CDN

User Guide

Issue 105

Date 2024-05-22

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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.

Contents

1 Domain Name Management

1.1 Functions

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

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

Scenarios

The following table describes the functions.

Table 1-1 Scenarios

Item	Description	API
Enabling/ Disabling CDN for a Domain Name	**Enable**: You can enable a domain name in the **Disabled** state. **Disable**: You can disable a domain name in the **Enabled** state.	Enabling CDN for a Domain Name Disabling CDN for a Domain Name
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.	Deleting a Domain Name

Item	Description	API
Copying Domain Configuration to Existing Domains	You can copy the configuration of a domain name to other domain names.	Copying Domain Configuration
Reviewing a Domain Name	If a domain name is banned due to ICP license expiration, you can apply to have it reviewed after the domain name is re-licensed. Once the review passes, CDN unbans the domain name.	-
Service Termination Policy	Huawei Cloud CDN service is terminated based on a preset policy. You can select **Redirect to origin server** or **Disable domain name** for the termination policy.	-
Domain Name Quota Management	Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas limit the number or amount of resources available to users. If the existing domain name quota cannot meet your service requirements, submit a service ticket to request a higher quota.	-

1.2 Enabling/Disabling CDN for a Domain Name

Scenarios

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

Precautions

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

Figure 1-1 Basic domain information

- Domain statuses include **Enabled**, **Disabled**, **Configuring**, **Error**, **Reviewing**, **Rejected**, and **Removing**.
- You can add remarks to a domain name.

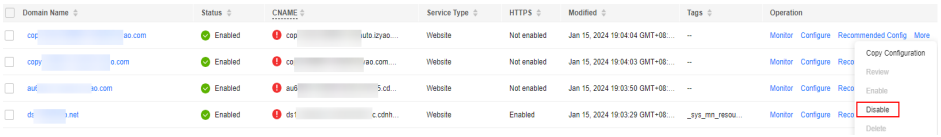
Disabling CDN for Domain Names

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

Disabling CDN for a single domain name

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

   Figure 1-2 Disabling CDN for a domain name

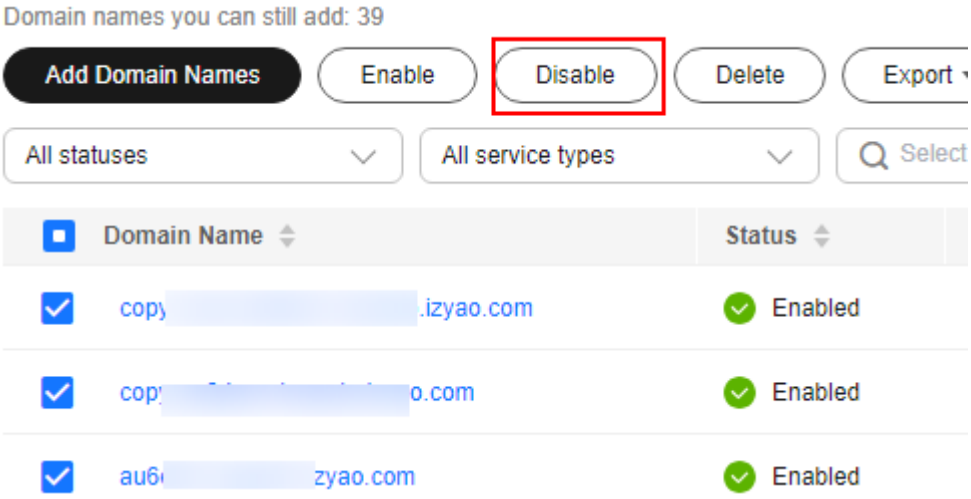


2. Confirm the information about the domain name and click **Yes**.

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.

Figure 1-3 Disabling CDN for multiple domain names



Enabling CDN for Domain Names

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

Enabling CDN for a single domain name

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

   Figure 1-4 Enabling CDN for a domain name

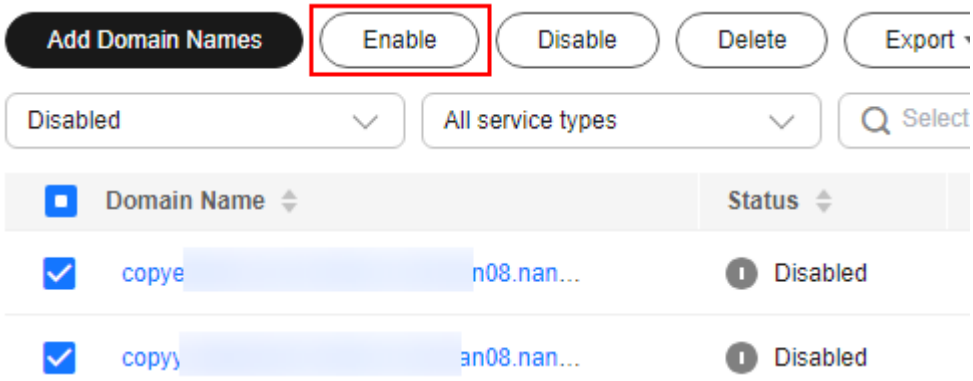
   

2. Confirm the information about the domain name and click **Yes**.

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.

Figure 1-5 Enabling CDN for multiple domain names



1.3 Deleting a Domain Name

Scenarios

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

Precautions

- You can only delete domain names in the **Disabled**, **Error**, 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 Configuring a Shared Cache Group

If different domain names point to the same resources, you can configure a shared cache group and set a primary domain name. Other domain names in the group share the cache of the primary domain name, improving the cache hit ratio.

Precautions

- Domain names in a shared cache group share the cached resources of the primary domain name. If no resources are cached, a large number of origin pull requests may be sent, occupying the origin server bandwidth. Exercise caution when adding a domain name to a shared cache group.
- A domain name can be added to a shared cache group only when **Query Parameters** is set to **Ignore all** or **Retain all**.
- Each shared cache group can contain up to 20 domain names.
- An account can have up to 500 shared cache groups.
- Before deleting a cache group, you need to clear the domain names associated with the group.

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. On the **Domains** page, click **Cache sharing** in the upper right corner.
4. Click **Create Group** to add a shared cache group.

   Figure 1-6 Creating a shared cache group

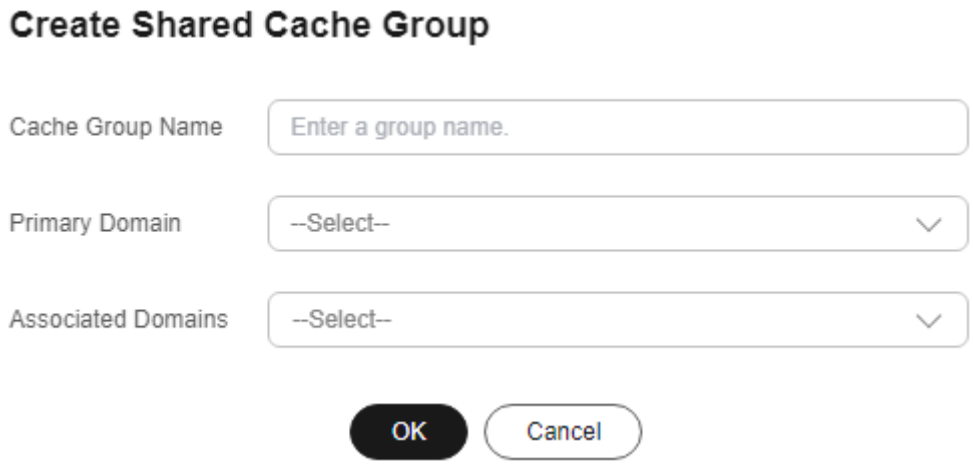
   

   Table 1-2 Parameters

Parameter	Description
Cache Group Name	Name of the shared cache group. A name contains 1 to 128 characters and does not support the following special characters: %&=?$"<>
Primary Domain	Primary domain name of the shared cache group. Other domain names in the group share the cache resources of this domain name.
Associated Domains	Domain names associated with the shared cache group. They share the cache resources of the primary domain name.

5. Set required parameters and click **OK**.

1.5 Copying Domain Configurations

1.5.1 Copying Domain Configuration to Existing Domains

You can copy the configuration of a domain name to existing domain names.

Precautions

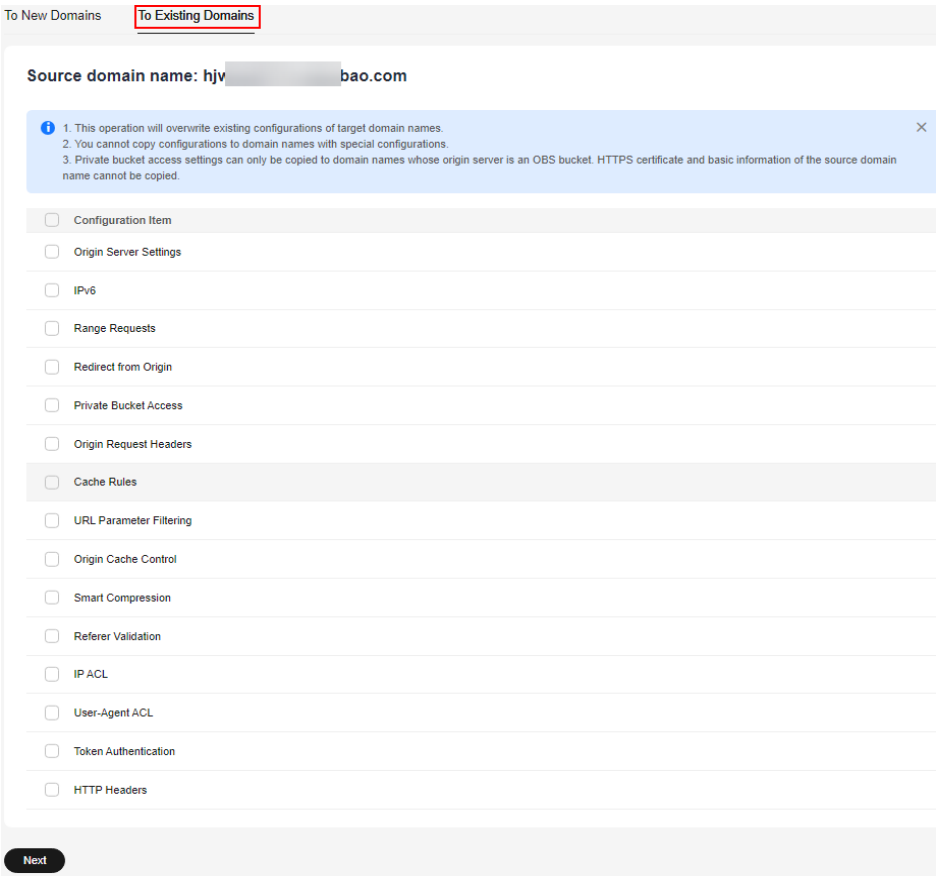
- The domain configuration can be copied only when a domain name in the **Enabled** state.
- Configuration copy cannot be undone. Before copying the configuration of a domain name, ensure that the configuration is correct.
- Special domain configurations cannot be copied.
- For a domain name with high traffic or bandwidth, exercise caution when copying its configuration to avoid economic loss.
- HTTPS certificates and basic information about domain names cannot be copied. To copy the private bucket access settings, the origin server of the target domain name must be an OBS bucket.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. On the **Domains** page, click **More** > **Copy Configuration** in the **Operation** column of the row containing the source domain name. On the displayed page, click the **To Existing Domains** tab.

Figure 1-7 Copying domain configurations

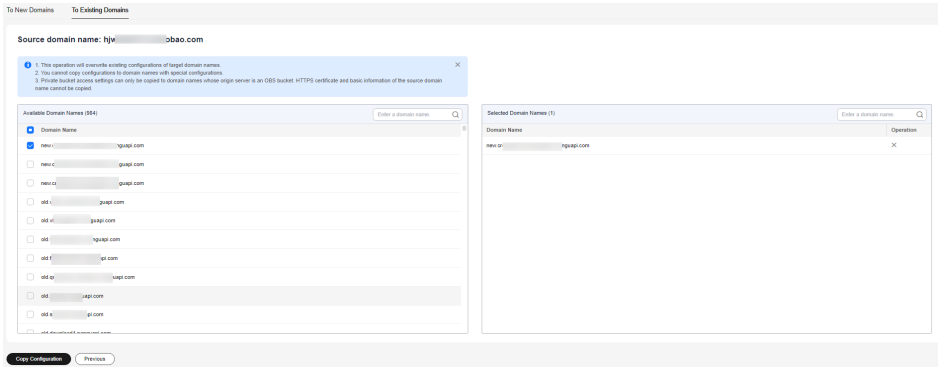


NOTE

If you copy the configuration to other domain names, the original configurations of these domain names will be overwritten.

4. Select the configuration items to be copied and click **Next**.

Figure 1-8 Selecting domain names



NOTE

- If you have enabled the enterprise project function, available domain names will be displayed by enterprise project.
- You can select up to 10 target domain names.
- Configurations cannot be copied to domain names with special configurations.

5. Select the domain names whose configurations need to be overwritten and click **Copy Configuration**.
   - Configuration copy cannot be undone. Ensure that the domain names selected are correct.
6. Click **OK**.

1.5.2 Copying Domain Configuration to New Domains

You can add new domain names to CDN and copy the configuration of an existing domain name to these names.

Scenarios

You can copy the configuration of an existing domain name to one or more new domain names, allowing you to quickly add and customize domain names.

Precautions

- You can copy the configuration of a domain name in the **Enabled**, **Disabled**, or **Rejected** state.
- If a domain name is in the **Deleting**, **Configuring**, **Reviewing**, **Error** state, its configuration cannot be copied.
- The configuration of a banned domain name cannot be copied.
- You can add up to 10 domain names at a time. New domain names occupy your domain **quota**.

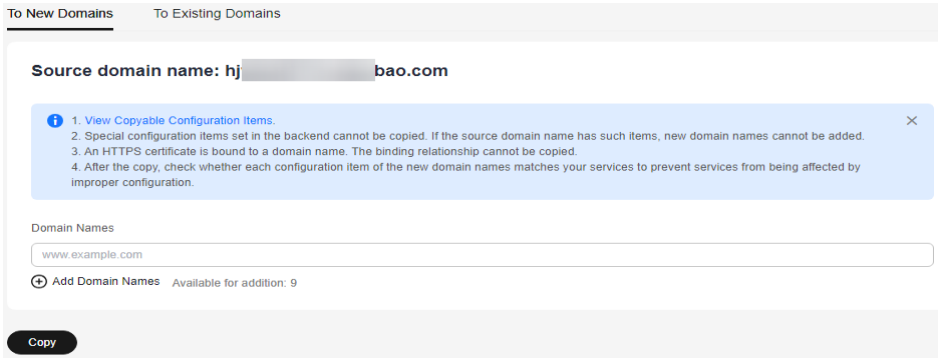
- Some configuration items can be copied. For details, see **Configuration Items That Can Be Copied**.
- Special configuration items set in the backend cannot be copied. If the source domain name has such items, new domain names cannot be added.
- The domain name status cannot be copied.
- An HTTPS certificate is bound to a domain name. The binding relationship cannot be copied.
- After the copy, you can check whether each configuration item of the new domain names matches your services to prevent services from being affected by improper configuration.

Procedure

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

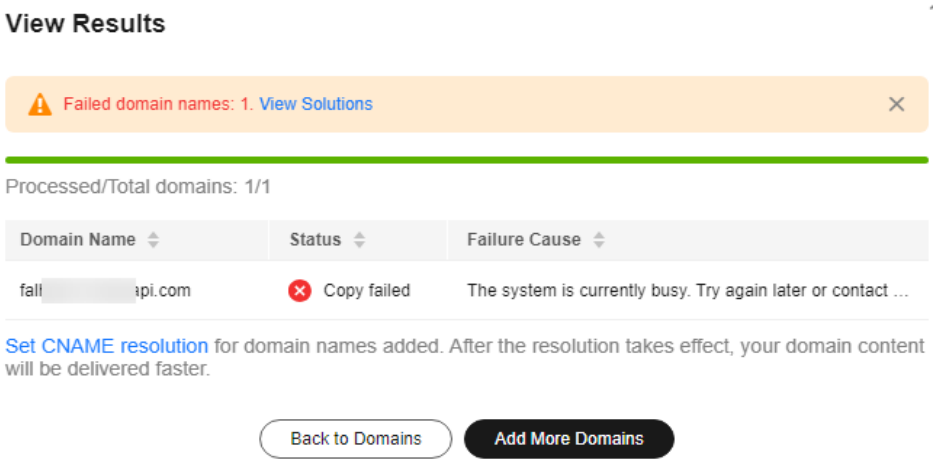
   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. On the **Domains** page, click **More** > **Copy Configuration** in the **Operation** column of the row containing the source domain name. On the displayed page, click the **To New Domains** tab.

   Figure 1-9 Copying configurations to new domain names

4. Enter the domain names to be added and click **Copy**.
   - The copy operation cannot be paused. You can modify the configuration items after the copy is complete.
5. In the displayed dialog box, click **OK** to copy the configuration.
6. View the copy progress and results of adding domain names.

Figure 1-10 Results of adding domain names



Configuration Items That Can Be Copied

The following table lists the configuration items that can be copied.

- The configuration items in the following table are visible on the console. If you have asked the O&M personnel to configure special configuration for the source domain name, the special configuration cannot be copied to new domain names. You can submit a service ticket to configure special configuration for new domain names.

Table 1-3 Supported configuration items

Category	Item
Basic settings	Enterprise project (If you log in as an IAM user and do not have the permission to access the enterprise project, domain names cannot be added.)
	Service type
	Service area

Category	Item
	Origin server settings • The host is also copied. The rules are as follows: – If the origin server of the source domain name is an IP address or domain name and a custom host is set, new domain names use this custom host. – If the origin server of the source domain name is an IP address or domain name and the host is the source domain name, new domain names use themselves as the host. – If the origin server of the source domain name is an OBS bucket, new domain names use the same host as the source domain name.
	IPv6 settings
Origin settings	Origin protocol
	Origin SNI
	Origin URL rewriting
	Advanced origins
	Range requests
	Redirect from origin
	ETag verification
	Origin response timeout
	Origin request header
Cache settings	Cache rules
	Browser cache TTL
	Status code cache TTL
	Access URL rewrite
Access control	Referer validation
	IP ACL
	User-Agent ACL
	Token authentication
	Remote authentication

Category	Item
Advanced settings	HTTP header settings (cross-origin requests)
	Custom error pages
	Smart compression
	Request rate limiting
	Usage capping
	WebSocket settings (copied when the service type of the source domain name is whole site acceleration)
Video settings	Video seek settings
Tag settings	Tags

1.6 Reviewing a Domain Name

Scenarios

If a domain name is banned due to ICP license expiration, you can apply to have it reviewed after the domain name is re-licensed. Once the review passes, CDN unbans the domain name.

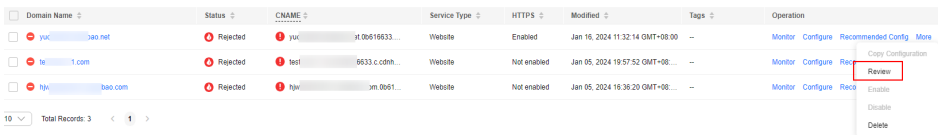
NOTE

- If a domain name is banned due to other reasons, it cannot be unbanned through reviews.
- If a domain name is banned due to violations of content regulations (sexually-explicit, illegal drug, gambling, or extremist content) or being attacked, it will be permanently banned.

Procedure

On the **Domains** page of the **CDN console**, choose **More** > **Review** on the row that contains the domain name to review.

Figure 1-11 Reviewing a domain name



Review Results

- When the domain name is banned because the ICP license expired:
  - If the domain name has been re-licensed, the system displays a message indicating that the domain name has been unbanned.

  - If the domain name has not been re-licensed yet, the system displays a message indicating that the domain name has not been licensed. In this case, obtain the license from the Ministry of Industry and Information Technology (MIIT) and try again.

- When the domain name is banned for other reasons

  If the domain name was banned for reasons other than or in addition to an expired ICP license, a message is displayed after you click **Review**, informing you of the reasons. Resolve the issues based on the reasons and submit a service ticket to try again.

1.7 Service Termination Policy

If a domain name meets conditions for service termination, Huawei Cloud CDN will stop providing acceleration services for it and you cannot configure settings for the domain name.

NOTE

To modify the policy, submit a service ticket.

Scenarios

When the retention period starts, Huawei Cloud CDN will terminate the domain name.

Table 1-4 Service termination policy description

Policy	Description
Redirect to origin server	All requests to your acceleration domain name are redirected to the primary origin server. The domain name status becomes **Disabled**. CDN acceleration service is stopped for the domain name. CDN retains the configuration details of this domain name (until the retention period ends). After the domain name issue is addressed, requests for the domain name will be forwarded to CDN PoPs for acceleration. **NOTE** • After an acceleration domain name is terminated for 30 days, Huawei Cloud CDN no longer redirects requests to the origin server, and the acceleration domain name cannot be accessed. • If you select **Redirect to origin server**, the domain name or IP address of your origin server will be exposed to users. If you do not want to expose the origin domain or origin IP address, select **Disable domain name**. • Whether your site works properly after requests are redirected to your origin server depends on the origin server.
Disable domain name	When your domain name is brought offline, CDN changes its status to **Disabled** and stops CDN acceleration. The domain name cannot be accessed but its configuration is retained (until the retention period ends). After you pay off the outstanding amount, CDN will enable acceleration for it.

NOTE

- When CDN service is terminated for a domain name, CDN will send an SMS or email notification to your reserved phone number or email address. You can top up your account to restore the CDN service.
- If you do not pay off the outstanding amount after the retention period expires, CDN domain names and configurations will be deleted. For details about the retention period, see **Resource Suspension and Release**.
- Your domain name will be banned if it is attacked, its ICP license has expired, or it has inappropriate content. Your CDN service will not be terminated.

Precautions

- The default termination policy is **Disable domain name**.
  - If your account is in arrears and enters the retention period before August 17, 2023, your domain names will be disabled and domain requests will be resolved to origin servers. If your account is in arrears and enters the retention period after August 17, 2023, your domain names will be disabled and their resolution records will be deleted. In this case, the domain names cannot be accessed.
  - If you need to resolve domain requests to origin servers when your account enters the retention period, change the termination policy to **Redirect to origin server**.
- The CDN service termination policy is a global policy. This takes effect for all domain names under your account.

Service Termination Process

The following table describes the process of disabling the CDN service for a domain name.

Scenario	Service Termination Process
Account in arrears	1. If your Huawei Cloud account is in arrears, your Huawei Cloud resources (such as CDN domain names) enter a grace period or retention period. For details, see **Resource Suspension and Release**. 2. If your account is in arrears and the retention period starts, CDN will terminate services for your domain name based on the termination policy you set.

Termination policy: **Redirect to origin server** or **Disable domain name**

- **Redirect to origin server**
  - Requests to the domain name are redirected to the primary origin server.
  - CDN disables the acceleration domain name.
  - CDN changes the domain name status to **Disabled** and stops the acceleration service.

- **Disable domain name**
  - CDN disables the acceleration domain name.
  - CDN changes the domain name status to **Disabled** and stops the acceleration service.

1.8 Domain Name Quota Management

Total Domain Name Quota

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

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

NOTE

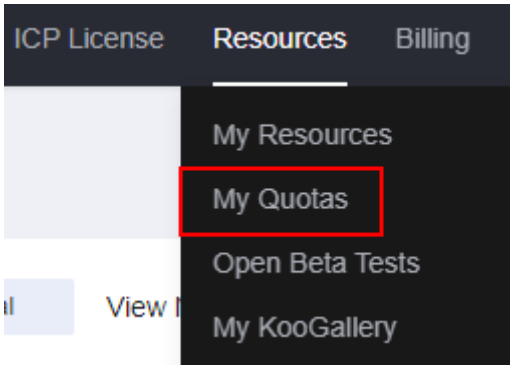
If any domain name under your account is banned due to violation, you cannot add new acceleration domain names and perform cache purge or prefetch.

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 1-12 My Quotas



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

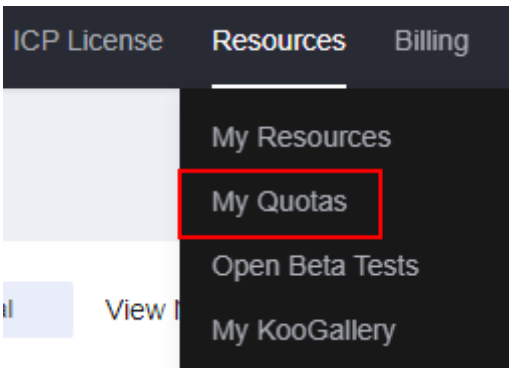
How Do I Apply for a Higher Quota?

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

   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 1-13 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 Domain Name Settings

2.1 Overview

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

OBS Authorization

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

Basic Settings

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

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

Item	Description
Service Area	If the region where your users are located changes, you can change the service area of your acceleration domain name to better match your services.
IPv6	To allow users to access CDN PoPs using IPv6, enable IPv6 on the CDN console.

Origin Settings

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

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

HTTPS Settings

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

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

Cache Settings

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

Item	Description
Cache Rules	• 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. • You can filter URL parameters to allow CDN PoPs to ignore the parameters following a question mark (?) when caching resources, improving the cache hit ratio and speeding up distribution. • You can set the cache TTL on CDN PoPs to be the same as that on your origin server.
Browser Cache TTL	You can set a browser cache TTL, so content requested by a user can be directly returned when the content is cached in their browser, reducing the origin pull ratio.
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 URL Rewrite	You can set access URL rewrite rules to redirect user requests to the URLs of cached resources.

Access Control

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

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

Advanced Settings

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

Item	Description
HTTP Header Settings (Cross-origin Requests)	You can customize values of HTTP response headers for your website.
Custom Error Pages	You can customize error pages returned to user clients.
Smart Compression	You can compress static content on your websites by reducing file size. This speeds up file transfer and saves you a lot of bandwidth.
WebSocket Settings	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.
Usage Cap	You can set a traffic or bandwidth cap for a domain name. When the usage reaches the cap, CDN acceleration will be disabled for the domain name, reduce high bills caused by traffic theft or attacks.

Video Settings

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

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

2.2 OBS Authorization

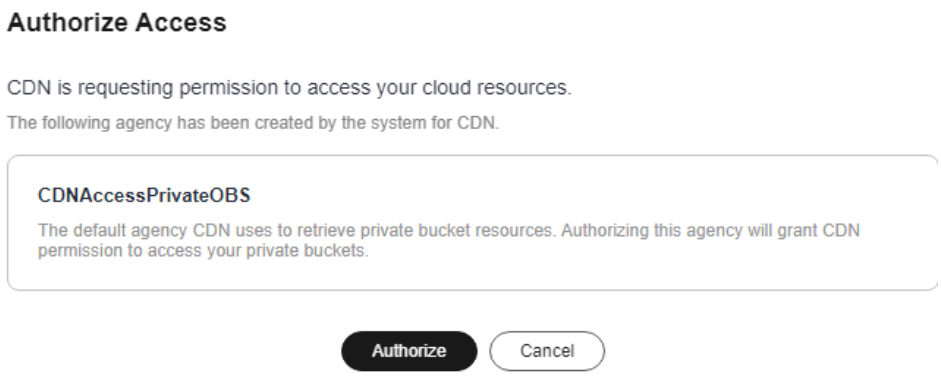
If you configure a Huawei Cloud OBS private bucket as the origin server, enable OBS authorization so that CDN can pull content from your private bucket.

Procedure

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

   The CDN console is displayed.

2. In the navigation pane, choose **Domains**.
3. In the upper right corner of the **Domains** page, click **Enable OBS Authorization**.



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

   NOTE

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

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

5. **(Optional)** Assign the **KMS Administrator** permissions to the CDNAccessPrivateOBS agency.

   a. Log in to **Huawei Cloud console**. Choose **Service List** > **Management & Government** > **Identity and Access Management** to access the IAM console.

   b. In the navigation pane, choose **Agencies**.

   c. On the **Agencies** page, click **Authorize** in the **Operation** column of the row containing **CDNAccessPrivateOBS**.

      The **Select Policy/Role** page is displayed.

   d. In the upper right corner of the table, search for **KMS Administrator**, select this role, and click **Next**.

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

   f. Click **OK**.

FAQ

1. When an OBS Private Bucket Is Used as the Origin Server, Agency Creation for OBS Fails

2.3 Basic Settings

2.3.1 Service Type

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

Important Notes

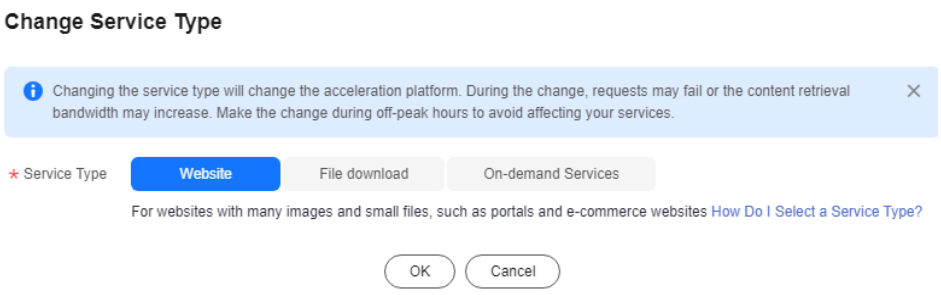
- The service type cannot be changed from or to whole site acceleration.
- Changing the service type will change the used acceleration platform. During the change, a small number of requests may fail or the origin pull bandwidth may increase. Change the service type during off-peak hours to avoid affecting your services.
- The service type of an acceleration domain name with special configurations cannot be changed.

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

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

2.3.2 Service Area

You can change the service area of an acceleration domain name on CDN Console.

Important Notes

- If you want to change the service area between **Chinese mainland** and **Outside Chinese mainland**, change the service area first to **Global** and then to the desired one to avoid affecting your services.
- The service area of a domain name with special configurations cannot be changed.
- CDN is billed by region. Changing the service area may change your fees. For details, see **Pricing Details**.

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.
4. On the **Basic Settings** tab page, click **Edit** next to **Service Area**. The **Change Service Area** dialog box is displayed.

   Figure 2-2 Changing the service area

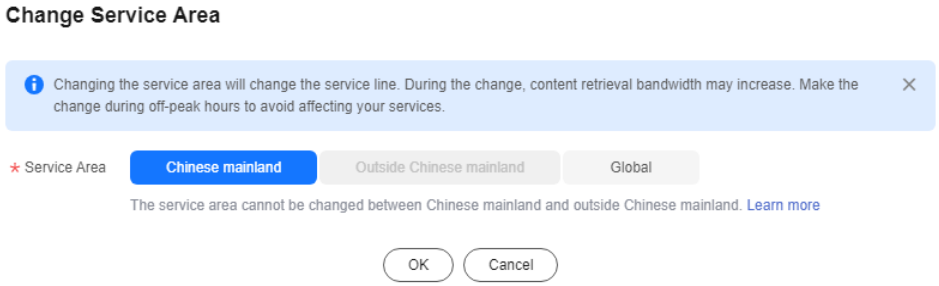
   

   Table 2-1 Parameter description

Service Area	Description
Global	User requests are scheduled to the optimal CDN PoP nearby. Apply for a license for your domain name from the Ministry of Industry and Information Technology (MIIT). For details, see **ICP License Service**.
Chinese mainland	User requests are scheduled to PoPs in the Chinese mainland. Apply for a license for your domain name from the MIIT. For details, see **ICP License Service**.
Outside Chinese mainland	User requests are scheduled to PoPs outside the Chinese mainland. You do not need to apply for a license from the MIIT.

5. Select the desired service area and click **OK**.

2.3.3 Origin Server Settings

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

Background

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

Precautions

- Ensure that the origin server configuration is correct. Incorrect configuration of the origin server causes origin pull failures.
- If you have modified content on the origin server, refresh the CDN cache.
- If you have configured multiple origin IP addresses for a domain name whose service type is whole site acceleration, CDN pulls content from the IP address with the lowest latency by default. To balance origin pull to all IP addresses, submit a service ticket.

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 2-3 Adding an origin server

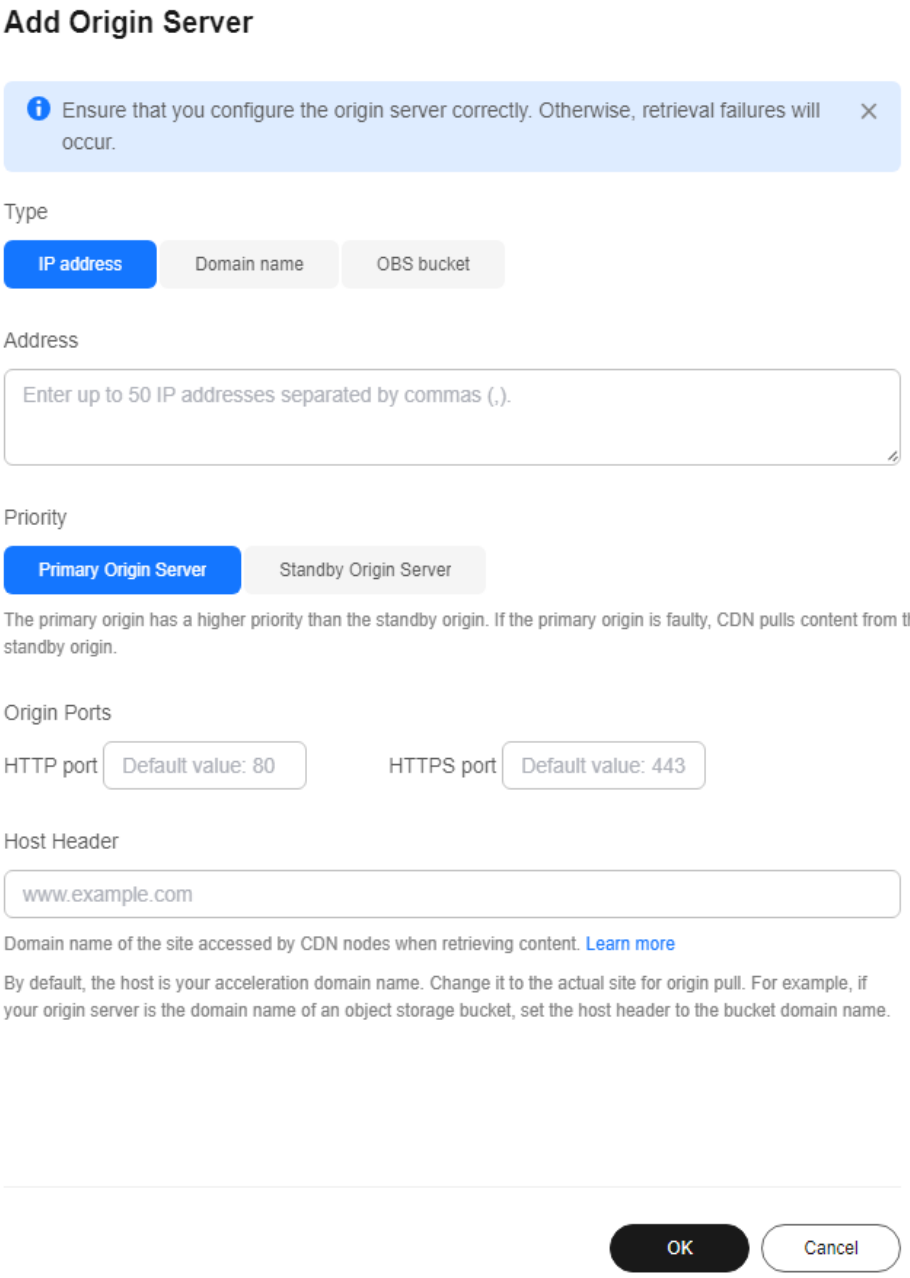


Table 2-2 Parameters

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. • 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. • 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 the billing standard for outgoing Internet traffic.
	OBS bucket Select an OBS bucket domain name under your account or customize one. OBS charges the CDN origin pull traffic based on the billing standard for outgoing Internet traffic. If you set a bucket of OBS 3.0 or a later version as the origin server, you can purchase OBS pull traffic packages to deduct origin pull traffic. For details, see **OBS Billing for CDN Acceleration**. **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 a custom OBS bucket is used as the origin server, the origin domain name must end with .myhuaweicloud.com or .myhuaweicloud.cn. 3. If an OBS private bucket is configured as an origin server, enable **OBS authorization** and select the **Private bucket** checkbox. Otherwise, origin pull will fail. 4. To use a **custom OBS private bucket** as the origin server, configure a policy for the private bucket. For details, see **Configuring a Policy for a Custom OBS Private Bucket**. 5. 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. 6. 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.

