CDN

User Guide

Issue 106

Date 2025-07-10

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 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 user permissions, as shown in **Process Flow**.

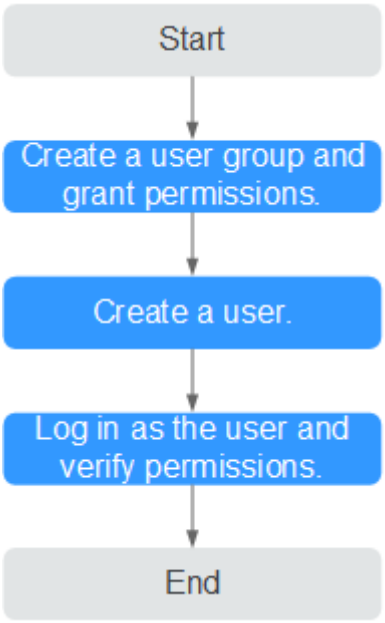
Prerequisites

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 1-1 shows the process of granting CDN permissions.

Figure 1-1 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.

2 Enabling CDN

Enable CDN before you use it. This section describes how to enable CDN.

Prerequisites

- You have registered a HUAWEI ID and have specified a payment method.

  NOTE

  You need to complete real-name authentication when you:

  - Purchase and use cloud services on Huawei Cloud PoPs in the Chinese mainland. Real-name authentication is required by the laws and regulations in the Chinese mainland.
  - Purchase a cloud service whose region includes Chinese mainland.

Precautions

- You can enable and use CDN in traffic-based billing. To do so, buy a CDN traffic package, refresh the page of enabling CDN, and enable CDN.

Procedure

1. Log in to **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.
2. Click **Enable Now**.
3. On the displayed page, click **Enable Now**.

Figure 2-1 Enabling CDN

3 Domain Name Management

3.1 Overview

After adding a domain name to CDN, if you need to stop acceleration or restart acceleration due to service changes, you can enable or disable CDN, review domain names, or delete domain names on the CDN console.

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

Scenarios

The following table describes the functions.

Table 3-1 Scenarios

Item	Description	API
Adding a Domain Name	Add a domain name to CDN and configure origin servers and other information to accelerate content delivery.	**Creating a Domain Name**
Enabling/ Disabling CDN for a Domain Name	**Disabling CDN**: Disable CDN for a domain name in the **Enabled** state. **Enabling CDN**: Enable CDN for a domain name in the **Disabled** state.	**Enabling CDN for a Domain Name** **Disabling CDN for a Domain Name**

Item	Description	API
Deleting a Domain Name	Delete a domain name in the **Disabled**, **Error**, or **Rejected** state. **NOTE** After a domain name is deleted, the system automatically deletes its related configuration. To use CDN for the removed domain name again, re-add and configure the domain name.	Deleting a Domain Name
Copying Domain Configurations	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, apply to have it reviewed after the domain name is re-licensed. Once the review passes, CDN unbans the domain name.	-
Service Termination Policy	After the CDN service is terminated, Huawei Cloud CDN either redirects user requests to your origin servers, or, by default, disables your domain names. You cannot modify the service termination policy on the console.	-
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.	Querying Quotas

3.2 Adding a Domain Name

If you want to use CDN to accelerate access to your site, add the domain name of your site to CDN. CDN caches origin content on PoPs so that your content loads faster.

Preparations

- Enable CDN for your account by referring to **Enabling CDN**.
- Prepare a domain name for acceleration and an origin server (service server) based on the domain name admission conditions, content moderation requirements, and domain name description in the **Restrictions**.

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 **Add Domain Names** and specify domain parameters.

Figure 3-1 Adding a domain name

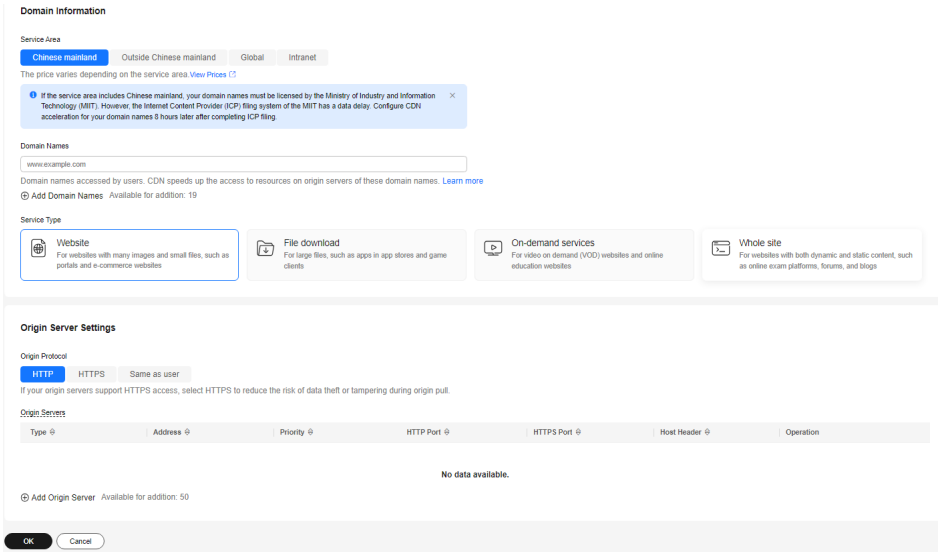


Table 3-2 Parameter description

Parameter	Item	Description
Domain Names	-	• A domain name can contain up to 200 characters, including letters, digits, hyphens (-), periods (.), and asterisks (*). It can start with a letter, digit, or asterisk. An asterisk, if any, must be the first character. • Each label of a domain name (for example, ***** in ****.***.com**) can contain up to 63 characters. • You can add up to 100 domain names under each account. • CDN does not allow access from websites containing illicit content. For details, see "Content moderation" in **Restrictions**. The existing domain names connected to CDN are reviewed regularly. If a domain name involves any violations, the CDN acceleration service will be suspended for the domain name and other domain names in your account. • 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. • 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. • An acceleration domain name must be unique. • You can add a domain name including a wildcard (*). For example, if you add ***.test.com** to CDN as an acceleration domain name and have it resolved to the CNAME provided by CDN, all of the level-2 domain names under ***.test.com**, such as **a.test.com**, will enjoy CDN acceleration by default. However, level-3 domain names (such as **b.a.test.com**) would not. 1. If you add a wildcard domain name to a particular account, you cannot add any of the level-2 domain names under that domain name to other accounts. 2. You will be billed for the acceleration service provided to all of the level-2 domain names under a wildcard domain name. If there are multiple level-2 domain names, billing will be based on the traffic generated by the wildcard domain name, not on each of the level-2 domain names.

Parameter	Item	Description
Enterprise Project	-	This parameter is only available if Huawei Cloud Enterprise Project Management Service is enabled. For details, see **Enterprise Management User Guide**. You cannot select disabled enterprise projects.
Service Area	Global	CDN schedules access requests from users around the world to the optimal PoP nearby. The domain name must be licensed by the MIIT. For details, see **ICP License Service**.
	Chinese mainland	CDN schedules access requests from users around the world to PoPs in the Chinese mainland. The domain name must be licensed by the MIIT. For details, see **ICP License Service**.
	Outside Chinese mainland	CDN schedules access requests from users around the world to PoPs outside the Chinese mainland. The domain name does not need to be licensed by the MIIT.
Service Type	Website	CDN is perfect for web portals, e-commerce platforms, news apps, and user generated content (UGC)-focused apps. The cache format includes but is not limited to .zip, .exe, .wmv, .gif, .png, .bmp, .wma, .rar, .jpeg, and .jpg.
	File download	CDN is useful for download clients, game clients, app stores, and websites that provide download services based on HTTP or HTTPS.
	On-demand services	CDN accelerates delivery of on-demand services, such as online education, video sharing, music or video on demand, and other audiovisual content.
	Whole site	CDN is a good option for websites that consist of both dynamic and static content and for sites that involve a large number of ASP, JSP, or PHP requests. **CAUTION** • WSA is an independent cloud service and is billed separately. It shares the same console with CDN. You need to enable WSA before adding **Whole site** domain names. For details about how to enable WSA, see **Enabling WSA**. • When **Service Type** is set to **Whole site**, the origin server type cannot be set to **OBS bucket**.

