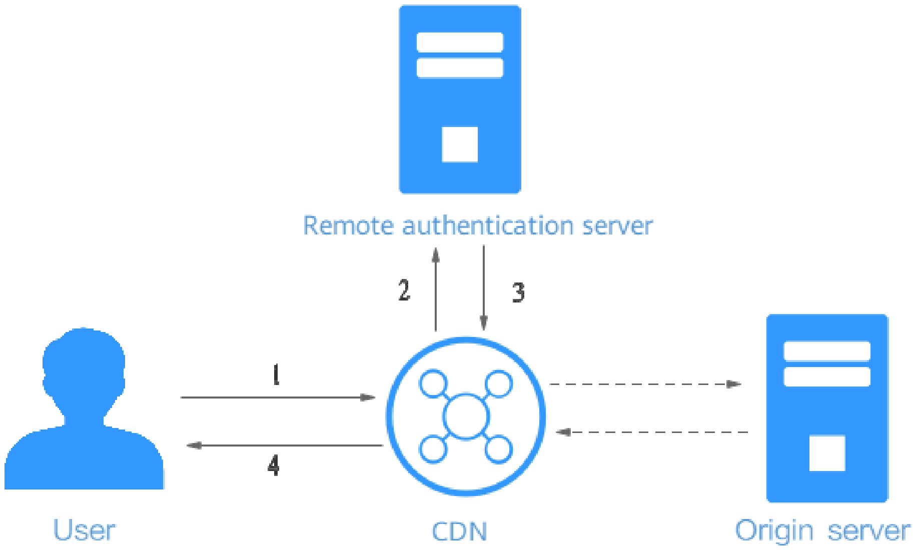


Table 2-28 Process description

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

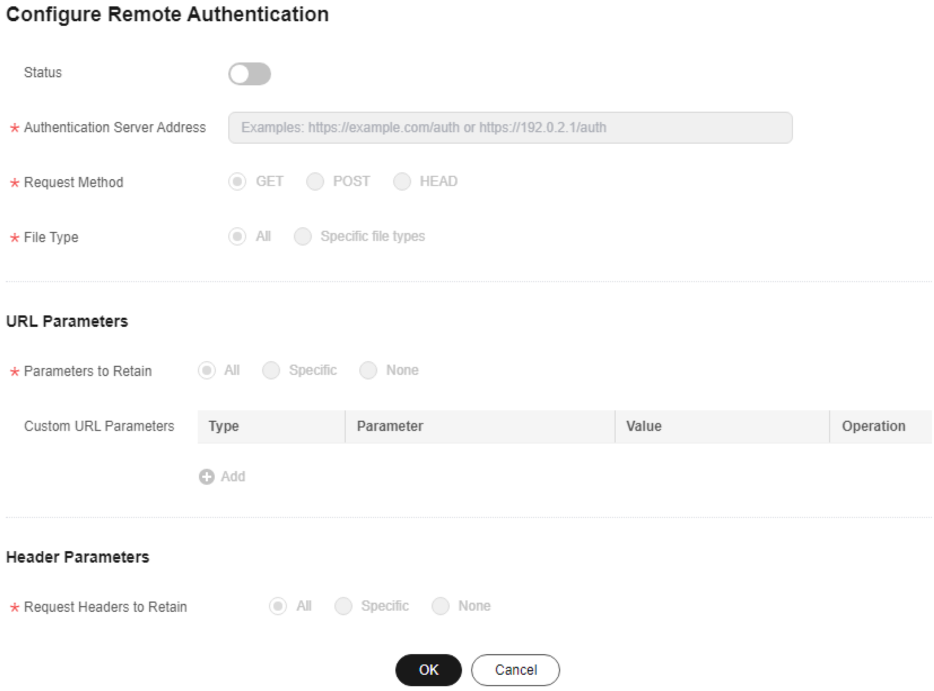
- Remote authentication is disabled by default.

Procedure

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 **Edit** next to **Remote Authentication**.

Figure 2-38 Configuring remote authentication



Configure Remote Authentication

Status ○

* Authentication Server Address: Examples: https://example.com/auth or https://192.0.2.1/auth

* 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

Header Parameters

* Request Headers to Retain: ● All ○ Specific ○ None

Table 2-29 Parameter description

Parameter	Description	Example
Authentication Server Address	IP address of a reachable server. ● 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	● **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**. – 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	Parameters that need to be authenticated in user requests. You can retain or ignore all URL parameters or retain specific URL parameters. ● Parameters are case insensitive. Use vertical bars (|) to separate them.	All
Custom URL Parameters	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). ● **Custom**: Customize a parameter and set the value to a string. ● **Select**: Select a preset or customized parameter and select a variable as the value.	Select **http_host**. Value: **$http_host**.
Request Headers to Retain	Headers to be authenticated in user requests. You can retain or ignore all request headers or retain specific request headers. Headers are case insensitive. Use vertical bars (|) to separate them.	All

Parameter	Description	Example
Custom Request Header Parameters	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). - **Custom**: Customize a parameter and set the value to a string. - **Select**: Select a preset or customized parameter and select a preset variable as the value.	Select **http_referer**. Value: **$http_referer**.
Success Status Code	Status code returned by the remote authentication server to CDN PoPs when authentication is successful. - Value range: 2*xx* and 3*xx*.	200
Failure Status Code	Status code returned by the remote authentication server to CDN PoPs when authentication fails. - Value range: 4*xx* and 5*xx*.	403
Custom Response Status Code	Status code returned by CDN PoPs to users when authentication fails. - Value range: 2*xx*, 3*xx*, 4*xx*, and 5*xx*.	403
Timeout Interval	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.	60
Action After Timeout	How CDN PoPs process a user request after authentication times out. - **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 2-30 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.

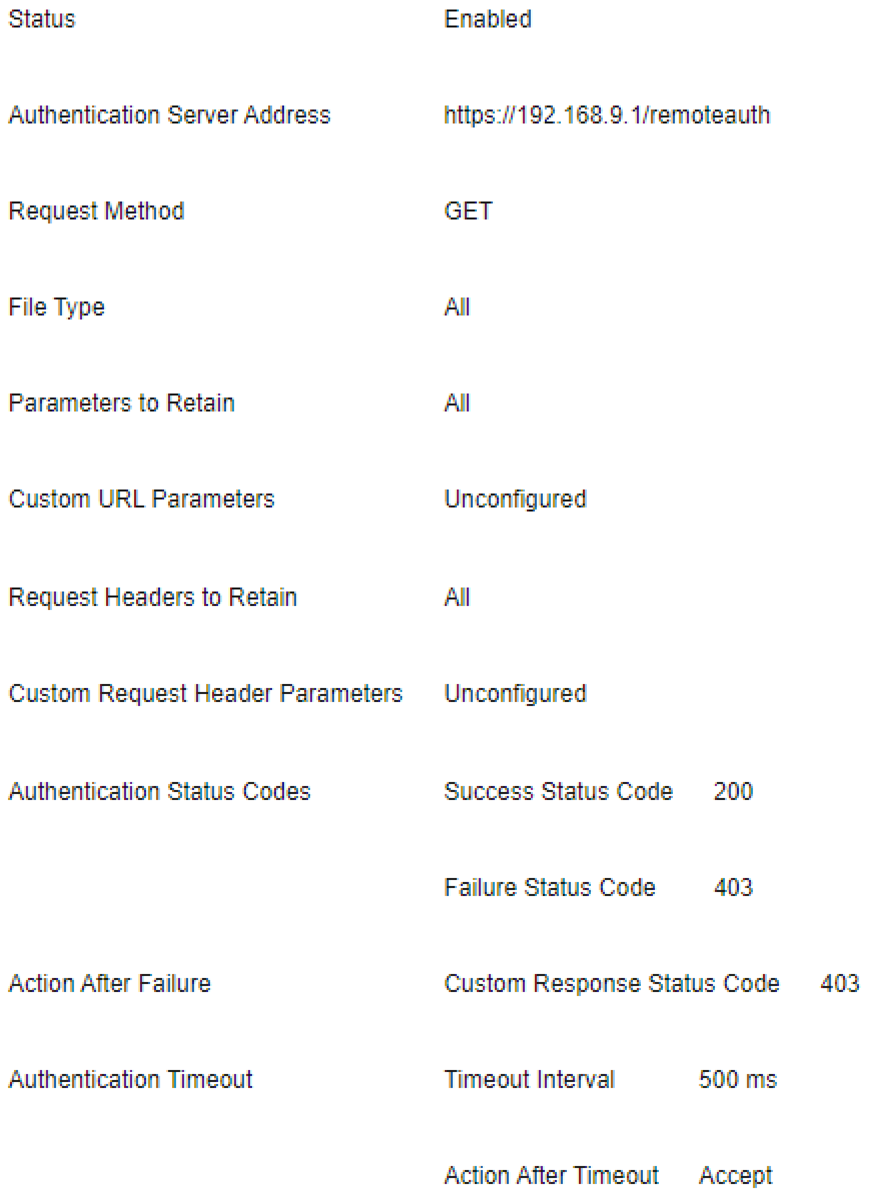
Example

Assume that you have enabled remote authentication for **example.com** and configured settings shown in **Figure 2-39**.

- Original request URL: **https://example.com/folder01/test.txt?key=** ***. The request carries header **test=123**.
- URL forwarded by CDN to the remote authentication server: **GET https://192.168.9.1/remoteauth?key=** ***. The request carries header **test=123**.
- Possible authentication results:
  - Successful. The CDN PoP serves cached content to the user.
  - Failed. The CDN PoP returns status code 403 to the user.

- Timed out. The CDN PoP takes the action specified by **Action After Timeout** and accepts the user request.

Figure 2-39 Remote authentication



Status	Enabled	
Authentication Server Address	https://192.168.9.1/remoteauth	
Request Method	GET	
File Type	All	
Parameters to Retain	All	
Custom URL Parameters	Unconfigured	
Request Headers to Retain	All	
Custom Request Header Parameters	Unconfigured	
Authentication Status Codes	Success Status Code	200
	Failure Status Code	403
Action After Failure	Custom Response Status Code	403
Authentication Timeout	Timeout Interval	500 ms
	Action After Timeout	Accept

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.