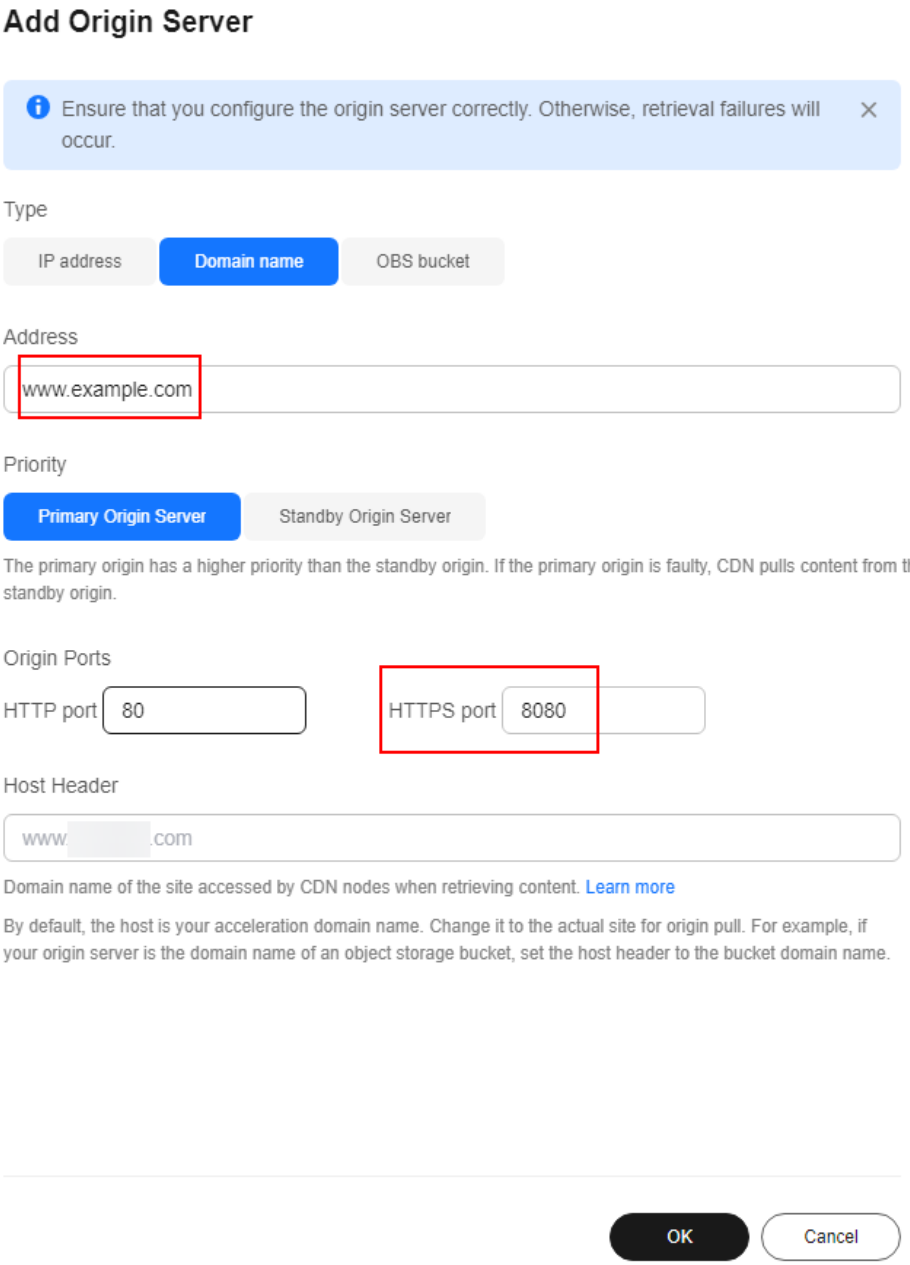
Parameter	Description
Bucket	This parameter is mandatory when **Type** is set to **OBS bucket**. • **Public bucket**: public read. All users can read objects in the bucket. • **Private bucket**: Only users granted permissions by the ACL can access the bucket.
Priority	Select **Primary Origin Server**, **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. – 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 IP address. • If there are multiple origin servers with the same priority, the weight determines the proportion of content pulled from each origin server.
Origin Port	Port number 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.

Parameter	Description
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:



FAQ

Helpful links:

1. **What Are the Differences Between an Acceleration Domain Name and an Origin Domain?**
2. **Can Multiple Acceleration Domain Names Use the Same Origin Server IP Address?**

2.3.4 Host Header

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

Background

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

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

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

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

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

 location / {
 root html;
 }
 }
```

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

Precautions

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

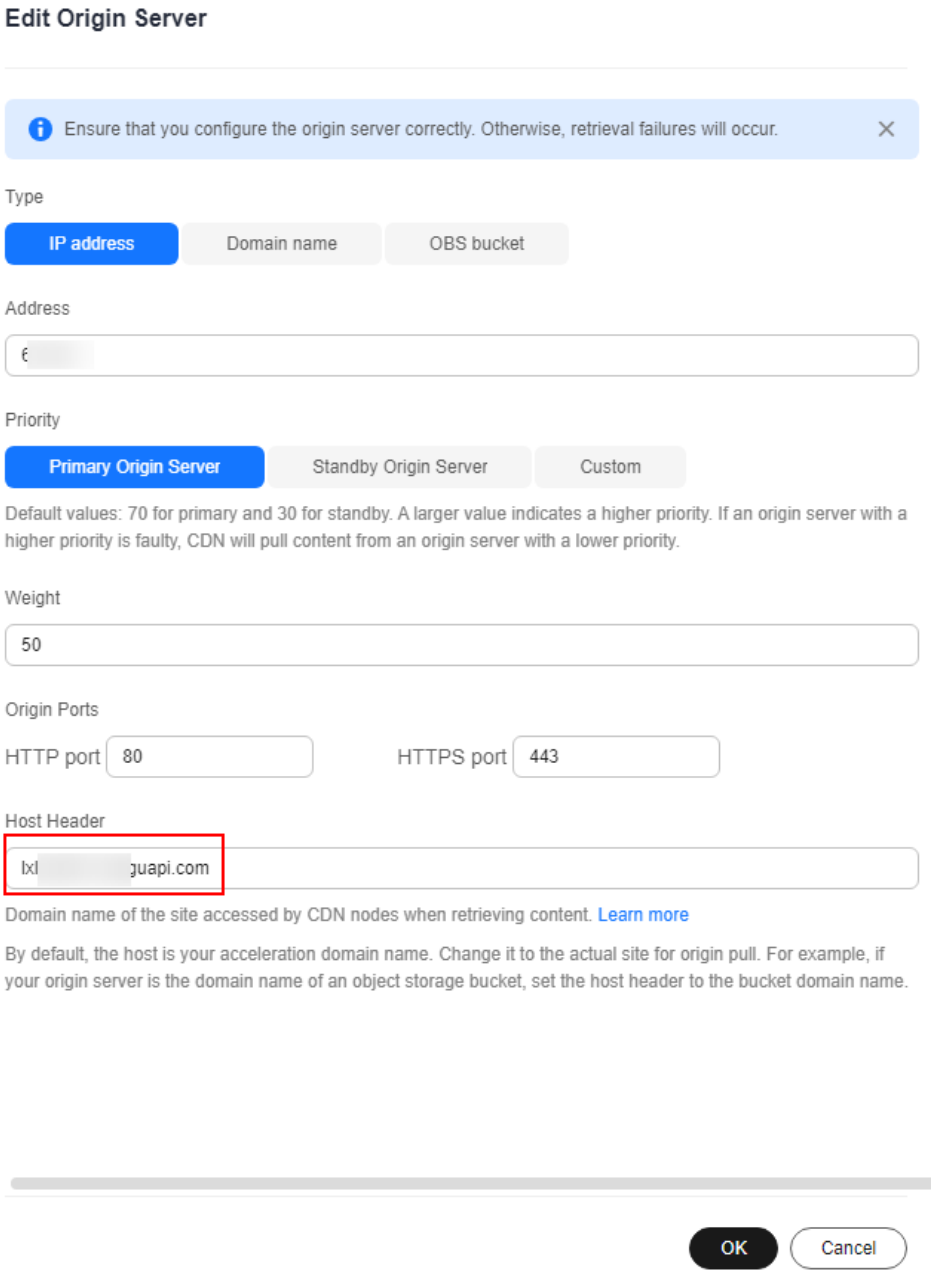
Procedure

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 2-4 Editing the origin server



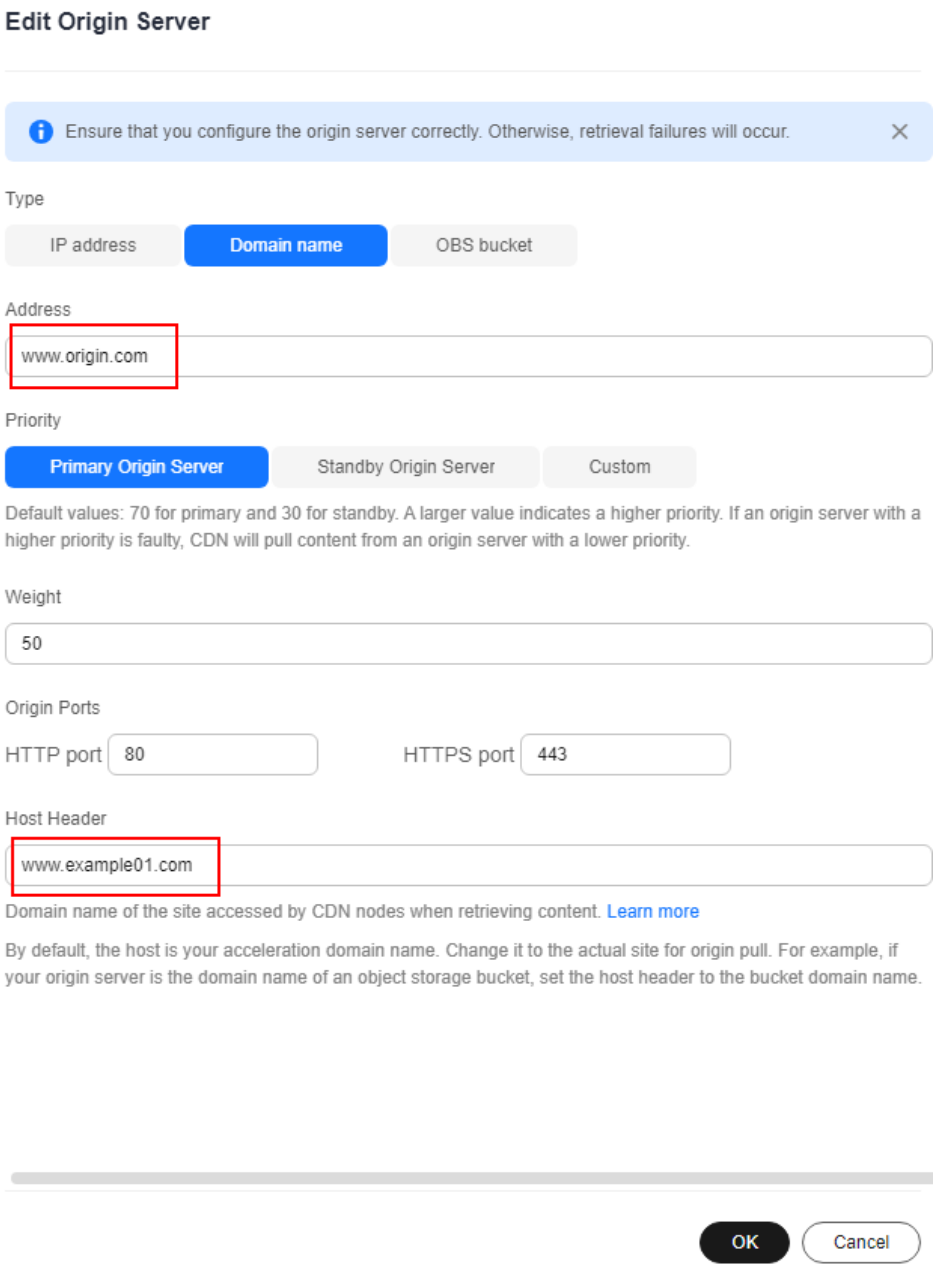
5. Enter the domain name of the host and click **OK**.
6. To edit host headers in a batch, click **Edit** above the origin server list.
   - In the **Host Header** column, modify the information and click **Save**.

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**.



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 IPv6

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

Precautions

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

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain name list, click the domain name or click **Configure** in the row containing the domain name.

   Figure 2-5 IPv6

   NOTE

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

2.4 Origin Settings

2.4.1 Overview

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

The following table describes the origin settings.

Function	Description
Origin Protocol	You can configure the request protocol used by CDN for origin pull.

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

2.4.2 Origin Protocol

You can configure the protocol used for origin pull.

Precautions

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

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.

3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. Click **Edit** next to **Origin Protocol**. The **Origin Protocol** dialog box is displayed.

Figure 2-6 Origin protocol

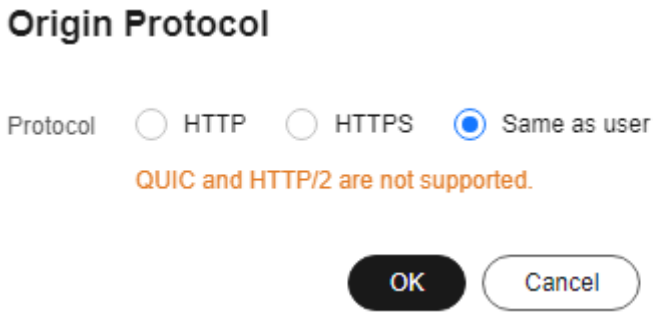


Table 2-3 Parameter description

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

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

2.4.3 Origin SNI

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

Precautions

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

Procedure

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

   The CDN console is displayed.

2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. Switch on **Origin SNI** and enter the origin SNI.

Figure 2-7 Origin SNI

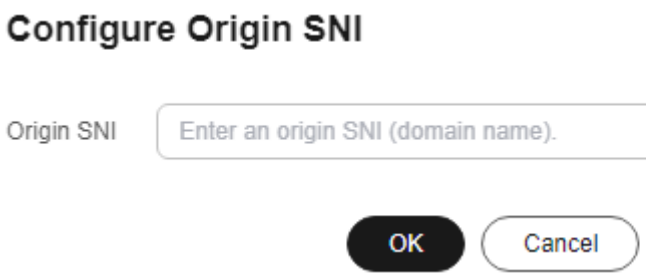


Table 2-4 Parameters

Parameter	Description
Configure Origin SNI	Origin domain name to be accessed when CDN pulls origin content, for example, **test.example.com**. • Wildcard domains are not supported. • The value can contain letters, digits, hyphens (-), and periods (.).

6. Click **OK**.

2.4.4 Origin URL Rewriting

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

Scenarios

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

Precautions

- You can add up to 20 URL rewrite rules.
- This function is not available if you have signed URLs using method B or C1.
- Domain names whose service type is whole site acceleration do not support this function.
- Origin URLs cannot be rewritten for domain names with special configurations.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. In the **Origin URL Rewrite** area, click **Edit**.

Figure 2-8 Rewriting origin URLs

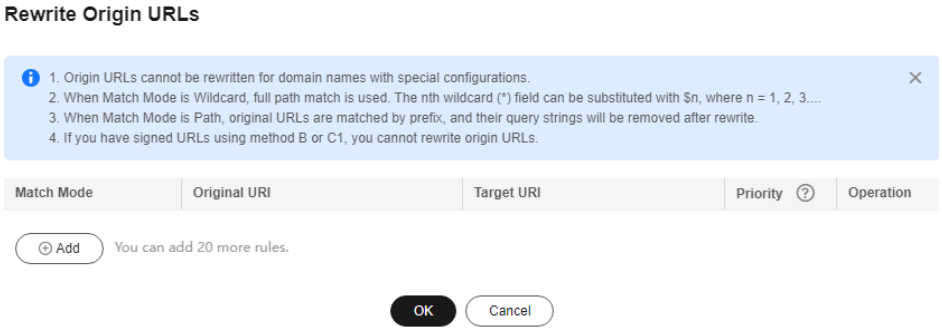


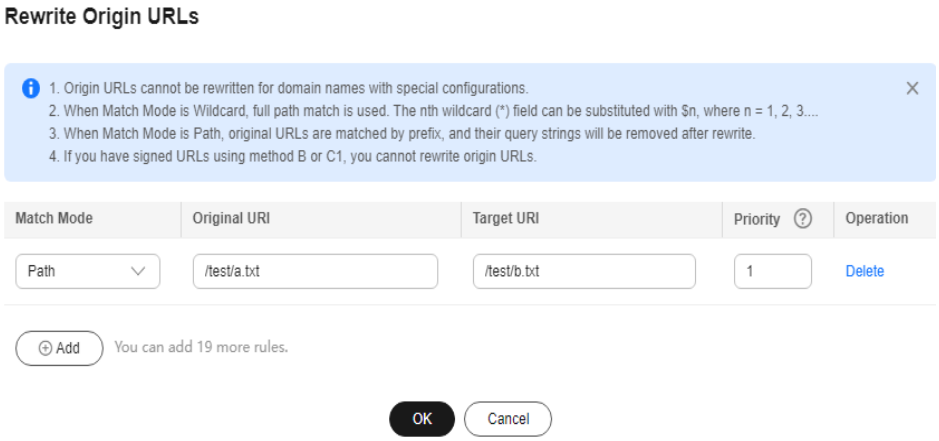
Table 2-5 Parameter description

Parameter	Description
Match Mode	**All files**: Rewrites URLs of pulling all files under this domain name from the origin server.
	Path: Rewrites URLs of pulling files under a specific path from the origin server. Prefix match is used. For example, if the original URI is **/test**, all files whose prefix is **/test** (such as **/test**, **/test01**, and **/test****) will be matched.
	Wildcard: Wildcard characters (*) are supported. Files are matched by full path. The original URI must be a specific path, for example, **/test/*/*.mp4**.
	Full path: Rewrites the entire URL. The original URI must be a specific path, for example, **/test/01/abc.mp4**.

Parameter	Description
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

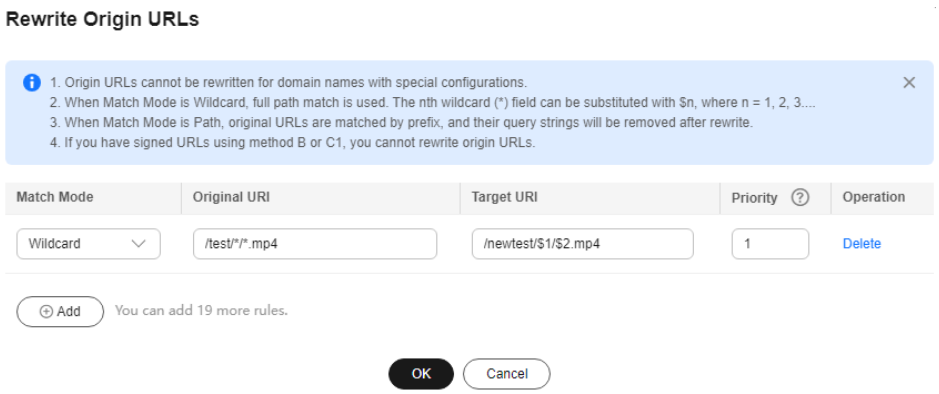
Example 1: Assume that you have configured the following rewrite rule for domain name www.example.com.



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

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

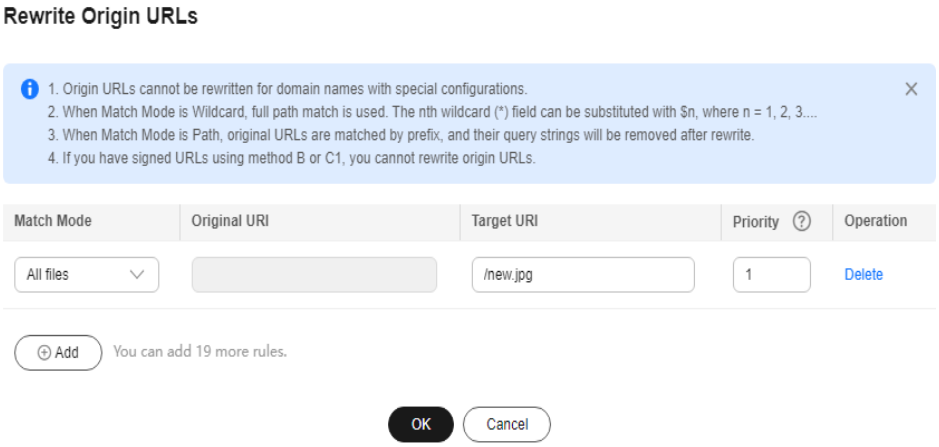
Example 2: Assume that you have configured the following rewrite rule for domain name www.example.com.



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

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

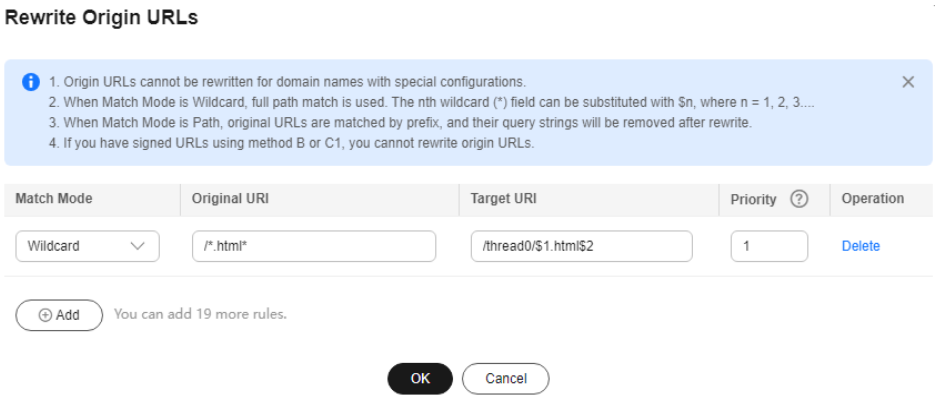
Example 3: Assume that you have configured the following rewrite rule for domain name www.example.com.



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.



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

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

2.4.5 Advanced Origins

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

Differences Between Advanced and Basic Origin Servers

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

Precautions

- You can configure up to 20 rules.
- You cannot configure advanced origins on the console for domain names with special configurations.
- 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. Click **Edit** next to **Advanced Origin**.

Figure 2-9 Advanced origins

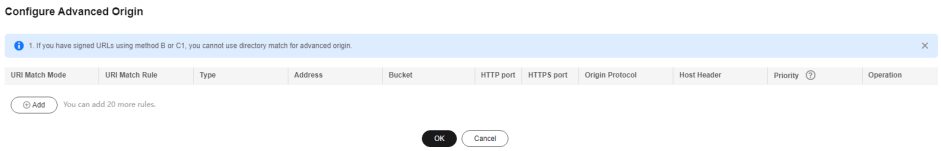


Table 2-6 Parameter description

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 each file name extension with a period (.), and separate file name extensions with semicolons (;). – Enter up to 20 file name extensions. – Enter up to 512 characters. – File name extensions are case sensitive. Example: **.JPG;.zip;.exe** • **Directory**: Start with a slash (/) and separate multiple directories by semicolons (;). Enter up to 20 directories and up to 512 characters. Example: **/test/folder01;/test/folder02** **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**.

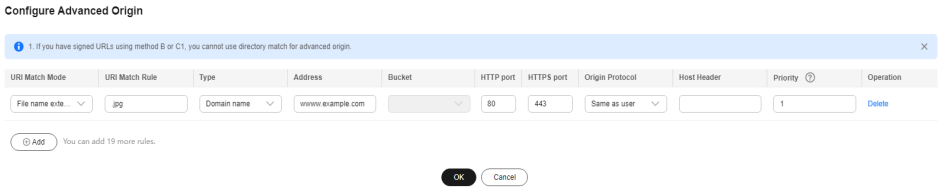
Parameter	Description
Address	**IP address** • Enter an IPv4 address. **Domain name** • Enter up to 250 characters. • Third-party object storage buckets (public buckets) can be accessed using origin server domain names. **OBS bucket** • Enter up to 250 characters. • Only OBS buckets of the current account can be accessed. • To access OBS private buckets, allow CDN to read OBS private buckets. For details, see **OBS Authorization**. **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** **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 **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 65,535. The larger the value, the higher the priority.
Operation	**Delete**: Delete the rule.

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

Example

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



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.

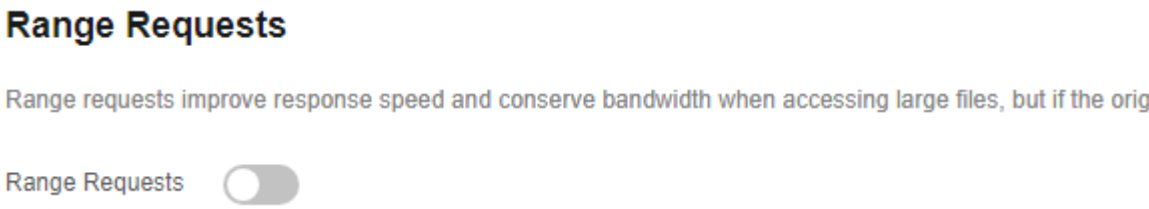
- Domain names whose service type is whole site acceleration do not support this function.
- By default, range requests are enabled for file download acceleration and on-demand service acceleration.
- If an origin server resource exceeds 1 GB and range requests are not enabled, origin pull for such resource will fail.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. In the **Range Requests** area, switch on or off **Range Requests** based on service requirements.

   Figure 2-10 Range requests



Example

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

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

2.4.7 Redirect from Origin

Background

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

- Disabled

  A CDN PoP returns the redirect address to the user and leaves the user to finish the request process. If the domain name of the redirect address is not added to CDN, the subsequent request process will not be accelerated by CDN.

- Enabled

  A CDN PoP pulls content from the redirect address and caches the content, which is then returned to the user. When another user requests the same content, the cache is returned directly.

Precautions

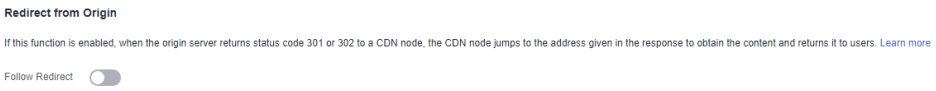
Domain names whose service type is whole site acceleration do not support this function.

Procedure

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

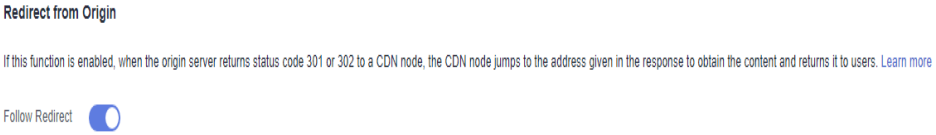
   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. In the **Redirect from Origin** area, switch on or off **Follow Redirect**.

   Figure 2-11 Configuring redirect from origin

Examples

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

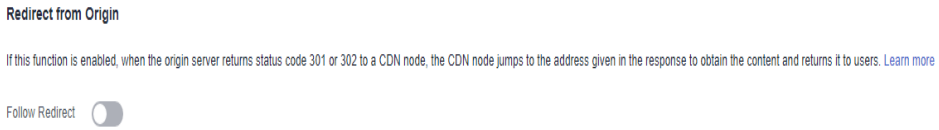
  

  If a user requests the **www.example.com/cdn.jpg** file and the CDN PoP does not cache the content, the PoP pulls the content from the origin server. The origin server returns the HTTP status code 301 or 302 and the redirect address www.example.com/test/cdn.jpg.

  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.



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.
- Domain names whose service type is whole site acceleration do not support this function.

Procedure

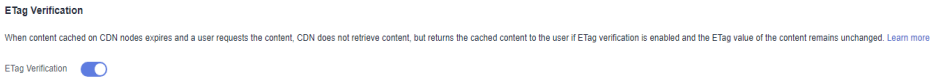
1. Log in to **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

   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. Configure **ETag Verification** as required.

Figure 2-12 ETag verification

Examples

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



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

2.4.9 Origin Response Timeout

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

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

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

Precautions

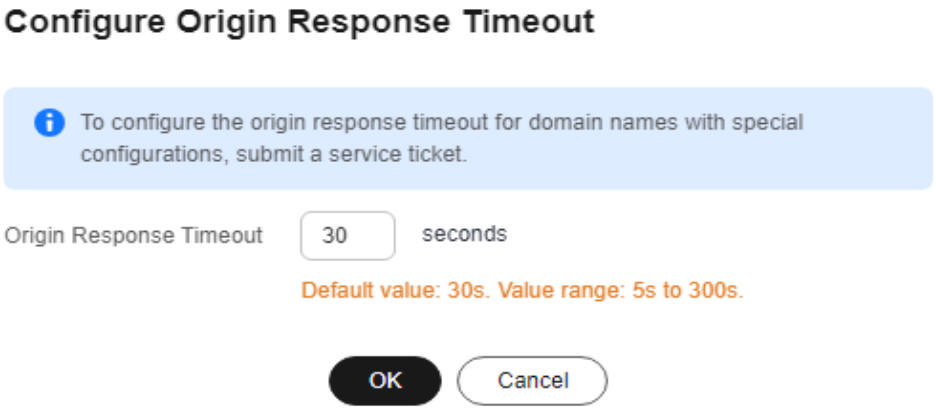
- To modify the origin response timeout interval for domain names with special configurations, submit a service ticket.

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 2-13 Origin response timeout

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

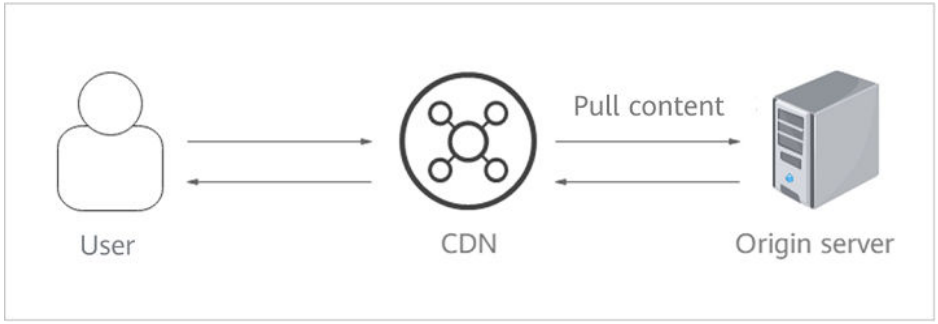
2.4.10 Origin Request Headers

You can configure HTTP headers in origin pull URLs.

Background

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

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



Precautions

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

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. In the **Origin Request Headers** area, click **Add**.
6. Configure the header details.
   - **Add**: Add a header to CDN to rewrite HTTP headers in user request URLs.

   Figure 2-14 Adding an origin request header

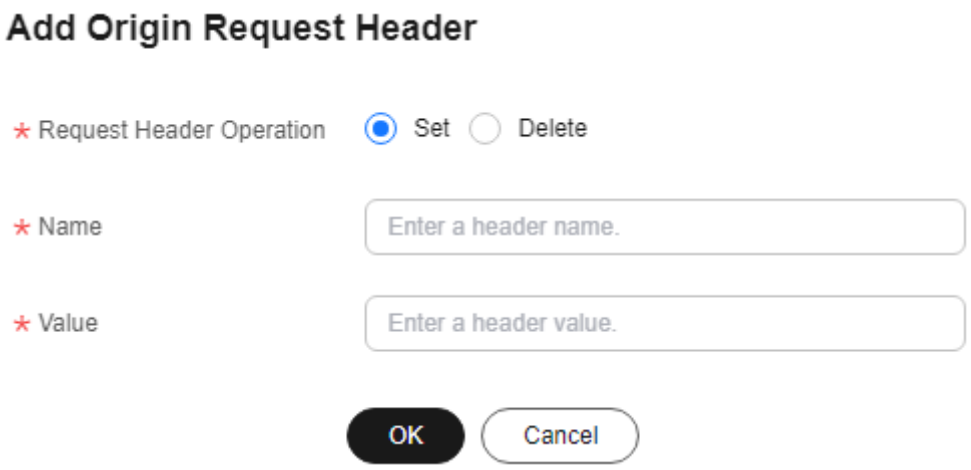
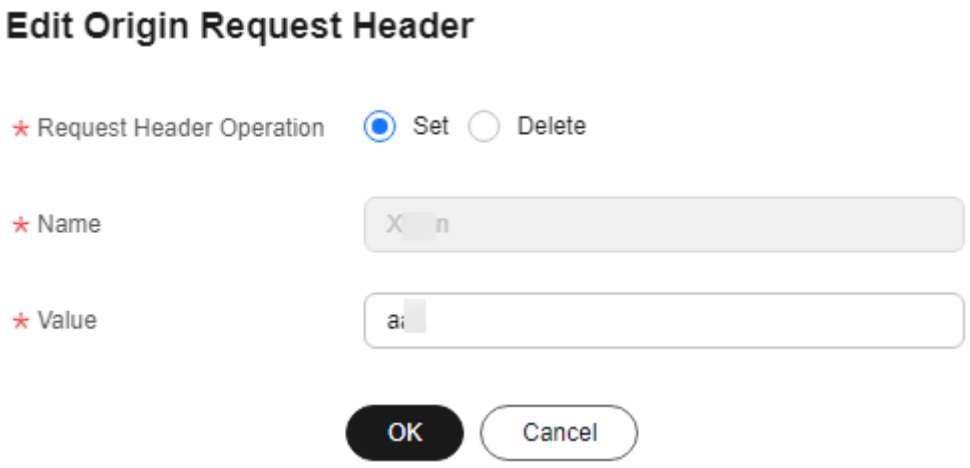


Table 2-7 Parameter description

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 64 characters. • Enter only letters, digits, or hyphens (-).
Value	aaa	• Enter 1 to 1,000 characters. When the header is **Content-Disposition** or **Content-Language**, the value contains up to 128 characters • Enter letters, digits, and the following special characters: .-_*#!&+|^~'"/:;,=@?<> • 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 2-15 Editing an origin request header



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. When the header is **Content-Disposition** or **Content-Language**, the value contains up to 128 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, the file is not cached on CDN, and CDN pulls that file from the origin server. The **X-cdn** header will be added and the **X-test** header will be deleted during origin pull.

Restrictions

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

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

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

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

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

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

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

2.4.11 FAQ

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

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

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

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

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

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

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



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

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

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

No.

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

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

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

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

2. Modify origin settings.

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

2.5 HTTPS Settings

2.5.1 Overview

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

The following table describes the HTTPS settings:

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

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

2.5.2 HTTPS Certificates

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

Background

- **HTTP**

  HTTP transfers content in plaintext without any data encryption. If an attacker intercepts packets transmitted between browsers and website servers, the transmitted content can be read directly.

- **HTTPS**

  Based on HTTP, HTTPS uses Secure Sockets Layer (SSL) to encrypt data transmission. With SSL, servers are authenticated using certificates, and communications between browsers and servers are encrypted.

Prerequisites

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

Precautions

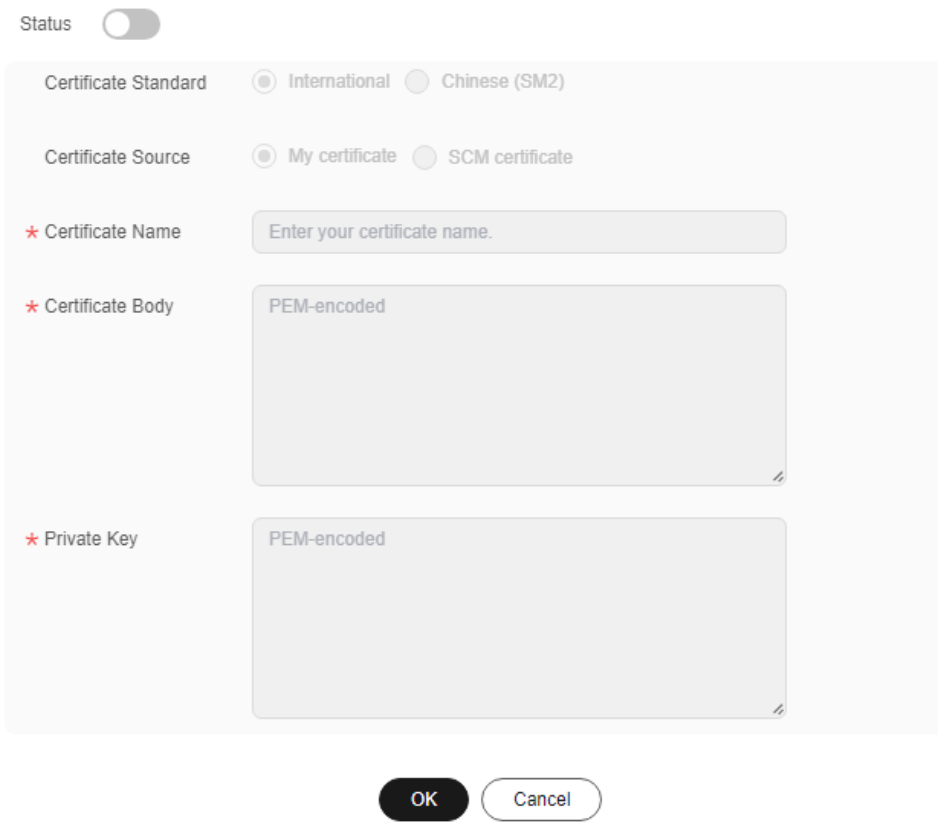
- Only certificates and private keys in PEM format are supported. If a certificate is not in PEM format, convert the certificate by referring to **HTTPS Certificate Requirements**.
- An acceleration domain name has its associated certificate. They must match. If your domain name is a wildcard domain, configure a certificate for it by referring to **How Do I Configure a Certificate If My Domain Name Is a Wildcard Domain?**
- Certificate settings will be automatically deleted once HTTPS secure acceleration is disabled. You need to re-configure the certificate if HTTPS secure acceleration is enabled again.
- If your certificate has changed, update certificate information on the CDN console in a timely manner.
  - For details about how to update your own certificate, see **Updating the HTTPS Certificate**.
  - For details about how to use the latest SCM certificate, see **Configuring HTTPS Certificates**.
- If two certificates are set for a domain name, the certificate standards must be different. That is, if you have added an international certificate for a domain name, you can only add a Chinese (SM2) certificate.
- To use HTTPS for all links, the origin protocol should be HTTPS (and the origin server must support HTTPS). For details, see **Origin Protocol**.

Configuring HTTPS Certificates

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **HTTPS Settings** tab.
5. On the **HTTPS Settings** tab page, click **Edit**. The **Configure HTTPS Secure Acceleration** dialog box is displayed.

Figure 2-16 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 Standard	**International**: SSL certificate that complies with international standards.
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.

Parameter	Description
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.
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.

Table 2-9 Parameters of a Chinese SM series cryptographic certificate

Parameter	Description
Certificate Standard	Chinese (SM2)
Certificate Source	Select **My certificate** or **SCM certificate**.
Certificate Name	• If you select **My certificate**, enter the certificate name containing 3 to 64 characters. • 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.
Signature Certificate	Open the PEM file in the signature certificate to be uploaded as a text file and copy the certificate content in the file to this text box. Note that you need to upload a combined certificate file that contains both the server certificate content and certificate chain content into this field. The content of the certificate chain should be pasted right below the content of the server certificate.

Parameter	Description
Signature Private Key	Open the KEY file in the signature certificate to be uploaded as a text file and copy the private key in the file to this text box.
Encryption Certificate	Open the PEM file in the encryption certificate to be uploaded as a text file and copy the certificate content in the file to this text box. You do not need to upload the certificate chain here.
Encryption Private Key	Open the KEY file in the encryption certificate to be uploaded as a text file and copy the private key in the file to this text box.

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

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

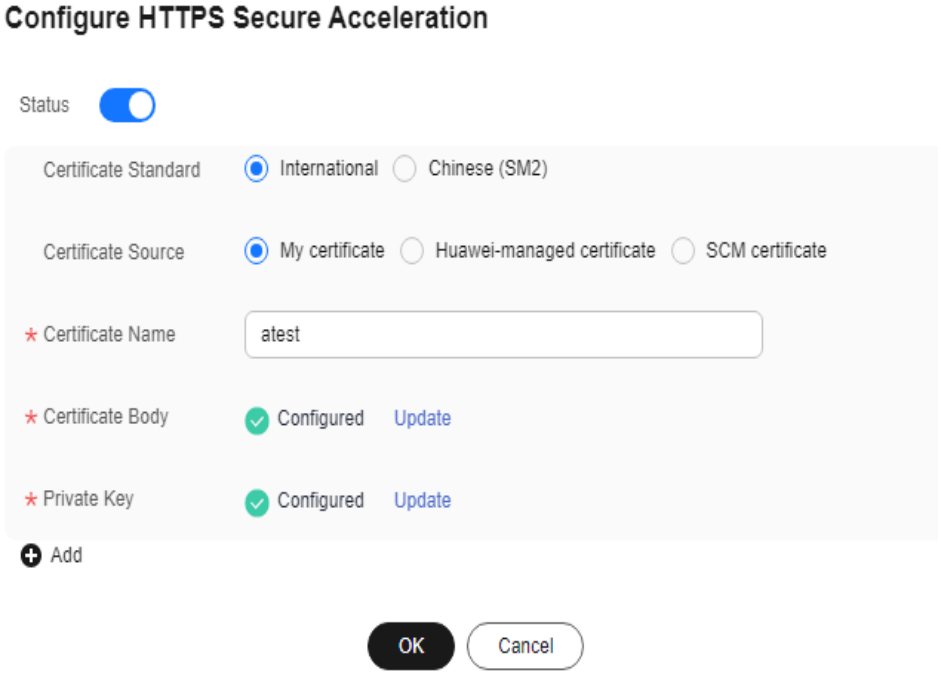
Updating the HTTPS Certificate

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

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **HTTPS Settings** tab.
5. On the **HTTPS Settings** tab page, click **Edit**. The **Configure HTTPS Secure Acceleration** dialog box is displayed.

Figure 2-17 Updating a certificate



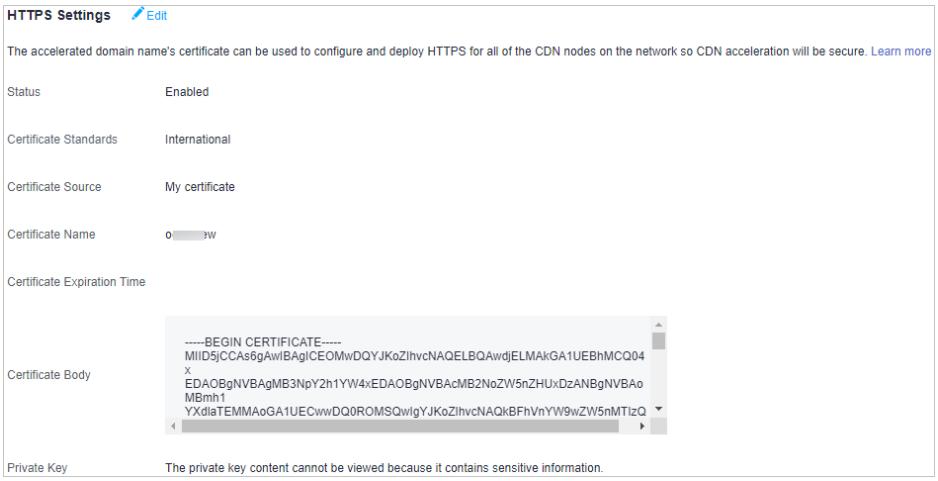
6. Click **Update** to update the configured certificate and private key. It takes approximately 5 to 10 minutes for the update to take effect.

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.



Certificate Expiration Time

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

FAQ

Helpful links:

1. **Are Self-Signed HTTPS Certificates Supported?**
2. **Access Succeeds Using HTTP but Failed Using HTTPS**

2.5.3 HTTPS Certificate Requirements

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

Certificates Issued by Root CA

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

Use a text editor to open the certificate. The certificate content should be something similar to what is in **Figure 2-18**.

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 2-18 PEM certificate