Parameter	Item	Description
Origin Protocol	-	Protocol used by CDN PoPs to pull content from the origin server. • **HTTP** • **HTTPS** (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.

4. In the **Origin Server Settings** area, click **Add Origin Server** to add an origin server for the domain names.

Figure 3-2 Adding an origin server

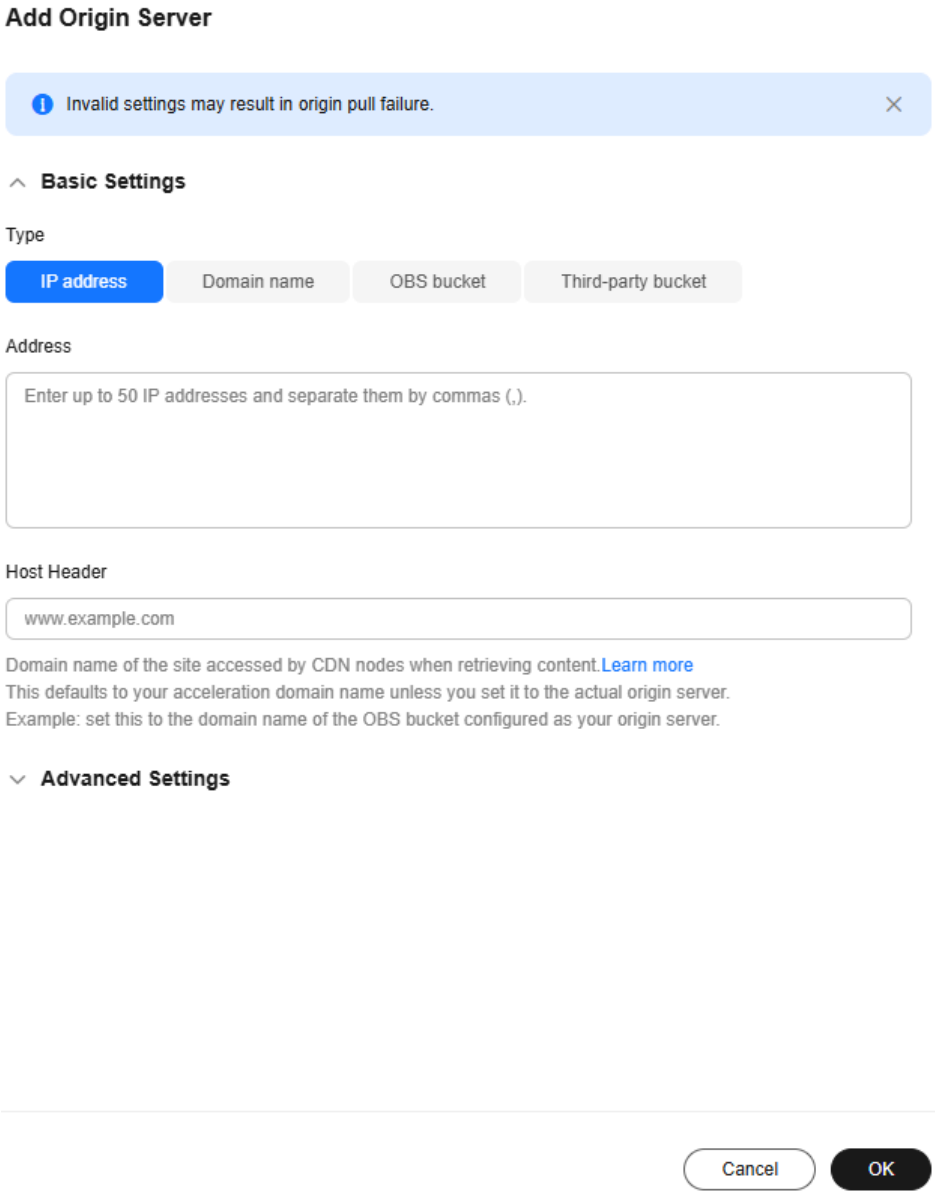


Table 3-3 Parameter description

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

Parameter	Description
	Domain name • Start with a letter or digit. Enter up to 255 characters, including letters, digits, hyphens (-), and periods (.). • Each label of a domain name (for example, *** in ***.***.**com**) can contain up to 63 characters. • An origin domain cannot be the same as an acceleration domain name. • You can also enter the domain name of an object storage bucket in this field. Pay attention to the following points when selecting this option: 1. You cannot use **private object storage buckets** as origin servers when you set **Type** to **Domain name**. 2. If you use an object storage bucket as your origin server, the object storage service will charge the origin pull traffic based on its billing standards. 3. 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. 4. If you use an OBS bucket created after January 1, 2022 as the origin server and want to enable online preview, log in to the CDN console, choose **Domains** in the navigation pane, click the target domain name, click the **Advanced Settings** tab, click **Edit** next to **HTTP Headers**, and set **Content-Disposition** to **inline**. For details, see **How Do I Preview OBS Objects in My Web Browser?**

Parameter	Description
	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 you enter a custom OBS bucket domain name, the origin domain name must end with .myhuaweicloud.com or .myhuaweicloud.cn. 3. If you set an OBS private bucket as the origin server and want to filter user requests, enable **OBS authorization** and **OBS Pull Authentication**. 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, a full list of 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. 7. When **Service Type** is set to **Whole site**, the origin server type cannot be set to **OBS bucket**. 8. If the origin server is an OBS private bucket, when a client requests the homepage of the acceleration domain name and origin pull is triggered, origin pull can succeed only when the request method is GET or HEAD. For other request methods, CDN blocks the request and returns status code 403. **NOTE** If you use an OBS bucket created after January 1, 2022 as the origin server and want to enable online preview, log in to the CDN console, choose **Domains** in the navigation pane, click the target domain name, click the **Advanced Settings** tab, click **Edit** next to **HTTP Headers**, and set **Content-Disposition** to **inline**. For details, see **How Do I Preview OBS Objects in My Web Browser?**

Parameter	Description
Address	Address accessed by CDN PoPs during origin pull. ● If the origin server type is IP address, you can enter multiple IP addresses and separate them with commas (,). – Each IP address is an origin server. A domain name can have up to 50 origin servers. The number of IP addresses you can enter cannot exceed the total number of available origin servers of the domain name.
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**.
OBS Pull Authentication	Applies when an OBS bucket is used as an origin server. Enable this switch if access to the bucket requires authentication. In this way, CDN PoPs carry the authentication information during origin pull. If the information does not match the OBS bucket, origin pull fails, preventing unauthorized traffic theft. ● Enabled by default for a private bucket ● Disabled by default for a public bucket
Priority	Enter a number from 1 to 100. A larger number indicates a higher 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. ● You can configure up to six rules with unique priorities. **NOTE** On April 10, 2025 (Beijing time), CDN updated the origin server priority function and stopped using the concept of primary and standby origin servers. Currently, the default priorities of the original primary and standby origin servers are as follows: ● Primary origin server: 70 ● Standby origin server: 30

Parameter	Description
Weight	The value ranges from 1 to 100. A larger value indicates that content is pulled from this origin server more frequently. • If there are multiple origin servers with the same priority, the weight determines the proportion of content pulled from each origin server.
Origin Ports	Port numbers for CDN PoPs to pull content. By default, the HTTP port is 80 and the HTTPS port is 443. • If **Type** is set to **OBS bucket**, the port numbers cannot be changed.