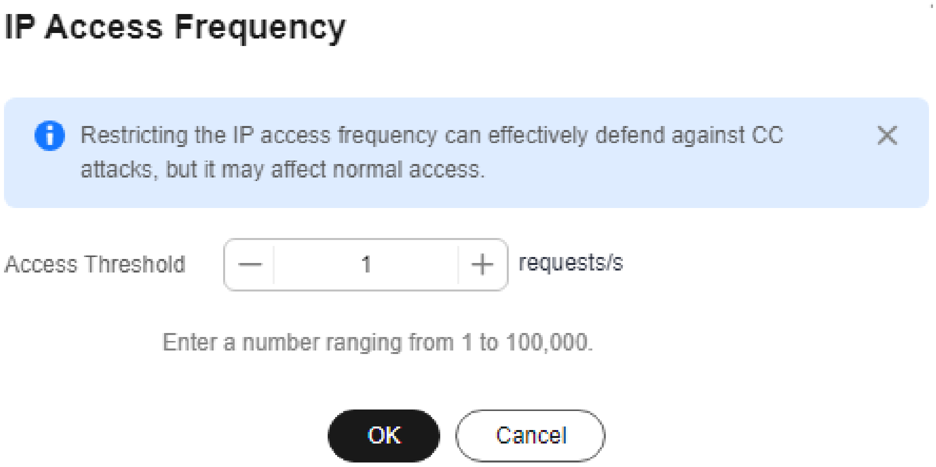
- By default, this function is disabled.

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 2-40 IP access frequency

   IP Access Frequency

   Restricting the IP access frequency can effectively defend against CC attacks, but it may affect normal access.

   Access Threshold 1 requests/s

   Enter a number ranging from 1 to 100,000.

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 requests/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 Overview

- You can modify advanced settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned.

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 to reduce the file size, speed up file transfer, and save bandwidth.
Request Rate Limiting	You can limit the user request rate within a specific range to reduce costs and the risk of burst bandwidth.

2.8.2 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 rules.
- 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.
- If a CORS rule is configured on the CDN console, synchronize it to your origin server. If your origin server is the domain name of an OBS bucket, configure **CORS** on OBS.

Supported Response Headers

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

- **Content-Disposition**

  This header can start a download on clients 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 example, TXT or JPG), the file is opened using the browser by default. You can use this header to treat the file as an attachment and let users save it with a specific file name.

- **Content-Language**

  This header specifies the preferred language or language combination of the browser. Content can be customized for different users.

- **Access-Control-Allow-Origin**

  This 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 content to the client based on this header. For a preflight request, the browser determines whether to initiate an actual CORS request to the server based on this header.

  NOTE

  To prevent cross-domain errors caused by browser cache, clear browser cache after configuring **Access-Control-Allow-Origin**.

- **Access-Control-Allow-Methods**

  This 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 content to the client based on this header. For a preflight request, the browser determines whether to initiate an actual CORS request to the server based on this header.

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

  This header determines how long the results of CORS preflight requests allowed by the server can be cached. The browser determines the TTL for preflight request results based on this header. As long as the TTL has not expired, the browser can determine whether to initiate a CORS request to the server. Once this TTL expires, the browser needs to send another preflight request to the server.

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

  This header specifies the response headers that the browser can expose to the client. You can use this header 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**.

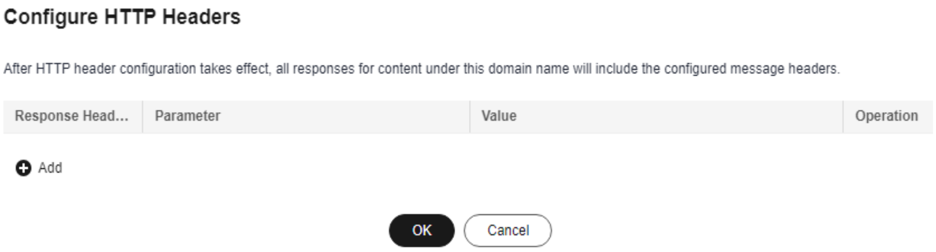
- **Custom**

  If the preceding response headers cannot meet your needs, you can create response headers. A custom response header contains 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 2-41 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

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

Response Header Operation	Description
Set	● 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	Starts a download on the client side and specifies the name of the file to be downloaded. **Value requirements**: Enter 1 to 1,000 characters. For a typical configuration, see the example on the right.	attachment;filename=FileName.xls

Parameter	Description	Example Value
Content-Language	Specifies the language of the response page of the client. **Value requirements**: Enter 1 to 1,000 characters. For a typical configuration, see the example on the right.	zh-CN en-US
Access-Control-Allow-Origin	Specifies the foreign domain URLs (request sources) that are allowed to access the resource in CORS. **Value requirements**: ● 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.	Example 1: https://www.example.com Example 2: * Example 3: https://www.example.com,https://www.example01.com,https://*.abc.com
Access-Control-Allow-Methods	Specifies the HTTP request methods that can be used in a CORS request. **Value requirements**: Enter 1 to 1,000 characters. Separate methods by commas (,).	GET,POST,HEAD

Parameter	Description	Example Value
Access-Control-Max-Age	Specifies how long to cache the results of CORS preflight requests on specific resources. **Value requirements**: This value is expressed in seconds and ranges from 0 to 1,000,000,000.	86400
Access-Control-Expose-Headers	Specifies the response header information visible to the client for a CORS request. **Value requirements**: Enter 1 to 1,000 characters. Multiple headers can be configured at the same time. Separate them by commas (,).	Content-Length,Content-Encoding
Access-Control-Allow-Headers	Specifies the fields that can be carried in a cross-domain request. **Value requirements**: Enter 1 to 1,000 characters. Multiple fields can be configured at the same time. Separate them by commas (,).	X- Custom-Header

Parameter	Description	Example Value
Custom	Specifies the custom response header for a CORS request. A response header starts with a letter and contains 1 to 100 characters, including letters, digits, and hyphens (-). **Value requirements**: Enter 1 to 1,000 characters, which can contain letters, digits, spaces, and the following special characters: .-_*#!&+|^~'"/:;,=@?<> **NOTE** ● 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). Enter up to 10 values and separate them 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 only be modified. **Response Header Operation** cannot be set to **Delete** for them.

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

- CDN does not support the following response headers.

a_dynamic	upgrade	content-md5
accept-ranges	meter	content-range
keep-alive	www-authenticate	date
allow	proxy-authenticate	range
set-cookie	connection	etag
authentication-info	content-encoding	retry-after
last-modified	proxy-authorization	error
location	content-length	if-modified-since
transfer-encoding	content-location	host

2.8.3 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 4*xx* and 5*xx*.
- If CDN acceleration is enabled for the custom error pages, you will be billed by CDN.

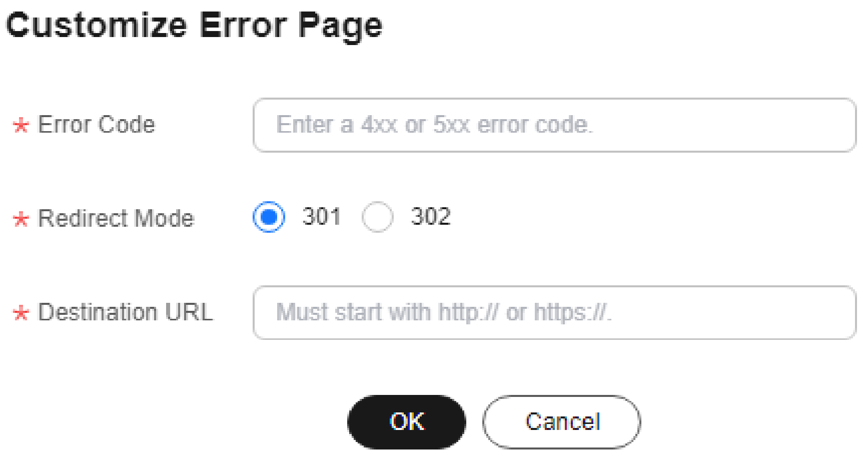
Procedure

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 2-42 Customizing an error page



Customize Error Page

* Error Code: Enter a 4xx or 5xx error code.

* Redirect Mode: ● 301 ○ 302

* Destination URL: Must start with http:// or https://.

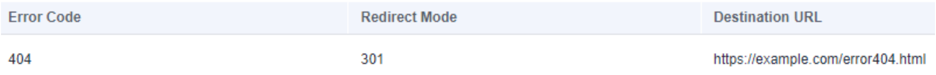
Table 2-31 Parameter description

Parameter	Description	Example
Error Code	Error code (4*xx* or 5*xx*) 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.

2.8.4 Smart Compression

When smart compression is enabled, CDN automatically compresses your static files. This saves you a lot of bandwidth by reducing file size and speeds 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

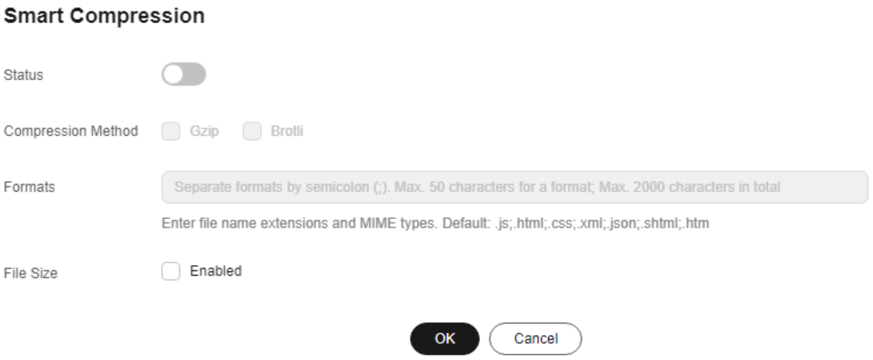
- Starting in late January 2025, CDN will change the default file size for compression. If you do not specify a file size when enabling smart compression:
  - Before the change, all files are compressed by default.
  - After the change, files whose size ranges from 0 MB to 30 MB are compressed by default.
- 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 2-43 Smart compression



Smart Compression

Status ○

Compression Method □ Gzip □ Brotli

Formats: Separate formats by semicolon (;). Max. 50 characters for a format; Max. 2000 characters in total

Enter file name extensions and MIME types. Default: .js;.html;.css;.xml;.json;.shtml;.htm

File Size □ Enabled

Table 2-32 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). ● 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 **.js;.html;.css;.xml;.json;.shtml;.htm** is used.
File Size	Select **Enabled** and specify a file size range (0 MB to 30 MB). Files in this range will be compressed.