```
-----BEGIN CERTIFICATE-----
MIIDxDCCAqygAwIBAgIEAJgGCTANBgkqhkiG9w0BAQUFADBuMQswCQYDVQQGEwJj
bjELMAkGA1UECAwCZ2QxCzAJBgNVBAcMAnN6MQswCQYDVQQKDAJodzELMAkGA1UE
CwwCaHcxGDAWBgNVBAMMD2lOT0MgUm9vdCBDQSBWMjERMA8GCSqGSIb3DQEJARYC
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
lJq8ekhn07Aqd7chFbDfW4qLSY7nEHT3uLzGME8Y9QQ4zs5H71CaJVGXtoTQfpXR
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 security acceleration. A combined certificate is shown as **Figure 2-19**.

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

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

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

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

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

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

Figure 2-19 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]
AgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMEIGA1UdEQQ7MDmCE3d3dy5odWF3ZWlj
bG91ZC5jb22CESouaHVhd2VpY2xvdWQuY29tgg9odWF3ZWljbG91ZC5jb20wDQYJ
KoZIhvcNAQELBQADggEBACsLP7Hj+4KY1ES38OnOWuwQ3st8axvhDD9jZGoninzW
JSGpdmO4NEshlvwSFdEHpjy/xKSLCIqg5Ue8tTI8zOF13U0ROnMeHSKSxJG6zc8X
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 2-20**.