5. Click **OK**. Repeat **4** to add more origin servers. You can add up to 50 origin servers.
6. After adding origin servers, click **OK** in the lower left corner of the page.

NOTE

- The configuration takes 5 to 10 minutes to take effect. When **Status** of the domain name becomes **Enabled**, the domain name has been added.
- If the CNAME status of a domain name is  , no CNAME has been configured for this domain name.

Optional Settings

Attacks and malicious traffic will result in a bill higher than your normal expenditures. This bill cannot be waived or refunded. Enable **burst bandwidth alert** for your domain name to reduce such risks.

1. With **burst bandwidth alerts**, CDN will alert you when the access bandwidth reaches the specified threshold, helping you identify abnormal request promptly and reduce risks of excess billing. By default, this function is enabled without a specific threshold. You can disable it as required.

Recommended Configuration

You can also follow the instructions in **Recommended Configurations** to configure cache rules, usage caps, and HTTPS certificates for domain names, to improve access performance, cache hit ratio, and access security and reduce high bill risks.

Configuring CNAME Resolution

After a domain name is added, the system automatically assigns a CNAME to this domain name. The CNAME cannot be accessed directly. You must **add the CNAME** to your domain's DNS records. Then requests for your domain name will be redirected to CDN PoPs for acceleration.

3.3 Enabling/Disabling CDN for a Domain Name

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

Precautions

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

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

You can add remarks to a domain name.

Figure 3-3 Basic domain information

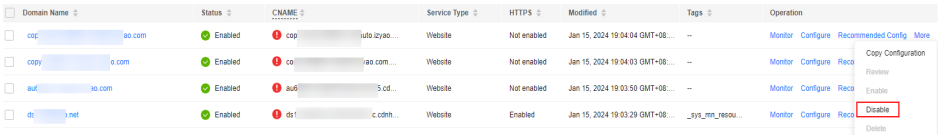
Disabling CDN for Domain Names

You can disable CDN for a domain name in the **Enabled** or **Error** state. CDN will no longer provide the acceleration service for this domain name, but the domain configuration will be temporarily retained. To restore acceleration, enable CDN for it again.

Disabling CDN for a single domain name

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

Figure 3-4 Disabling CDN for a domain name

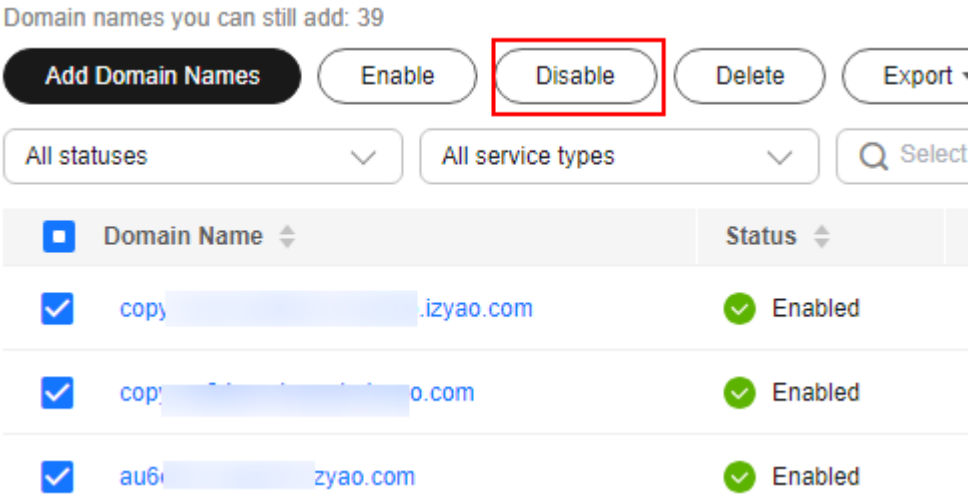


2. Confirm the information about the domain name and click **Yes**.

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 3-5 Disabling CDN for multiple domain names



Enabling CDN for Domain Names

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

Enabling CDN for a single domain name

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

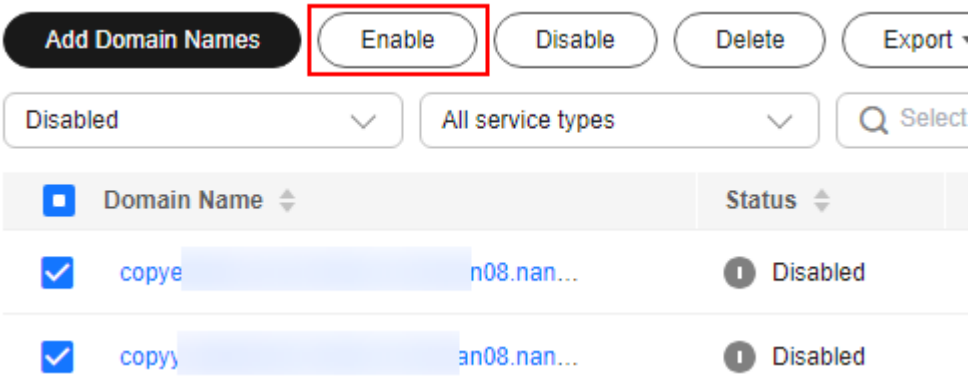
Figure 3-6 Enabling CDN for a domain name

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 3-7 Enabling CDN for multiple domain names



3.4 Deleting a Domain Name

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

Precautions

- You can only delete domain names in the **Disabled**, **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.

3.5 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.

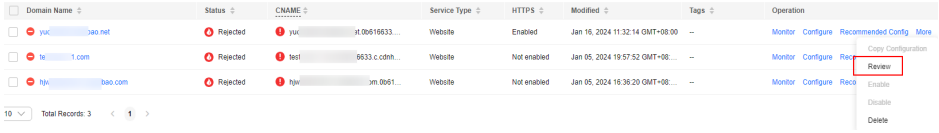
CAUTION

- 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 3-8 Reviewing a domain name



Examples

1. When a domain name was **banned because its 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.
2. If a domain name was **banned for other reasons**, a message is displayed after you click **Review**, informing you of the fact. In this case, resolve this issue and submit a service ticket.

3.6 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 3-4 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.

3.7 Domain Name Quota Management

What Is a Quota?

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas limit the number or amount of resources available to accounts. If an existing resource quota cannot meet your service requirements, submit a service ticket to increase the quota.

Table 3-5 CDN domain name quotas

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

NOTE

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

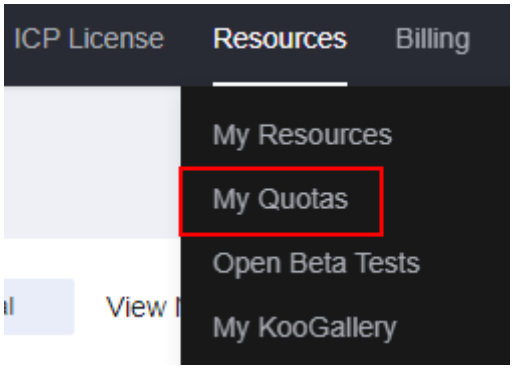
How Do I View My Quota?

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

   The CDN console is displayed.

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

Figure 3-9 My Quotas



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

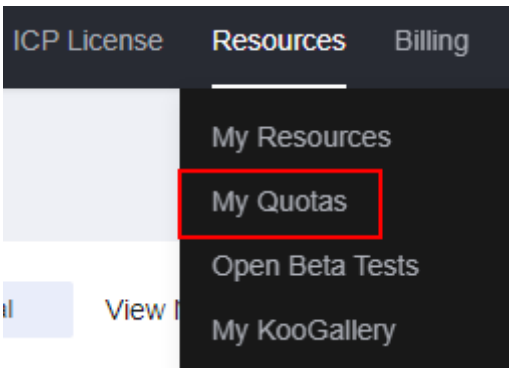
How Do I Apply for a Higher Quota?