6. Select a compression method, specify formats of files to compress, and click **OK**.

2.8.5 WebSocket

If you have added whole site acceleration domain names to CDN to meet requirements such as on-screen commenting, collaborative session, market data broadcast, sports live update, online education, and IoT connectivity, you can configure WebSocket to implement long-term bidirectional data transmission.

Background

WebSocket is a protocol providing full-duplex communication channels over a single TCP connection. It allows a server to proactively push data to clients, simplifying data exchange between the clients and server. A persistent connection can be established between a browser and the server after one handshake and bidirectional data transmission can be performed, saving server resources and bandwidth.

Precautions

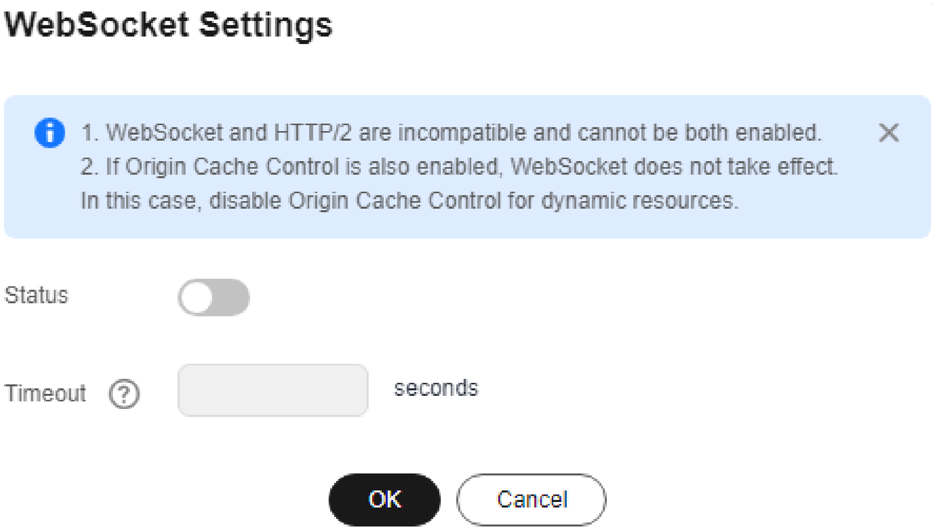
- This function applies only to domain names whose service type is whole site acceleration and whose resources are not cached on CDN PoPs. That is, the cache TTL in cache rules of the resources is set to **0**.
- This function is in OBT and is available for free trial.
- The maximum timeout interval is 300 seconds. If no message is transferred within the specified interval, the connection is closed.
- Do not enable both WebSocket and **HTTP/2**. Otherwise, your domain name cannot be accessed.

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 **WebSocket Settings** area, click **Edit**.

   Figure 2-44 WebSocket Settings

   WebSocket Settings

   1. WebSocket and HTTP/2 are incompatible and cannot be both enabled.
   2. If Origin Cache Control is also enabled, WebSocket does not take effect. In this case, disable Origin Cache Control for dynamic resources.

   Status

   Timeout seconds

6. Enable **Status**, set a proper timeout interval (1s to 300s), and click **OK**.

2.8.6 Request Rate Limiting

You can 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**.

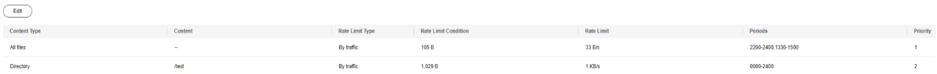
Procedure

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**.
6. Click **Add** to add a rule.

Figure 2-45 Configuring request rate limiting



Content Type	Content	Rate Limit Type	Rate Limit Condition	Rate Limit	Periods	Priority
All files	--	By traffic	105 B	33 B/s	2200-2400,1330-1500	1
Directory	/test	By traffic	1,029 B	1 KB/s	0000-2400	2

Table 2-33 Parameters

Parameter	Description
Content Type	● **All files** ● **Directory**: files in a specific directory
Content	● This parameter is left blank when **Content Type** is set to **All files**. ● When **Content Type** is set to **Directory**, specify this parameter. 1. Start with a slash (/), for example, **/test/folder**. 2. Do not end with a slash (/). 3. Enter one directory per 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. ● 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. ● The maximum value is 100 Mbit/s.
Periods	Periods when the rate is limited, in the 24-hour clock. Period format: HHMM-HHMM (in UTC+08:00). Periods are separated by commas (,). Example: **0100-0200,2200-2300**. Default value: **0000-2400**, indicating all day. ● You can set up to 10 periods.
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. ● Enter an integer ranging from 1 to 100. A greater number indicates a higher priority.