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 2-20 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
```

FAQ

What Can I Do If HTTPS Certificate Configuration Fails and the Message "Incomplete certificate chain" Is Displayed?

2.5.4 HTTPS Certificate Format Conversion

The HTTPS configuration only supports certificates or private keys in PEM format. It is recommended that **OpenSSL** be used to convert certificates in other formats into the PEM format. The following examples illustrate some popular converting 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 to convert certificates into different formats.

2.5.5 TLS Versions

You can configure TLS versions as required.

Background

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

Table 2-10 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

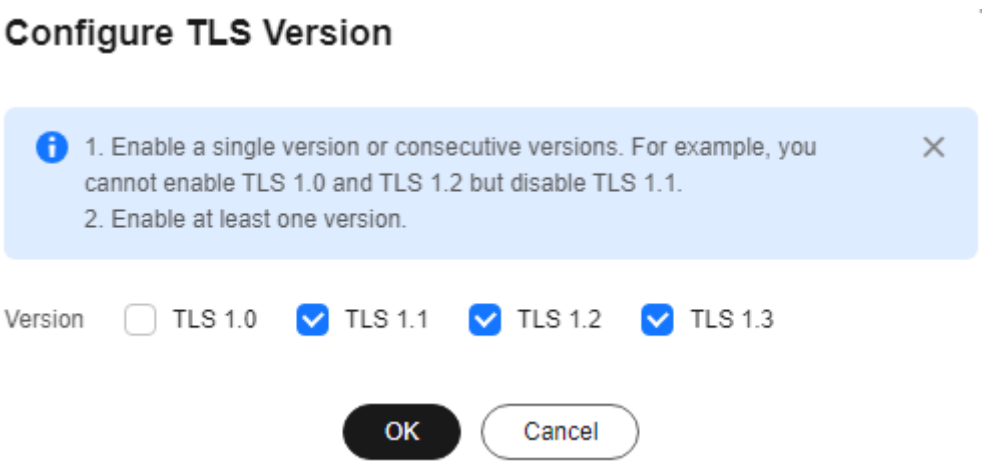
- An international HTTPS certificate has been configured. For details, see **HTTPS Certificates**.
- If the domain name is bound to a certificate with Chinese cryptographic algorithm, TLS versions cannot be configured.
- If you change the certificate type from **International** to **Chinese (SM2)**, TLS version settings will become invalid.
- If you configure two certificates for a domain name, TLS version settings take effect only for the international 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.
- TLS versions cannot be configured for domain names with special configurations.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **HTTPS Settings** tab.
5. In the **TLS Version** area, click **Edit**.

   Figure 2-21 Configuring the TLS versions

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

2.5.6 Force Redirect

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

Scenarios

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

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

Precautions

- To redirect requests to HTTPS, **configure an HTTPS certificate** for your domain name first.
- If you have configured force redirect to HTTPS, disabling the certificate will also disable force redirect to HTTPS.
- If you enable HTTP/2, force redirect to HTTP does not take effect.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **HTTPS Settings** tab.
5. Click **Edit** next to **Force Redirect**. The **Force Redirect** dialog box is displayed.

Figure 2-22 Force redirect

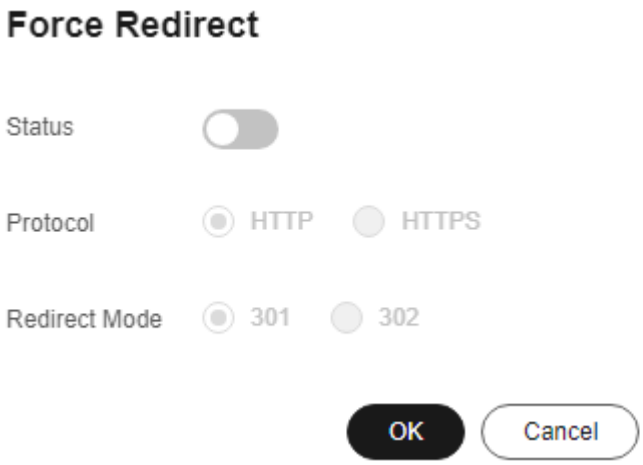


Table 2-11 Parameter description

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 or 302

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

2.5.7 HSTS

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

Working Principles

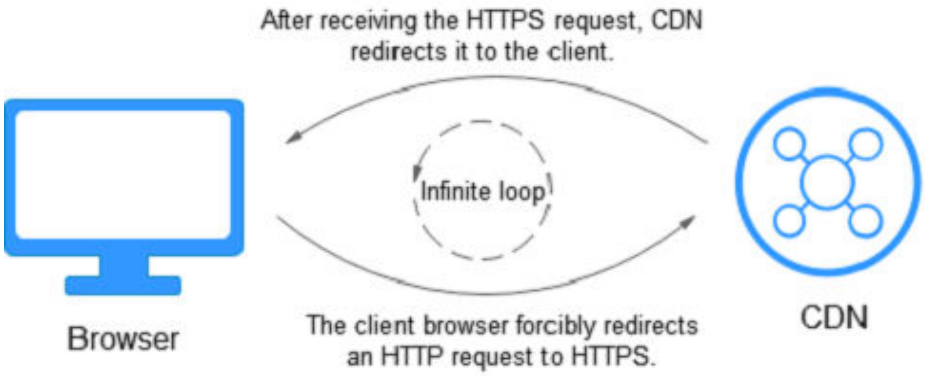
If HSTS is configured on CDN, when a client (such as a browser) uses HTTPS to access a CDN PoP for the first time, the PoP responds to the browser with the **Strict-Transport-Security** header. The browser caches this header if it supports HSTS and uses HTTPS to access CDN PoPs until the cache expires.

Prerequisites

You have **configured an HTTPS certificate**.

Precautions

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



- To enable HSTS for domain names with special configuration, submit a service ticket.

Procedure

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

   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 2-23 HSTS

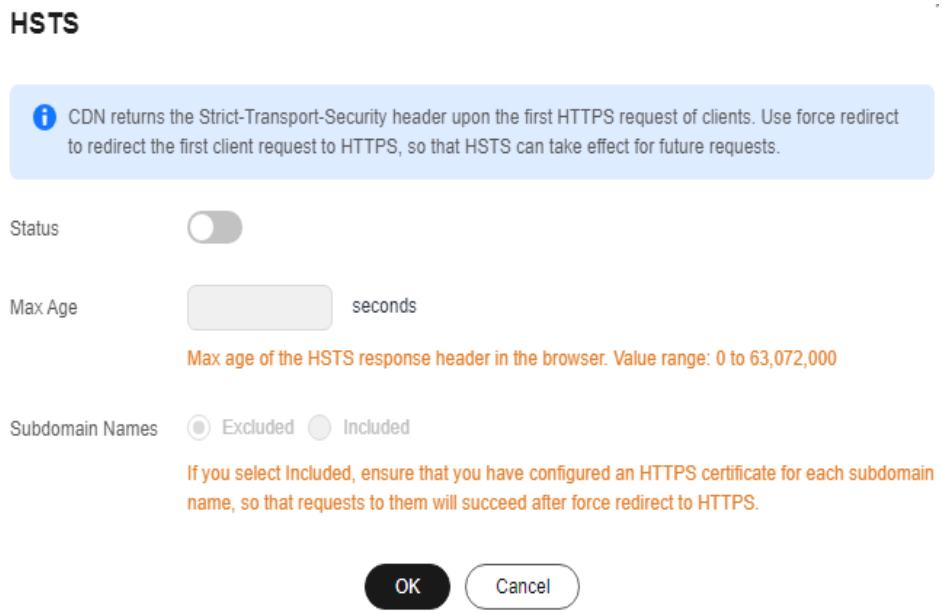


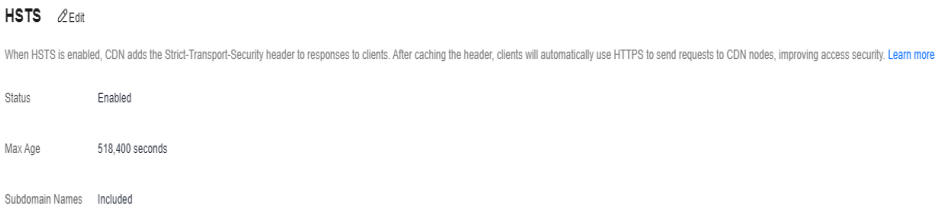
Table 2-12 Parameters

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. Otherwise, subdomain names cannot be accessed.

7. Click **OK**.

Example

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



Configuration effect:

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

2.5.8 HTTP/2

Background

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

Prerequisites

An HTTPS certificate has been configured. For details, see **HTTPS Certificates**.

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

Precautions

- If you set two certificates for a domain name, HTTP/2 takes effect only for the international certificate.

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

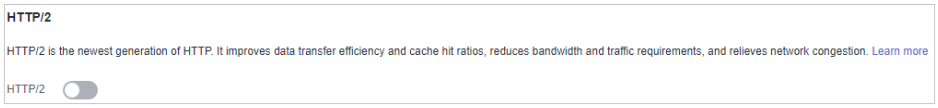
  HTTP/2 multiplexes multiple requests or responses over a single TCP connection. While HTTP/1.1 establishes a TCP connection for each request or response in order. By sending requests concurrently, HTTP/2 lessens the pressure on server connection and alleviates the network blocking problem.

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**.



2.5.9 OCSP Stapling

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

Working Principles

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

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

Constraints

- An international HTTPS certificate has been configured. For details, see **HTTPS Certificates**.
  - Disabling the HTTPS certificate will disable OCSP stapling.
  - After configuring the HTTPS certificate, wait about 5 minutes for the configuration to complete and then enable OCSP stapling.
- OCSP stapling cannot be applied to whole site acceleration or domain names that also require acceleration services outside the Chinese mainland.
- If you change the certificate type from **International** to **Chinese (SM2)**, OCSP stapling will become invalid.
- If you configure two certificates for a domain name, OCSP stapling takes effect only for the international certificate.

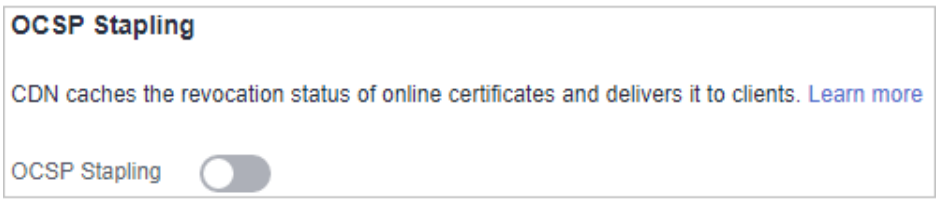
Procedure

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 2-24 OCSP stapling



NOTE

By default, OCSP stapling is disabled.

5. Switch on **OCSP Stapling**.

2.5.10 QUIC

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

What Is QUIC?

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

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

Supported Version

IETF-v1 (H3)

Prerequisites

An international HTTPS certificate has been configured. For details, see **HTTPS Certificates**.

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

Precautions

- QUIC cannot be enabled for domain names with special configurations.
- QUIC cannot be used for origin pull.

- This function is in OBT and is available for free trial.
- If you change the certificate type from **International** to **Chinese (SM2)**, QUIC will become invalid.
- If you configure two certificates for a domain name, QUIC takes effect only for the international certificate.

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 2-25 QUIC

2.5.11 Client Certificates

You can configure a client certificate to enforce mutual certificate authentication between the clients and CDN PoPs, securing website communication.

Prerequisites

- You have configured an international HTTPS certificate. For details, see **HTTPS Certificates**.
- You have applied for a client CA certificate.

Precautions

A client certificate cannot be configured for domain names with special configurations.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **HTTPS Settings** tab.

5. In the **Client Certificate** area, click **Edit**. The **Configure Client Certificate** dialog box is displayed.

Figure 2-26 Configuring a client certificate

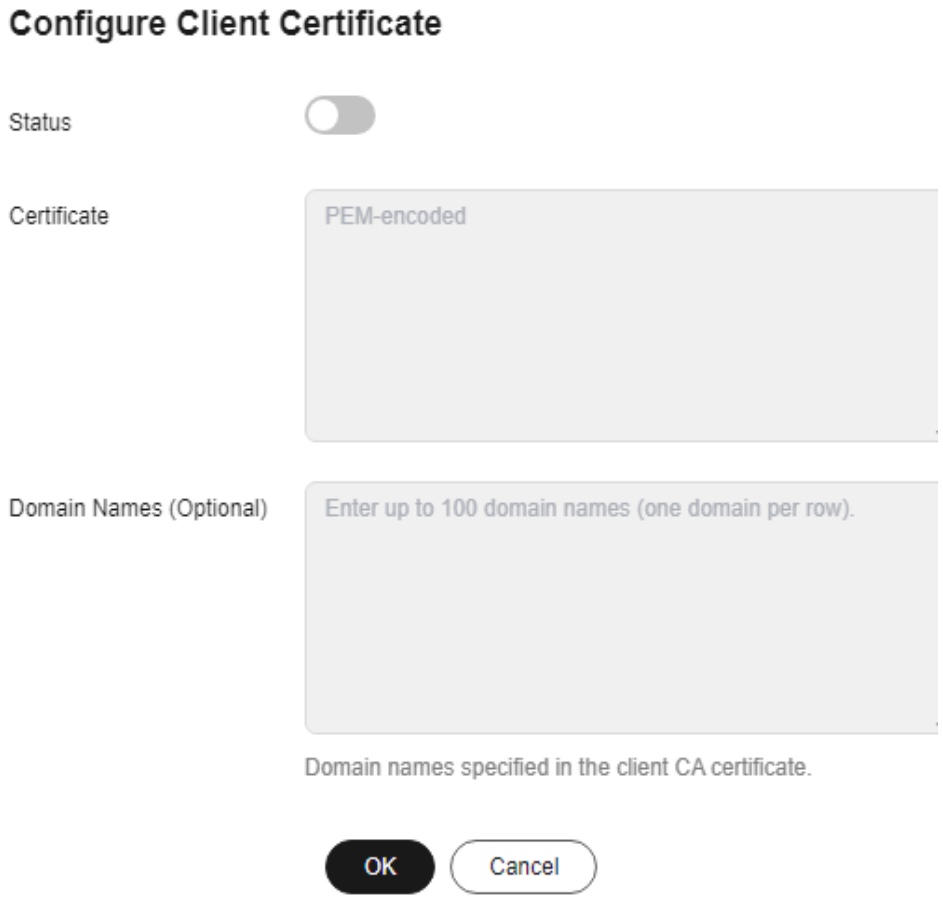


Table 2-13 Parameters

Parameter	Description
Certificate	Content of the client CA certificate. Only the PEM format is supported.
Domain Names (Optional)	Domain names specified in the client CA certificate. • Leave this parameter blank to allow all requests from clients that hold the CA certificate. • Enter up to 100 domain names. Separate them by commas (,) or enter one domain per row.

6. Enable the **Status** switch, enter the certificate content, and click **OK**.
   - After the configuration is complete, a CDN PoP verifies the client certificate when a client requests resources using HTTPS. If the verification is successful, the PoP returns the resource to the client. If the verification fails, the access is rejected.

2.5.12 FAQ

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

This is maybe because:

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

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

  For details about how to get the certificate chain right, see **HTTPS Certificate Requirements**.

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

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

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

2.6 Cache Settings

2.6.1 Overview

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

The following table describes the cache settings.

Function	Description
Cache Rules	• You can set the cache TTL and priority for different resources to increase the hit ratio and reduce the back-to-source rate. • You can filter URL parameters to allow CDN PoPs to ignore the parameters following a question mark (?) when caching resources, improving the cache hit ratio and speeding up distribution. • You can set the cache TTL on CDN PoPs to be the same as that on your origin server.

Function	Description
Browser Cache TTL	You can set a browser cache TTL, so content requested by a user can be directly returned when the content is cached in their browser, reducing the origin pull ratio.
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.
Access URL Rewrite	You can set access URL rewrite rules to redirect user requests to the URLs of cached resources.

NOTE

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

2.6.2 Cache Rules

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

Background

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

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

Precautions

- Up to 60 cache rules can be added to each domain name.

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

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Cache Settings** tab.
5. In the **Cache Rules** area, click **Edit**. The **Configure Cache Rule** dialog box is displayed.
6. Click **Add** to add cache rules. See **Figure 2-27**. **Table 2-14** describes the parameters. You can click **Suggested Rules** to view the recommended configuration.

Figure 2-27 Configuring a cache rule

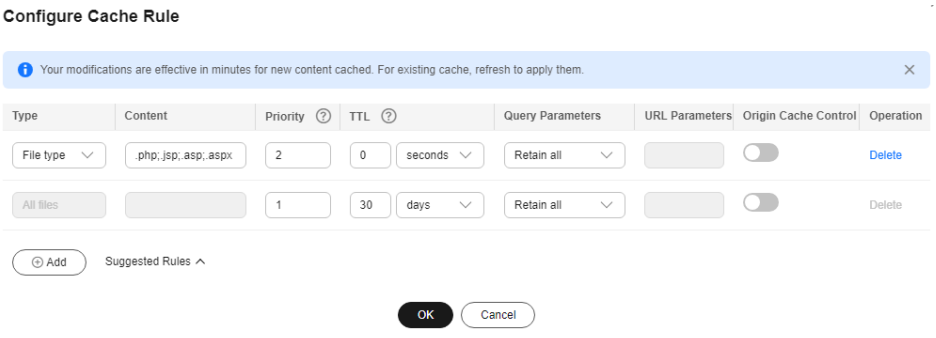


Table 2-14 Cache rule parameters

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 (the default TTL of content on a domain name with whole site acceleration is 0). You can modify but cannot delete this rule.
File type	Files of a specific type If the service type of a new domain name is **Website**, **File download**, or **On-demand service** and its origin server is a private one, CDN adds a rule to it by default. The rule specifies that the TTL is 0 for common dynamic files, such as .php .jsp .asp, and .aspx files. CDN pulls such files from the origin server for every request. You can modify and delete this rule.	• All file types are supported. • Start each file name extension with a period (.), and separate file name extensions with semicolons (;). • Enter up to 50 file name extensions. • Enter up to 1,000 characters. • File name extensions are case-insensitive. Example: **.JPG;.zip;.exe** **NOTE** If your domain name has special configurations, enter up to 20 file name extensions and up to 255 characters.

Parameter	Description	Configuration Rule
Directory	Files in a directory	Start a directory with a slash (/), and separate multiple directories with semicolons (;). Enter a maximum of 20 directories with a maximum of 255 characters in total. Example: **/test/folder01;/test/folder02** • 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 of a cache rule is **/test/***, **/test/abc** and **/test/abc/001** also use this rule. – Wildcards cannot be set for domain names with special configurations. – Wildcards cannot match slashes (/). For example, **/test/*/abc** cannot match **/test/folder01/folder02/abc**. – A wildcard can match one or more characters but cannot match zero characters. For example, **/test*** cannot match **/test**. – **/*** cannot be set as a path.

Parameter	Description	Configuration Rule
Full path	A specific file	A full path must start with a slash (/) and cannot end with a wildcard (*). A file in the specified directory or file with the wildcard (*) can be matched. Enter only one full path. Examples: **/test/index.html** or **/test/*.jpg**
Homepage	Root directory	The root directory of a website is the top-level directory of the website folder, which contains all subfolders of the website. For example, for **abc/file01/2.png**, **abc/** is the root directory, and a cache rule is configured for **abc/**.
Priority	Priority of a cache rule Each cache rule must have a unique priority. If a resource is specified in multiple cache rules, the rule with the highest priority is applied.	Enter an integer ranging from 1 to 100. A greater number indicates a higher priority.
TTL	Duration that a file can be cached. If the TTL of the file has reached, CDN requests the most recent content of the file from the origin server when a user requests the file from a CDN PoP. In addition, the CDN caches that content on the CDN PoP.	The TTL of a cached file cannot exceed 365 days. You are advised to set the time according to the following rules: • For static files (such as .jpg and .zip files) that are not frequently updated, set the TTL to more than one month. • For static files (such as .js and .css files) that are frequently updated, set the TTL based on service requirements. • For dynamic files (such as .php, .jsp, and .asp files), set the TTL to 0 seconds.

Parameter	Description	Configuration Rule
Query Parameters	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, do not ignore 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.
Origin Cache Control	If **Cache-Control: max-age** or **Expires** has been configured for the origin server and you want the cache TTL on the CDN side to be the same as that configured on the origin server, you can switch on **Origin Cache Control**. Then **Cache-Control: max-age** or **Expires** determines how long content is cached on CDN PoPs. **NOTE** • If both **Cache-Control** and **Expires** are configured on the origin server, **Cache-Control** is preferentially used. • If origin cache control is enabled on CDN but neither **Cache-Control** nor **Expires** is configured on the origin server, CDN PoPs use the cache rules configured on CDN.	By default, this function is disabled.

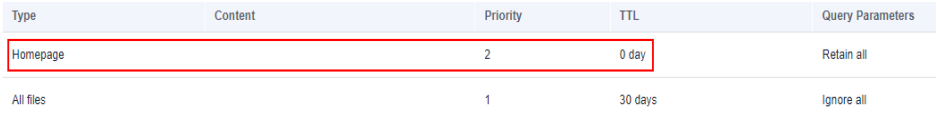
Parameter	Description	Configuration Rule
Forcible Cache	Whether CDN PoP cache ignores the **no-cache**, **private**, and **no-store** fields in the **Cache-Control** response header sent from the origin server. Forcible cache supplements origin cache control. The default rules are as follows: 1. When origin cache control is enabled, 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 origin cache control is disabled, forcible cache is enabled. ● CDN ignores response headers from the origin server and uses the cache TTL configured on the CDN console.	Enabled

Parameter	Description	Configuration Rule
	NOTE • This parameter is a special configuration parameter and is for display only. You cannot modify it. If necessary, submit a service ticket to modify it. • When both origin cache control and forcible cache are disabled, there are two cases: 1. 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. 2. If **no-cache**, **private**, or **no-store** is not set, CDN uses the cache TTL configured on the CDN console.	

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.

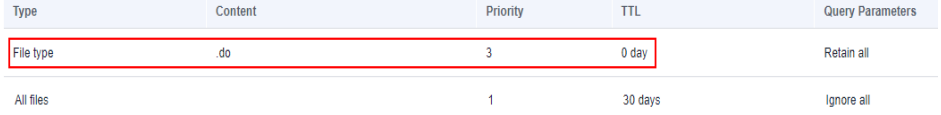


The homepage of the website is not cached, and URL parameters are not ignored in requests for all pages.

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**.



   NOTE

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

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

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

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

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

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

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

2.6.3 Browser Cache TTL

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

Precautions

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

Procedure

1. Log in to **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 domain name you want to modify or click **Configure** in the **Operation** column.
4. Click the **Cache Settings** tab.
5. In the **Browser Cache TTL** area, click **Edit**.

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

Figure 2-28 Browser cache TTL

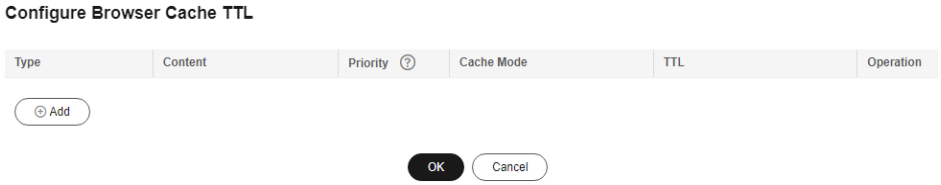


Table 2-15 Parameters

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**, leave this parameter blank. 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.
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**: Comply with 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.

7. Click **OK**.

2.6.4 Status Code Cache TTL

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

Scenarios

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

- **Application**: If users are continuously accessing image **abc.jpg** that is not cached on CDN PoPs and that has been deleted from the origin server, CDN PoPs will pull the image for each user request and the origin server will return a 4*xx* status code, increasing 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

- The status code cache TTL cannot be configured for domain names with special configurations.
- Domain names whose service type is whole site acceleration do not support this function.
- By default, CDN caches status codes 400, 404, 416, 500, 502, and 504 for 3 seconds and does not cache other status codes.
- You can modify the cache TTL of the following status codes:
  - 4*XX*: 400, 403, 404, 405, and 414
  - 5*XX*: 500, 501, 502, 503, and 504
  - 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

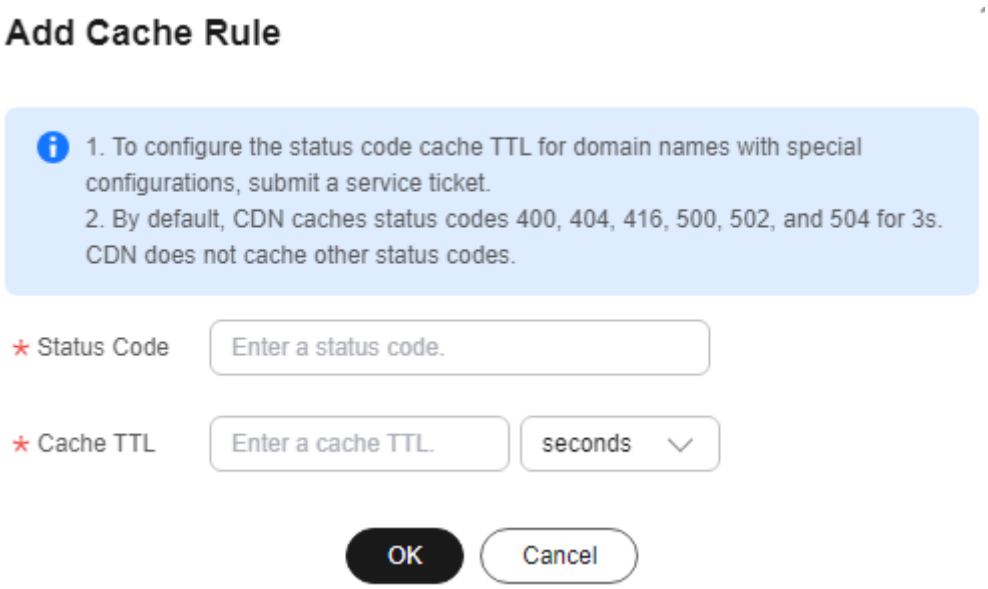


Table 2-16 Parameters

Parameter	Description	Example
Status Code	Status code to be cached.	404
Cache TTL	Duration for caching the status codes on CDN PoPs. • If it is set to **0**, the status code is not cached. • The maximum value is 365 days.	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.

2.6.5 Access URL Rewrite

Set access URL rewrite rules to redirect user requests to the URLs of cached resources.

Scenario

If the path for storing server resources changes, the path for storing resources on CDN PoPs changes accordingly. For example, the path of an image has changed from **/test** to **/testnew**. If a user sends a request to the original URL, CDN PoPs need to rewrite the requested URL.

If a URL rewrite rule has been configured, CDN matches URLs in redirection mode and uses the HTTP 302 status code (**302 Found**) to indicate that the requested resource has been temporarily moved to another location. Specifically, CDN PoPs add the new URL to the HTTP **Location** header in the 302 response sent to the client. After receiving the response, the client sends a request to the new URL. **Table 2-17** lists the redirection status codes and their meanings.

Table 2-17 Redirection modes

Code	Meaning	Processing Method	Description
301	Moved Permanently	The GET method does not change. Other methods may change to the GET method.	The resource is moved permanently.
302	Found	The GET method does not change. Other methods may change to the GET method.	This page is temporarily unavailable for unforeseen reasons.
303	See Other	The GET method does not change. Other methods are changed to the GET method (the message body is lost).	Used to redirect after a PUT or a POST, so that refreshing the result page does not re-trigger the operation.
307	Temporary Redirect	Neither the method nor the message body changes.	This page is temporarily unavailable for unforeseen reasons. Better than 302 when non-GET operations are available on the site.

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 domain name you want to modify or click **Configure** in the **Operation** column.
4. Click the **Cache Settings** tab.
5. In the **Access URL Rewrite** area, click **Add**.

Figure 2-30 Adding an access URL rewrite rule

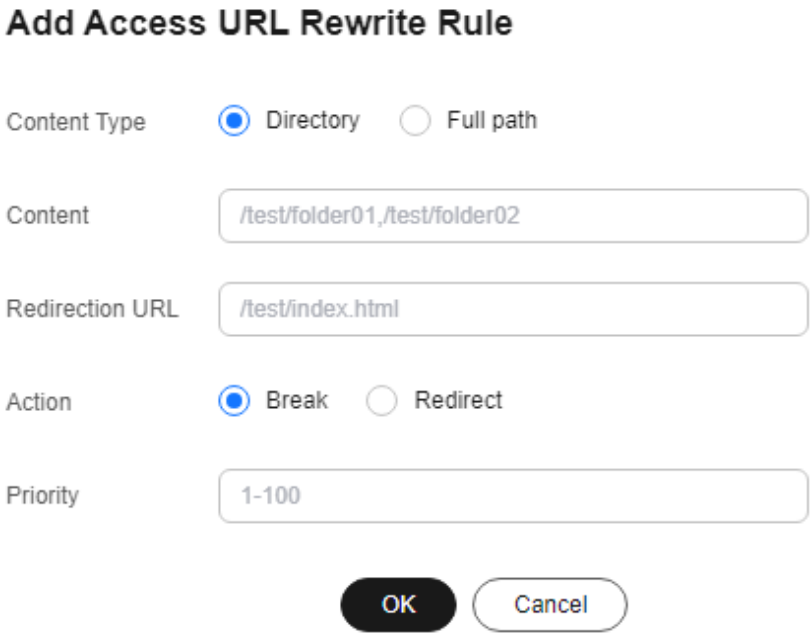


Table 2-18 Parameters

Parameter	Description
Content Type	• **Directory**: Execute the rule for files in the specified directory. • **Full path**: Execute the rule for the file of the specified path.
Content	• When **Content Type** is set to **Directory**, enter up to 20 directories and separate them by commas (,). A directory starts with a slash (/). Wildcards (*) are not supported. Example: **/test/folder01,/test/folder02** • When **Content Type** is set to **Full path**, enter the path of a file or a path with wildcards (*). A path must start with a slash (/) and cannot end with a wildcard (*). Only one wildcard (*) can be entered. Examples: **/test/index.html** or **/test/*.jpg** • Regular expression match is not supported.

Parameter	Description
Redirection URL	Target URL. Start with a slash (/) and do not contain **http://**, **https://**, or the domain name. Example: **/newtest/index.html** • When **Content Type** is set to **Full path**, the wildcard (*) can be captured by **$1**. For example, if **Content** is set to **/test/*.jpg** and **Redirection URL** is set to **/newtest/$1.jpg**, when a user requests **/test/11.jpg**, **$1** is replaced by **11**, so the requested URL after redirection is **/newtest/11.jpg**.
Action	Select **Redirect** or **Break**. • **Redirect**: If the requested URL matches this rule, the request is redirected to the target URL. After this rule is executed, if other rules exist, CDN continues to execute these rules. • **Break**: If the requested URL matches this rule, the request is redirected to the target URL. After this rule is executed, CDN does not execute any other rules and returns status code 200. You cannot set the status code.
Redirection Host	Domain name to which client requests are redirected. Specify the value when **Action** is set to **Redirect**. • By default, the acceleration domain name is used. • The value contains 1 to 255 characters and starts with **http://** or **https://**, for example, **http://www.example.com**.
Redirection Status Code	Specify the value when **Action** is set to **Redirect**. The status code can be 301, 302, 303, or 307. For details about their differences, see **Table 2-17**.
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.

6. Click **OK**.

2.6.6 FAQ

1. **How Do I Improve the Cache Hit Ratio?**
2. **Why Some Files Can't Be Downloaded Although They Have Not Expired (365 Days)?**
3. **Does CDN Cache Status Codes 404 and 403?**
4. **Why Can't I Log In to My Domain Name or Why Is the Information of Other Users Displayed?**

2.7 Access Control

2.7.1 Overview

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

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

2.7.2 Referer Validation

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

Background

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

When receiving access requests from users, the CDN PoPs identify and check users against the referer blacklist or whitelist. Only users meeting blacklist and whitelist requirements can access the content. Unqualified users will receive a 403 error response.

Precautions

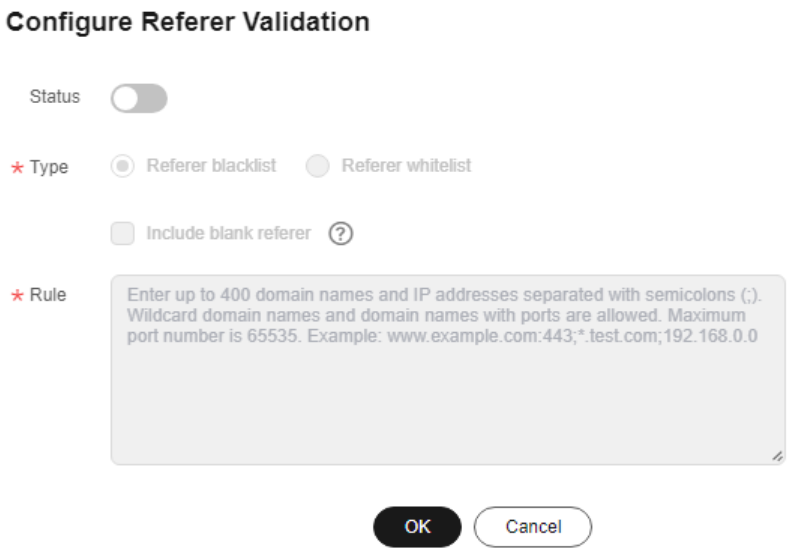
- This function is disabled by default.
- Either a referer blacklist or whitelist can be configured.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab.
5. In the **Referer Validation** area, click **Edit**. The **Configure Referer Validation** dialog box is displayed.

   Figure 2-31 Configuring referer validation

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 2-19 Parameters

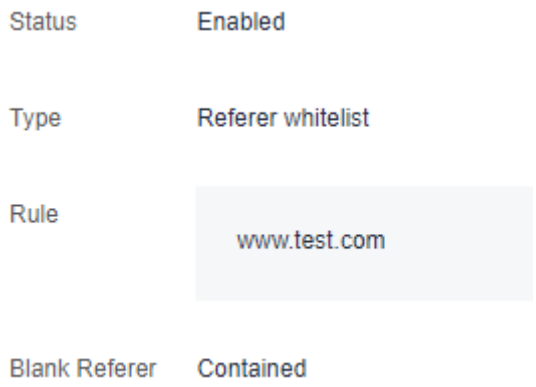
Parameter	Description	Filling Rule
Include blank referer	A blank referer is when the referer field in an HTTP request is left blank or when an HTTP request does not contain the referer field. If this option is selected, such requests will also be filtered out based on configured whitelists and blacklists. **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.	/
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 400 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 400 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.

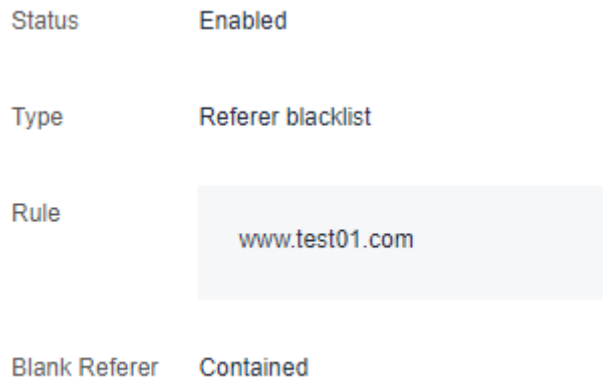
Examples

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



- 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.



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

2.7.3 IP ACL

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

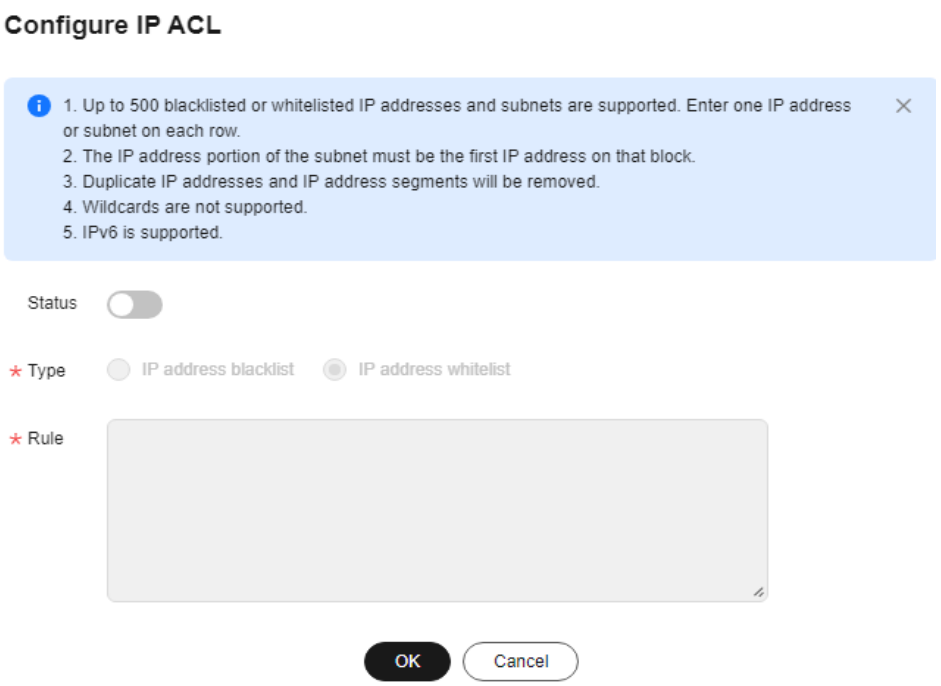
Precautions

- This function is disabled by default.
- If your domain name is connected to **EdgeSec** and an IP address blacklist/whitelist rule is configured in both services, the rule in CDN is executed first.

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 2-32 Configuring an IP ACL

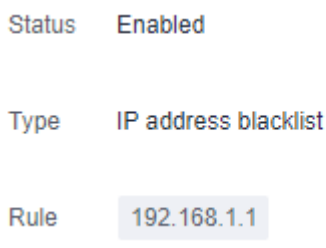
6. Switch on **Status** to enable this configuration item.
7. Select a type and enter rules.

Parameter	Description
Type	• **IP address blacklist**: If the IP address of a user is included in the IP address blacklist, status code 403 will be returned when the user accesses a CDN PoP. • **IP address whitelist**: If the IP address of a user is not included in the IP address whitelist, status code 403 will be returned when the user accesses a CDN PoP. **NOTE** • 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**:



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

2.7.4 User-Agent ACL

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

Background

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

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

Precautions

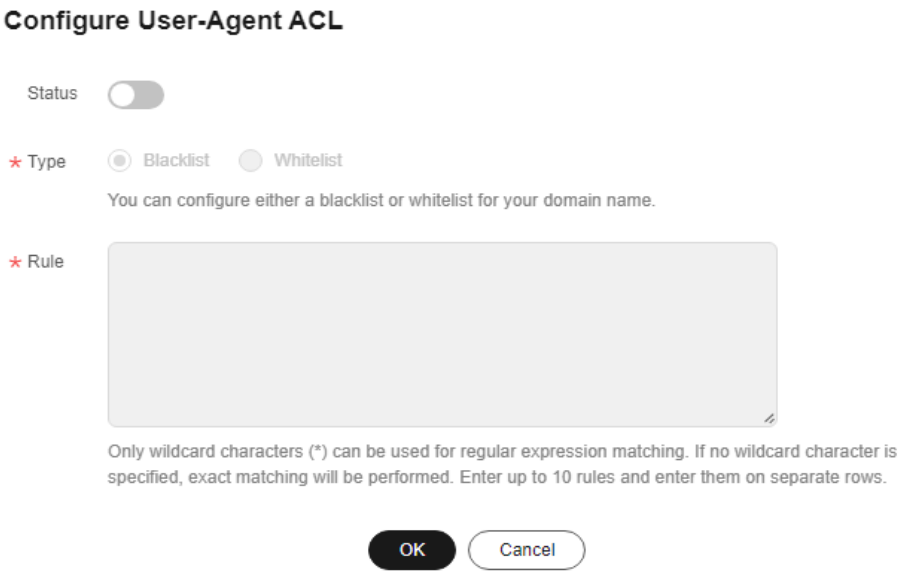
- This function is disabled by default.
- Either a User-Agent blacklist or whitelist can be configured.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab.
5. In the **User-Agent Access Control** area, click **Edit**. The **Configure User-Agent Access Control** dialog box is displayed.

   Figure 2-33 Configuring a User-Agent ACL



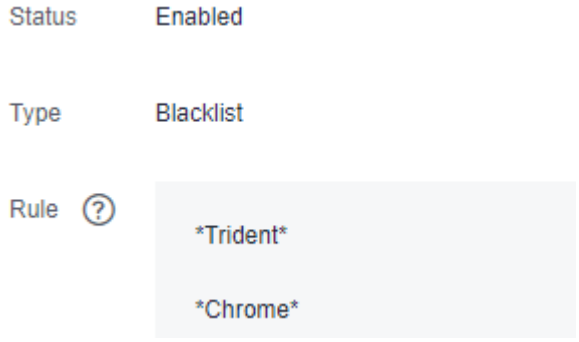
6. Switch on **Status** to enable this configuration item.
7. Select a type and enter rules.

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.
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 10 rules, and enter them at separate rows.

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

Example

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



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

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

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

2.7.5 Token Authentication

2.7.5.1 Signing Method A

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

NOTE

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

How It Works

An example signed URL looks like:

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

The following table describes the parameters in a signed URL.

Table 2-20 Parameter description

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

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

Verification Method

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

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

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

   Or

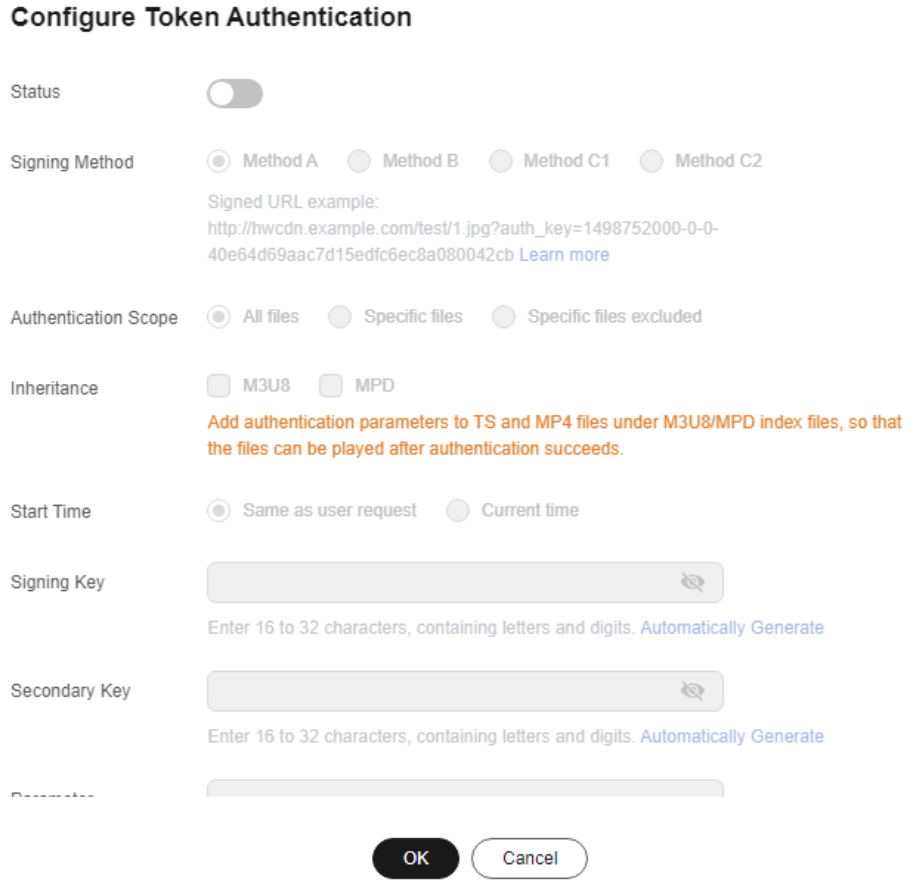
   ```
   sstring = "Filename-Timestamp-rand-uid-PrivateKey"
   HashValue = sha256sum(sstring)
   ```

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab and click **Configure** under **Token Authentication**.

Figure 2-34 Configuring token authentication



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

Table 2-21 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 authentication parameters 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 Extension	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. Enter 16 to 32 characters. The password can only and must contain both letters and digits.
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. • Enter 16 to 32 characters. The password can only and must contain both letters and digits.
Parameter	Authentication parameter carried in a URL. The default value is **auth_key**. • Enter up to 100 characters. • Enter letters, digits, and underscores (_). Do not start with a digit.

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

Authentication Calculator

Using the authentication calculator, you can generate a signed URL for users. Set parameters according to **Table 2-21** and **Table 2-22**, 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 2-22 Parameter description

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

Disabling Token Authentication

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

Example

The following uses the MD5 algorithm as an example:

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

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

2.7.5.2 Signing Method B