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 3-10 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.

4 Custom Domain Name Configuration

4.1 Overview

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

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

OBS Authorization

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

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

Configuration Replication

This function is available for domain names in the **Enabled**, **Disabled**, or **Rejected** state.

Item	Description
Copying Domain Configurations to Existing Domains	Copy the configuration of a domain name to existing domain names, to quickly modify domain configurations.
Copying Domain Configurations to New Domains	Quickly add and customize domain names by copying the configuration of one domain name to one or more new domain names.

Basic Settings

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

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

Origin Settings

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

Item	Description
Origin Protocol	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, set the Server Name Indication (SNI) to specify the domain to be visited by CDN.
Origin URL Rewrite	If the URLs of origin pull requests do not match the origin server URLs, rewrite the request URLs to improve the origin pull hit ratio.
Advanced Origins	Configure advanced origins to allow CDN to pull content of different resource types or paths from different origin servers.
Range Requests	Enable range requests to speed up large file distribution.
Redirect from Origin	Prevent CDN from directly sending a 301/302 redirect address to users when 301/302 redirect is performed for your origin server address. Force CDN to cache the requested content and then forward the content to users.
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, enable ETag verification.
Origin Request Headers	Rewrite a header in an origin pull request on the CDN console.
Origin Response Timeout	Adjust the origin response timeout based on the features and service scenarios of your origin server.
Dynamic Content Pull Mode	By default, CDN pulls dynamic content from the origin server with the best performance. Choose to pull content from origin servers based on their weights.

HTTPS Settings

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

Function	Description
SCM Authorization	Before configuring an SCM certificate, enable SCM authorization.
Configuring an HTTPS Certificate	Add a certificate for HTTPS acceleration.

Function	Description
HTTPS Certificate Requirements	Learn how to combine and upload certificates issued by different authorities.
HTTPS Certificate Format Conversion	Convert certificates in other formats to the PEM format that CDN supports.
TLS Versions	Enable or disable TLS versions as required.
Force Redirect	Force clients to request content from CDN PoPs using HTTP or HTTPS.
HSTS	Force clients (such as browsers) to use HTTPS to access your server, improving access security.
HTTP/2	Understand the background and advantages of HTTP/2.
OCSP Stapling	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 CAs, accelerating the verification.
QUIC	Configure the QUIC protocol to improve transmission security, reduce transmission and connection latency, and prevent network congestion.
Client Certificates	Configure a client certificate to enforce mutual certificate authentication between clients and CDN PoPs, securing website communication.

Cache Settings

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

Item	Description
PoP Cache Rules	• Set the time to live (TTL) and priority for different resources to increase the hit ratio and reduce the back-to-source rate.
Browser Cache TTL	Set a browser cache TTL, during which users can obtain content directly from their browser cache (if available), reducing origin pulls.
Status Code Cache TTL	Cache error status codes returned by the origin server to CDN PoPs for a specified TTL. CDN returns the error codes to users when they request resources within this TTL, reducing the origin pull ratio and origin server pressure.

Item	Description
Access URL Rewrite	Set access URL rewrite rules to redirect user requests to the URLs of cached content.
Shared Cache Groups	Configure a shared cache group with a primary domain name to share its cache with other domain names. This improves the cache hit ratio when these domain names host the same resources.

Access Control

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

Item	Description
Referer Validation	Identify and filter visitors to restrict their access.
IP ACL	Filter out requests from specific IP addresses.
User-Agent ACL	Filter out requests from specific user agents.
Geo-blocking	Prevent users in certain geographical locations from accessing your content.
Token Authentication	Protect your website resources from being downloaded by malicious users.
Remote Authentication	Allow CDN to forward user requests to a specific server for authentication, to prevent malicious resource download.
IP Access Frequency	Restrict the number of times that a single IP address requests a URL from a PoP per second to defend against CC attacks and malicious theft.

Advanced Settings

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

Item	Description
HTTP Header Settings (Cross-origin Requests)	Customize values of HTTP response headers for your website.

Item	Description
Custom Error Pages	Customize error pages returned to user clients.
Smart Compression	Compress static content on your websites by reducing file size. This speeds up file transfer and saves you a lot of bandwidth.
WebSocket	If you have enabled whole site acceleration in scenarios such as on-screen commenting, collaborative session, market data broadcast, sports live update, online education, and IoT, configure WebSocket to implement long-term bidirectional data transmission.
Request Rate Limiting	Limit the user request rate within a specific range to reduce costs and the risk of burst bandwidth.
Usage Cap	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, reducing high bills caused by traffic theft or attacks.

Video Settings

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

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

4.2 OBS Authorization

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

WARNING

Do not delete the agency for authorizing CDN to access OBS. Otherwise, CDN cannot pull resources from OBS private buckets.

Constraints

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

IAM permissions

- Listing agencies: **iam:agencies:listAgencies**
- Creating an agency: **iam:agencies:createAgency**
- Granting permissions to an agency for a region-specific project: **iam:permissions:grantRoleToAgencyOnProject**

CDN permissions

- Changing the billing option: **cdn:configuration:modifyChargeMode**
- Granting CDN read-only permissions: **CDN ReadOnlyAccess**

Precautions

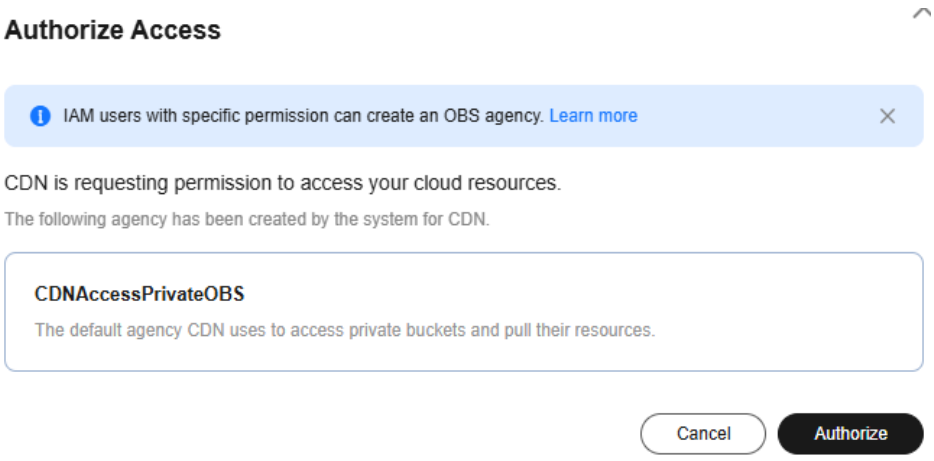
- CDN depends on other cloud services. Therefore, after enabling OBS authorization, configure related policies to make the OBS private bucket available for CDN acceleration by referring to **Dependencies Between CDN and Other Services**.
- Since April 2, 2025 (Beijing time), Huawei Cloud CDN has enabled the new OBS agency. It has fewer permissions than the old one. If you have enabled the OBS agency of the old version, you can reduce permissions by referring to **How Do I Replace the Old OBS Agency Permissions with New Ones?**

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**.

Figure 4-1 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.

If files in your OBS bucket are **encrypted using KMS**, assign the **kms:cmk:get** and **kms:dek:crypto** policies to the CDNAccessPrivateOBS agency so that CDN can read and accelerate delivery of the encrypted files.