7. Set required parameters and click **Save**.

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
  ```

  In this example, 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 **Query Parameters** is set to **Ignore all** for MP4 and FLV files. For details, see **PoP Cache Rules**.
- Video seek is valid only when your origin server supports range requests.
- Only MP4 and FLV videos are supported.

Table 2-34 File formats

File Format	Meta Information	Start Parameter	Example
MP4	The meta information of a video on your origin server must be contained in the file header rather than the file tail.	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.	`http://www.example.com/test.mp4?start=50` The playback starts from the 50th second.
FLV	A video on your 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.	`http://www.example.com/test.flv?start=500` The playback starts from the 500th byte.

Precautions

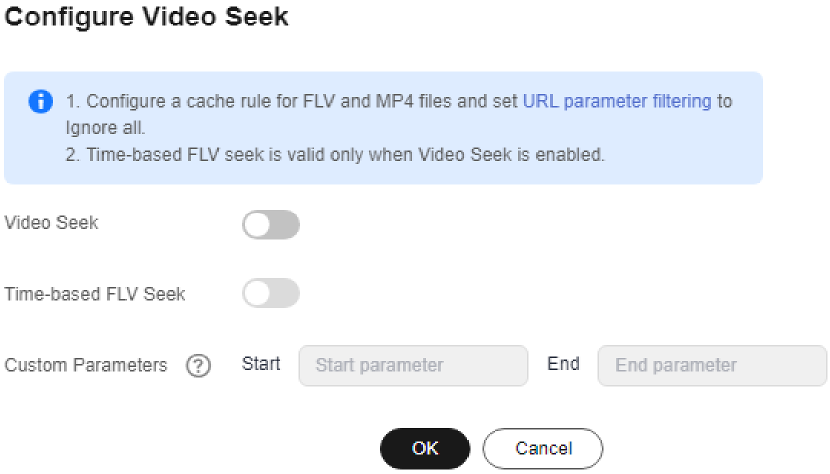
- You have configured a cache rule for FLV and MP4 files and .
- If the service type of your domain name is whole site acceleration, this function takes effect only for static resources.

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 **Video Settings** tab.
5. Click **Edit** next to **Video Seek**.

Figure 2-46 Configuring video seek



Configure Video Seek

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.

6. (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.
7. (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 (_).
8. 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.

Constraints

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

Adding a Tag in the Domain Name List

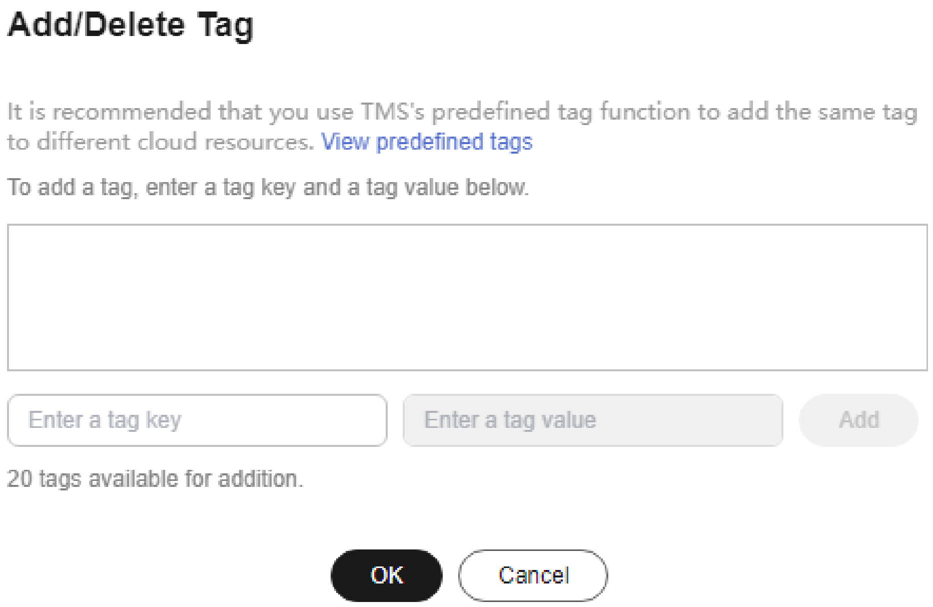
1. Log in to **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

   The CDN console is displayed.

2. In the navigation pane, choose **Domains**.

3. Click ✎ in the **Tags** column in the row containing the target domain name.

   Figure 2-47 Editing a tag



Add/Delete Tag

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

To add a tag, enter a tag key and a tag value below.

20 tags available for addition.

Table 2-35 Parameter description

Parameter	Description	Example
Tag key	● 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
Tag value	● Enter 1 to 255 characters. ● Enter letters, digits, spaces, and special characters (_.:=+-@/). Do not start or end with a space.	HTTPS

4. Enter the tag key and value and click **Add**.

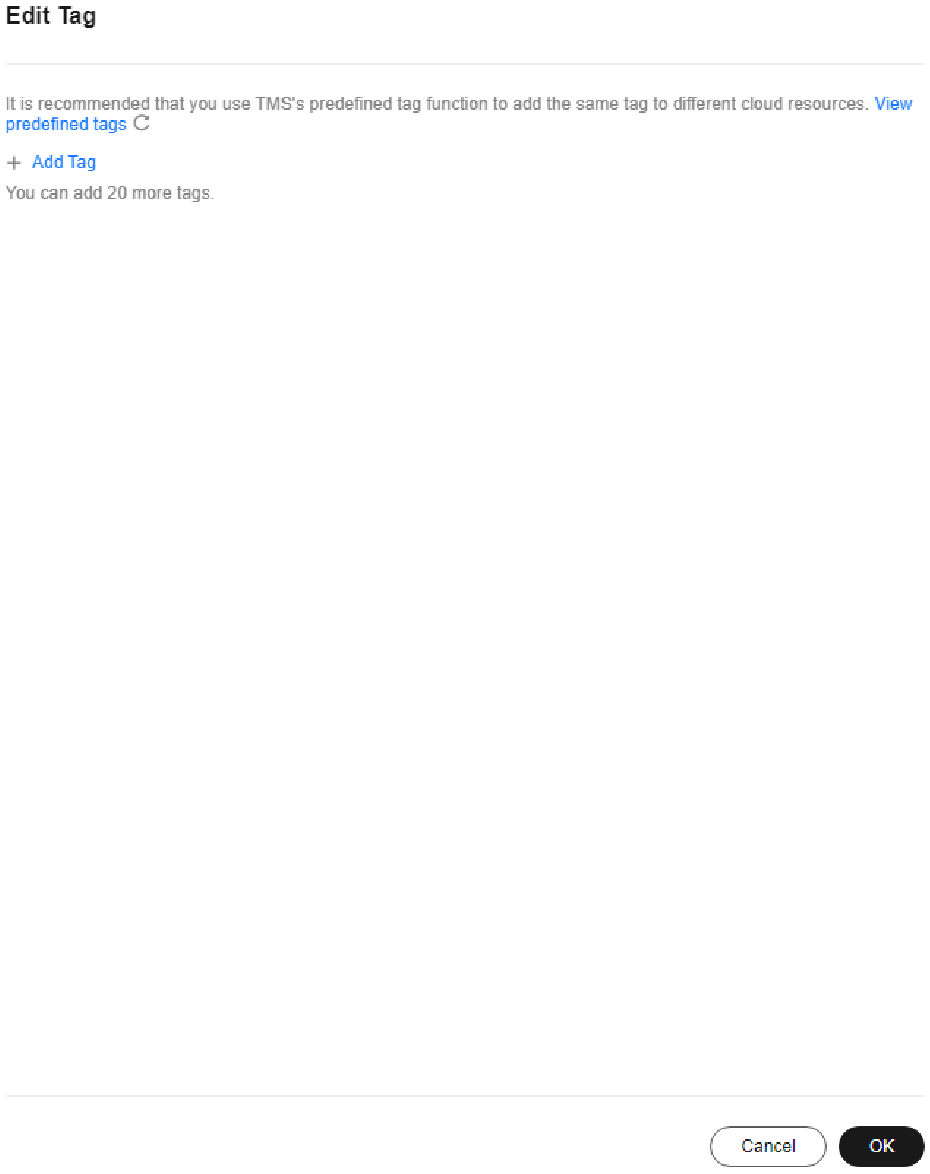
   The tag is added to the text box above.
5. Click **OK**.

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 2-48 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 ↻

You can add 20 more tags.

Table 2-36 Parameter description

Parameter	Description	Example
Tag key	- 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	● 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 **Domains** 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. Click ✎ in the **Tags** column in the row containing the target domain name.

  d. Delete the tag key-value pair in the text box and click **OK**.
- 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 Prefetch and Purge

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 caches that new content.
- **Cache Prefetch** allows the origin server to proactively send the most current content to CDN PoPs. If users request the content, CDN PoPs immediately return the cached content. They do not need to pull any new content.

Prerequisites

Cache purge and prefetch can only be performed for unbanned domain names in the **Enabled** or **Configuring** state. For more information about the domain status, see **Viewing Basic Domain Information**.

3.2 Cache Prefetch

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.

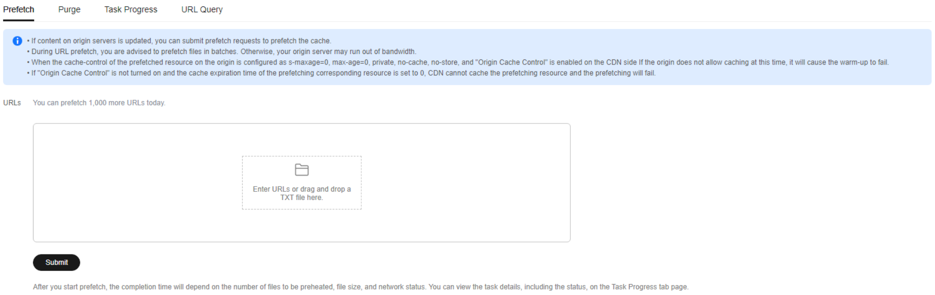
Procedure

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



- If content on origin servers is updated, you can submit prefetch requests to prefetch the cache.
- During URL prefetch, you are advised to prefetch files in batches. Otherwise, your origin server may run out of bandwidth.
- When the cache-control of the prefetched resource on the origin is configured as s-maxage=0, max-age=0, private, no-cache, no-store, and "Origin Cache Control" is enabled on the CDN side If the origin does not allow caching at this time, it will cause the warm-up to fail.
- If "Origin Cache Control" is not turned on and the cache expiration time of the prefetching corresponding resource is set to 0, CDN cannot cache the prefetching resource and the prefetching will fail.

URLs You can prefetch 1,000 more URLs today.

Enter URLs or drag and drop a TXT file here.

After you start prefetch, the completion time will depend on the number of files to be preheated, file size, and network status. You can view the task details, including the status, on the Task Progress tab page.

Table 3-1 Parameter description

Type	Description
URL prefetch ● CDN prefetches a specific file.	The format of a URL in the text box or in the TXT file must meet the following requirements: ● http:// or https:// must be included. ● Enter one URL per row. ● End the homepage URL with a slash (/). Example: http://www.example.com/ ● Each account can prefetch a maximum of 1,000 URLs per day or per task. Examples: 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

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.

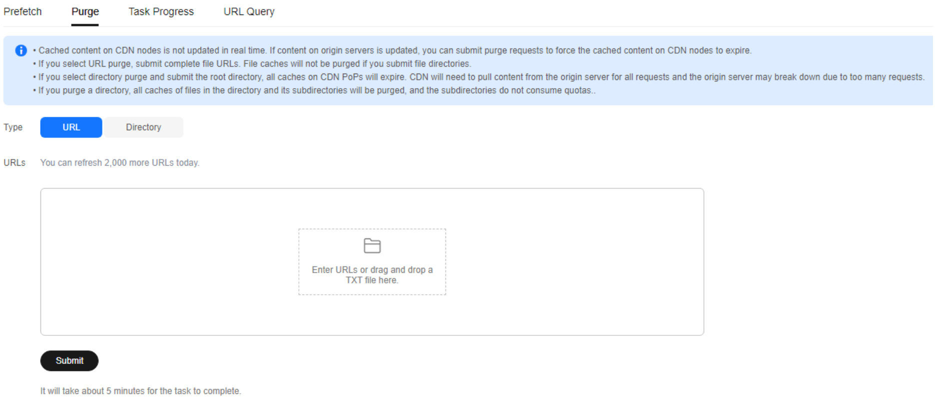
Procedure

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



- Cached content on CDN nodes is not updated in real time. If content on origin servers is updated, you can submit purge requests to force the cached content on CDN nodes to expire.
- If you select URL purge, submit complete file URLs. File caches will not be purged if you submit file directories.
- If you select directory purge and submit the root directory, all caches on CDN PoPs will expire. CDN will need to pull content from the origin server for all requests and the origin server may break down due to too many requests.
- If you purge a directory, all caches of files in the directory and its subdirectories will be purged, and the subdirectories do not consume quotas..

Type: URL

URLs: You can refresh 2,000 more URLs today.