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

NOTE

- Token authentication is disabled by default.
- If your domain name has special configurations, token authentication cannot be configured for this domain name on the CDN console.
- Domain names whose service type is **whole site acceleration** do not support **signing method B**.
- When token authentication is configured, user requests will include authentication parameters. If **Ignore specific parameters** is not configured:
  - Origin pull will become frequent.
  - If your origin server is an OBS bucket, fees for bucket outbound traffic will incur.

How It Works

An example signed URL looks like:

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

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

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

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

The following table describes the parameters in a signed URL.

Table 2-23 Parameter description

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

Verification Method

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

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

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

   Or

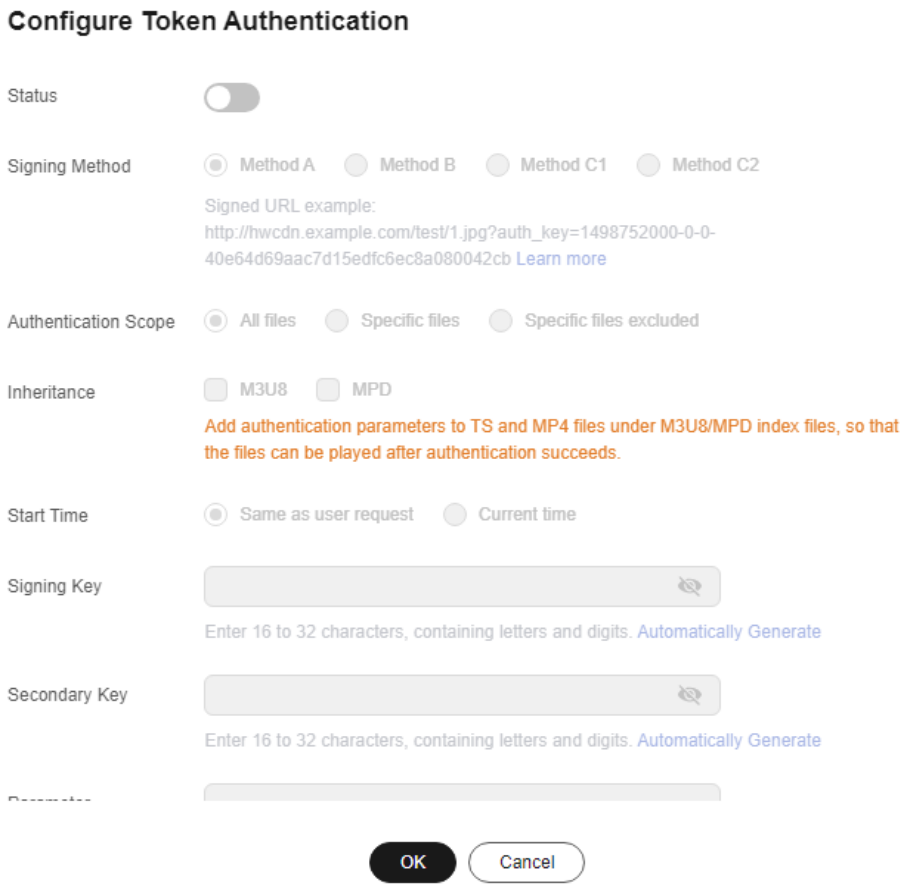
   ```
   sstring = "PrivateKeytimestampFilename"
   HashValue = md5sum(sstring)
   ```


Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab and click **Configure** under **Token Authentication**.

   Figure 2-35 Configuring token authentication

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

   Table 2-24 Parameter description

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

Parameter	Description
Inheritance	Add authentication parameters 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 Extension	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. Enter 16 to 32 characters. The password can only and must contain both letters and digits.
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. • Enter 16 to 32 characters. The password can only and must contain both letters and digits.
Encryption Algorithm	**MD5** or **SHA256**.
Validity Period	How long a 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 2-24** and **Table 2-25**, and click **Generate** to generate a signed URL that will expire at a specific time.

Table 2-25 Parameter description

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

NOTE

Escape special characters in the signed URL if any.

Disabling Token Authentication

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

Example

The following uses the MD5 algorithm as an example:

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


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

6. The request URL is:

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

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

2.7.5.3 Signing Method C1

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

NOTE

- Token authentication is disabled by default.
- If your domain name has special configurations, token authentication cannot be configured for this domain name on the CDN console.
- Domain names whose service type is **whole site acceleration** do not support **signing method C1**.
- When token authentication is configured, user requests will include authentication parameters. If **Ignore specific parameters** is not configured:
  - Origin pull will become frequent.
  - If your origin server is an OBS bucket, fees for bucket outbound traffic will incur.

How It Works

An example signed URL looks like:

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

The following table describes the parameters in a signed URL.

Table 2-26 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.

Parameter	Description
Validity Period	How long a signed URL remains effective. The value ranges from 0s to 31,536,000s. Example: If the validity period is set to 1,800s, users can access CDN within 1,800s since the time indicated by **timestamp**. Authentication fails and the URL is inaccessible if users access CDN 1,800s later.
md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of digits (0 to 9) and lowercase letters.
sha256	A string of 64 characters calculated using the SHA256 algorithm. The string consists of digits and lowercase letters.
Filename	Back-to-origin URL. Its value must start with a slash (/) and does not include the parameters following the question mark (?).
PrivateKey	Signing key, which is used to generate a signed URL, for example, **huaweicloud12345**. Enter 16 to 32 characters. The password can only and must contain both letters and digits.

Verification Method

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

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

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

   Or

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

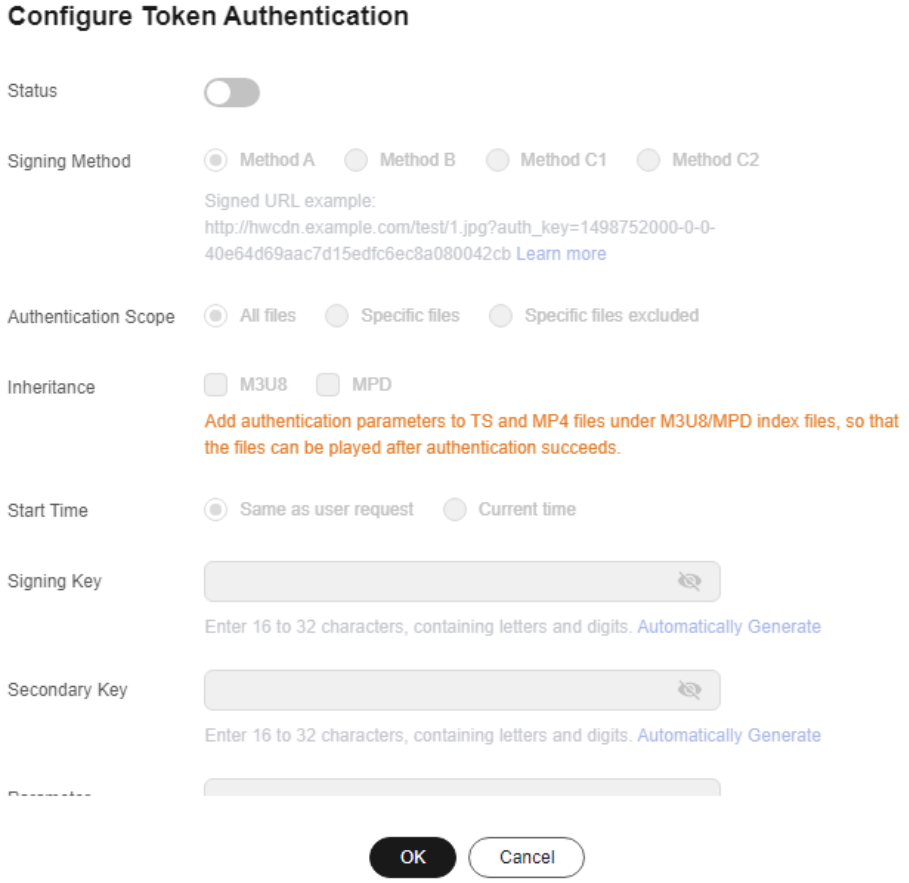
Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.

3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab and click **Configure** under **Token Authentication**.

Figure 2-36 Configuring token authentication



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

Table 2-27 Parameter description

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

Parameter	Description
Inheritance	Add authentication parameters 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 Extension	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. Enter 16 to 32 characters. The password can only and must contain both letters and digits.
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. • Enter 16 to 32 characters. The password can only and must contain both letters and digits.
Encryption Algorithm	**MD5** or **SHA256**.
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s.

Authentication Calculator

Using the authentication calculator, you can generate a signed URL for users. Set parameters according to **Table 2-27** and **Table 2-28**, 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 2-28 Parameter description

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

Disabling Token Authentication

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

Example

The following uses the MD5 algorithm as an example:

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

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

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

2.7.5.4 Signing Method C2

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

NOTE

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

How It Works

An example signed URL looks like:
http://DomainName/FileName?auth_key=<sha256>&timestamp=<timestamp>
http://DomainName/FileName?auth_key=<md5hash>&timestamp=<timestamp>

The following table describes the parameters in a signed URL.

Table 2-29 Parameter description

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

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

Verification Method

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

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

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

   Or

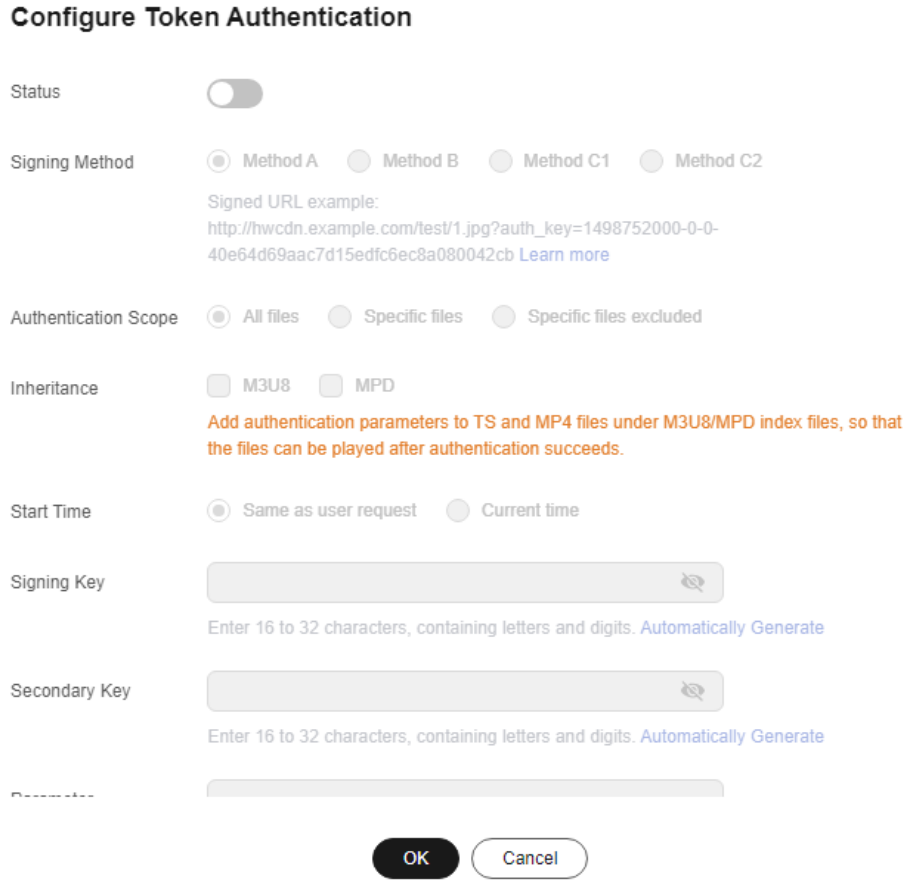
   ```
   sstring = "PrivateKeyFilenameTimestamp"
   HashValue = sha256sum(sstring)
   ```

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab and click **Configure** under **Token Authentication**.

Figure 2-37 Configuring token authentication



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

Table 2-30 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 authentication parameters 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 Extension	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. Enter 16 to 32 characters. The password can only and must contain both letters and digits.
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. • Enter 16 to 32 characters. The password can only and must contain both letters and digits.
Parameter	Authentication parameter carried in a URL. The default value is **auth_key**. • Enter up to 100 characters. • Enter letters, digits, and underscores (_). Do not start with a digit.

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

Authentication Calculator

Using the authentication calculator, you can generate a signed URL for users. Set parameters according to **Table 2-30** and **Table 2-31**, 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 2-31 Parameter description

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

Disabling Token Authentication

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

Example

The following uses the MD5 algorithm as an example:

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

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

2.7.6 Remote Authentication

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

Background

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

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

The remote authentication process is as follows.

Figure 2-38 Remote authentication process

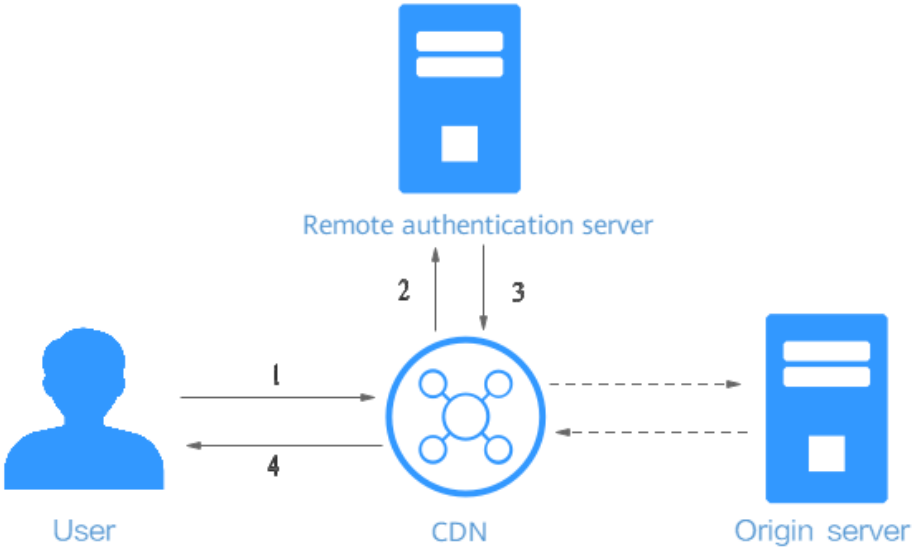


Table 2-32 Process description

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.
- Domain names with special configurations do not support remote authentication.

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 **Remote Authentication**.

Figure 2-39 Configuring remote authentication

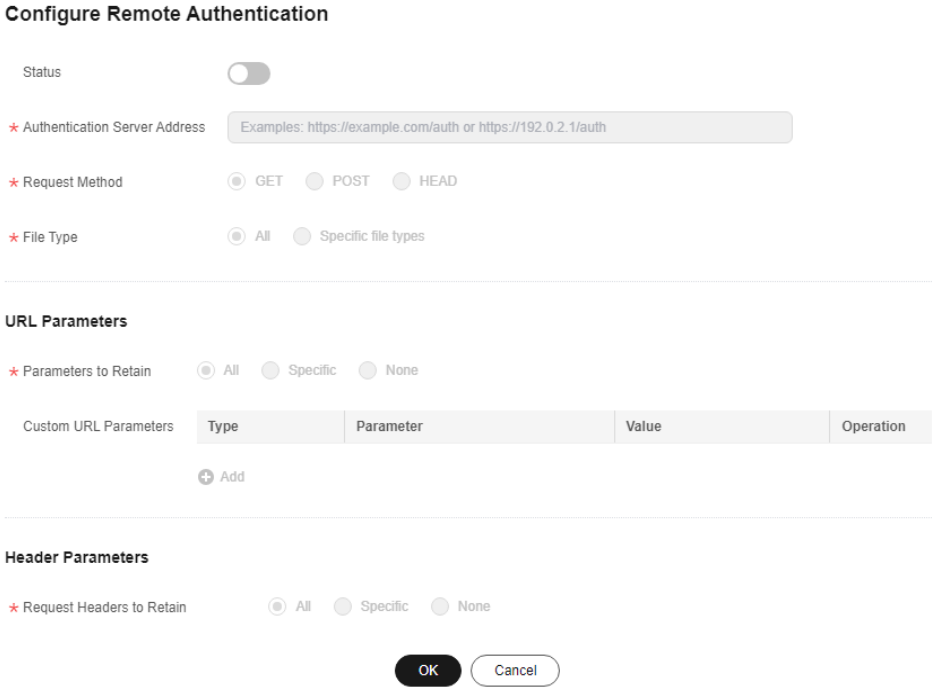


Table 2-33 Parameter description

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). • Customize a parameter, which does not support variables. • Select a preset or customized parameter, which supports variables.	Select **http_host**. Value: **$http_host**.
Request Headers to Retain	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). • Customize a parameter, which does not support variables. • Select a preset or customized parameter, which supports preset variables.	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 2-34 Preset parameters

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

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

2.7.7 IP Access Frequency

You can restrict the number of queries per seconds (QPS) to a URL from a single IP address to a single PoP to defend against CC attacks and malicious theft.

Precautions

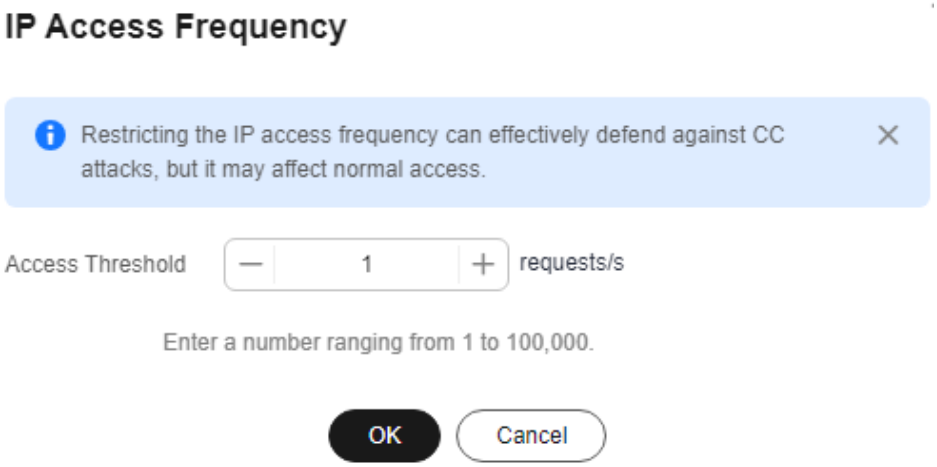
- Restricting the IP access frequency can effectively defend against CC attacks, but it may affect normal access.
- When the QPS of an IP address reaches the threshold, CDN returns status code 403. The restriction is removed 10 minutes later.
- By default, this function is disabled.

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



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.

2.8 Advanced Settings

2.8.1 HTTP Header Settings (Cross-origin Requests)

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

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

Precautions

- Some headers cannot be set or deleted. For details, see **Constraints**.
- You can add up to 10 HTTP response header configurations.
- HTTP header configuration is domain name-specific. When the configuration takes effect, the specified headers will be added to or removed from response messages for any resources under the entire domain. However, HTTP header configuration only affects the response behavior of the clients (browsers). They do not affect the cache behavior of CDN PoPs.
- If your domain name is an OBS bucket and CORS rules are configured on CDN, you also need to configure **CORS** on OBS.

Supported Response Headers

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

- **Content-Disposition**

  The Content-Disposition header can start a download on the client side and specify the name of the file to be downloaded.

  When a server sends a file to a browser, as long as the file format is supported (for instance TXT or JPG), the file is opened using the browser by default. If the file needs to be treated as an attachment and saved with a specific file name, you can use the Content-Disposition header field to specify this requirement.

  NOTE

  If you use an OBS bucket created after January 1, 2022 as the origin server and want to enable online preview, set Content-Disposition to inline. For details, see **How Do I Preview Objects in OBS Through a Browser?**

- **Content-Language**

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

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

  The Access-Control-Allow-Origin header carries the domain names that are allowed for CORS after server authentication. For a simple CORS request, the browser determines whether to return the requested resource content to the client based on this message header. For a pre-check request, the browser determines whether to initiate an actual CORS request to the server based on this message header.

  NOTE

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

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

  The Access-Control-Allow-Methods header carries the methods that are allowed for CORS after server authentication. For a simple CORS request, the browser determines whether to return the requested resource content to the client based on this message header. For a pre-check request, the browser determines whether to initiate an actual CORS request to the server based on this message header.

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

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

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

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

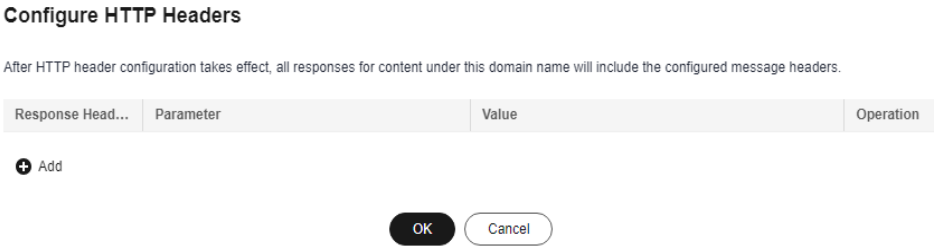
- **Custom**

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

Procedure

1. Log in to the **CDN 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

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.

Response Header Operation	Description
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**: For a typical configuration, see the example on the right.	attachment;filename=FileName.xls
Content-Language	Specifies the language of the response page of the client. **Value requirements**: For a typical configuration, see the example on the right.	zh-CN en-US

Parameter	Description	Example Value
Access-Control-Allow-Origin	Specifies the foreign domain URLs (request sources) that are allowed to access the resource in cross-origin resource sharing (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**: Multiple methods can be configured at the same time. Separate them with commas (,).	GET,POST,HEAD
Access-Control-Max-Age	Specifies how long to cache the pre-check results of CORS requests on specific resources. **Value requirements**: This value is expressed in seconds and ranges from 0 to 1,000,000,000.	86400

Parameter	Description	Example Value
Access-Control-Expose-Headers	Specifies the response header information visible to the client for a CORS request. **Value requirements**: Enter 1 to 256 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
Custom	Specifies the custom response header for a CORS request. **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 **max-age=******* (***** is a number), **private**, **no-cache**, **no-store**, or **public**. Only one value can be configured.	x-testcdn

8. Click **OK**.

Constraints

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

Content-Base	Content-Disposition

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

- CDN does not support the following response headers:

A_Dynamic	If-None-Match	Sec-WebSocket-Origin	X-Forward-Peer
Accept-Ranges	If-Range	Sec-WebSocket-Protocol	X-Forward-Type
X-Forward-Ip	Keep-Alive	Sec-WebSocket-Version	X-Forward-Uri
Allow	Key	Set-Cookie	X-Forwarded-For
Authentication-Info	Last-Modified	Tcp-Retrans	X-IP-Region
Authorization	Link	Title	X-IP-Region-CN
X-Forward-Measured	Location	Transfer-Encoding	X-Ip-Blackwhite-List
Cdn-Qos	Max-Forwards	Upgrade	X-Local-Ip
Cdn-Server-Ip	Meter	Vary	X-Log-Url
Cdn-Src-Ip	Mime-Version	Via	X-MAA-Alias
Conf-Err-Host	Negotiate	WWW-Authenticate	X-MAA-Auth
Conf-File	Origin	Warning	X-Max-Conns
Conf-File-List	Partition-Block-Size	Ws-Hdr	X-Mem-Url
Conf-Option	Pragma	WsTag	X-Mgr-Traffic
Conf-Other	Proxy-Authenticate	X-Accelerator-Vary	X-Miss-Rate-Limit
Connection	Proxy-Authentication-Info	X-Appa	X-Miss-Times-Limit
Content-Encoding	Proxy-Authorization	X-Appa-Origin	X-No-Referer
Content-Length	Proxy-Connection	X-Black-List	X-Query-Key
Content-Location	Proxy-Support	X-Bwctrl-Limit	X-Rate-Limit

Content-MD5	Public	X-Bwctrl-Para	X-Refresh-Pattern
Content-Range	Purge-Domain	X-Cache	X-Request-Id
Sec-WebSocket-Nonce	Purge-Extra	X-Cache-2	X-Request-Uri
Date	Range	X-Cache-Lookup	X-Request-Url
Dynamic	Request-Range	X-Cacheable	X-Resp-Time
ETag	Retry-After	X-Cdn-Src-Port	X-Rewrite-Url
Error	Sec-WebSocket-Accept	X-Client-Ip	X-Squid-Error
Expect	Sec-WebSocket-Draft	X-DNS-Time	X-Times-Limit
If-Modified-Since	Sec-WebSocket-Extensions	X-Denyattack-Dynconf	X-Url-Blackwhite-List
From	Sec-WebSocket-Key	X-Error-Status	X-Via-CDN
Front-End-Https	Sec-WebSocket-Key1	X-Error-URL	X-White-List
Host	Sec-WebSocket-Key2	X-Forward-Host	-
If-Match	Sec-WebSocket-Location	-	-

2.8.2 Custom Error Pages

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

Precautions

- You can customize error pages for status codes 4*xx* and 5*xx*.
- If CDN acceleration is enabled for the custom error pages, you will be billed by CDN.
- Error pages cannot be customized for domain names with special configurations.

Procedure

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

   The CDN console is displayed.

2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Advanced Settings** tab.
5. In the **Custom Error Pages** area, click **Add**.

Figure 2-42 Customizing an error page

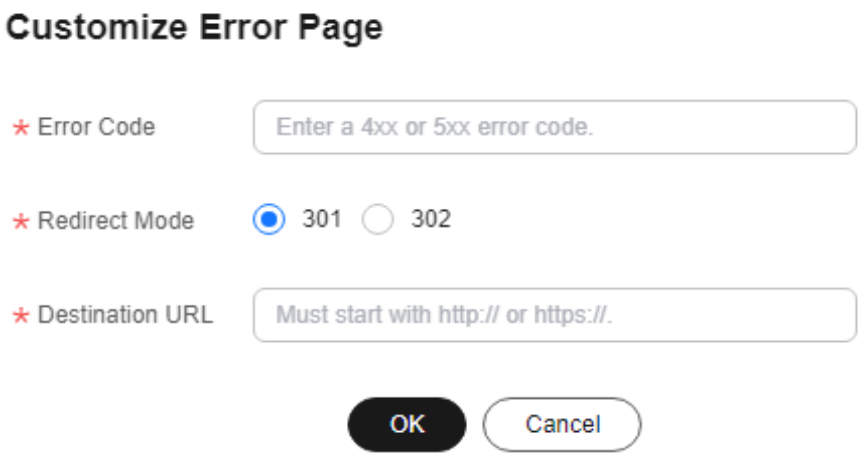


Table 2-35 Parameter description

Parameter	Description	Example
Error Code	Error code 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**.

Examples

Image **abc.jpg** has been deleted from the origin server and the cache on CDN PoPs has expired. When a user accesses https://example.com/abc.jpg, a status code 404 is returned. Assume that you configure the following settings on the CDN console:

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

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

2.8.3 Smart Compression

Background

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

Precautions

- Smart compression applies to JS, HTML, CSS, XML, JSON, SHTML, and HTM files.
- Do not enable this function if MD5 verification has been configured for your origin server. When CDN compresses static files, the MD5 value is changed. As a result, the MD5 value of the compressed file is different from that of the file on the origin server.
- Some browsers do not support Brotli compression. Check supported browsers on **this website**.
- 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

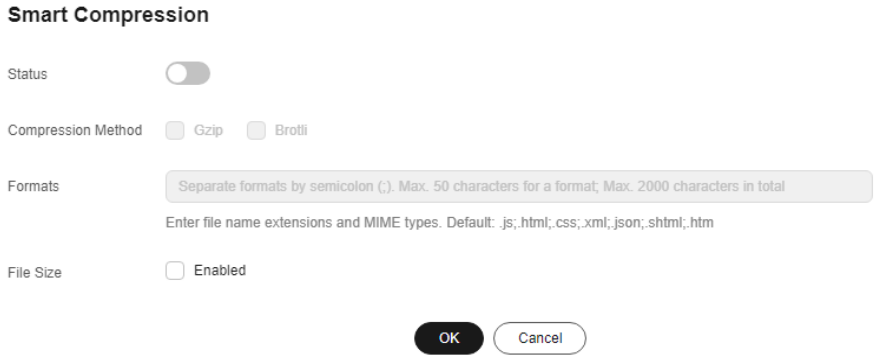


Table 2-36 Parameter description

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 and click **OK**.

2.8.4 WebSocket Settings

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.

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.

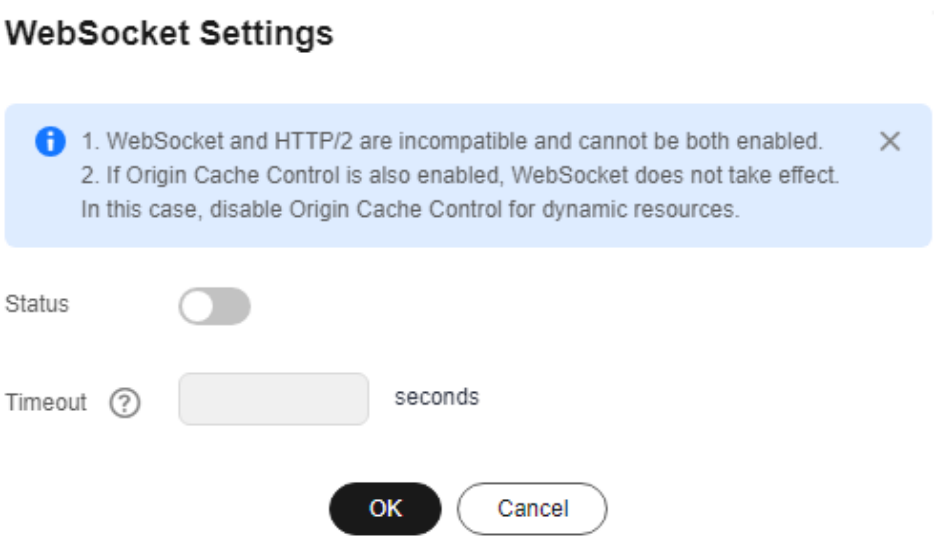
Precautions

- This function applies only to domain names whose service type is **whole site acceleration**.
- 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.
- WebSocket cannot be configured for domain names with special configurations.
- 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

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

2.8.5 Request Rate Limiting

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

Precautions

- Rate limiting takes effect for all user requests to the domain name, which affects the acceleration effect and user experience.

- You can configure up to 60 rate limiting rules.
- You can configure only one rate limiting rule for **All files**.

Procedure

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

Figure 2-45 Configuring request rate limiting

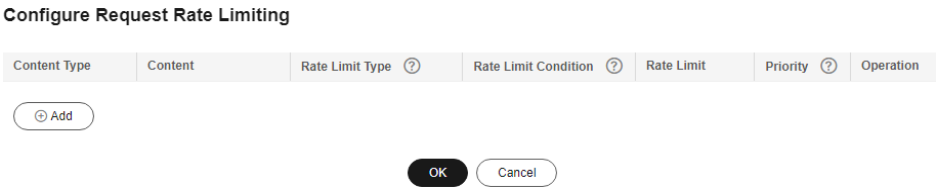


Table 2-37 Parameters

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. Each rule corresponds to a directory. Multiple directories cannot be configured for a rule.
Rate Limit Type	Rate limiting by transmission traffic is supported. That is, when the traffic of a single HTTP request reaches the specified value, the access speed is limited. The access speed of subsequent requests cannot exceed the specified rate limit.
Rate Limit Condition	Volume of the transmitted traffic that triggers rate limiting. • 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.

Parameter	Description
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.

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

2.8.6 Usage Cap

You can set a traffic or bandwidth cap for a domain name. When the usage reaches the cap, CDN acceleration will be disabled for the domain name, reduce high bills caused by traffic theft or attacks.

Scenario

If your domain name is attacked or has malicious traffic coming, there may be sudden traffic spikes that result in a bill higher than your normal expenditures. In this case, you can enable usage cap. Once the consumed bandwidth or traffic reaches the cap in a specified period, CDN acceleration will be disabled for this domain name.

Precautions

- Statistics data has a delay of about 10 minutes. When your domain name reaches the cap, CDN acceleration will be disabled about 10 minutes later. The traffic, bandwidth, and number of requests generated during this time are charged.
- When CDN acceleration is disabled for your domain name, the domain name cannot be accessed (status code 403 is returned). Set a proper usage cap to prevent service loss.
  - After CDN acceleration is disabled for a domain name, the CNAME record will be deleted. If the local DNS has a resolution cache or a user uses a host to forcibly resolve the domain name to a CDN PoP, CDN will refuse to provide services after receiving the request. However, traffic and request data will be generated. You need to pay for the traffic and request data.
- Exercise caution when setting a usage cap for a wildcard domain name (for example, ***.test.com**). The total usage of all subdomain names, such as **a.test.com**, **b.test.com**, and **c.test.com**, is collected. Once the total usage reaches the cap, CDN acceleration is disabled for the wildcard domain name and all subdomain names become inaccessible.
- You can set usage caps for up to 20 domain names. Each domain name can have only one bandwidth cap rule.
- Domain names with special configurations do not support usage cap.
- When a domain name reaches the usage cap and CDN is disabled, the usage cap function is not in effect during the current statistical period. For example:

  - On October 19, 2023, a customer set a traffic cap rule, that is, when the accumulated traffic usage within an hour reaches 400 GB, CDN acceleration will be disabled for 1 hour. From 20:00 to 20:35 on October 25, 2023, the traffic suddenly increased to 400 GB. Due to a delay in monitoring data, CDN acceleration was disabled for this domain name at about 20:41 on October 25, 2023. In this case, the usage cap function was not in effect from 20:41 to 20:59:59.

- When the bandwidth or traffic cap is reached, CDN delivers the settings of returning the status code 403 to all PoPs. In this case, there is a delay between the cap being reached and the status code being returned to users.
- Usage capping is free of charge on CDN. Simple Message Notification (SMN) charges you for alarm notifications sent to you. For details about SMN pricing, see **SMN Pricing Details**.

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 and enable the switch next to **Usage Cap**.

Figure 2-46 Setting the usage cap

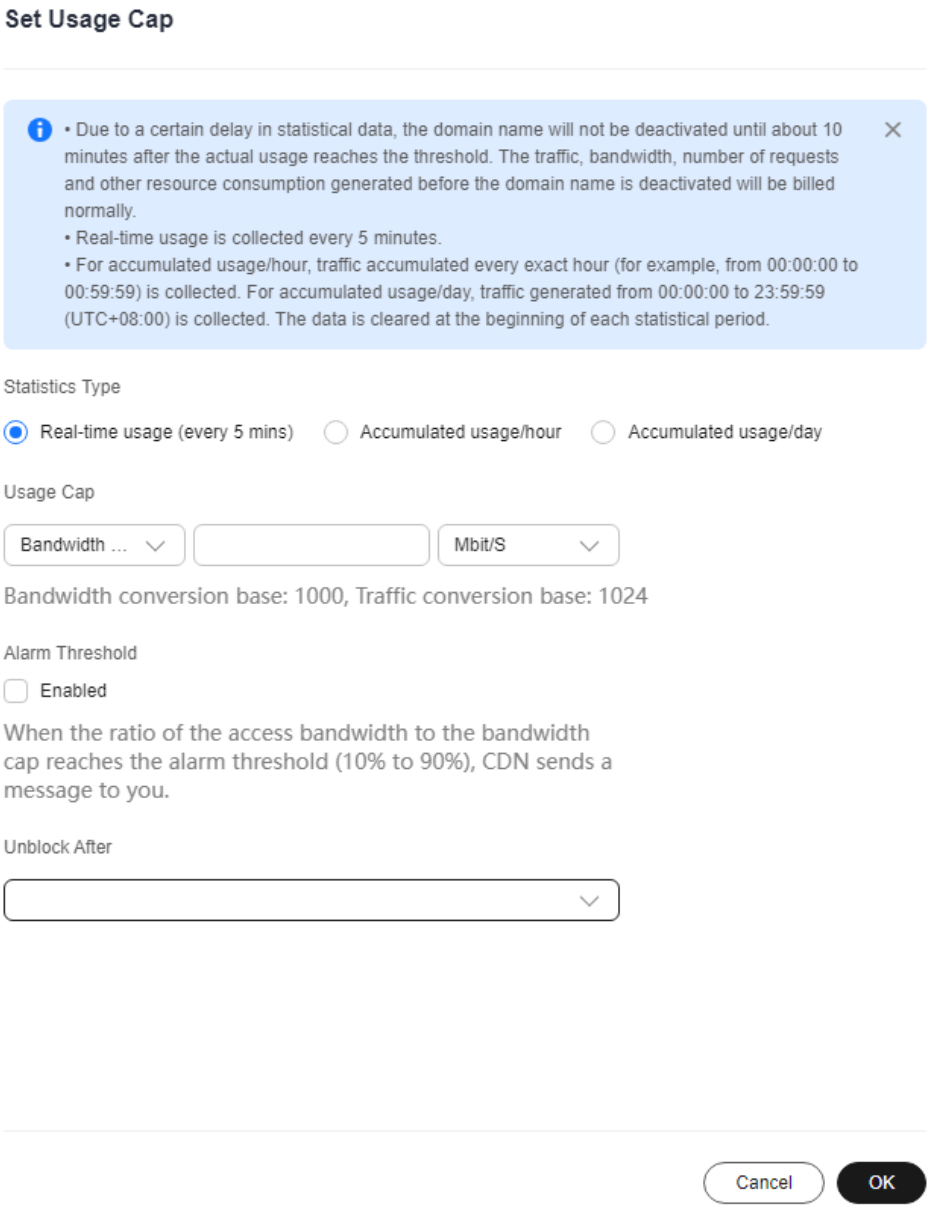


Table 2-38 Parameters

Parameter	Description	Example
Statistics Type	**Real-time usage**: Collects the traffic/bandwidth statistics every 5 minutes. • The start time of a statistical period is a multiple of 5 minutes. For example, if a rule is configured at a time from 00:10:01 to 00:14:59, the start time of the first statistical period is 00:10:00 (rounding down to the nearest 5 minutes). **Accumulated usage/hour**: Collects statistics on the traffic accumulated every exact hour. For example, the first statistical period on October 19, 2023 is 00:00:00 to 00:59:59. • After a usage cap is set, the first statistical period may be less than one hour. For example, if the usage cap is set at 00:25:00 on October 19, 2023, the usage from 00:25:00 to 00:59:59 is collected in the first statistical period. **Accumulated usage/day**: Collects statistics on the traffic accumulated every day (UTC+08:00). For example, the statistical period on Oct 19, 2023 is 00:00:00 to 23:59:59.	Real-time usage
Usage Cap	For real-time usage, you can set a traffic or bandwidth cap. For accumulated usage, you can only set a traffic cap. **Bandwidth cap**: Collects bandwidth usage every 5 minutes. You can set a bandwidth cap as required. **Traffic cap**: Collects traffic usage in the specified period. You can set a traffic cap as required. **NOTE** The bandwidth and traffic conversion rules for usage capping are the same as those for billing. The default conversion rules are: 1 GB = 1,024 MB and 1 Gbit/s = 1,000 Mbit/s.	Bandwidth cap 10 Gbit/s

Parameter	Description	Example
Alarm Threshold	When the ratio of the access traffic/bandwidth to the configured cap reaches the alarm threshold, CDN sends a message to you. The alarm threshold ranges from 10% to 90%. • Alarms are sent to the mobile number and email address bound to your account through SMS messages and emails. For details about how to change the mobile number and email address, see **Binding or Changing the Service Mobile Number** and **Changing the Service Email Address**.	80%
Unblock After	Duration for disabling CDN after the bandwidth or traffic cap is reached. After the specified duration expires, CDN is automatically enabled for the domain name. • Select **60 minutes**, **12 hours**, **24 hours**, **3 days**, or **Manually**. If you select **Manually**, you need to enable CDN for the domain name on the console if you want to use it again after it is blocked.	12 hours

5. Set required parameters and click **OK**.

Fee Description

The monitoring data has a delay of about 10 minutes. After the actual usage reaches the cap, CDN acceleration will be disabled about 10 minutes later. The traffic and bandwidth generated during this period are charged.

- Example 1 (billing by peak bandwidth):

  Customer A is billed by peak bandwidth and adds domain name **example.com** to CDN. The customer enables usage cap and sets the bandwidth cap to 15 Gbit/s.

  The bandwidth suddenly increased to 15 Gbit/s from 22:00 to 22:05 on October 10, 2023. Due to the monitoring data delay, CDN acceleration was disabled at about 22:11 on the same day and the peak bandwidth reached 23 Gbit/s. In this case, 23 Gbit/s bandwidth was charged in the bill for peak bandwidth generated on October 10, 2023.

- Example 2 (billing by traffic):

  Customer B is billed by traffic and adds domain name **example.com** to CDN. The customer enables usage cap and sets the traffic cap to 400 GB.

  From 22:00 to 22:05 on October 10, 2023, the traffic usage surged to 400 GB. Due to the monitoring data delay, CDN acceleration was disabled at about

22:11 on October 10, 2023. The traffic usage during this time reached 550 GB. Any traffic generated before CDN acceleration was disabled was included in the bill of 22:00 to 23:00 on October 10, 2023.

2.9 Video Settings

2.9.1 Video Seek

Background

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

- If video seek is configured, a user client sends a request similar to the following to the server when the user drags the progress bar during video playback:
  ```
  http://www.example.com/test.flv?start=50
  ```
  Data starting from the 50th byte is returned to the client. If the video has been cached on a CDN PoP, the CDN PoP directly returns the data to the user.
- Video seek is valid only when URL parameter filtering is set to **Ignore URL Parameters** for MP4 and FLV files. For details, see **Cache Rules**.
- Video seek is valid only when your origin server supports Range requests.
- Only MP4 and FLV videos are supported.

Table 2-39 File formats

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

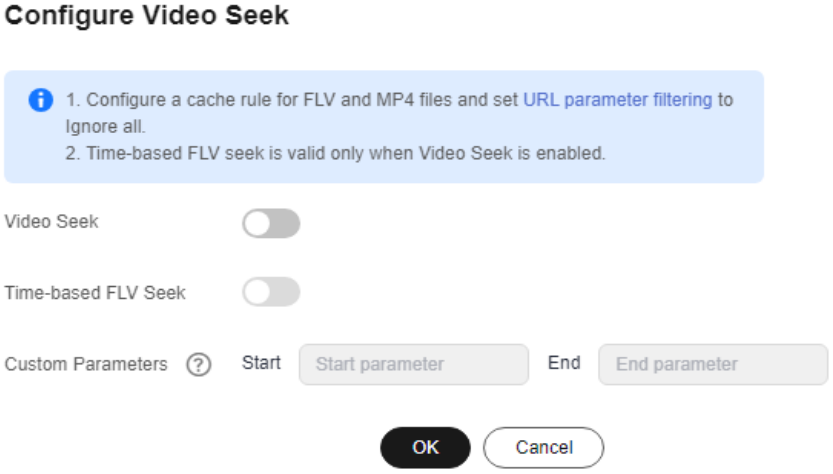
Precautions

- Domain names whose service type is whole site acceleration do not support this function.
- You have configured a cache rule for FLV and MP4 files and set **URL Parameter Filtering** to **Ignore all**.

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 2-47 Configuring video seek

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.

Restrictions

- You can add up to 20 tags to each domain name.
- If your organization has set CDN tag policies, you need to add tags to domain names based on the tag policies. Contact your organization administrator to learn about the tag policy details.