5. **(Optional)** Assign the **kms:cmk:get** and **kms:dek:crypto** policies to the CDNAccessPrivateOBS agency.
   a. Log in to **Huawei Cloud console**. Choose **Service List** > **Management & 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. Click **Create Policy** in the upper right corner and set the parameters as follows:

      - **Policy Name**: Enter a custom name.
      - **Policy View**: Select **Visual editor**.
      - **Policy Content**:
        - Select **Allow**.
        - Service: Select **Key Management Service**.
        - Actions: Select **kms:cmk:get** and **kms:dek:crypto**.
        - Resources: Select **All**.
   e. Click **Next**.
   f. Select the policy created in the previous step and click **Next**.
   g. Set **Scope** to **Region-specific projects** and select the region based on the region of the OBS bucket.
   h. Click **OK**.

FAQ

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

4.3 Template Management

CDN allows you to customize templates for quick domain configuration. You can define function settings in one template and apply it to multiple domain names.

Scenarios

This function is useful when you want to use the same rule for multiple domain names, for example, the same referer validation rule for five domain names.

Constraints

- Templates can include HTTP header, cache rule, redirect from origin, smart compression, range requests, referer validation, IP ACL, User-Agent ACL, and usage cap settings.

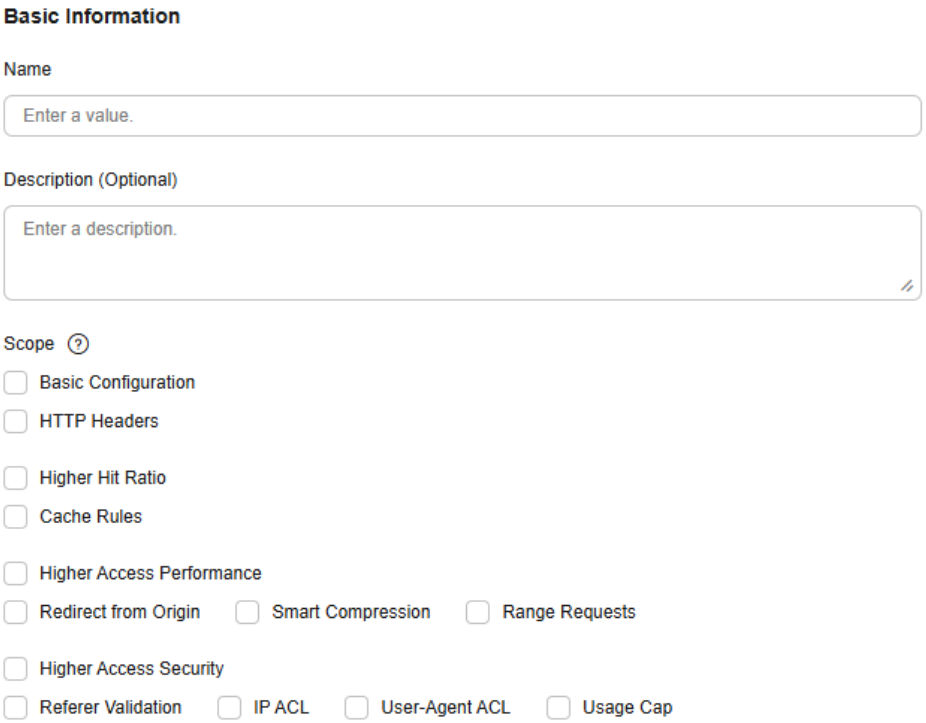
- The system automatically creates a cache rule whose type is **All files** and priority is **1** for a template, unless you have set one **All files** rule when creating the template. The priority of other rules cannot be **1**.

Creating a Template

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 the **Templates** tab.
4. In the **Templates** area, click **Create**. The **Create Template** page is displayed.

   Figure 4-2 Creating a template



5. Enter the template name and description, and select the configuration items to be contained in the template.
6. Configure rules for the selected configuration items and click **OK**.
   - After a template is created, you can click buttons in the **Operation** column of the template list to edit or delete the template, or **apply the template to domain names**.

Applying a Template to Domain Names

You can apply a created template to domain names. This will overwrite their original configuration with that in the template.

1. In the template list, click **Apply to Domains** in the **Operation** column of a template.

2. In the displayed dialog box, select target domain names and click to add them to the right area.
   - Select up to 50 domain names at a time.
3. Click **OK**.

Checking Template Application Records

In the **Application Records** area, you can view the following information of a template application record:

- Domain names to which the template is applied: Click **View Domains** in the **Operation** column to view the target domain names and whether the application is successful.
- Whether the template is used: In the **Status** column, view the number of domain names that the template is used, fails to be used, or is being configured.
- Template configuration: Click **Template Snapshot** in the **Operation** column to view the configuration items contained in the template when the template is used.

Figure 4-3 Template application records

4.4 Copying Domain Configurations

4.4.1 Copying Domain Configurations to Existing Domains

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

CAUTION

- For a domain name with high traffic or bandwidth, exercise caution when copying its configuration to avoid economic loss.
- This function will overwrite the original configurations of target domain names.

Constraints

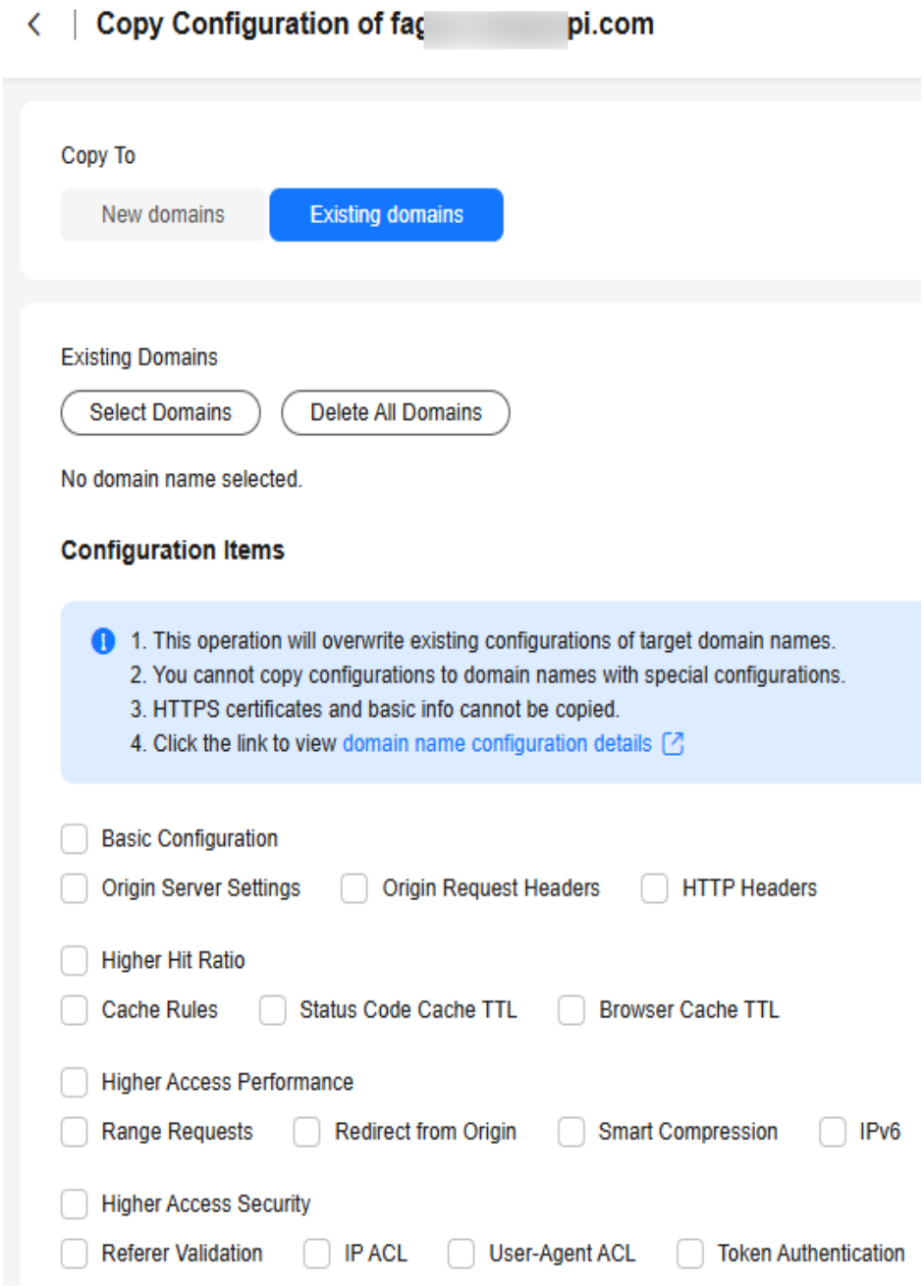
- This function is available for **unbanned** domain names in the **Enabled**, **Disabled**, or **Rejected** state.
- Configuration replication cannot be undone. Before copying the configuration of a domain name, ensure that the configuration is correct.
- This function is unavailable for domain names with special configurations.
- HTTPS certificates and basic information about domain names cannot be copied.