It will take about 5 minutes for the task to complete.

Table 3-2 Parameter description

Type	Description
URL ● CDN refreshes a specific file.	The format of a URL in the text box or in the TXT file must meet the following requirements: ● Each account can refresh a maximum of 2,000 URLs per day and a maximum of 1,000 URLs per task. ● http:// or https:// must be included. ● End the homepage URL with a slash (/). Example: http://www.example.com/ ● Enter one URL per row. **Examples:** http://www.example.com/file01.html http://www.example.com/file02.html https://example.huawei.com/download/app/abc.apk **NOTE** ● 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
Directory ● CDN refreshes all files in a directory.	**Mode**: ● **Purge updated resources**: Purge resources that have been updated in a directory (including subdirectories). ● **Purge all resources**: Purge all resources in a directory, including resources in subdirectories. **Configuration rules:** ● 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. **Examples:** http://www.example01.com/folder01/ http://www.example01.com/folder02/ NOTE ● URLs in the text box or in the TXT file have the same format. ● If you select **Purge 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 **Purge 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

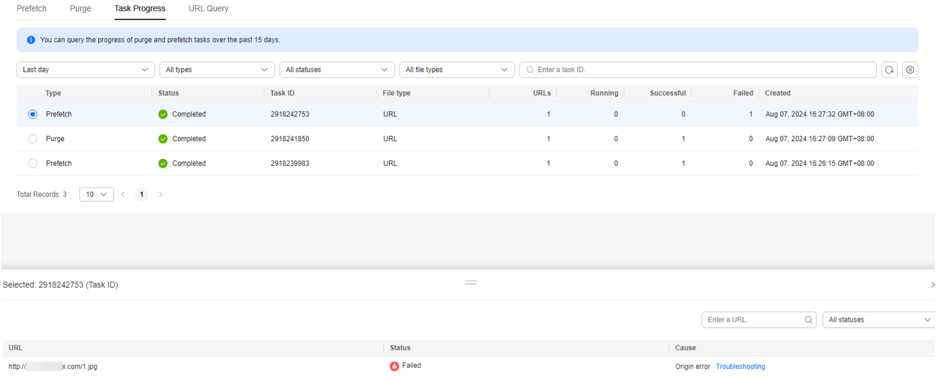
After a cache purge or prefetch task is submitted, you can view the task status on the **Task Progress** tab page.

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. Click the **Task Progress** tab to check the task status.
   - You can view the failure cause of a failed task.

Figure 3-3 Purge and prefetch history



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

Last day | All types | All statuses | All file types | Enter a task ID.

	Type	Status	Task ID	File type	URLs	Running	Successful	Failed	Created
●	Prefetch	Completed	2918242753	URL	1	0	0	1	Aug 07, 2024 16:27:32 GMT+08:00
○	Purge	Completed	2918241850	URL	1	0	1	0	Aug 07, 2024 16:27:09 GMT+08:00
○	Prefetch	Completed	2918239983	URL	1	0	1	0	Aug 07, 2024 16:26:15 GMT+08:00

Total Records: 3 10 < 1 >

Selected: 2918242753 (Task ID)

Enter a URL. | All statuses

URL	Status	Cause
http://[redacted]i.com/1.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.

4 Analytics

4.1 Service Monitoring

4.1.1 Access Requests

You can view the traffic/bandwidth usage and number of requests/QPS of all domain names by **visitor region** or **carrier**. (If you have enabled the enterprise project function, domain names deleted do not support this function).

Precautions

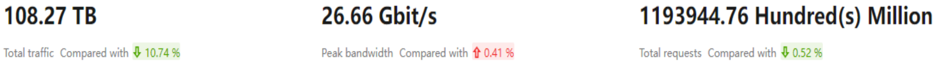
- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- If no data is available for the queried domain name within the specified time span, no data is displayed in the trend charts.
- The minimum granularity is 5 minutes. If the query time range is 8 days or longer, the minimum granularity is 1 hour.
- There is a delay of about one hour for data displayed on the **Access Requests** tab.
- You can export the query results.
- You can filter statistics by tag, service type, region, carrier, HTTP version, and Internet Protocol (IP) version.
- 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 **Analytics (New)** > **Service Monitoring**.
3. Click the **Access Requests** tab and set search criteria. You can query the following data:

- Period over period change: displays the data comparison result between the current statistical period and the previous period.



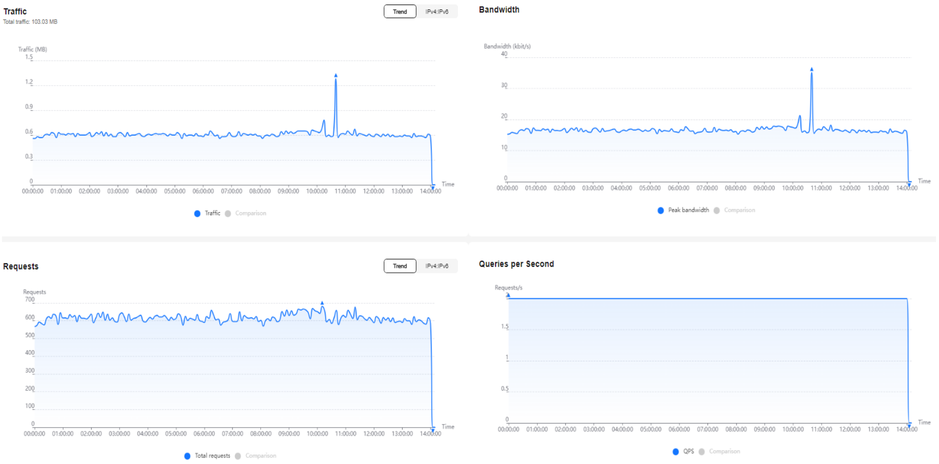
108.27 TB
Total traffic Compared with ⇩ 10.74 %

26.66 Gbit/s
Peak bandwidth Compared with ⇧ 0.41 %

1193944.76 Hundred(s) Million
Total requests Compared with ⇩ 0.52 %

- **Traffic/Bandwidth**: displays the traffic/bandwidth of specific domain names over time.
  - The 95th percentile bandwidth and the average daily peak bandwidth are both shown for the same time span. If no bandwidth statistics are generated within the queried time span, the 95th percentile bandwidth line or the average daily peak bandwidth line is not displayed.
  - You can view the comparison between the IPv4 and IPv6 traffic.
- **Requests/Queries per Second (QPS)**: displays the number of requests or queries per second of specific domain names over time.
  - You can view the comparison between the number of IPv4 requests and IPv6 requests.

Figure 4-1 Data trend charts



4.1.2 Origin Pulls

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

Precautions

- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- If no data is available for the queried domain name within the specified time span, no data is displayed in the trend charts.
- The minimum granularity is 5 minutes. If the query time range is 8 days or longer, the minimum granularity is 1 hour.
- There is a delay of about one hour for data displayed on the **Origin Pulls** tab.

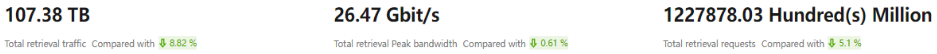
- You can filter domain names by tag, service type, region, and enterprise project.
- You can export origin pull statistics.

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 (New)** > **Service Monitoring**.
3. Click the **Origin Pulls** tab and set search criteria. You can query the following data:
   - Period over period change: displays the data comparison result between the current statistical period and the previous period.

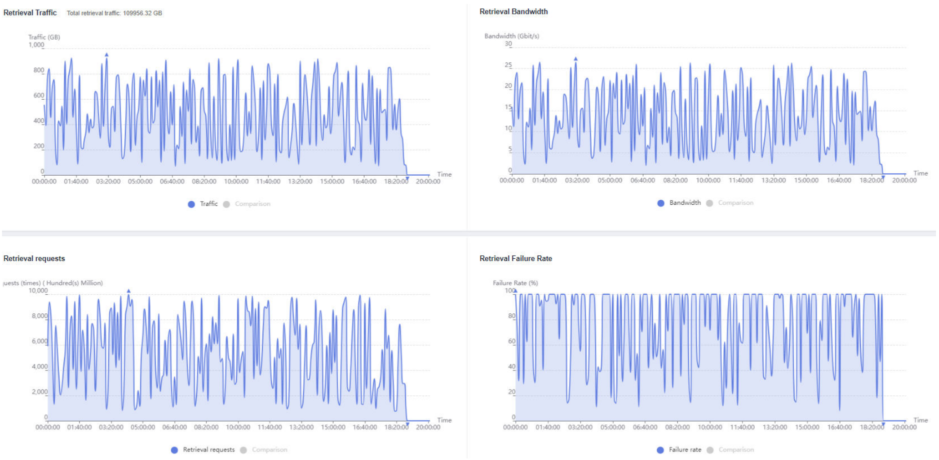
     107.38 TB
     Total retrieval traffic Compared with ⇩ 8.82 %

     26.47 Gbit/s
     Total retrieval Peak bandwidth Compared with ⇩ 0.61 %

     1227878.03 Hundred(s) Million
     Total retrieval requests Compared with ⇩ 5.1 %

   - **Retrieval Traffic**: displays the origin traffic of specific domain names in the specified period.
   - **Retrieval Bandwidth**: displays the origin bandwidth of specific domain names in the specified period.
   - **Origin Requests**: displays the number of origin pull requests in the specified period.
   - **Retrieval Failure Rate**: displays the origin pull failure rate in the specified period.
     - Retrieval failure rate = Number of failed origin pull requests/Number of total origin pull requests
     - 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 2*xx*, 3*xx*, 404, or 416, the request is successful. Other status codes indicate that the request fails.