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 2-48 Editing a tag

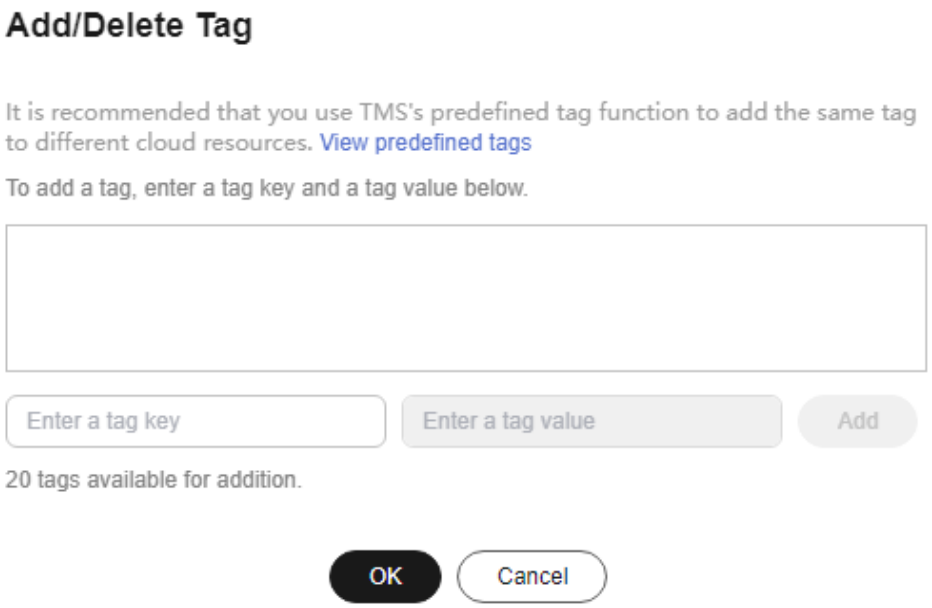


Table 2-40 Parameter description

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 2-49 Editing tags

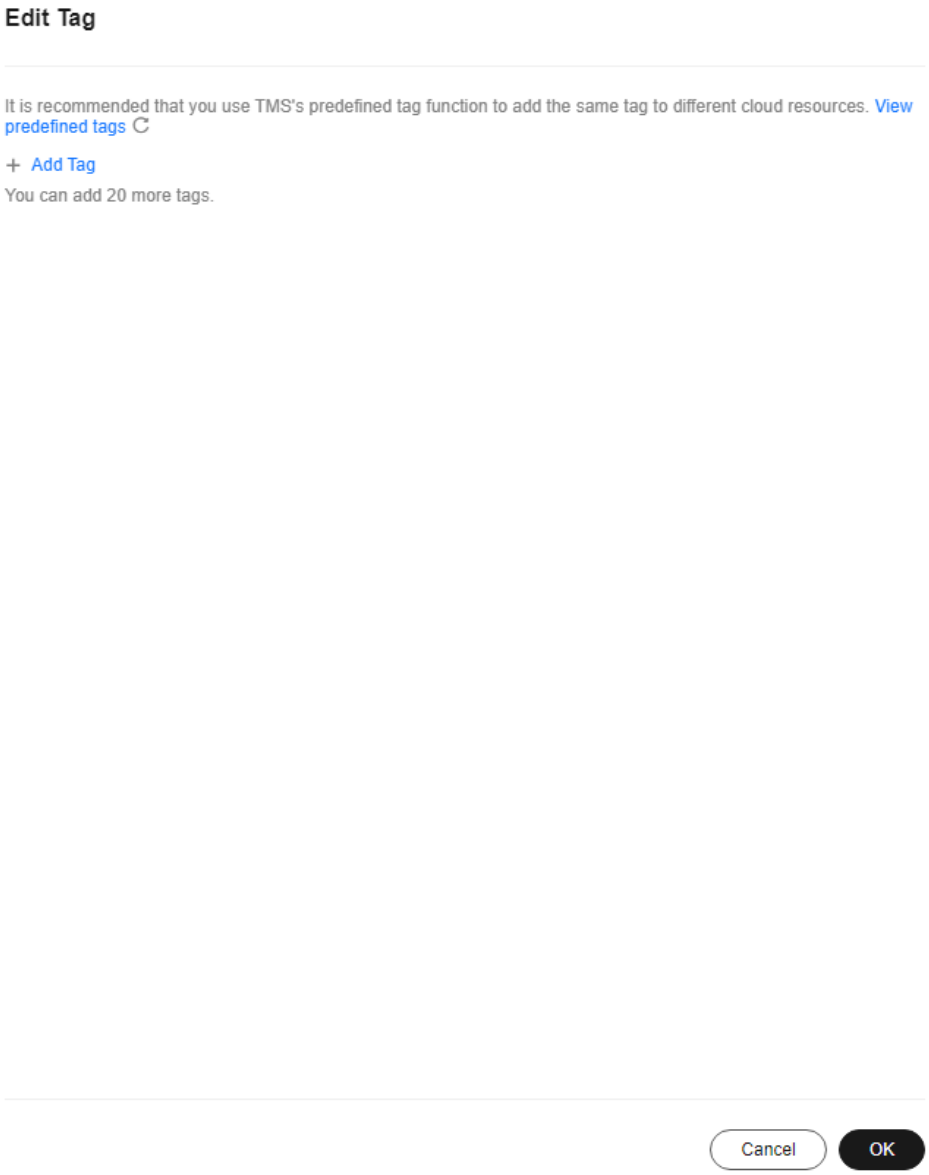


Table 2-41 Parameter description

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 Purge and Prefetch

3.1 Overview

CDN can purge and prefetch content.

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

Prerequisites

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

3.2 Cache Prefetch

Background

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

Typical Scenarios

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

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

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

Precautions

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

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 or drag a TXT file to the text box.

Figure 3-1 Cache prefetch

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. • Each account can prefetch a maximum of 1,000 URLs per day or per task. Example: http://www.example.com/file01.html http://www.example.com/file02.html https://example.huawei.com/download/app/abc.apk
URL Encode	If enabled, Chinese characters in URLs are automatically transcoded and only content of transcoded URLs is prefetched.

4. Click **Submit**.

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

3.3 Cache Purge

Background

After resources on the origin server are updated, if the old resources cached on CDN PoPs do not expire, CDN still returns the old resources to users. You can use cache purge to forcibly expire resources cached on CDN PoPs. When a user

accesses a resource, CDN pulls the latest resource from the origin server, returns it to the user, and caches it on CDN PoPs.

Typical Scenarios

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

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

Precautions

- Cache purge can be performed only for unbanned domain names in **Enabled** or **Configuring** state. For more information about the domain status, see **Viewing Basic Domain Information**.
- If a URL is rewritten, you must use the actual resource path of the new URL for cache purge.
- Some resources may be cached in browsers. Refresh the browser cache after the PoP cache is refreshed.
- You can also create a cache purge task for a domain name by calling an API. For details, see **API Overview**.
- 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 or drag a TXT file to the text box.

Figure 3-2 Cache purge

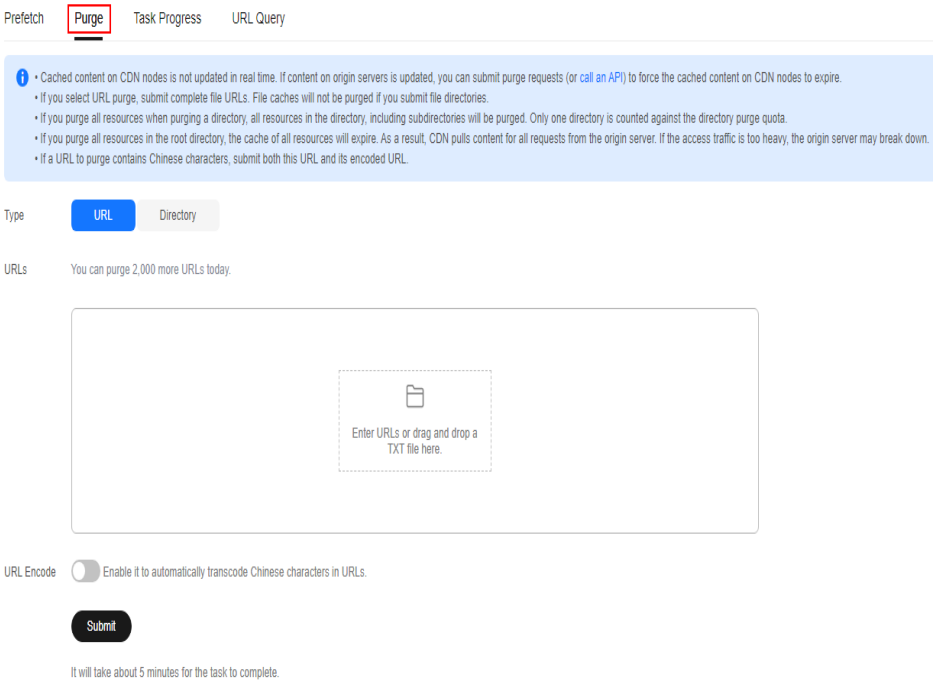


Table 3-2 Parameter description

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. • The http:// or https:// part of the URL must be included. • 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.

Type	Description
Directory	**Refreshing modes:** • **Refresh updated resources**: Refresh resources that have been updated in a directory (including subdirectories). • **Refresh all resources**: Refresh all resources in a directory, including resources in subdirectories. **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 requirements. • If you select **Refresh all resources** when refreshing the root directory, the cache of all resources will expire. As a result, CDN pulls content for all requests from the origin server. If the access traffic is too heavy, the origin server may break down. • If you select **Refresh all resources** when refreshing a directory, all resources in the directory, including subdirectories will be refreshed. Only one directory is counted against the directory refreshing quota.
URL Encode	If enabled, Chinese characters in URLs are automatically transcoded and cache is purged only for transcoded URLs.

4. Click **Submit**.

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

3.4 Viewing Task Progresses

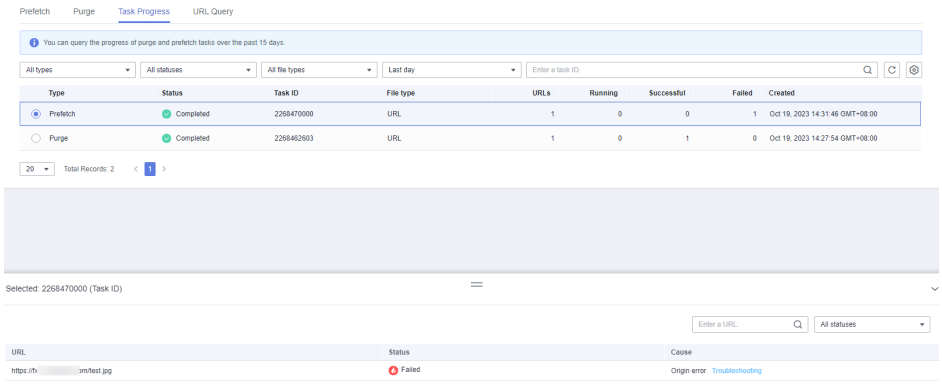
After a cache purge or prefetch task is submitted, you can view the task status on the **Task Progress** tab page.

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

   The CDN console is displayed.

2. In the navigation pane, choose **Prefetch & Purge**.

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



NOTE

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

3.5 FAQ

What Are the Differences Between Cache Purge and Prefetch?

The differences between cache purge and prefetch are:

- Cache purge

  After you submit a cache purge request, cached content on CDN PoPs will be forcibly expired. If a user requests that content, CDN will have to request fresh content from the origin server and then cache that new content.

- Cache prefetch

  After you submit a cache prefetch request, the origin server proactively sends the most current content to a CDN PoP to be cached. If a user requests the content, the CDN PoP immediately returns the cached content. It does not need to pull any new content.

For details, see **Cache Purge and Prefetch**.

Is There a Sequence Between CDN Cache Purge and Prefetch?

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

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

Does Cache Purge Refresh Content Cached on All PoPs?

Yes.

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

Possible causes include:

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

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

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

Example:

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

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

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

What Do I Do If a Cache Prefetch Operation Fails?

It is possible that:

- A large number of files are being prefetched at the same time, and this operation has occupied all of the origin server's bandwidth. In this case, you are advised to perform prefetch operations in batches. You can also increase the bandwidth of the origin server to improve the efficiency.

- The cache TTL of your requested content is 0. In this case, change the cache TTL.
- **Cache-Control** is **private**, **no-cache**, or **no-store**. If **Cache-Control** is not configured, the default value **private** is used.
- You requested to prefetch directories, dynamic content, or URLs whose cache TTL is set to 0.

Does CDN Support Directory Prefetch?

No. Only complete URLs can be prefetched. Prefetching directories is not supported. For details, see **Cache Purge and Prefetch**.

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

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

If CDN Is Enabled in and Outside the Chinese Mainland, Does It Need to Be Differentiated When Prefetch and Purge?

No. You can directly prefetch or purge the corresponding URLs.

Can I Prefetch M3U8 Files?

Yes.

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

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

Can the Cache Be Automatically Updated After a Static File on the Origin Server Is Updated?

No. However, you can call APIs to force the current content to expire and then prefetch new content. For details, see **API Overview**.

Are Cache Purge and Prefetch Mandatory?

It depends.

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

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

4 Analytics

4.1 Statistics Description

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

Table 4-1 Statistics description

Indicator	Description
Traffic	You can query the used traffic/bandwidth and traffic hit ratio for all your domain names, and export the statistics.
Requests	You can query the total requests, cache hit ratio, and queries per second for all your domain names, and export the statistics.
Origin	You can query the traffic, bandwidth, and failure rate of origin pulls for all your domain names, and export the statistics.
Data Analysis	You can query the top 100 URLs based on traffic usage or total requests for all domain names, and export the details of these top 100 URLs.
Regions & Carriers	You can query the traffic/bandwidth usage and total requests for all domain names by region or carrier, and export statistics by region or carrier.
Status Codes	You can query the status codes of requests to all domain names, and export the details of these status codes.
Whole Site Acceleration	You can query the traffic or bandwidth consumed by domain names whose service type is whole site acceleration.

Indicator	Description
Data Export	You can export statistics from different dimensions (such as domain names and accounts).

NOTE

- CDN allows you to query statistics about deleted domain names.
- If you have enabled the enterprise project function, statistics of deleted domain names cannot be queried.
- On the CDN console, there is a delay of about 1 hour for data on the **Analytics** and **Dashboard** pages.

You can also query the following information on the **Dashboard** page:

- Total traffic, peak bandwidth, number of requests, and hit ratio in the current month
- Traffic, peak bandwidth, number of requests, and hit ratio today
- Trends of today's traffic and peak bandwidth of all domain names
- Today's top 5 domain names by traffic, bandwidth, and number of requests
- Total number of added domain names
- Remaining quota in your traffic packages

FAQ

- **Why Is There No Data in Analytics?**
- **How Long Is the API Delay of the Top 100 URLs in CDN Popular Content Statistics?**
- **What Could Fall Into the "Other" Category in the Visitor Region Statistics?**

4.2 Traffic

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

- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- If no data is available within the queried time range, no data is displayed on the traffic/bandwidth and traffic hit ratio trend charts or in the domain name traffic/bandwidth utilization list.
- The minimum granularity is 5 minutes. If the query time range is 8 days or longer, the minimum granularity is 4 hours.
- The logged traffic statistics are displayed. However, the billable traffic is 10% higher than the logged statistics because TCP/IP packet headers and TCP retransmissions also consume traffic.
- There is a delay of about one hour for data displayed on the **Traffic** page.
- You can export the query results.

- You can compare data.
- You can filter domain names by tag or service type.

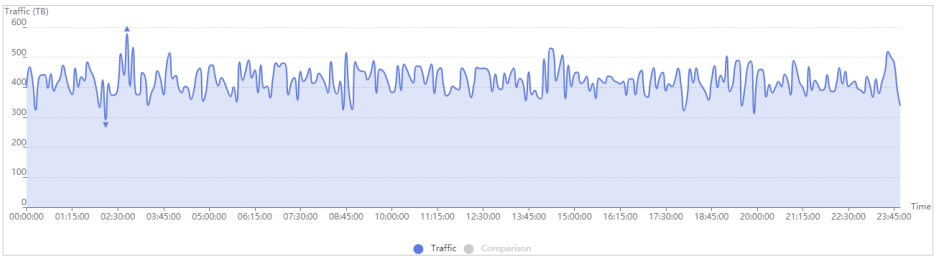
Restrictions

- If the service area of your domain name is global, you must query the statistics of this domain name by choosing Chinese mainland and **International** respectively.
- You can query the traffic hit ratio only when setting **Region** to **Chinese mainland** or **International**.

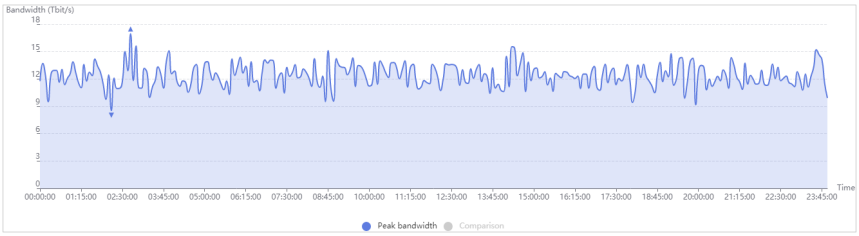
Procedure

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** > **Traffic**.
3. Set search criteria to query the following data:
   - **Traffic Monitoring**: displays the traffic of specific domain names over time. You can click legend entries, for example, Traffic, to hide or display the corresponding statistics.

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

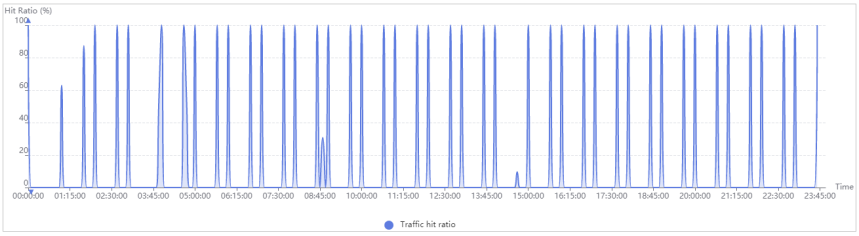
     

     NOTE

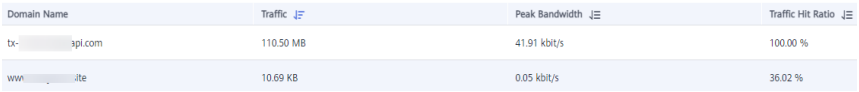
     The 95th percentile bandwidth and the average daily peak bandwidth are both shown for the same time span. If no bandwidth statistics are generated within the queried time span, the 95th percentile bandwidth line or the average daily peak bandwidth line is not displayed.
   - **Traffic Hit Ratio**: displays the traffic hit ratio of specific domain names over time.

     Traffic hit ratio = Traffic generated when the cache is hit/Total traffic of requests

Total traffic of requests is the sum of the traffic generated when the CDN PoP cache is hit and the traffic generated during origin pull.



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



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

4.3 Requests

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

- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- The access information is displayed based on the log statistics. The data is updated once an hour.
- If no data is available within the queried time range, no data is displayed on the total requests, cache hit ratio, and queries per second trend charts or in the domain name access details list.
- You can export the query results.
- The minimum granularity is 5 minutes. If the query time range is 8 days or longer, the minimum granularity is 4 hours.
- You can filter domain names by tag or service type.

Restrictions

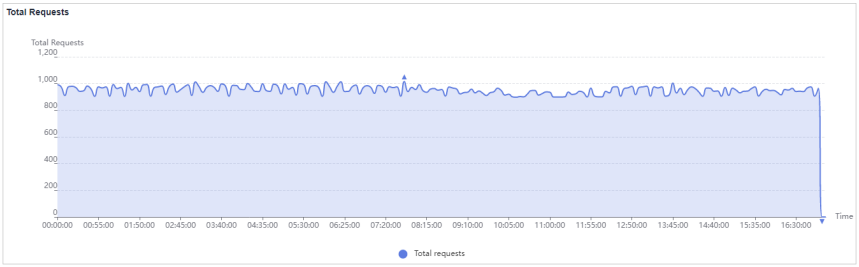
- If the service area of your domain name is global, you must query the statistics of this domain name by choosing Chinese mainland and **International** respectively.
- You can query the request hit ratio only when setting **Region** to **Chinese mainland** or **International**.

Procedure

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

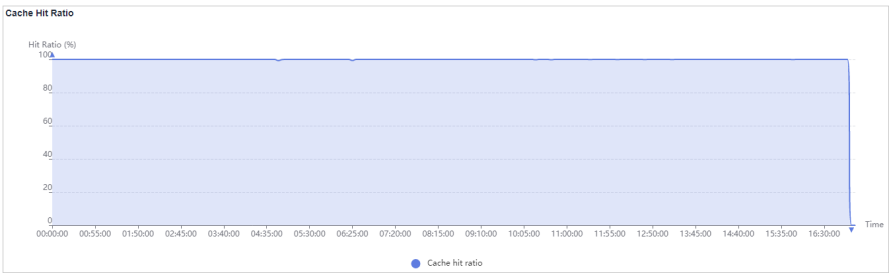
   The CDN console is displayed.
2. In the navigation pane, choose **Analytics** > **Requests**.

3. Set search criteria to query the following data:
   - **Total Requests**: displays the number of requests to specific domain names over time.

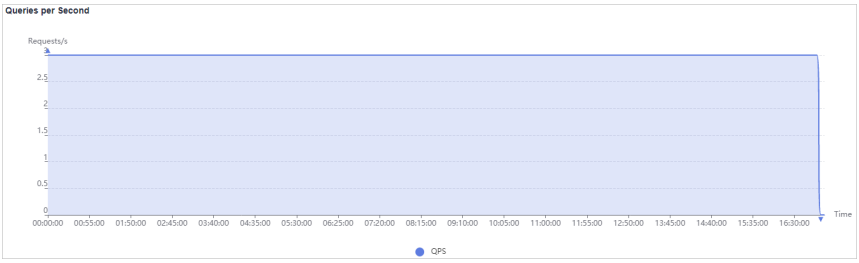
   - **Cache Hit Ratio**: displays the cache hit ratio of specific domain names over time.

     Cache hit ratio = Number of requests that hit caches/Number of total requests

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

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

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

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

Domain Name	Total Requests	Cache Hit Ratio	Queries per Second
ca ao.net	2,975,387	100.00 %	34
1.c op	1,547,309	100.00 %	18
or p	1,547,309	100.00 %	18

4.4 Origin

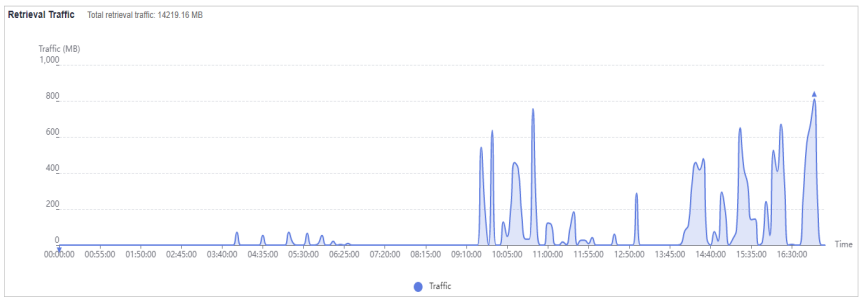
You can view the traffic, bandwidth, and failure rate of origin pulls for all your domain names (excluding those deleted if you have enabled the enterprise project function).

- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- If no data is available within the queried time range, no data is displayed on the retrieval traffic/bandwidth and retrieval failure rate trend charts or in the domain name retrieval details list.
- The minimum granularity is 5 minutes. If the query time range is 8 days or longer, the minimum granularity is 4 hours.
- You can export the query results.
- You can filter domain names by tag or service type.

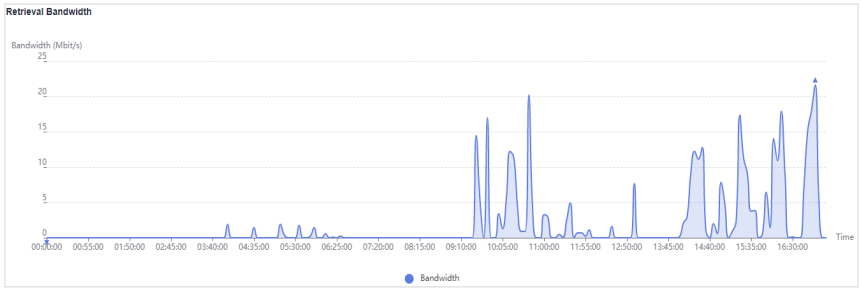
Procedure

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** > **Origin**.
3. Set search criteria to query the following data:
   - **Retrieval Traffic**: displays the origin pull traffic of specific domain names over time.

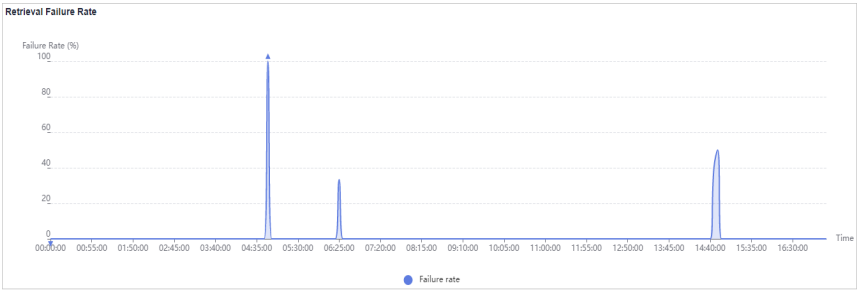
     

   - **Retrieval Bandwidth**: displays the origin pull bandwidth of specific domain names over time.

   - **Retrieval Failure Rate**: displays the origin pull failure rate over time.

     Retrieval failure rate = Number of failed origin pull requests/Number of total origin pull requests



NOTE

- Origin pull failures may be caused by host configuration errors, disconnection between CDN and the host, HTTP incompatibility, and host errors.
- If the last status code of an origin pull request is 2*xx*, 3*xx*, 404, or 416, the request is successful. Other status codes indicate that the request fails.

– **Domain Name Retrieval Details**: displays the traffic, bandwidth, and failure rates of origin pull from specific domain names.

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

4.5 Data Analysis

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 an operations report.
- A custom operations report can be valid for up to one year.
- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- The minimum statistical granularity is day.
- The statistical latency and algorithm error may cause the difference between the statistical data and the logged data. The logged data is used.
- 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.

Restrictions

If the service area of your domain name is **Global**, you must query the statistics of this domain name by choosing **Chinese mainland** and **International** respectively. Query by **Global** is not available.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Analytics** > **Data Analysis**.
3. View domain name rankings and region/carrier rankings.
   - **Domain Rankings**: displays the rankings of all domain names under your account. By default, domain names are sorted by traffic in descending order. This report is displayed by default and does not need to be customized.
   - **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**, **Chinese mainland**, **International**, or **Global**).
     - You can filter domain names by tag or network protocol.
4. On the **Operations Reports** tab, click **Customize Report**.

Figure 4-1 Customizing an operations report

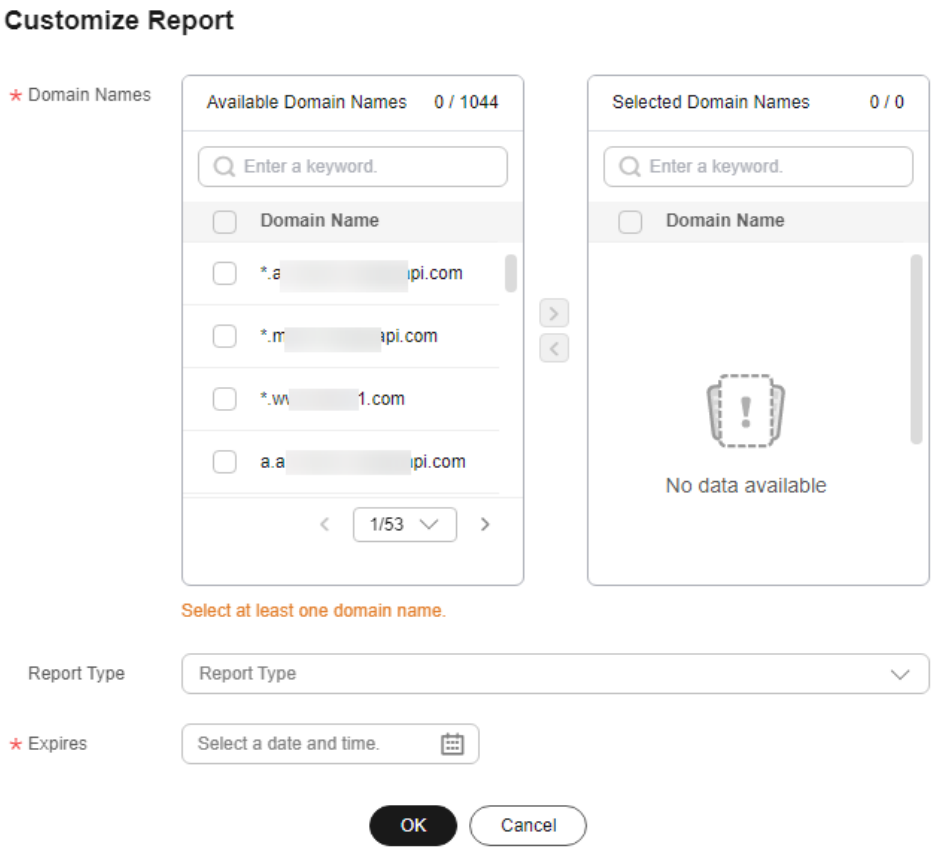


Table 4-2 Parameters

Parameter	Description
Domain Names	Select 1 to 100 domain names. • Domain names cannot be filtered by enterprise project.
Report Type	• **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
Expires	Validity period of the report. After the report expires, statistics cannot be collected.

5. Set required parameters and click **OK**.
6. On the next day, click a tab on the **Operations Reports** tab to view the corresponding data.

4.6 Regions & Carriers

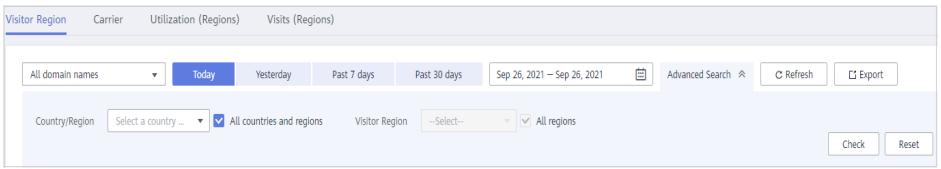
You can query the traffic/bandwidth usage, number of requests, and visitor distribution of all domain names (excluding those deleted if you have enabled the enterprise project function) by region or carrier.

- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- If no data is available within the queried time range, no data is displayed in the list of carrier index statistical details.
- The minimum granularity is 5 minutes. If the query time range is 8 days or longer, the minimum granularity is 4 hours.
- You can export the query results.
- You can filter domain names by tag, service type, or network protocol.

Procedure

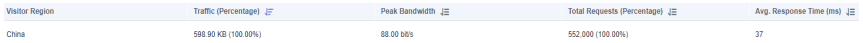
1. Log in to **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

   The CDN console is displayed.
2. In the navigation pane, choose **Analytics**.
3. Under **Analytics**, choose **Regions & Carriers**.



4. Select a tab and set search criteria to query the following data:
   - **Visitor Region**: displays the region where visitors are located.

     When **Scope** is set to **China**, you can query details about visitors in 34 provincial administrative regions in China.

     
Visitor Region	Traffic (Percentage)	Peak Bandwidth	Total Requests (Percentage)	Avg. Response Time (ms)
China	598.90 KB (100.00%)	88.00 bit/s	552,000 (100.00%)	37

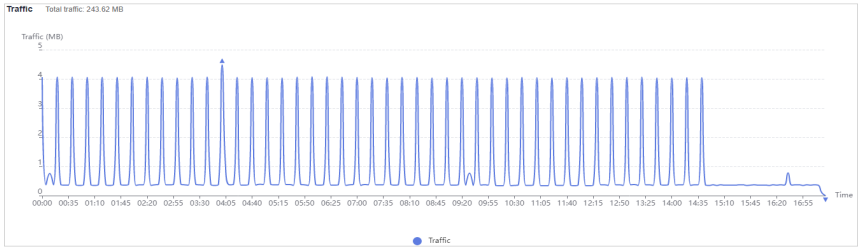
   - **Carriers**: China Mobile, China Telecom, China Unicom, China Education and Research Network (CERNET), Dr. Peng, and China Mobile Tietong
     i. **Carrier Index Distribution**: displays the proportion each carrier occupies in different index statistics.

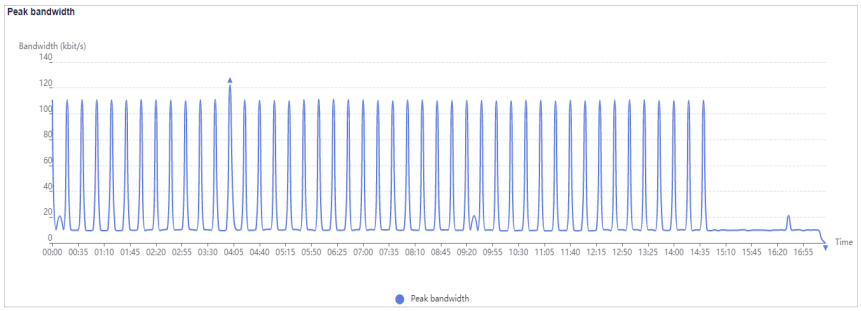
     ii. **Carrier Index Statistical Details**: displays the traffic, peak bandwidth, and number of requests by carrier. You can click **Traffic**, **Peak Bandwidth** or **Total Requests** in the table heading of **Carrier Index Statistical Details** to see the data in ascending or descending order.

     
Carrier	Traffic (Percentage)	Peak Bandwidth (Percentage)	Total Requests (Percentage)	Avg. Response Time (ms)
China Telecom	589.13 KB (100.00%)	88.00 bit/s (100.00%)	543,000 (100.00%)	37

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

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

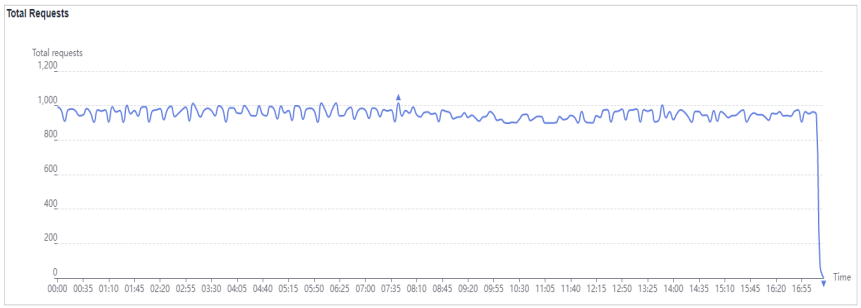


iii. **Domain Name Traffic/Bandwidth Utilization**: displays the traffic and bandwidth of specific domain names.

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

– **Visits (Regions)**

i. **Total Requests**: displays the number of requests to the domain name by region and carrier.



ii. **Domain Name Access**: displays access details about the domain name by region and carrier.

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

4.7 Status Codes

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

- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- If no data is available within the queried time range, no data is displayed in the list of status codes.
- The minimum granularity is 5 minutes. If the query time range is 8 days or longer, the minimum granularity is 4 hours.
- You can export the query results.
- You can filter domain names by tag or service type.

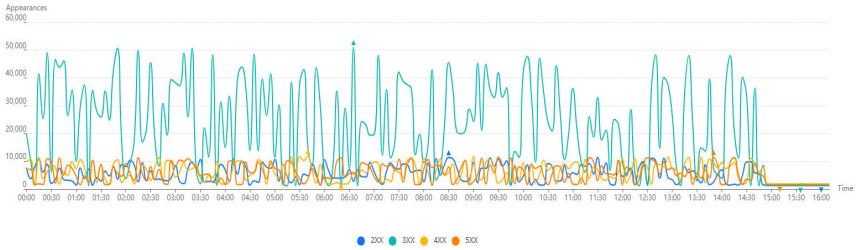
Restrictions

If the service area of your domain name is **Global**, you must query the statistics of this domain name by choosing **Chinese mainland** and **International** respectively. Query by **Global** is not available.

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** > **Status Codes**.
3. Set search criteria to query the following data:
   - **Status Codes Overview**: displays the number of each status code over time.

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

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

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

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

4.8 Whole Site Acceleration

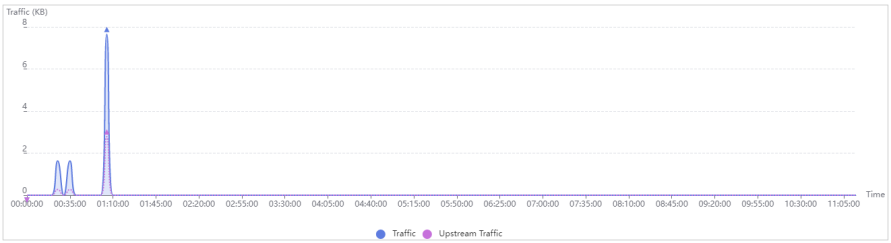
You can query traffic statistics of all domain names whose service type is whole site acceleration (excluding those deleted if you have enabled the enterprise project function).

- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- The minimum granularity is 5 minutes. If the query time range is 8 days or longer, the minimum granularity is 4 hours.
- You can filter domain names by tag or service type.

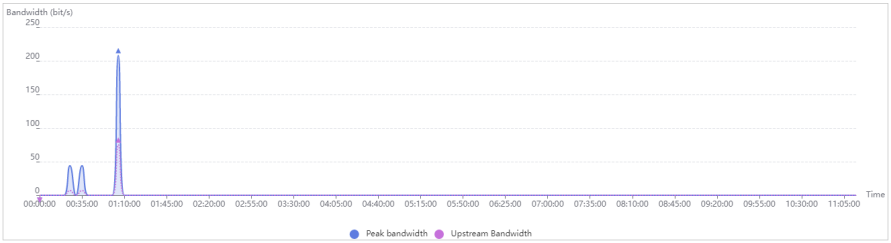
Procedure

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** > **Whole Site Acceleration**.
3. Set search criteria to query the following data:
   - **Traffic**: displays the traffic and the upstream traffic used for whole site acceleration.

   - **Bandwidth**: displays the peak bandwidth and upstream bandwidth used for whole site acceleration.

4.9 Data Export

You can export statistics from different dimensions (such as domain names and accounts).

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** > **Data Export**.
3. Click **Create Export Task** in the upper right corner.

Figure 4-2 Creating an export task

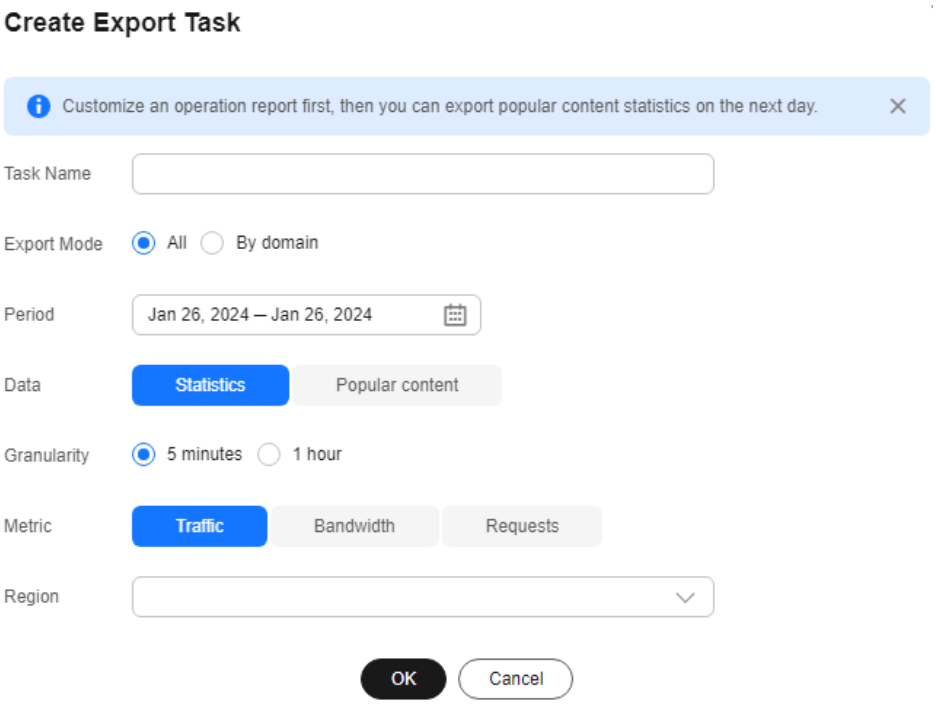


Table 4-3 Parameter description

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

Parameter	Description	Example
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 300 URLs. • After an operations report is customized, related data can be exported the next day.	Statistics
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 either **Chinese mainland** or **International**.	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.

4.10 Operations Reports

CDN provides operations reports for you to query offline statistics about domain names, analyze the domain status, and adjust operations policies properly.

Function Description

You can subscribe to reports of access area distribution, country/region distribution, carrier distribution, domain name rankings (sorted by traffic), popular URLs (sorted by traffic), and popular URLs (sorted by number of requests). Then you will receive reports in the specified email after they are generated.

Table 4-4 Reports

Report	Description
Access area distribution	Distribution of visitors to a domain name in the Chinese mainland in a specific period. **NOTE** Data is available only for domain names whose service area includes the Chinese mainland.
Country distribution	Country/Region distribution of device visitors of a domain name in a specific period.
Carrier distribution	Distribution of carriers used by device visitors of a domain name in a specific period.
Domain name rankings (by traffic)	Domain names sorted by traffic generated on CDN PoPs.
Popular URLs (by traffic)	Popular URLs sorted by traffic.
Popular URLs (by number of requests)	Popular URLs sorted by the number of requests.

Precautions

- This function is in OBT. You can create up to five subscriptions.
- Up to 100 domain names can be selected for each subscription.

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** > **Operations Reports**.
3. Click **Create** in the upper right corner.

Figure 4-3 Creating a subscription task

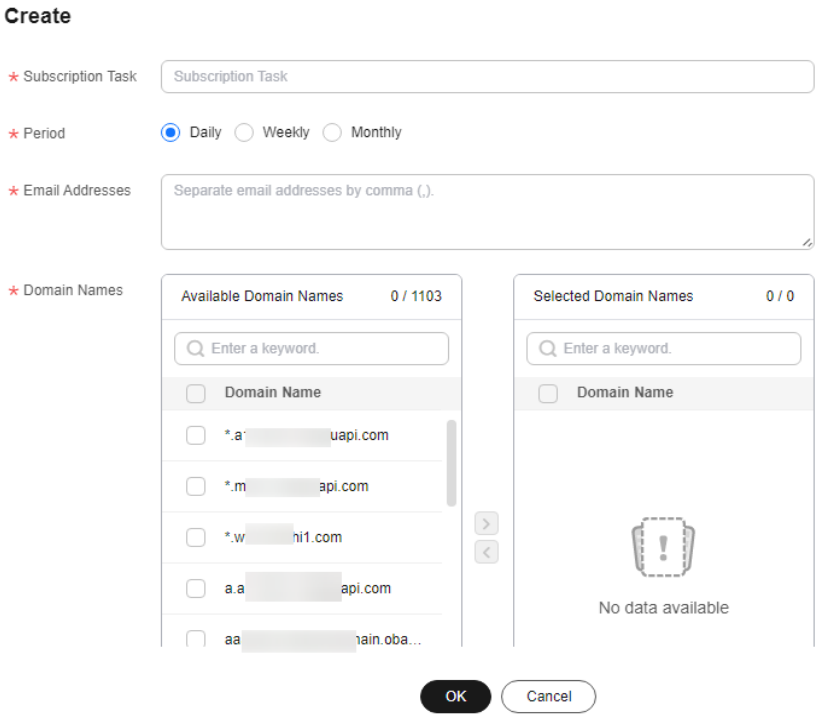


Table 4-5 Parameters

Parameter	Description
Subscription Task	Name of a subscription task. • Enter letters and hyphens (-). • Enter up to 32 characters.
Period	Period for subscribing to the report. Select **Daily**, **Weekly**, or **Monthly**. • **Daily**: The report of the previous day is sent to the specified email address in the afternoon of the second day. • **Weekly**: The report of the previous week is sent to the specified email address on Monday afternoon of the next week. • **Monthly**: The report of the previous month is sent to the specified email address in the afternoon of the first day of the next month.
Email Addresses	Email addresses for receiving operations reports. • Separate email addresses by comma (,). • Email addresses must be unique.

Parameter	Description
Domain Names	Domain names whose statistics are collected. • Domain names cannot be filtered by enterprise project.
Report Type	Select the type of the report to be subscribed to. For details, see **Table 4-4**. **NOTE** To subscribe to the popular URL report, **customize a report** first.

4. Click **OK** to complete report subscription.

4.11 Cloud Eye Monitoring

Scenario

You can interconnect CDN with Cloud Eye to monitor CDN metrics, such as traffic, bandwidth, and traffic hit ratio. CDN reports domain data to Cloud Eye in real time. You can also set alarm rules. When the value of a metric exceeds the alarm threshold, an alarm is generated. This helps you learn about the business status in real time and prevent risks in a timely manner.

Precautions

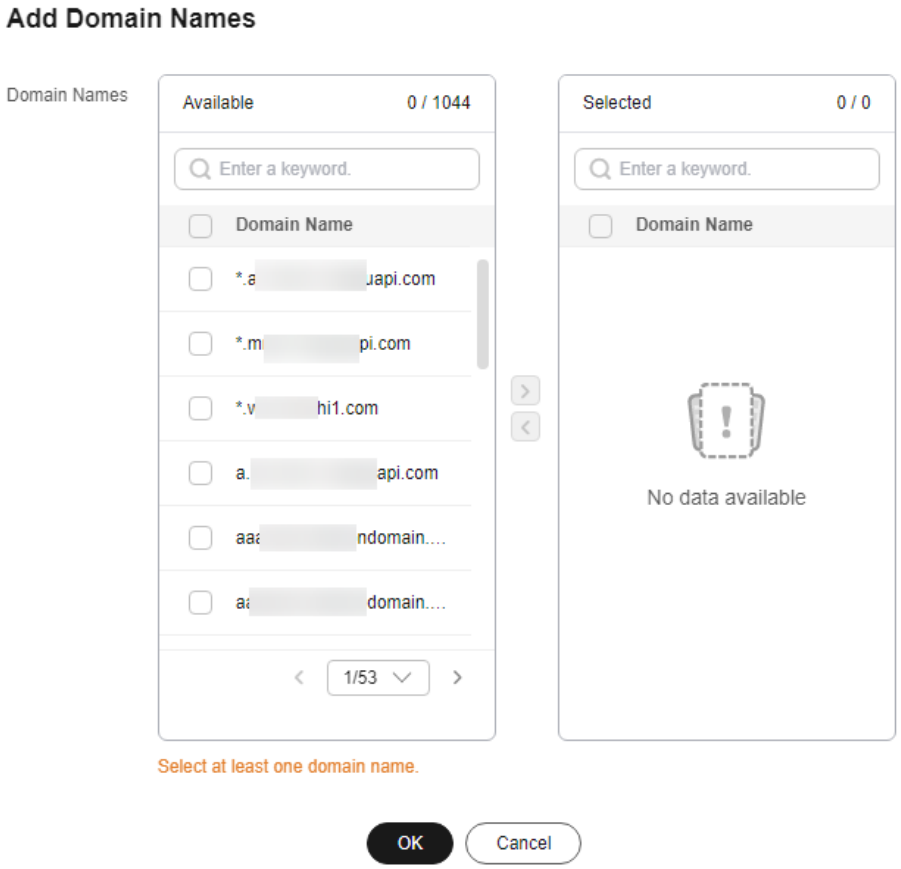
- You can add up to 100 domain names.
- Domain names with special configurations are not supported.
- The data reporting latency is about 4 minutes.
- Data is reported to Cloud Eye in the CN North-Beijing4 region.
- Cloud Eye monitoring is free of charge on CDN. If you configure alarms on Cloud Eye, Simple Message Notification (SMN) will charge you for alarm notifications sent to you. For details about SMN pricing, see **SMN Pricing Details**.

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** > **Cloud Eye Monitoring**.
3. Click **Add Domain Names**, select the domain names to be added, and add them to the **Selected** area.

Figure 4-4 Adding domain names



4. Click **OK**.

Stopping Monitoring

To stop reporting metrics of domain names, remove them from the **Cloud Eye Monitoring** page.

- Click **Delete** in the **Operation** column of a domain name.
- Select multiple domain names and click **Delete** above the domain name list. However, you cannot remove all domain names.
- To stop data reporting for all domain names, turn off the **Cloud Eye Monitoring** switch.

4.12 FAQ

Why There Is No Data in Analytics?

- The CNAME record configured for your domain name is wrong.
- CDN statistics on the **Analytics** page are one hour later than real-time data.

If the problem is not caused by either of the preceding reasons, **submit a service ticket**.

What Could Fall Into the "Other" Category in the Visitor Region Statistics?

Other refers to those whose region cannot be identified because their IP addresses are not recorded in the IP address library or their IP addresses cannot be obtained by CDN.

How Long Is the API Delay of the Top 100 URLs?

Calling the API of top 100 URLs has a delay of about 6 hours. This situation returns to normal at 12:00 on the next day.

What Are the Meanings of HEAD, HIT, and MISS in CDN Logs?

- **HEAD**

  The HEAD method is the same as the GET method except that the server does not return the HEAD message body. In a response to a HEAD request, the metadata contained in the HTTP header is the same as that in a response to a GET request. HEAD can be used to obtain the hidden metadata in a request, instead of transmitting the entity itself. It is also often used to test the validity, availability, and recent changes of hyperlinks.

- **HIT**

  This indicates a cache hit. A PoP directly serves the content.

- **MISS**

  This indicates a cache miss. A PoP needs to pull content from the origin server.

How Long of Data Can Be Queried?

You can query CDN data over the past 90 days. The maximum query time range is 31 days.

Why Is the Message "Fine-grained Authentication Failed" Returned When I Call an API to Download CDN Logs?

It is possible that the enterprise project is not found. You can add **enterprise_project_id=ALL** to the request path.

Example:

```
GET https://cdn.myhuaweicloud.com/v1.0/cdn/logs?
query_date=1502380500000&domain_name=www.example.com&page_size=10&page_number=1&enterprise_project_id=ALL
```

What Does User-Agent OkHttp in CDN Logs Mean?

OkHttp is a request protocol used by the Android network framework to process network requests.

5 Analytics (New)

5.1 Service Monitoring

5.1.1 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.

Restrictions

- If the service area of your domain name is **Global**, you must query the statistics of this domain name by choosing **Chinese mainland** and **International** respectively. Query by **Global** is not available.
- You can query the traffic hit ratio only when setting **Region** to **Chinese mainland** or **International**.

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.

   - **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 5-1 Data trend charts

5.1.2 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).

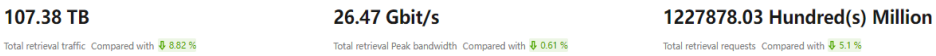
Precautions

- 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.

   - **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 5-2 Data trend charts

5.1.3 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 span 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.

Procedure

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

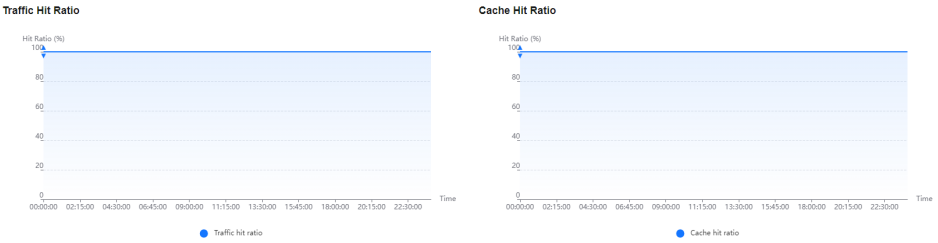
   The CDN console is displayed.
2. In the navigation pane, choose **Analytics (New)** > **Service Monitoring**.
3. Click the **Hit Ratios** tab and set search criteria. You can query the following data:

   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 5-3 Hit ratio statistics



5.1.4 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.

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 5-1**.
   - **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 view the number of status codes of each domain name.

Figure 5-4 Status code statistics

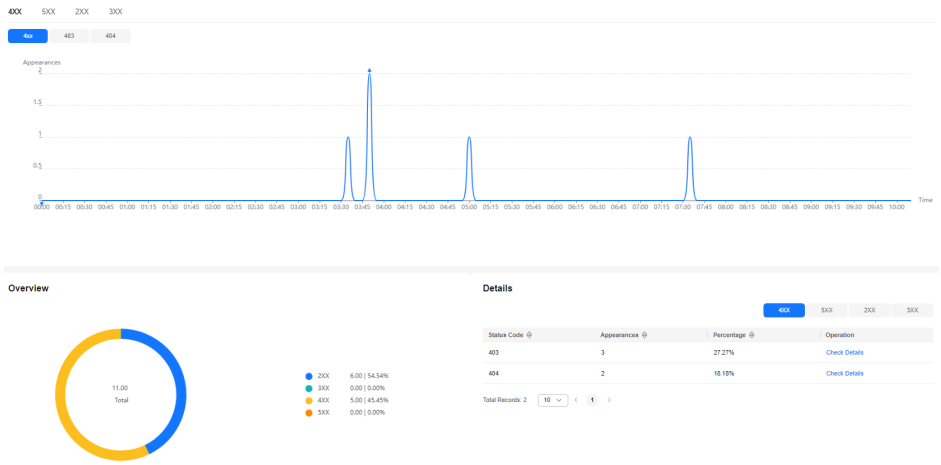


Table 5-1 Status code description

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.

5.1.5 Cloud Eye Monitoring

Scenario

You can interconnect CDN with Cloud Eye to monitor CDN metrics, such as traffic, bandwidth, and traffic hit ratio. CDN reports domain data to Cloud Eye in real time. You can also set alarm rules. When the value of a metric exceeds the alarm threshold, an alarm is generated. This helps you learn about the business status in real time and prevent risks in a timely manner.

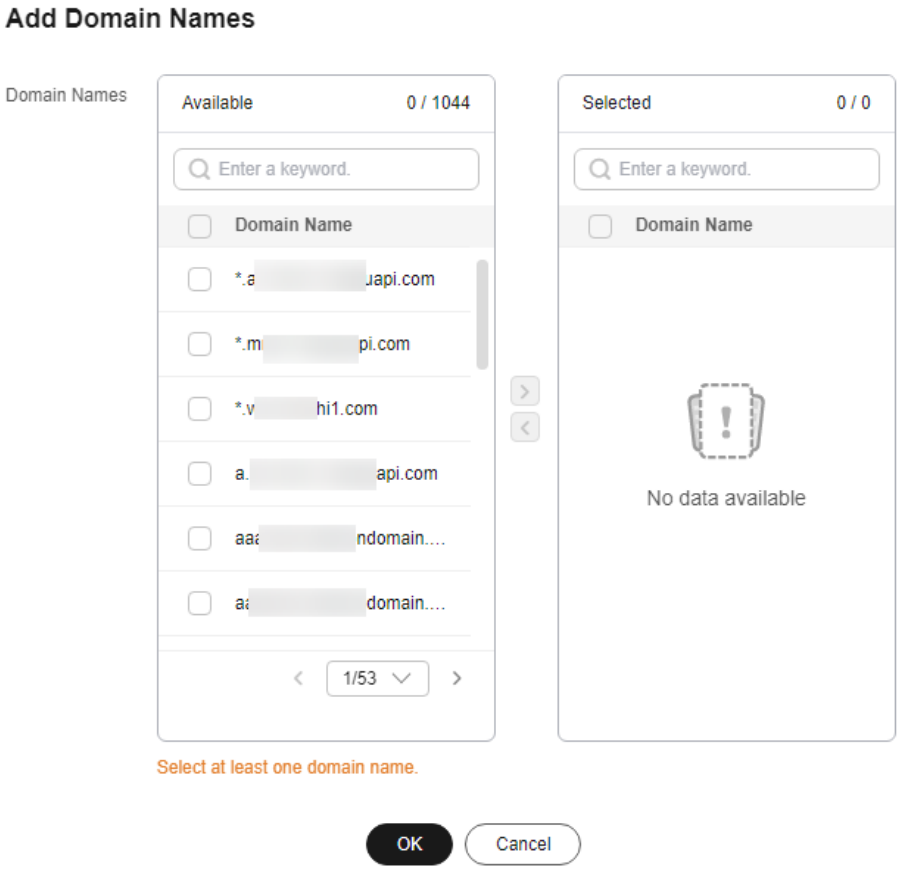
Precautions

- You can add up to 100 domain names.
- Domain names with special configurations are not supported.
- The data reporting latency is about 4 minutes.
- Data is reported to Cloud Eye in the CN North-Beijing4 region.
- Cloud Eye monitoring is free of charge on CDN. If you configure alarms on Cloud Eye, SMN will charge you for alarm notifications sent to you. For details about SMN pricing, see **SMN Pricing Details**.

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 **Cloud Eye Monitoring** tab and turn on the switch.

   Figure 5-5 Adding domain names



4. Add the domain names whose data needs to be reported and click **OK**.

Stopping Monitoring

To stop reporting metrics of domain names, remove them from the **Cloud Eye Monitoring** page.

- Click **Delete** in the **Operation** column of a domain name.
- Select multiple domain names and click **Delete** above the domain name list. However, you cannot remove all domain names.
- To stop data reporting for all domain names, turn off the **Cloud Eye Monitoring** switch.

5.2 Data Analysis

5.2.1 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. By default, CDN provides domain name rankings and region/carrier rankings.
   - **Domain Rankings**: displays the rankings of all domain names under your account. By default, domain names are sorted by traffic in descending order. 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**, **Chinese mainland**, **International**, or **Global**).
     - You can filter statistics by tag or network protocol.
     - Data of the past 90 days can be queried, and each query can include data of up to 31 days.
4. To customize an operations report, click **Customize Report**.

Figure 5-6 Customizing an operations report

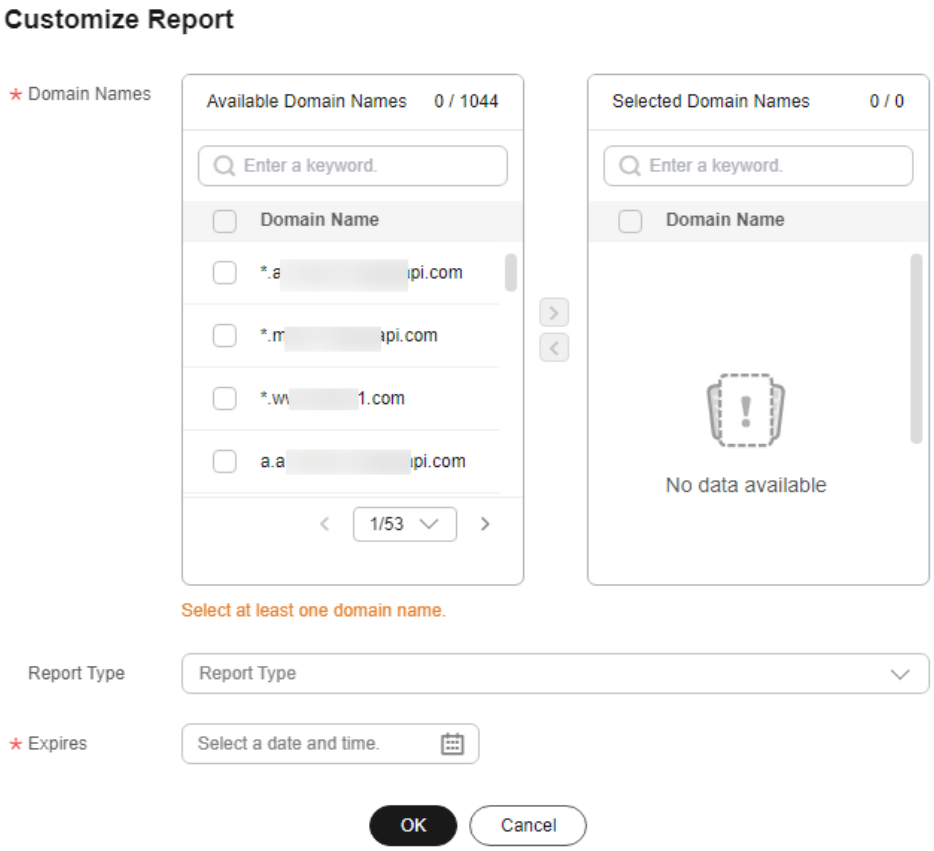


Table 5-2 Parameters

Parameter	Description
Domain Names	Select 1 to 100 domain names. • Domain names cannot be filtered by enterprise project.
Report Type	• **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
Expires	Validity period of the report. After the report expires, statistics cannot be collected.

5. Set required parameters and click **OK**.
6. On the next day, click a tab on the **Operations Reports** tab to view the corresponding data.

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.

5.2.2 Report Subscription

CDN provides operations reports for you to query offline statistics about domain names, analyze the domain status, and adjust operations policies properly.

Function Description

You can subscribe to reports of access area distribution, country/region distribution, carrier distribution, domain name rankings (sorted by traffic), popular URLs (sorted by traffic), and popular URLs (sorted by number of requests). Then you will receive reports in the specified email after they are generated.

Table 5-3 Reports

Report	Description
Access area distribution	Distribution of visitors to a domain name in the Chinese mainland in a specific period. **NOTE** Data is available only for domain names whose service area includes the Chinese mainland.
Country distribution	Country/Region distribution of device visitors of a domain name in a specific period.
Carrier distribution	Distribution of carriers used by device visitors of a domain name in a specific period.
Domain name rankings (by traffic)	Domain names sorted by traffic generated on CDN PoPs.
Popular URLs (by traffic)	Popular URLs sorted by traffic.
Popular URLs (by number of requests)	Popular URLs sorted by the number of requests.

Precautions

- This function is in OBT. You can create up to five subscriptions.
- Up to 100 domain names can be selected for each subscription.

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. On the **Subscriptions** tab, click **Create**.

Figure 5-7 Creating a subscription task

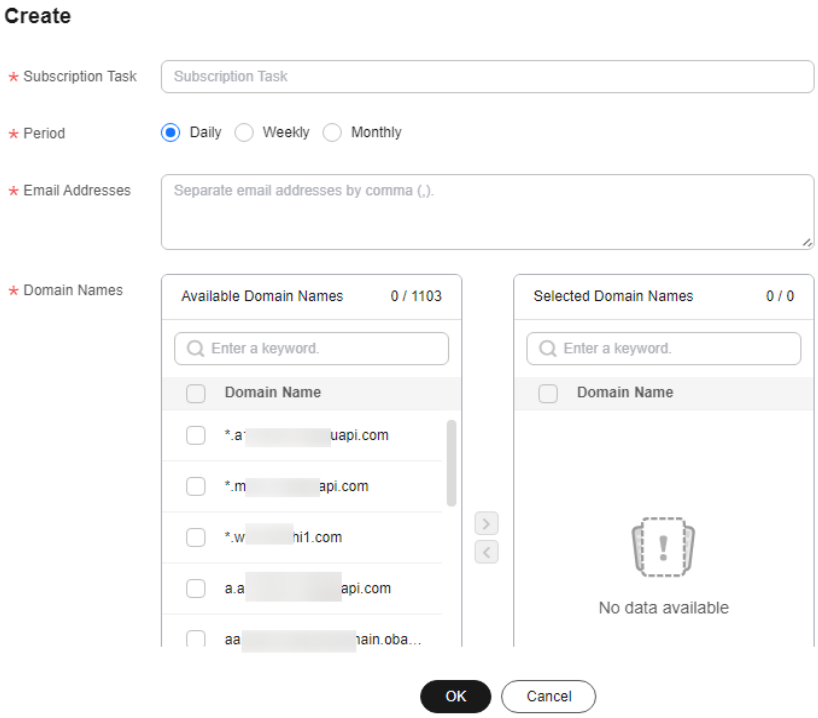


Table 5-4 Parameters

Parameter	Description
Subscription Task	Name of a subscription task. • Enter letters and hyphens (-). • Enter up to 32 characters.
Period	Period for subscribing to the report. Select **Daily**, **Weekly**, or **Monthly**. • **Daily**: The report of the previous day is sent to the specified email address in the afternoon of the second day. • **Weekly**: The report of the previous week is sent to the specified email address on Monday afternoon of the next week. • **Monthly**: The report of the previous month is sent to the specified email address in the afternoon of the first day of the next month.
Email Addresses	Email addresses for receiving operations reports. • Separate email addresses by comma (,). • Email addresses must be unique.

Parameter	Description
Domain Names	Domain names whose statistics are collected. • Domain names cannot be filtered by enterprise project.
Report Type	Select the type of the report to be subscribed to. For details about the default report types, see **Table 5-2**. **NOTE** To subscribe to popular URL, user agent, and referer reports, **customize operations reports** first.

4. Click **OK** to complete report subscription.

Exporting Reports

You can export reports in all subscription tasks. Click **Export** on the **Subscriptions** tab to export reports in XLSX format.

5.3 Traffic Query

5.3.1 Query

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

Restrictions

If the service area of your domain name is **Global**, you must query the statistics of this domain name by choosing **Chinese mainland** and **International** respectively. Query by **Global** is not available.

Precautions

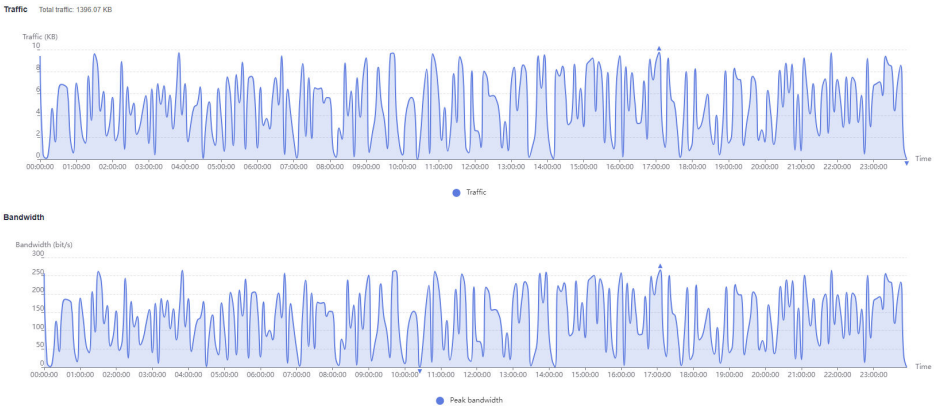
- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- If no data is available for the queried domain name within the specified time span, no data is displayed in the traffic or bandwidth trend chart.
- The minimum granularity is 5 minutes. If the query time range 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 5-8 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.

5.3.2 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.
- By default, statistics about domain names are displayed by region (Chinese mainland and outside the Chinese mainland).

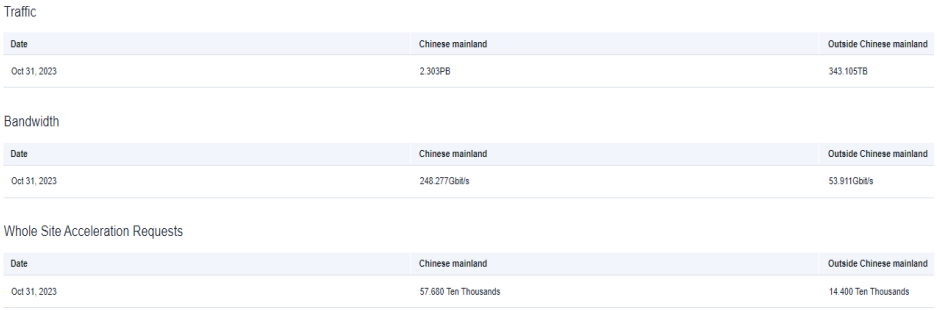
Procedure

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.

Figure 5-9 Summary



5.3.3 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).

Restrictions

- If the service area of your domain name is **Global**, you must query the statistics of this domain name by choosing **Chinese mainland** and **International** respectively. Query by **Global** is not available.
- 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 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 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 **Whole Site Acceleration** tab and set the search criteria. You can query 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 5-10 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.

5.4 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 5-11 Creating an export task

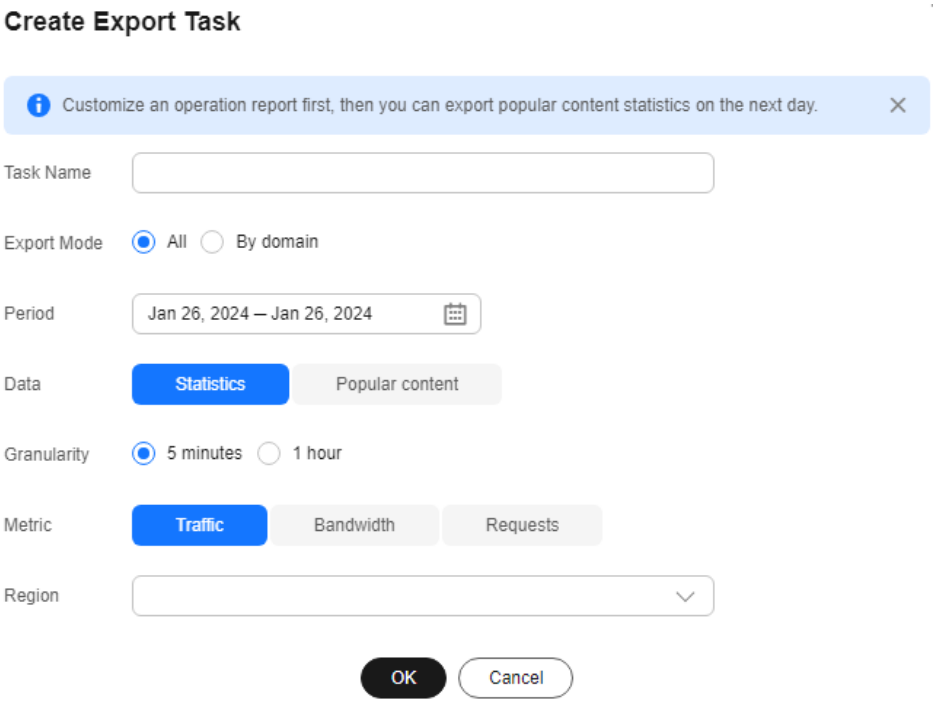


Table 5-5 Parameter description

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

Parameter	Description	Example
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. • After an operations report is customized, related data can be exported the next day.	Statistics
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 either **Chinese mainland** or **International**.	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.

6 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.

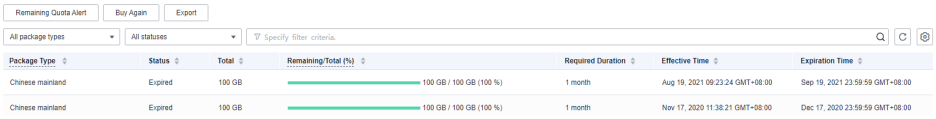
Procedure

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 6-1 Managing resource packages

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

7 Log Management

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

Log Description

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

The log naming rules are as follows: *Start time of the query period-Domain name-Service area*.gz. For the service area, **cn** indicates the Chinese mainland, and **ov** indicates outside the Chinese mainland. So a typical log name might be, **2018021123-www.example01.com-ov.gz**.

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

Example of log file content

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

Table 7-1 describes each field (from left to right) in the log.

Table 7-1 Description of a CDN log file

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

No.	Field Description	Example
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's version information	Mozilla/5.0 (Linux; U; Android 6.0; en-us; EVA-AL10 Build/HUAWEIEVA-AL10) AppleWebKit/533.1 (KHTML, like Gecko) Mobile Safari/533.1
13	Range information. It specifies the positions of the first and last bytes for the data to be returned. **bytes** can be expressed by the following three methods: • 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 (available from late May 2024), that is, the IP address used by the CDN server to send responses	x.x.x.x

Downloading Logs

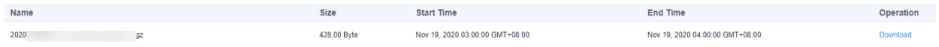
1. Log in to **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

   The CDN console is displayed.

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

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

Figure 7-1 Log management



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

8 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 **Cloud Certificate Manager (CCM)**.

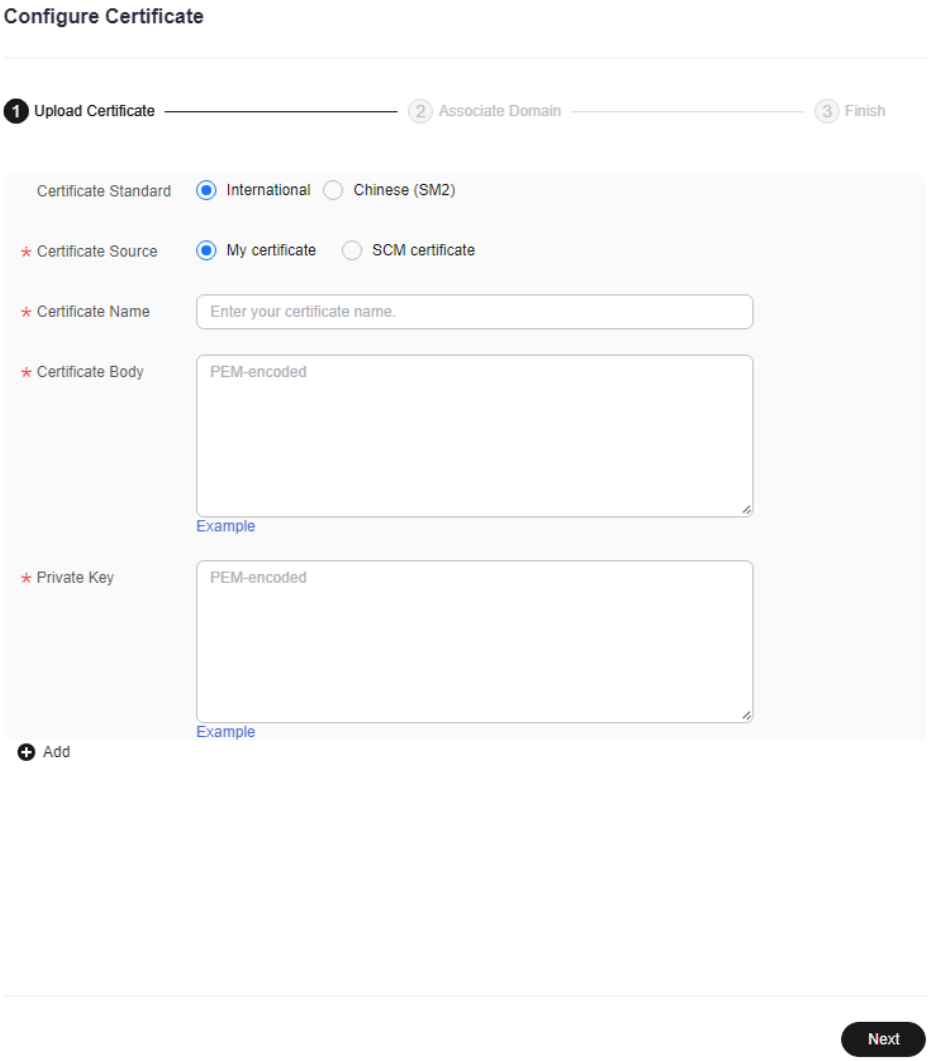
Configuring a Certificate

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 8-1 Configuring a certificate



4. Set related parameters.

Table 8-1 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.

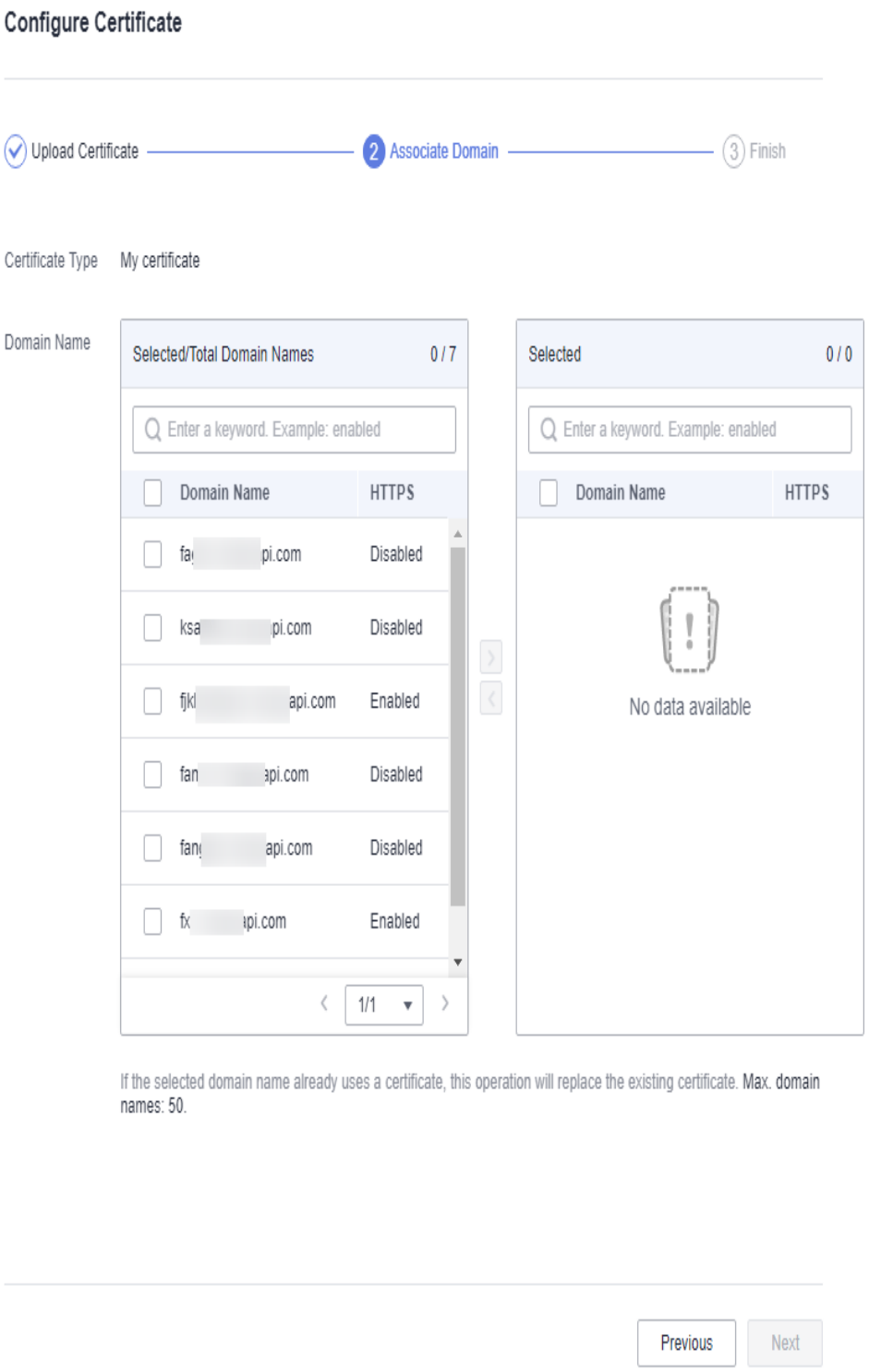
Parameter	Description
Certificate Body	• If you select **My certificate**, use a local text editor to open the certificate and copy the certificate content to the text box. For details about the certificate format, see **HTTPS Certificate Requirements**. • If you select **SCM certificate**, the content 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.

Table 8-2 Parameters of a Chinese SM series cryptographic certificate

Parameter	Description
Certificate Standard	Chinese (SM2)
Certificate Source	Either **My certificate** or **SCM certificate**
Certificate Name	• If you select **My certificate**, enter the certificate name containing 3 to 64 characters. • 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.
Signature Certificate	Open the PEM file in the signature certificate to be uploaded as a text file and copy the certificate content in the file to this text box. Note that you need to upload a combined certificate file that contains both the server certificate content and certificate chain content into this field. The content of the certificate chain should be pasted right below the content of the server certificate.

Parameter	Description
Signature Private Key	Open the KEY file in the signature certificate to be uploaded as a text file and copy the private key in the file to this text box.
Encryption Certificate	Open the PEM file in the encryption certificate to be uploaded as a text file and copy the certificate content in the file to this text box. You do not need to upload the certificate chain here.
Encryption Private Key	Open the KEY file in the encryption certificate to be uploaded as a text file and copy the private key in the file to this text box.

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



6. Select the domain names to be associated on the left 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.

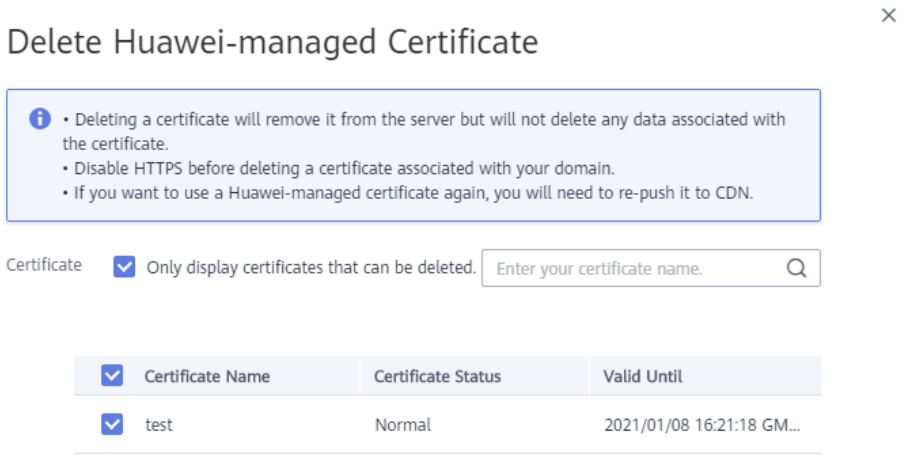
7. Click **Finish** to implement HTTPS secure acceleration for the associated domain names.

Deleting a Managed Certificate

- Deleting a certificate will remove it from the server but will not delete any data associated with the certificate.
- Disable HTTPS before deleting a certificate associated with your domain name.
- To use the certificate again, re-push it from SCM to CDN.

Procedure

1. Click **Delete Huawei-managed Certificate** in the upper left corner.
2. On the displayed page, select the certificate to be deleted and click **OK**.



3. In the displayed dialog box, click **OK**.

NOTE

To use the certificate again, re-push it from SCM to CDN.

9 Checking PoP IP Addresses

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.

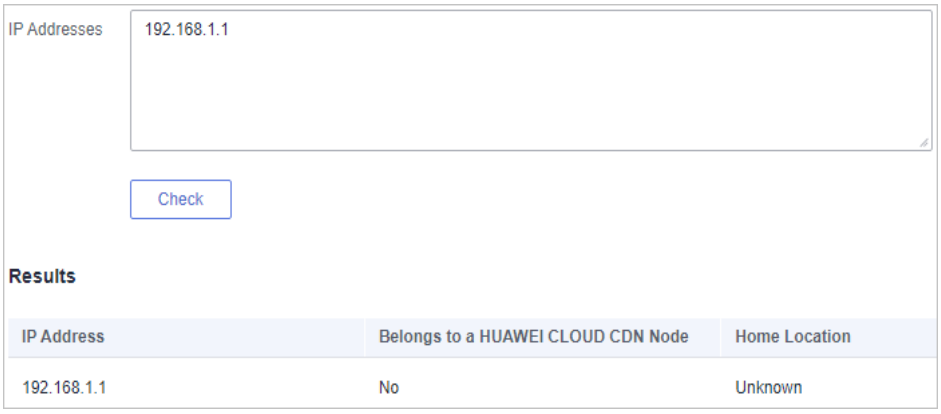
- If the check result shows that the IP address is not that of a Huawei Cloud CDN PoP, the problem may lie in the carrier network. In this case, contact your carrier.
- If the IP address belongs to a Huawei Cloud CDN PoP, rectify the fault by referring to **Troubleshooting**.

Procedure

1. Log in to the **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.



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.

10 Permissions Management

10.1 Creating a User and Granting CDN Permissions

This chapter describes how to use **IAM** 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 in Huawei Cloud to perform professional and efficient O&M on your CDN resources.

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

This section describes the procedure for granting permissions.

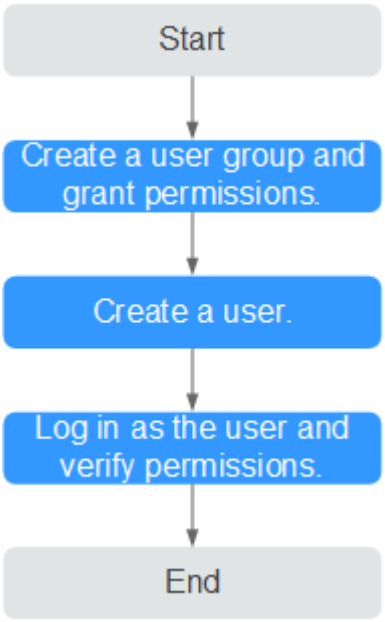
Prerequisites

Learn about the permissions (see **Permissions Management**.) supported by CDN and choose policies or roles according to your requirements. For the system policies of other services, see **System Permissions**.

Process Flow

Figure 10-1 shows the process of granting CDN permissions.

Figure 10-1 Process of granting CDN permissions



1. **Create a user group and assign permissions**.

   Create a user group on the IAM console, and assign the **CDN DomainReadOnlyAccess** policy to the group.

2. **Create an IAM user and add it to the user group**.

   Create a user on the IAM console and add the user to the group created in 1.

3. **Log in as the IAM user** and verify permissions.

   Log in to the CDN console as the created user, and verify that it only has read permissions for CDN domain names.

   - Enable or disable an acceleration domain name. If a message appears indicating that you have insufficient permissions to perform the operation, the **CDN DomainReadOnlyAccess** policy has already taken effect.

   - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **CDN DomainReadOnlyAccess** policy has already taken effect.

10.2 Creating a Custom Policy

Custom policies can be created to supplement the system-defined policies of CDN. For the actions that can be added to custom policies, see **Permissions Policies and Supported Actions**.

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.

For details, see **Creating a Custom 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"
          }
      ]
  }
  ```