Procedure

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

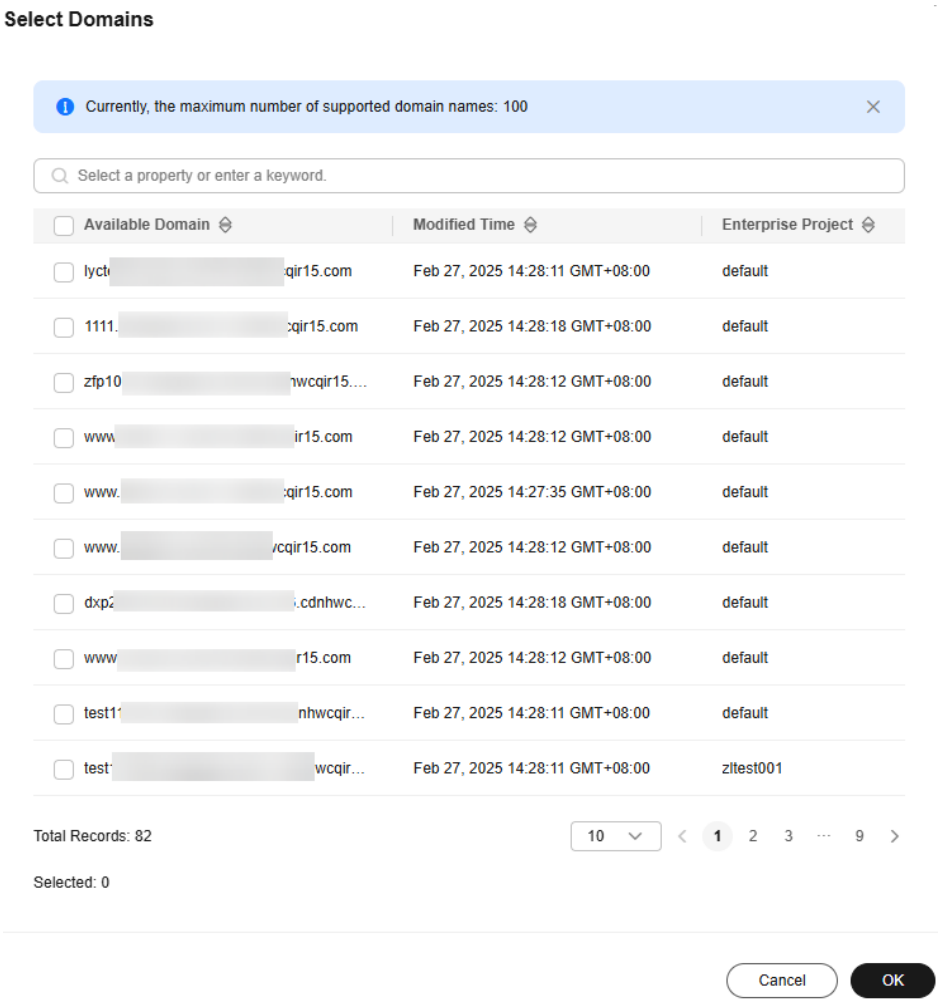
   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. On the **Domains** page, click **More** > **Copy Configuration** in the **Operation** column of the row containing the source domain name. On the displayed page, set **Copy To** to **Existing domains**.

   Figure 4-4 Copying domain configurations

4. Under **Existing Domains**, click **Select Domains**.

Figure 4-5 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 100 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 **OK**.
6. Under **Configuration Items**, select the configuration items to be copied and click **OK**.
   - **Configuration copy cannot be undone**. Ensure that the domain names selected are correct.

4.4.2 Copying Domain Configurations to New Domains

This function allows you to add new domain names with the same configuration as that of an existing domain name. You do not need to add and configure domain names one by one.

Constraints

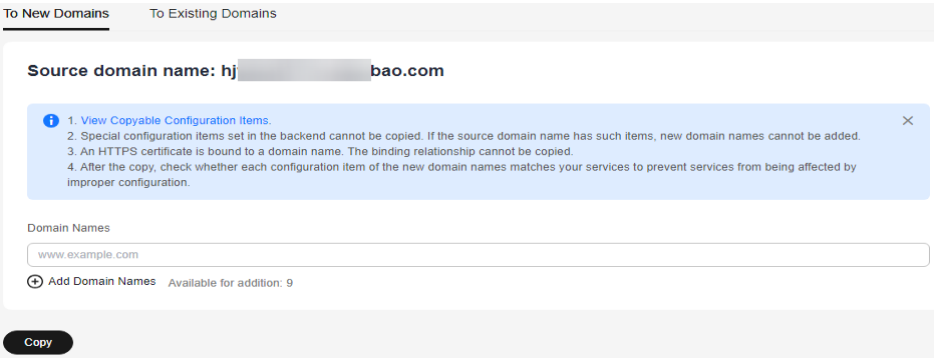
- You can copy the configuration of a domain name in the **Enabled**, **Disabled**, or **Rejected** state.
- If a domain name is in the **Deleting**, **Configuring**, **Reviewing**, **Error** state, its configuration cannot be copied.
- The configuration of a banned domain name cannot be copied.
- You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

Procedure

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

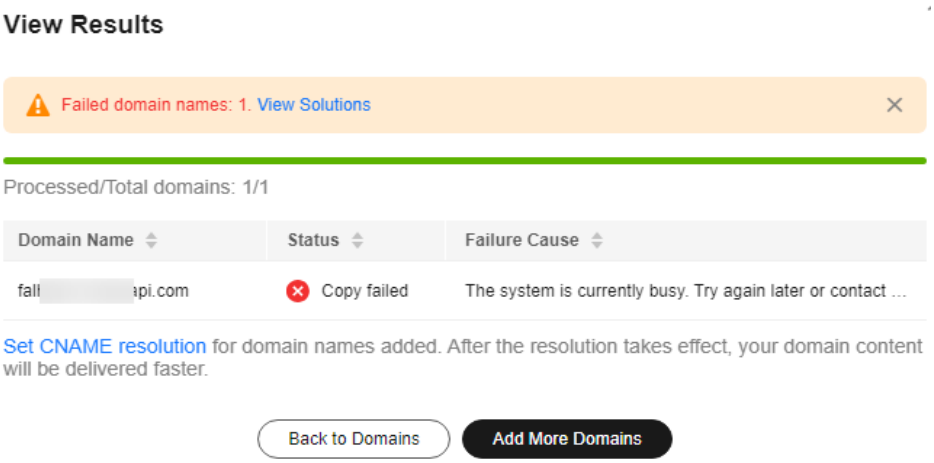
   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. On the **Domains** page, click **More** > **Copy Configuration** in the **Operation** column of the row containing the source domain name. On the displayed page, click the **To New Domains** tab.
   - The copy operation cannot be paused. You can modify the configuration items after the copy is complete.
   - You can copy configuration items listed in **Configuration Items That Can 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.