Figure 4-2 Data trend charts



4.1.3 Hit Ratios

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

Precautions

- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- If no data is available for the queried domain name within the specified time span, no data about the hit ratios is displayed.
- The default minimum statistical granularity is 5 minutes. If the query time range is 8 days or longer, the minimum statistical granularity is 1 hour.
- There is a delay of about one hour for data displayed on the **Hit Ratios** tab.
- You can filter domain names by tag, service type, region, and enterprise project.
- You can export hit ratio data.

Procedure

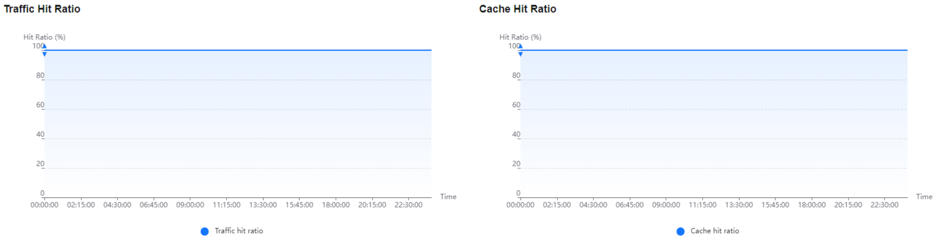
1. Log in to **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

   The CDN console is displayed.
2. In the navigation pane, choose **Analytics (New)** > **Service Monitoring**.
3. Click the **Hit Ratios** tab and set search criteria. You can query the following data:

   Traffic Hit Ratio/**Cache Hit Ratio**: displays the traffic/request hit ratio of specific domain names over time.
   - **Traffic hit ratio** = Traffic generated by requests that hit the cache/Total traffic of requests

     Total request traffic = Traffic generated when CDN PoP caches are hit + Traffic generated during origin pull
   - **Cache hit ratio** = Number of requests that hit caches/Number of total requests

Figure 4-3 Hit ratio statistics



4.1.4 Status Codes

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

Precautions

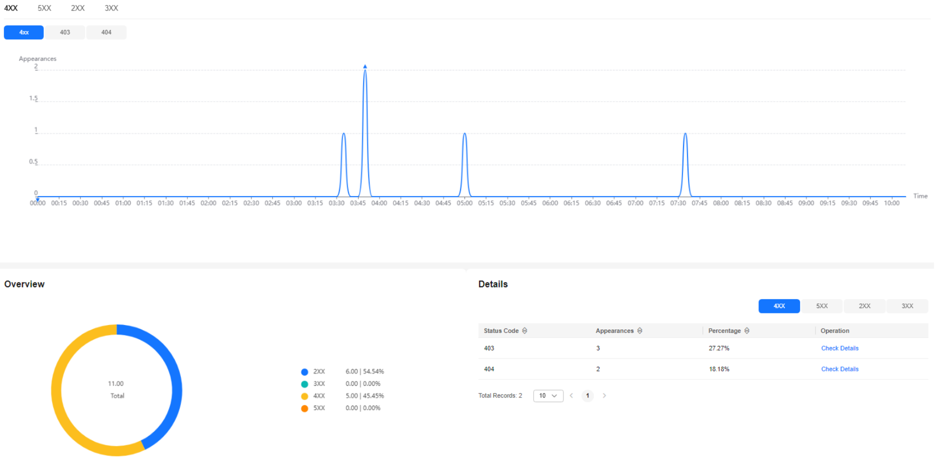
- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- The minimum granularity is 5 minutes. If the query time range is 8 days or longer, the minimum granularity is 1 hour.
- There is a delay of about one hour for data displayed on the **Status Codes** tab.
- You can filter domain names by tag, service type, region, and enterprise project.
- You can export status code statistics.

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 (New)** > **Service Monitoring**.
3. Click the **Status Codes** tab and set search criteria. You can query the following data:
   - Status code tabs: display the appearances of status codes of each type. You can view the trend chart of a status code. Status codes include 2*XX*, 3*XX*, 4*XX*, and 5*XX*. For details, see **Table 4-1**.
   - **Overview**: displays the total number and proportion of appearances of each type of status codes in the query period.
   - **Details**: displays the total number and proportion of each status code in the query period. You can also click **Check Details** to check domain names and top URLs of this status code.

Figure 4-4 Status code statistics



● 2XX 6.00 | 54.54%
● 3XX 0.00 | 0.00%
● 4XX 5.00 | 45.45%
● 5XX 0.00 | 0.00%

Status Code	Appearances	Percentage	Operation
403	3	27.27%	Check Details
404	2	18.18%	Check Details

Total Records: 2 10 < 1 >

Table 4-1 Status code description

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.

4.2 Data Analysis

4.2.1 Operations Reports

You can customize operations reports for domain names to view statistics in different time segments, so that you can learn about the domain status and promptly adjust businesses.

Precautions

- You can add up to 100 domain names to a custom operations report.
- A custom operations report can be valid for up to one year.
- 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.
- You can view the corresponding data only after customizing an operations report. Due to the log integrity latency, a report will be generated on the next day. For example, a report customized on August 2, 2023 will be generated on August 3, 2023.

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 (New)** > **Data Analysis**.
3. CDN provides the following operations reports:
   - **Domain Rankings**: displays domain names by the volume of user visit traffic and origin pull traffic in descending order by default. This report is displayed by default and does not need to be customized.
     - Data of the past 90 days can be queried, and each query can include data of up to 31 days.

- **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.
  - You can filter domain names by service area (**All**, **Europe**, **Chinese mainland**, or **International**).
  - You can filter domain names by service type.
  - You can filter statistics by tag, HTTP version, and IP version.
  - You can filter visitor data by region (global or China). China includes Chinese mainland, Hong Kong, Macao, and Taiwan.
  - Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- **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

Exporting Reports

You can export custom reports to your device. Click **Export** on tabs under the **Operations Report** page to export desired reports in XLSX format.

4.3 Traffic Query

4.3.1 Query

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

Precautions

- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- The query time uses UTC.
- If no data is available for the queried domain name within the specified time span, no data is displayed in the traffic or bandwidth trend chart.
- The minimum granularity is 5 minutes. If the query time range is 8 days or longer, the minimum granularity is 1 hour.
- 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.
- The current usage can be queried about one hour later.
- You can export the query results.
- You can filter domain names by tag or service type.

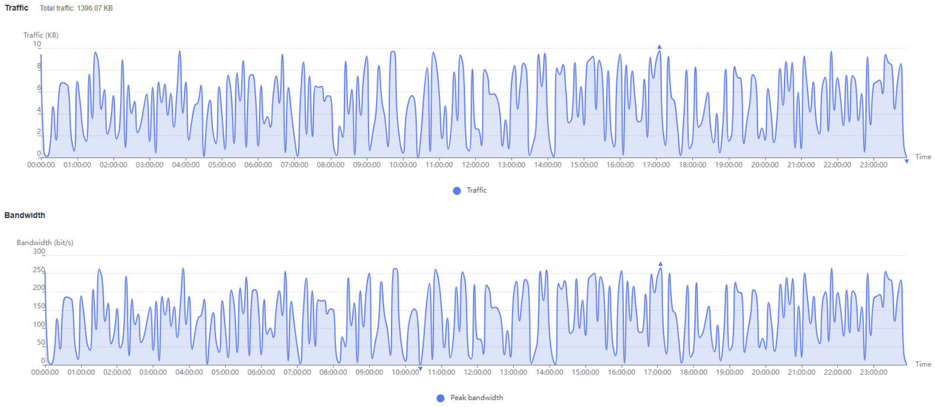
Procedure

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 (New)** > **Traffic Query**.
3. Click the **Traffic Query** tab and set search criteria. You can query the following data:
   - **Traffic**: displays the traffic of specific domain names over time.
   - **Bandwidth**: displays the peak bandwidth of specific domain names over time.

Figure 4-5 Traffic/Bandwidth trend



NOTE

The 95th percentile bandwidth and the average daily peak bandwidth are both shown for the same time span. If no bandwidth statistics are generated within the queried time span, the 95th percentile bandwidth line or the average daily peak bandwidth line is not displayed.

4.3.2 Summary

You can view the traffic/bandwidth usage and number of whole site acceleration requests on a specific day of all domain names (excluding those deleted if you have enabled the enterprise project function).