- Example 4: Defining permissions for multiple services in a policy

  A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:


```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "cdn:configuration:enableDomains",
            "cdn:configuration:createDomains",
            "scm:cert:get",
            "scm:certProduct:get",
            "scm:certType:get"
         ]
      }
   ]
}
```


11 Enterprise Projects

Huawei Cloud 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. For details, see **Creating an Enterprise Project**.
2. After an enterprise project is created, you can migrate your domain name resources to a specified enterprise project. For details, see **Cloud Services Supported by EPS**.

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.

Enterprise Project Authorization

After an enterprise project is created and CDN resources are migrated to the enterprise project, you can add existing user groups and set user group permission policies for the enterprise project based on site requirements. Without these policies, user group members will be unable to access or operate the CDN domain resources in the enterprise project. For details about how to set user group permission policies, see **Permissions Management**.

12 Auditing

Cloud Trace Service (CTS) records operations on cloud resources in your account. You can use the logs to perform security analysis, track resource changes, audit compliance, and locate faults.

Enabling CTS

A tracker will be automatically created after CTS is enabled. All traces recorded by CTS are associated with a tracker. Currently, only one tracker can be created for each account.

For details about how to enable the cloud audit service, see **Enabling CTS**.

CDN Operations Recorded by CTS

Table 12-1 CDN operations that can be recorded by CTS

Operation	Description
createDomain	Creating a domain name

Operation	Description
updateDomain	Updating a domain name Configuring range requests Configuring redirect from origin Configuring an IP ACL Configuring the host header Configuring the origin server Configuring OBS private bucket access Configuring an HTTPS certificate Configuring cache rules Configuring HTTP headers Configuring domain names in a batch Configuring HTTPS for domain names in a batch Creating a resource tag Deleting a resource tag
deleteDomain	Removing a domain name
enableDomain	Enabling domain names
disableDomain	Disabling domain names
updateOrigin	Configuring an origin server
updateOriginHost	Configuring a host header
createRefer	Creating a referer rule
createCertificate	Configuring a domain certificate
createCacheRule	Creating a cache rule
createRefreshTask	Creating a cache purge task
createPreheatingTask	Creating a cache prefetch task

Viewing CTS Traces

After you enable CTS, the system starts to record CDN operations. You can view operations of the past seven days on the CTS console. For details, see **Querying Real-Time Traces**.

Disabling CTS

You can disable trackers on the CTS console. After a tracker is disabled, the system will stop recording operations, but you can still view historical records. For details about how to disable a tracker, see **Disabling or Enabling a Tracker**.

13 Monitoring

13.1 CDN Metrics

After CDN monitoring metrics are reported to Cloud Eye, you can view the data on the Cloud Eye console in real time. This section describes the metrics reported to Cloud Eye.

Namespace

SYS.CDN

Monitoring Metrics Supported by CDN

Table 13-1 CDN metrics that can be monitored

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
bw	Bandwidth	Average bandwidth of a domain name within one minute (Traffic within one minute x 8/60)	bit/s	1,000	1 minute
flux	Traffic	Total traffic of a domain name within one minute	Byte	1,024	1 minute

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
bs_bw	Origin pull bandwidth	Average origin pull bandwidth of a domain name within one minute (Origin pull traffic within one minute x 8/60)	bit/s	1,000	1 minute
bs_flux	Origin pull traffic	Total origin pull traffic of a domain name within one minute	Byte	1,024	1 minute
bs_num	Origin pulls	Number of origin pulls of a domain name within one minute	Count	-	1 minute
bs_fail_num	Failed origin pulls	Number of failed origin pulls of a domain name within one minute	Count	-	1 minute
bs_fail_rate	Origin pull failure rate	Percentage of failed origin pulls of a domain name within one minute (Number of failed origin pulls/Total number of origin pulls x 100)	%	-	1 minute
req_num	Requests	Number of requests of a domain name within one minute	Count	-	1 minute
hit_flux	Hit traffic	Traffic generated when requests to a domain name hit the cache within one minute	Byte	1,024	1 minute

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
hit_flux_rate	Traffic hit ratio	Percentage of hit traffic of a domain name within one minute (Hit traffic/Traffic x 100)	%	-	1 minute
http_code_2xx	Status codes 2*xx*	Total appearances of HTTP status codes 2*xx* returned for a domain name within one minute	Count	-	1 minute
http_code_3xx	Status codes 3*xx*	Total appearances of HTTP status codes 3*xx* returned for a domain name within one minute	Count	-	1 minute
http_code_4xx	Status codes 4*xx*	Total appearances of HTTP status codes 4*xx* returned for a domain name within one minute	Count	-	1 minute
http_code_5xx	Status codes 5*xx*	Total appearances of HTTP status codes 5*xx* returned for a domain name within one minute	Count	-	1 minute
http_code_2xx_rate	Percentage of status codes 2*xx*	Percentage of HTTP status codes 2*xx* returned for a domain name within one minute (Appearances of status codes 2*xx*/ Total number of requests x 100)	%	-	1 minute

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
http_code_3xx_rate	Percentage of status codes 3*xx*	Percentage of HTTP status codes 3*xx* returned for a domain name within one minute (Appearances of status codes 3*xx*/ Total number of requests x 100)	%	-	1 minute
http_code_4xx_rate	Percentage of status codes 4*xx*	Percentage of HTTP status codes 4*xx* returned for a domain name within one minute (Appearances of status codes 4*xx*/ Total number of requests x 100)	%	-	1 minute
http_code_5xx_rate	Percentage of status codes 5*xx*	Percentage of HTTP status codes 5*xx* returned for a domain name within one minute (Appearances of status codes 5*xx*/ Total number of requests x 100)	%	-	1 minute
bs_http_code_2xx	Origin status codes 2*xx*	Total appearances of origin HTTP status codes 2*xx* returned for a domain name within one minute	count	-	1 minute
bs_http_code_3xx	Origin status codes 3*xx*	Total appearances of origin HTTP status codes 3*xx* returned for a domain name within one minute	count	-	1 minute

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
bs_http_code_4xx	Origin status codes 4*xx*	Total appearances of origin HTTP status codes 4*xx* returned for a domain name within one minute	count	-	1 minute
bs_http_code_5xx	Origin status codes 5*xx*	Total appearances of origin HTTP status codes 5*xx* returned for a domain name within one minute	count	-	1 minute
bs_http_code_2xx_rate	Percentage of origin status codes 2*xx*	Percentage of origin HTTP status codes 2xx returned for a domain name within one minute (Appearances of origin status codes 2*xx*/Total number of origin pull requests x 100)	%	-	1 minute
bs_http_code_3xx_rate	Percentage of origin status codes 3*xx*	Percentage of origin HTTP status codes 3*xx* returned for a domain name within one minute (Appearances of origin status codes 3*xx*/Total number of origin pull requests x 100)	%	-	1 minute

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
bs_http_code_4xx_rate	Percentage of origin status codes 4*xx*	Percentage of origin HTTP status codes 4*xx* returned for a domain name within one minute (Appearances of origin status codes 4*xx*/Total number of origin pull requests x 100)	%	-	1 minute
bs_http_code_5xx_rate	Percentage of origin status codes 5*xx*	Percentage of origin HTTP status codes 5*xx* returned for a domain name within one minute (Appearances of origin status codes 5*xx*/Total number of origin pull requests x 100)	%	-	1 minute
http_code_400	Status code 400	Total appearances of HTTP status code 400 returned for a domain name within one minute	count	-	1 minute
http_code_403	Status code 403	Total appearances of HTTP status code 403 returned for a domain name within one minute	count	-	1 minute
http_code_404	Status code 404	Total appearances of HTTP status code 404 returned for a domain name within one minute	count	-	1 minute

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
http_code_416	Status code 416	Total appearances of HTTP status code 416 returned for a domain name within one minute	count	-	1 minute
http_code_499	Status code 499	Total appearances of HTTP status code 499 returned for a domain name within one minute	count	-	1 minute
http_code_500	Status code 500	Total appearances of HTTP status code 500 returned for a domain name within one minute	count	-	1 minute
http_code_502	Status code 502	Total appearances of HTTP status code 502 returned for a domain name within one minute	count	-	1 minute
http_code_503	Status code 503	Total appearances of HTTP status code 503 returned for a domain name within one minute	count	-	1 minute
http_code_504	Status code 504	Total appearances of HTTP status code 504 returned for a domain name within one minute	count	-	1 minute

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
http_code_400_rate	Percentage of status code 400	Percentage of HTTP status code 400 returned for a domain name within one minute (Appearances of status code 400/ Total number of requests x 100)	%	-	1 minute
http_code_403_rate	Percentage of status code 403	Percentage of HTTP status code 403 returned for a domain name within one minute (Appearances of status code 403/ Total number of requests x 100)	%	-	1 minute
http_code_404_rate	Percentage of status code 404	Percentage of HTTP status code 404 returned for a domain name within one minute (Appearances of status code 404/ Total number of requests x 100)	%	-	1 minute
http_code_416_rate	Percentage of status code 416	Percentage of HTTP status code 416 returned for a domain name within one minute (Appearances of status code 416/ Total number of requests x 100)	%	-	1 minute

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
http_code_499_rate	Percentage of status code 499	Percentage of HTTP status code 499 returned for a domain name within one minute (Appearances of status code 499/ Total number of requests x 100)	%	-	1 minute
http_code_500_rate	Percentage of status code 500	Percentage of HTTP status code 500 returned for a domain name within one minute (Appearances of status code 500/ Total number of requests x 100)	%	-	1 minute
http_code_502_rate	Percentage of status code 502	Percentage of HTTP status code 502 returned for a domain name within one minute (Appearances of status code 502/ Total number of requests x 100)	%	-	1 minute
http_code_503_rate	Percentage of status code 503	Percentage of HTTP status code 503 returned for a domain name within one minute (Appearances of status code 503/ Total number of requests x 100)	%	-	1 minute

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
http_code_504_rate	Percentage of status code 504	Percentage of HTTP status code 504 returned for a domain name within one minute (Appearances of status code 504/ Total number of requests x 100)	%	-	1 minute
bs_http_code_400	Origin status code 400	Total appearances of origin HTTP status code 400 returned for a domain name within one minute	count	-	1 minute
bs_http_code_403	Origin status code 403	Total appearances of origin HTTP status code 403 returned for a domain name within one minute	count	-	1 minute
bs_http_code_404	Origin status code 404	Total appearances of origin HTTP status code 404 returned for a domain name within one minute	count	-	1 minute
bs_http_code_416	Origin status code 416	Total appearances of origin HTTP status code 416 returned for a domain name within one minute	count	-	1 minute
bs_http_code_499	Origin status code 499	Total appearances of origin HTTP status code 499 returned for a domain name within one minute	count	-	1 minute

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
bs_http_code_500	Origin status code 500	Total appearances of origin HTTP status code 500 returned for a domain name within one minute	count	-	1 minute
bs_http_code_502	Origin status code 502	Total appearances of origin HTTP status code 502 returned for a domain name within one minute	count	-	1 minute
bs_http_code_503	Origin status code 503	Total appearances of origin HTTP status code 503 returned for a domain name within one minute	count	-	1 minute
bs_http_code_504	Origin status code 504	Total appearances of origin HTTP status code 504 returned for a domain name within one minute	count	-	1 minute
bs_http_code_400_rate	Percentage of origin status code 400	Percentage of origin HTTP status code 400 returned for a domain name within one minute (Appearances of origin status code 400/Total number of origin pull requests x 100)	%	-	1 minute

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
bs_http_code_403_rate	Percentage of origin status code 403	Percentage of origin HTTP status code 403 returned for a domain name within one minute (Appearances of origin status code 403/Total number of origin pull requests x 100)	%	-	1 minute
bs_http_code_404_rate	Percentage of origin status code 404	Percentage of origin HTTP status code 404 returned for a domain name within one minute (Appearances of origin status code 404/Total number of origin pull requests x 100)	%	-	1 minute
bs_http_code_416_rate	Percentage of origin status code 416	Percentage of origin HTTP status code 416 returned for a domain name within one minute (Appearances of origin status code 416/Total number of origin pull requests x 100)	%	-	1 minute

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
bs_http_code_499_rate	Percentage of origin status code 499	Percentage of origin HTTP status code 499 returned for a domain name within one minute (Appearances of origin status code 499/Total number of origin pull requests x 100)	%	-	1 minute
bs_http_code_500_rate	Percentage of origin status code 500	Percentage of origin HTTP status code 500 returned for a domain name within one minute (Appearances of origin status code 500/Total number of origin pull requests x 100)	%	-	1 minute
bs_http_code_502_rate	Percentage of origin status code 502	Percentage of origin HTTP status code 502 returned for a domain name within one minute (Appearances of origin status code 502/Total number of origin pull requests x 100)	%	-	1 minute

ID	Name	Description	Minimum Unit	Conversion Unit	Monitoring Period (Original Value)
bs_http_code_503_rate	Percentage of origin status code 503	Percentage of origin HTTP status code 503 returned for a domain name within one minute (Appearances of origin status code 503/Total number of origin pull requests x 100)	%	-	1 minute
bs_http_code_504_rate	Percentage of origin status code 504	Percentage of origin HTTP status code 504 returned for a domain name within one minute (Appearances of origin status code 504/Total number of origin pull requests x 100)	%	-	1 minute

Dimension

Key	Value
domain_name	Domain name

13.2 Setting Alarm Rules

You can customize monitoring metrics and notification policies in an alarm rule to learn about the status of domain names in a timely manner. This section describes how to set alarm rules.

Procedure

1. Log in to **Huawei Cloud console**. Choose **Service List** > **Management & Governance** > **Cloud Eye**.
2. Click  in the upper left corner of the console and select **CN North-Beijing4**.

3. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
4. In the upper right corner of the page, click **Create Alarm Rule**.
5. Set parameters as prompted.

   For more information, see **Creating an Alarm Rule**. The key parameters are as follows:

   - **Name**: alarm rule name. The system generates a random name, which you can modify.
   - **Resource Type**: **Content Delivery Network**
   - **Dimension**: **Domain name**
   - **Monitoring Scope**: Select **All resources**, **Resource groups**, or **Specified resources**.
6. After the configuration is complete, click **Next**.

13.3 Viewing Monitoring Metrics

Cloud Eye can help you monitor the status of domain names. You can obtain the monitoring metrics of CDN on the Cloud Eye console.

Procedure

1. Log in to **Huawei Cloud console**. Choose **Service List** > **Management & Governance** > **Cloud Eye**.
2. Click  in the upper left corner of the console and select **CN North-Beijing4**.
3. In the navigation pane, choose **Cloud Service Monitoring** > **Content Delivery Network**.
4. Click a domain name in the **ID** column or click **View Metric** in the **Operation** column to view the monitoring metrics of the domain name.

A Change History

Released On	Description
2024-04-10	This issue is the 105th official release. ● You can set the size of files to be compressed in **Smart Compression**.
2024-03-28	This issue is the 104th official release. ● You can set both international and Chinese (SM2) certificates for a domain name.
2024-03-26	This issue is the 103rd official release. ● Added the function of configuring client certificates. ● Removed the log combination tool.
2024-03-13	This issue is the 102nd official release. ● Up to 500 IP addresses are supported in an IP ACL.
2024-03-06	This issue is the 101st official release. ● Removed the function of setting the service termination policy.
2024-02-21	This issue is the 100th official release. ● Added the cache sharing function.
2024-01-26	This issue is the ninety-ninth official release. ● Updated figures in this document due to console UI changes.
2024-01-24	This issue is the ninety-eighth official release. ● You can filter domain names by service type in **Analytics**.
2024-01-18	This issue is the ninety-seventh official release. ● During batch certificate configuration, domain names can be searched by HTTPS status.

Released On	Description
2024-01-11	This issue is the ninety-sixth official release. ● Added the section "Copying Domain Configuration to New Domains."
2023-12-28	This issue is the ninety-fifth official release. ● You can cache the 3*XX* status codes.
2023-12-20	This issue is the ninety-fourth official release. ● You can set an alarm threshold for usage capping.
2023-12-14	This issue is the ninety-third official release. ● You can view the forcible cache logic in cache rules.
2023-11-24	This issue is the ninety-second official release. ● Added the usage cap function.
2023-11-23	This issue is the ninety-first official release. ● Added the service monitoring function to **Analytics (New)**.
2023-11-02	This issue is the ninetieth official release. ● Launched the new version of **Analytics**.
2023-10-24	This issue is the eighty-ninth official release. ● Added the access URL rewrite function.
2023-10-19	This issue is the eighty-eighth official release. ● You can set the origin response timeout interval to 300s. ● The value of a custom HTTP header can contain up to 1,024 characters. ● You can view the failure cause of cache purge and prefetch tasks.
2023-10-18	This issue is the eighty-seventh official release. ● Added the browser cache TTL function. ● Added the encode-based transcoding function to cache purge and prefetch.
2023-10-12	This issue is the eighty-sixth official release. ● The data export function allows you to export data in the created operations reports.
2023-09-15	This issue is the eighty-fifth official release. ● You can customize the priority for origin servers.
2023-09-12	This issue is the eighty-fourth official release. ● You can use token authentication for files with specific file name extensions.

Released On	Description
2023-09-08	This issue is the eighty-third official release. • Added the **origin SNI** function.
2023-09-05	This issue is the eighty-second official release. • Changed the **Export Tasks** function in **Analytics** to **Data Export**.
2023-08-30	This issue is the eighty-first official release. • You can configure up to 200 IP addresses in the IP address blacklist or whitelist. • You can configure the origin protocol and host for advanced origins.
2023-08-23	This issue is the eightieth official release. • The **Access-Control-Allow-Origin** parameter supports domain names with port numbers. For details, see **HTTP Header Settings (Cross-origin Requests)**. • Removed the third-party bucket origin server function.
2023-08-17	This issue is the seventy-ninth official release. • Changed the resolution logic from redirect to origin server to deleting resolution records when the termination policy is set to **Disable domain name**.
2023-08-08	This issue is the seventy-eighth official release. • Changed the origin pull mechanism. If there are multiple origin server IP addresses, the load balancing mechanism is used. For details, see **Origin Server Settings**.
2023-08-07	This issue is the seventy-seventh official release. • Replaced the popular content statistics function with the **Data Analysis** function.
2023-07-27	This issue is the seventy-sixth official release. • Added the **Cloud Eye Monitoring** function.
2023-07-26	This issue is the seventy-fifth official release. • Modified setting restrictions. **Origin URL Rewriting**, **Advanced Origins**, **Range Requests**, **Redirect from Origin**, **ETag Verification**, **Status Code Cache TTL**, and **Video Seek** cannot be configured for domain names whose service type is whole site acceleration.
2023-07-13	This issue is the seventy-fourth official release. • You can add remarks to domain names. For details, see **Enabling/Disabling CDN for a Domain Name**. • Added the **IP Access Frequency** function.

Released On	Description
2023-07-11	This issue is the seventy-third official release. • You can set more special characters for the **User-Agent ACL** function.
2023-07-10	This issue is the seventy-second official release. • You can drag and drop a TXT file to the **Prefetch & Purge** page.
2023-06-26	This issue is the seventy-first official release. • Released the new origin server configuration page.
2023-06-13	This issue is the seventieth official release. • Rolled out the new version of the **Resource Packages** page. Multi-dimensional search and export are supported.
2023-06-09	This issue is the sixty-ninth official release. • When setting the advanced origin to an IP address or domain name, you can configure a port number.
2023-06-06	This issue is the sixty-eighth official release. • HSTS is supported.
2023-05-29	This issue is the sixty-seventh official release. • Certificates encrypted using Chinese cryptographic algorithms are supported. • SCM certificates are supported.
2023-05-17	This issue is the sixty-sixth official release. • Added the request rate limiting function.
2023-05-11	This issue is the sixty-fifth official release. • Added the operations report function to **Statistical Analysis**.
2023-05-08	This issue is the sixty-fourth official release. • The service area can be modified for domain names with whole site acceleration. • The M3U8/MPD file supports authentication inheritance.
2023-04-26	This issue is the sixty-third official release. • When modifying the origin server settings, you can configure a third-party object storage bucket as the origin server.
2023-04-24	This issue is the sixty-second official release. • Smart compression supports user-defined compression formats.

Released On	Description
2023-04-19	This issue is the sixty-first official release. ● Added the "Export Tasks" function to **Statistical Analysis**.
2023-04-06	This issue is the sixtieth official release. ● Removed the OBS private bucket retrieval function and incorporated it into the origin server settings. When using a private bucket as the origin server, you must select the **Private bucket** option.
2023-03-29	This issue is the fifty-ninth official release. ● Added the tag function.
2023-03-20	This issue is the fifty-eighth official release. ● Optimized descriptions in some sections, added examples, added application scenarios, and optimized parameter descriptions. ● Incorporated origin cache control into the "Cache Rules" section.
2023-03-16	This issue is the fifty-seventh official release. ● Optimized descriptions in some sections, added examples, added application scenarios, and optimized parameter descriptions.
2023-02-24	This issue is the fifty-sixth official release. ● Wildcard domain names and multiple domain names can be configured for cross-origin requests.
2023-02-20	This issue is the fifty-fifth official release. ● You can configure authentication parameters and a secondary key for some authentication methods.
2023-02-14	This issue is the fifty-fourth official release. ● Added the **SCM certificate** option to HTTPS settings. ● Added **Redirect Mode** to force redirect. The redirect mode can be 301 or 302.
2023-02-09	This issue is the fifty-third official release. ● Added the WebSocket settings to domain names with whole site acceleration.
2022-12-13	This issue is the fifty-second official release. ● Added the function of verifying ETag for content retrieval.

Released On	Description
2022-12-06	This issue is the fifty-first official release. ● Added the advanced retrieval function. ● Referer validation supports IP addresses with port numbers.
2022-11-08	This issue is the fiftieth official release. ● Added the function of changing the service type. ● You can specify the authentication scope when signing URLs.
2022-10-27	This issue is the forty-ninth official release. ● Added the video seek function.
2022-09-27	This issue is the forty-eighth official release. ● Added the description of refreshing updated resources in a directory to section "Cache Refreshing."
2022-08-25	This issue is the forty-seventh official release. ● Moved smart compression to the **Advanced Settings** tab.
2022-08-05	This issue is the forty-sixth official release. ● Remote authentication can be configured on the console.
2022-04-26	This issue is the forty-fifth official release. ● Added the IPv6, retrieval timeout interval, TLS version, status code cache age, and custom error page functions.
2022-03-24	This issue is the forty-fourth official release. ● Rolled out the function of changing the service area. ● You can configure up to 60 cache rules.
2022-03-22	This issue is the forty-third official release. ● OCSP stapling can be configured on the CDN console.
2022-03-10	This issue is the forty-second official release. ● Separated the force redirect, HTTP/2, and content retrieval protocol settings from the HTTPS settings. ● If the origin server is the domain name of an OBS bucket, a standby origin server can be configured. ● The domain name of an OBS bucket under an account can be added as the origin server of CDN by another account.

Released On	Description
2022-03-04	This issue is the forty-first official release. ● Moved the retrieval host settings from the **Retrieval Settings** tab to the **Modify Origin Server** dialog box on the **Basic Settings** tab.
2022-01-06	This issue is the fortieth official release. ● Brotli compression can be configured on the CDN console.
2021-12-06	This issue is the thirty-ninth official release. ● Encryption algorithms can be configured during URL signing.
2021-11-25	This issue is the thirty-eighth official release. ● You can select and copy specific configuration items.
2021-11-09	This issue is the thirty-seventh official release. ● Added the function of rewriting retrieval request URLs.
2021-10-26	This issue is the thirty-sixth official release. ● IPv6 addresses can be added to IP address whitelists/blacklists. ● Added recommended configurations for cache rules. ● Domain names with ports can be added to referer whitelists/blacklists.
2021-10-11	This issue is the thirty-fifth official release. ● Added the function of configuring User-Agent access control on the CDN console. ● Added the function of exporting basic domain configurations from the CDN console.
2021-09-28	This issue is the thirty-fourth official release. ● Added the function of configuring User-Agent access control on the CDN console. ● Added section "Utilization Statistics for Whole Site Acceleration" to chapter "Statistical Analysis." ● Adjusted statistics functions on the CDN console.
2021-09-06	This issue is the twenty-first official release. ● Added examples to retrieval request header, cache rule, retrieval host, and IP address blacklist/whitelist settings.
2021-05-27	This issue is the twentieth official release. ● URL signing is available on the CDN console.

Released On	Description
2021-03-11	This issue is the nineteenth official release. ● Added section "Copying Domain Configurations."
2021-02-02	This issue is the eighteenth official release. ● Added section "Retrieval Request Headers." ● Added "Overview" to section "Retrieval Settings." ● Added "Overview" to section "Cache Settings."
2020-10-09	This issue is the seventeenth official release. ● Optimized section "Cache Refreshing and Preheating."
2020-06-11	This issue is the sixteenth official release. ● Removed the origin verification methods from section "Modifying Origin Server Details." ● Optimized some descriptions.
2020-04-10	This issue is the fifteenth official release. ● Added section "Domain Certificate Management." ● Optimized some descriptions.
2020-01-02	This issue is the fourteenth official release. ● Added the origin verification methods in section "Modifying Origin Server Details." ● Optimized some descriptions.
2019-10-28	This issue is the thirteenth official release. ● Added section "Functions" to the "Domain Name Management" chapter. ● Added the FAQ links to related sections. ● Optimized some descriptions.
2019-06-21	This issue is the twelfth official release. ● Added section "HTTPS Certificate Format Conversion." ● Added sections "Enabling/Disabling a Domain Name", "Removing a Domain Name", and "Reviewing a Domain Name." ● Optimized some descriptions.
2019-05-31	This issue is the eleventh official release. ● Added section "Permissions Management." ● Optimized some descriptions.

Released On	Description
2019-05-08	This issue is the tenth official release. ● Combined "Enabling/Disabling CDN", "Removing a Domain Name", and "Reviewing a Domain Name" to "Domain Name Operations." ● Moved "HTTPS Certificate Requirements" and "HTTP/2 Introduction" to "HTTPS Settings." ● Moved the non-Huawei Cloud DNS configuration method in "Configuring CNAME Records" to "Related Resources." ● Optimized the operation steps in the document and incorporated the configuration description into operation procedures. ● Optimized the document description and added hyperlinks to the description.
2019-03-29	This issue is the ninth official release. ● Added section "Service Termination Policy."
2019-02-28	This issue is the eighth official release. ● Optimized the document content.
2019-02-14	This issue is the seventh official release. ● Added section "Domain Name Quota Management." ● Added section "Quota Management for Refreshing and Preheating."
2019-01-28	This issue is the sixth official release. ● Optimized detail descriptions. ● Added troubleshooting methods.
2018-12-28	This issue is the fifth official release. ● Optimized description in section "Retrieval Host." ● Added troubleshooting methods.
2018-11-30	This issue is the fourth official release. ● Optimized the document outline structure. ● Optimized some detailed description. ● Added section "Domain Name Requirements." ● Added section "Limitations and Constraints."

Released On	Description
2018-09-21	This issue is the third official release. ● Combined chapters "Subscribing to CDN" and "Quick Start" into one manual *Quick Start Guide*. ● Added section "Configuring HTTP Headers." ● Added description of supporting wildcard domain names in section "Configuring Referer Validation." ● Added section "Configuring the IP Address Blacklist." ● Added description of full path in section "Configuring the Cache Policy." ● Added description of log combination in section "Log Management." ● Added description of range-based retrieval, 302 redirect retrieval, and private bucket retrieval in section "Configuring Retrieval Parameters."
2018-05-21	This issue is the second official release. ● Added section 4.6 "Diagnosis Tool".
2018-05-05	This issue is the first official release.