   Figure 4-6 Copying configurations to new domain names

4. Enter the domain names to be added and click **Copy**.
5. In the displayed dialog box, click **OK** to copy the configuration.
6. View the copy progress and results of adding domain names.

Figure 4-7 Results of adding domain names



Configuration Items That Can Be Copied

Table 4-1 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 4-1 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
	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

Category	Item
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
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

4.5 Basic Settings

4.5.1 Overview

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

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

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

4.5.2 Modifying the Service Type

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

Precautions

- 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 a domain name with special configurations cannot be changed.

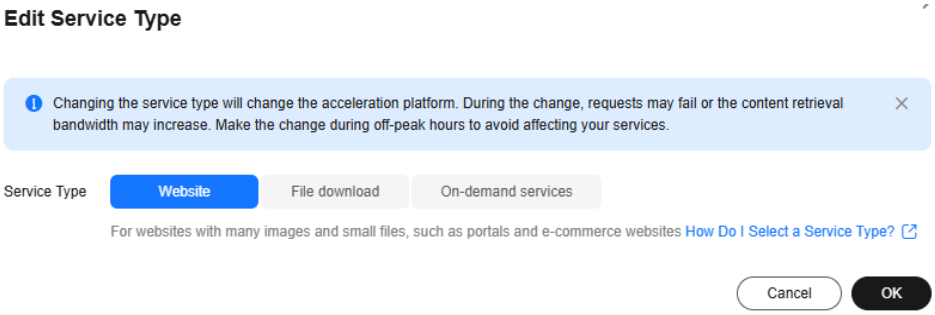
Procedure

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 list, click the target domain name or click **Configure** in the **Operation** column.
4. On the **Basic Settings** tab, click **Edit** next to **Service Type**. The **Edit Service Type** dialog box is displayed.

Figure 4-8 Changing the service type



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

4.5.3 Modifying the Service Area

You can change the service area of a domain name on the CDN console.

Precautions

- 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 list, click the target domain name or click **Configure** in the **Operation** column.
4. On the **Basic Settings** tab, click **Edit** next to **Service Area**. The **Change Service Area** dialog box is displayed.

Figure 4-9 Changing the service area

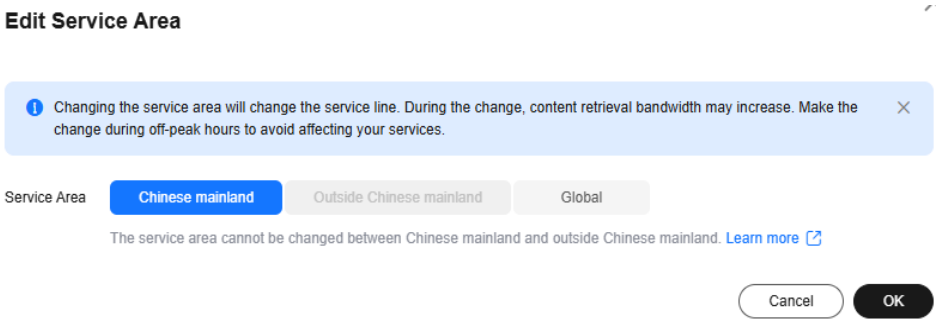


Table 4-2 Parameter description

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 for this domain name from the MIIT.

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

4.5.4 Modifying Origin Server Settings

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

CDN Origin Pull Mechanism

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

Precautions

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

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Basic Settings** tab.
5. In the **Origin Server Settings** area, click **Edit**.
6. Click **Add** below the origin server list. The **Add Origin Server** drawer is displayed.

Figure 4-10 Adding an origin server

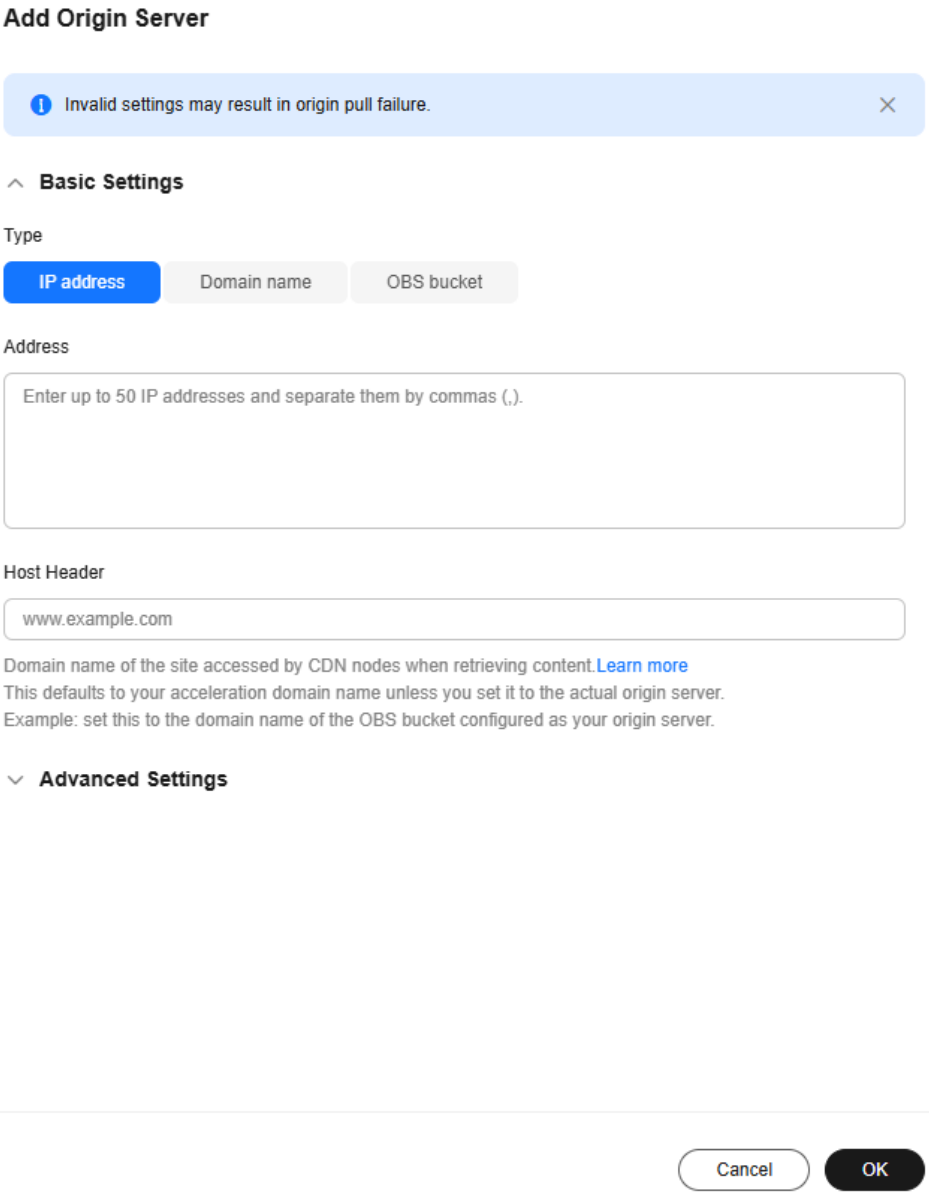


Table 4-3 Parameter description

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

Parameter	Description
	Domain name • The origin domain cannot be the same as the acceleration domain name. Otherwise, user requests will be repeatedly resolved to CDN PoPs, and CDN PoPs will not be able to obtain content from the origin server. • An origin domain starts with a letter or digit and contains up to 255 characters, including letters, digits, hyphens (-), and periods (.). • Each label of a domain name (for example, ***** in ***.***.com**) can contain up to 63 characters. • You can also enter the domain name of an object storage bucket in this field. Pay attention to the following points when selecting this option: 1. You cannot use **private object storage buckets** as origin servers when you set **Type** to **Domain name**. 2. If you use an object storage bucket as your origin server, the object storage service will charge the origin pull traffic based on its billing standards. 3. 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. 4. If you use an OBS bucket created after January 1, 2022 as the origin server and want to enable online preview, log in to the CDN console, choose **Domains** in the navigation pane, click the target domain name, click the **Advanced Settings** tab, click **Edit** next to **HTTP Headers**, and set **Content-Disposition** to **inline**. For details, see **How Do I Preview OBS Objects in My Web Browser?**