Precautions

- You can view the usage data of a day in the last 90 days.
- The query time uses UTC.
- By default, statistics about domain names are displayed by charging region.

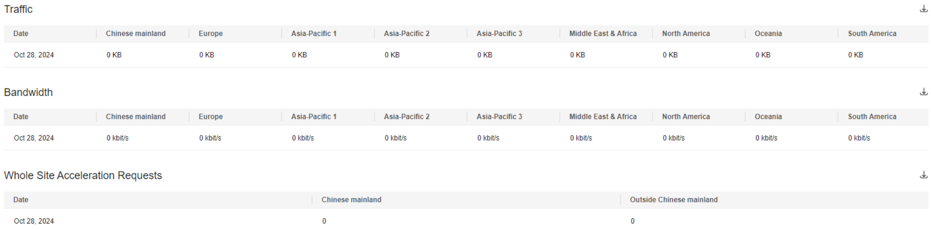
Procedure

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 (New)** > **Traffic Query**.
3. Click the **Summary** tab and select a date.
   - You can export summary data.

Figure 4-6 Summary



Traffic

Date	Chinese mainland	Europe	Asia-Pacific 1	Asia-Pacific 2	Asia-Pacific 3	Middle East & Africa	North America	Oceania	South America
Oct 28, 2024	0 KB	0 KB	0 KB	0 KB	0 KB	0 KB	0 KB	0 KB	0 KB

Bandwidth

Date	Chinese mainland	Europe	Asia-Pacific 1	Asia-Pacific 2	Asia-Pacific 3	Middle East & Africa	North America	Oceania	South America
Oct 28, 2024	0 kbit/s	0 kbit/s	0 kbit/s	0 kbit/s	0 kbit/s	0 kbit/s	0 kbit/s	0 kbit/s	0 kbit/s

Whole Site Acceleration Requests

Date	Chinese mainland	Outside Chinese mainland
Oct 28, 2024	0	0

4.3.3 Whole Site Acceleration

You can view the traffic/bandwidth usage and number of requests sent to all whole site acceleration domain names (excluding those deleted if you have enabled the enterprise project function).

Constraints

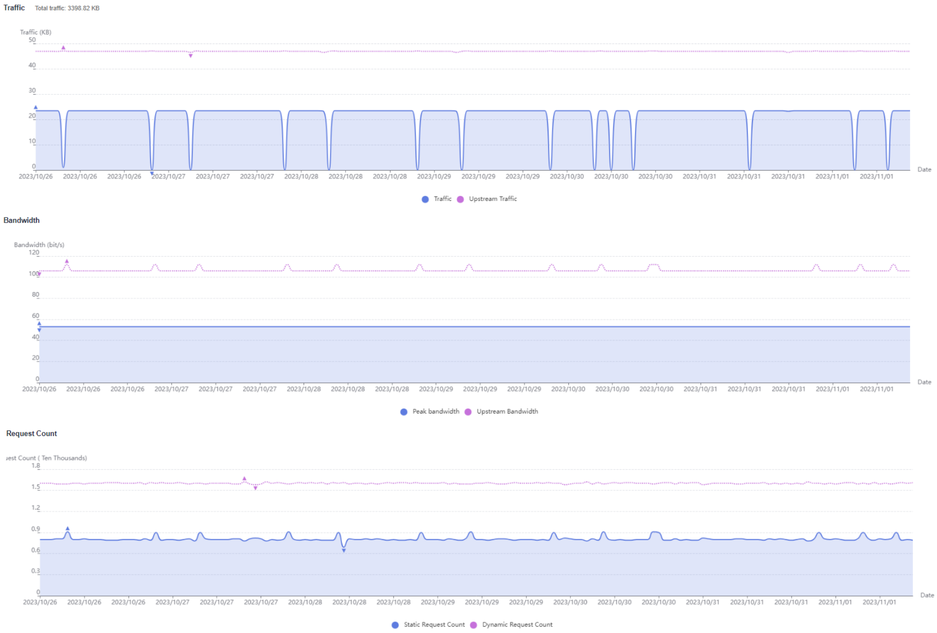
- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- The query time uses UTC.
- If no data is available for the queried domain name within the specified time span, no data is displayed in the traffic, bandwidth, or request quantity trend chart.
- The minimum granularity is 5 minutes. If the query time range is 8 days or longer, the minimum granularity is 1 hour.
- 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.
- The current usage can be queried about one hour later.
- You can filter domain names by tag, service type, or enterprise project.

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 (New)** > **Traffic Query**.
3. Click the **Whole Site Acceleration** tab and set the search criteria. You can query and export the following data:
   - **Traffic**: displays the traffic and upstream traffic of specific domain names over time.
   - **Bandwidth**: displays the peak bandwidth and upstream bandwidth of specific domain names over time.
   - **Request Appearances**: displays the number of dynamic and static requests sent to specific domain names over time.

Figure 4-7 Trend charts



NOTE

The 95th percentile bandwidth and the average daily peak bandwidth are both shown for the same time span. If no bandwidth statistics are generated within the queried time span, the 95th percentile bandwidth line or the average daily peak bandwidth line is not displayed.

4.4 Data Export

You can export statistics about all domain names or specific domain names.

Precautions

- Exported data is retained for seven days. It cannot be downloaded after expired.
- Data is exported in Excel files.

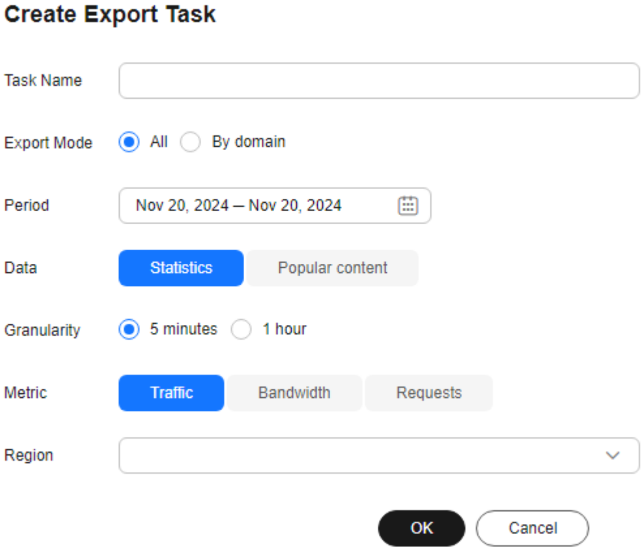
Procedure

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 **Analytics (New)** > **Data Export**.
3. On the **Data Export** page, click **Create Export Task**.

Figure 4-8 Creating an export task



Create Export Task

Task Name

Export Mode ● All ○ By domain

Period Nov 20, 2024 – Nov 20, 2024

Data Statistics | Popular content

Granularity ● 5 minutes ○ 1 hour

Metric Traffic | Bandwidth | Requests

Region

OK Cancel

Table 4-2 Parameter description

Parameter	Description	Example
Task Name	Name of an export task. This parameter is user-defined.	test
Export Mode	- **All**: all data under the entire account - **By domain**: data related to specific domain names – You can specify up to 100 domain names. – Select at least one domain name.	All
Period	Select the time segment of the data to be exported. - Data generated within 365 days can be exported. Bandwidth data generated more than 90 days ago cannot be exported. - The maximum time span is 31 days.	Mar 01, 2023 – Mar 31, 2023
Data	- **Statistics**: data displayed under **Analytics** - **Popular content**: data related to custom operations reports, such as popular URLs, popular referers, and popular user agents **NOTE** - The number of top URLs can be configured on the backend, for example, top 1,000 URLs.	Statistics

Parameter	Description	Example
Granularity	Minimum interval for collecting statistics. Select **5 minutes** or **1 hour**. ● When **Period** exceeds 90 days, only the 1-hour granularity is supported.	5 minutes
Metric	Select **Traffic**, **Bandwidth**, or **Requests** (number of requests). ● When **Data** is set to **Popular content**, **Bandwidth** is unavailable.	Traffic
Region	Region where the data to export is generated. Supported regions include Chinese mainland, outside Chinese mainland, Asia Pacific 1, Asia Pacific 2 (India), Asia Pacific 3 (other regions in Asia Pacific), Europe, North America, Middle East and Africa, South America, and Oceania. Asia Pacific 1 includes Hong Kong (China), Macao (China), Taiwan (China), Japan, and South Korea. **NOTE** When **Data** is set to **Popular content**, **Region** can be **Global**.	Chinese mainland

4. Set required parameters and click **OK** to deliver the task.
5. When the task status is **Exported**, click **Download** in the **Operation** column to download the data to your device.

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.

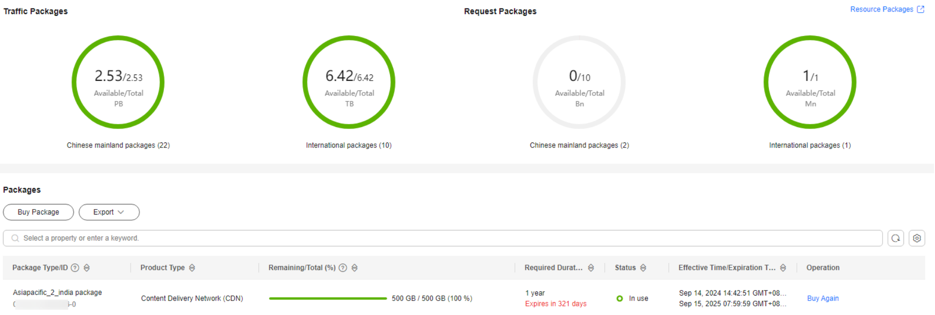
Procedure

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/ID	Product Type	Remaining/Total (%)	Required Durat...	Status	Effective Time/Expiration T...	Operation
Asiapacific_2_india package ([redacted]-0	Content Delivery Network (CDN)	500 GB / 500 GB (100 %)	1 year Expires in 321 days	○ In use	Sep 14, 2024 14:42:51 GMT+08... Sep 15, 2025 07:59:59 GMT+08...	Buy Again

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.
   - 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

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

NOTE

Due to the synchronization latency of the log system, user access logs may not be generated in the first hour after a domain name is connected to CDN. To view logs generated in this period, submit a service ticket.

Log naming: *Period start time-Acceleration domain name-Extended field*.**gz**

Log generation: 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 a period is too large, it will be divided into multiple files, with an extended field added to their names.

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 (client IP address)	x.x.x.x
3	Time to last byte (ms)	1

No.	Field Description	Example
4	Referer information	-
5	HTTP protocol identifier	HTTP/1.1
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 version	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: ● bytes=x-y: requesting content from the *x*th to *y*th byte. ● bytes=-y: requesting content from the last *y* bytes. ● bytes=x-: requesting content from the *x*th to the last byte.	bytes=-256
14	Server IP address, that is, the IP address used by the CDN server to send responses	x.x.x.x

Downloading Logs

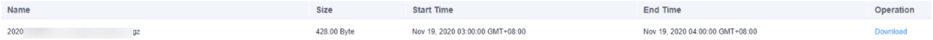
1. Log in to **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

   The CDN console is displayed.

2. In the navigation pane, choose **O&M Tools** > **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[redacted]gz	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 Domain Certificate Management

Background

This topic describes how to set an HTTPS certificate of domain names and deploy the HTTPS configuration on all CDN PoPs to implement secure acceleration.

- **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.

Scenarios

- If you have a certificate, you can directly upload it. You can also view and delete existing certificates.
- You can update certificates in batches. The new certificates will overwrite the original ones.
- You can buy certificates on **CCM**.

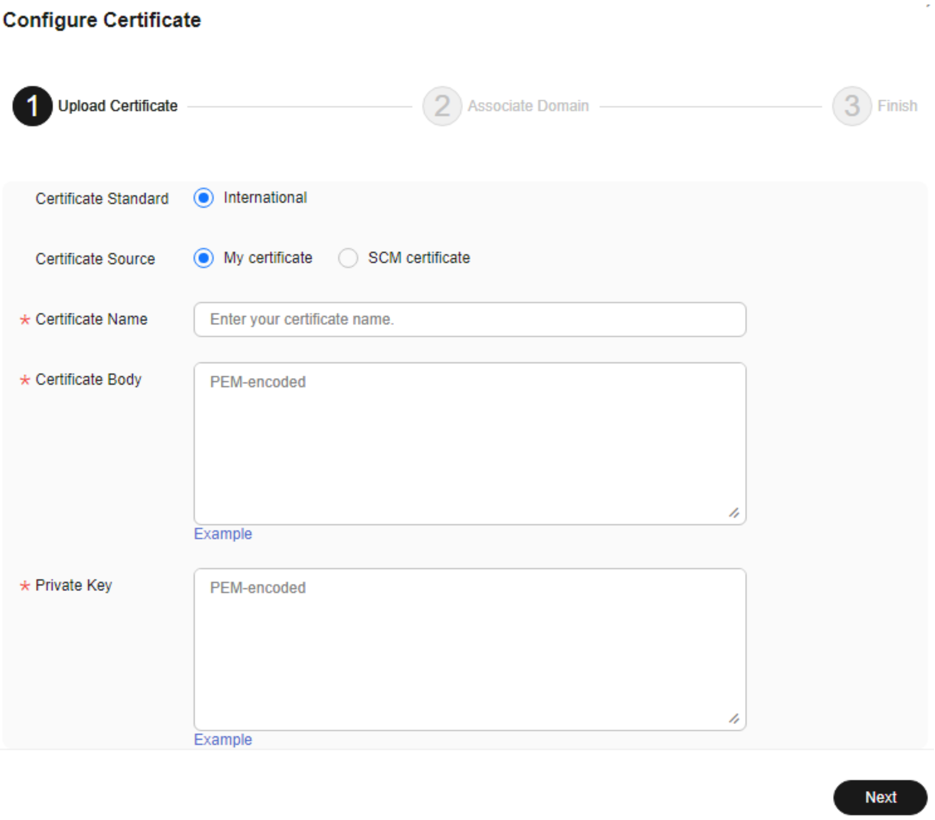
Configuring a Certificate

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 **Certificates**.
3. Click **Configure Certificate** in the upper left corner.

Figure 7-1 Configuring a certificate



Configure Certificate

Certificate Standard ● International

Certificate Source ● My certificate ○ SCM certificate

* Certificate Name: Enter your certificate name.

* Certificate Body: PEM-encoded

Example

* Private Key: PEM-encoded

Example

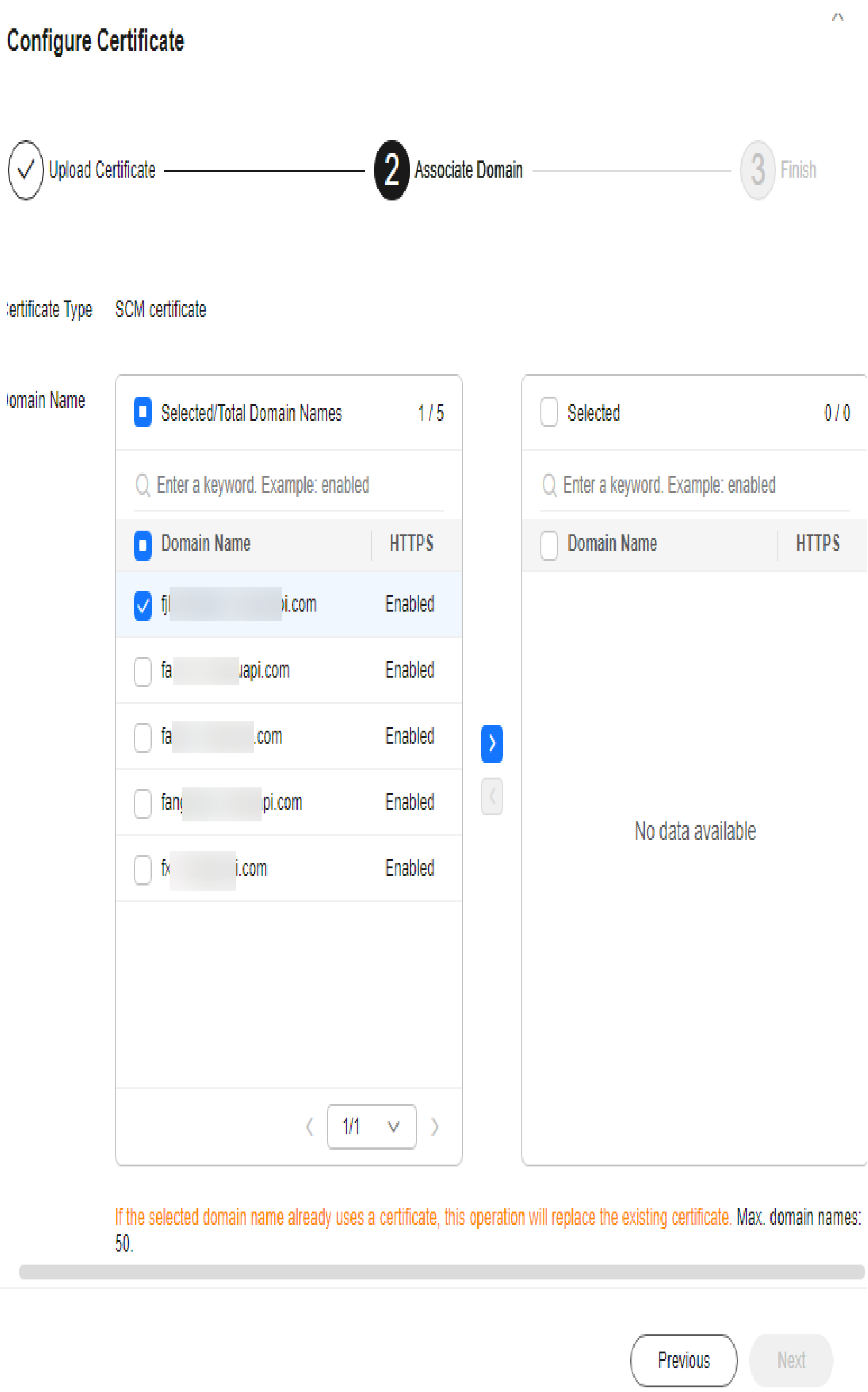
4. Set related parameters.

Table 7-1 Parameters of an international certificate

Parameter	Description
Certificate Standard	International
Certificate Source	Either **My certificate** or **SCM certificate**
Certificate Name	● If you select **My certificate**, enter the certificate name. A certificate name can be up to 32 characters long. ● If you select **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.

Parameter	Description
Certificate Body	● If you select **My certificate**, use a local text editor to open the certificate and copy the certificate content to the text box. For details about the certificate format, see **HTTPS Certificate Requirements**. ● If you select **SCM certificate**, the content is automatically filled in. **NOTE** The certificate body cannot contain spaces or blank lines. Otherwise, a message is displayed indicating that certificate parameters are incorrect.
Private Key	● If you select **My certificate**, use a local text editor to open the private key and copy the content to the text box. For details about private key format requirements, see **RSA Private Key**. ● If you select **SCM certificate**, the content is automatically filled in.

5. Click **Next** to associate the certificate with your domain names.



Configure Certificate

✓ Upload Certificate — 2 Associate Domain — 3 Finish

ertificate Type SCM certificate

omain Name

■ Selected/Total Domain Names	1 / 5
■ Domain Name	HTTPS
☑ fj[redacted]i.com	Enabled
□ fa[redacted]api.com	Enabled
□ fa[redacted].com	Enabled
□ fan[redacted]pi.com	Enabled
□ fx[redacted]i.com	Enabled

Enter a keyword. Example: enabled

1/1

□ Selected	0 / 0
□ Domain Name	HTTPS

Enter a keyword. Example: enabled

No data available

If the selected domain name already uses a certificate, this operation will replace the existing certificate. Max. domain names: 50.

6. Select the domain names to be associated on the left, click > to add them to the right, and click **Next**.

NOTE

- If a selected domain name already uses a certificate, this operation will replace the existing certificate.
- You can search for domain names by HTTPS status.
- You can select up to 50 domain names.

7. Click **Finish** to implement HTTPS secure acceleration for the associated domain names.

8 Diagnosis

8.1 IP Address Check

If the content shown on the access page of the acceleration domain name is abnormal, you can use the PoP IP address checking tool to check whether the specified IP address is the IP address of a Huawei Cloud CDN PoP. In this way, you can know whether the abnormality is caused by the carrier network or other reasons.

- If the check result shows that the IP address is not that of a Huawei Cloud CDN PoP, the problem may lie in the carrier network. In this case, contact your carrier.
- If the IP address belongs to a Huawei Cloud CDN PoP, rectify the fault by referring to **Troubleshooting**.

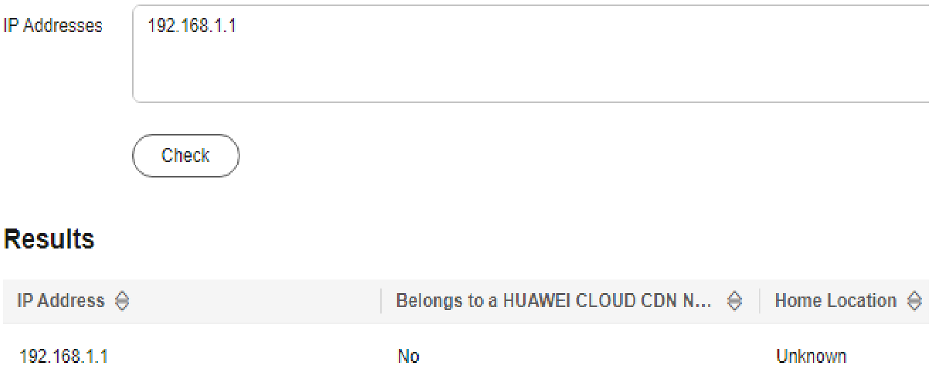
Procedure

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 **Diagnosis** > **IP Address Check** to go to the PoP IP address check page.

   Figure 8-1 Checking PoP IP addresses



IP Addresses: 192.168.1.1

Results

IP Address	Belongs to a HUAWEI CLOUD CDN N...	Home Location
192.168.1.1	No	Unknown

3. Enter the IP addresses to be checked in the **IP Addresses** text box.

   Enter each IPv4 or IPv6 address on separate lines. A maximum of 20 IP addresses can be checked at a time.

4. Click **Check**.

   After the diagnosis is complete, the system displays the results in the list.

9 Permissions Management

9.1 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.

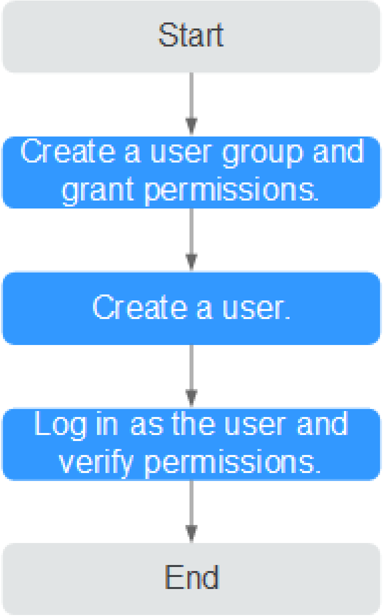
Prerequisites

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

Process Flow

Figure 9-1 shows the process of granting CDN permissions.

Figure 9-1 Process of granting CDN permissions


Start
Create a user group and grant permissions.
Create a user.
Log in as the user and verify permissions.
End

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.

9.2 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"
                }
        ]
}
```

10 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.