Parameter	Description
	OBS bucket You can select the domain name of an OBS bucket under your account or customize one (OBS bucket under other Huawei Cloud accounts). 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**. **Important notes:** 1. If your OBS private bucket is unsuitable as an origin for your domain name, do not set the private bucket as the origin server. 2. If you enter a domain name of an OBS bucket, the origin domain name must end with .myhuaweicloud.com or .myhuaweicloud.cn. 3. If you set an OBS private bucket as the origin server and want to filter user requests, enable **OBS authorization** and **OBS Pull Authentication**. 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, a full list of 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. 7. When **Service Type** is set to **Whole site**, the origin server type cannot be set to **OBS bucket**. 8. If the origin server is an OBS private bucket, when a client requests the homepage of the acceleration domain name and origin pull is triggered, origin pull can succeed only when the request method is GET or HEAD. For other request methods, CDN blocks the request and returns status code 403. **NOTE** If you use an OBS bucket created after January 1, 2022 as the origin server and want to enable online preview, log in to the CDN console, choose **Domains** in the navigation pane, click the target domain name, click the **Advanced Settings** tab, click **Edit** next to **HTTP Headers**, and set **Content-Disposition** to **inline**. For details, see **How Do I Preview OBS Objects in My Web Browser?**

Parameter	Description
Address	Address accessed by CDN PoPs during origin pull. If the origin server type is IP address, you can enter multiple IP addresses and separate them with commas (,). Each IP address is an origin server. A domain name can have up to 50 origin servers. The number of IP addresses you can enter cannot exceed the total number of available origin servers of the domain name.
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**.
OBS Pull Authentication	Applies when an OBS bucket is used as an origin server. Enable this switch if access to the bucket requires authentication. In this way, CDN PoPs carry the authentication information during origin pull. If the information does not match the OBS bucket, origin pull fails, preventing unauthorized traffic theft. • Enabled by default for a private bucket • Disabled by default for a public bucket
Priority	Enter a number from 1 to 100. A larger number indicates a higher 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. • You can configure up to six rules with unique priorities. **NOTE** On April 10, 2025 (Beijing time), CDN updated the origin server priority function and stopped using the concept of primary and standby origin servers. Currently, the default priorities of the original primary and standby origin servers are as follows: • Primary origin server: 70 • Standby origin server: 30

Parameter	Description
Weight	The value ranges from 1 to 100. A larger value indicates that content is pulled from this origin server more frequently. If there are multiple origin servers with the same priority, the weight determines the proportion of content pulled from each origin server.
Origin Ports	Port numbers for CDN PoPs to pull content. By default, the HTTP port is 80 and the HTTPS port is 443. If **Type** is set to **OBS bucket**, the port numbers cannot be changed.

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.

4.5.5 Modifying the Host Header

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

Background

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

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

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

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

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

 location / {
 root html;
 }
 }
```

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

www.a.com on CDN. If you want CDN to obtain content from the **www.b.com** site, set the host to **www.b.com** on CDN.

Precautions

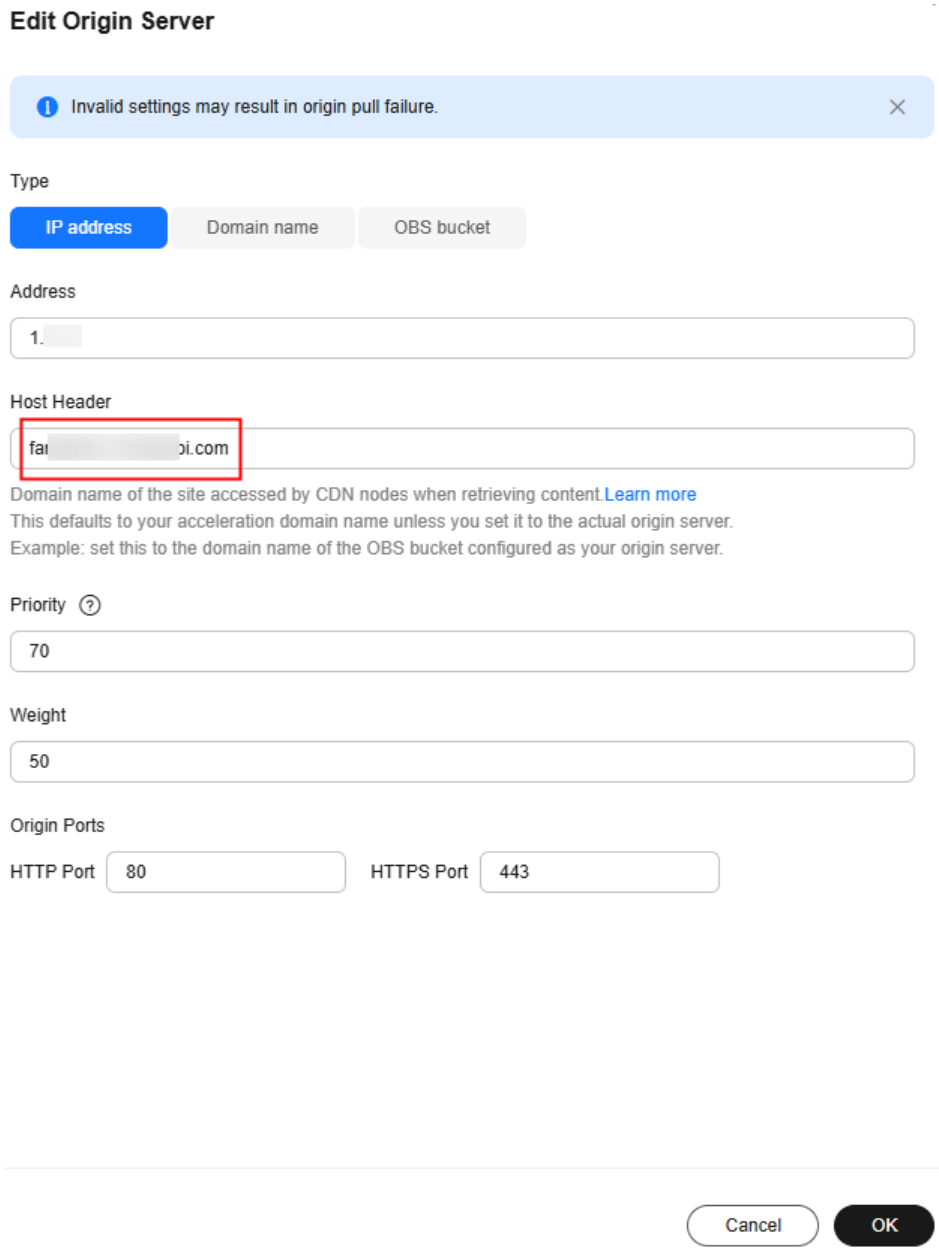
- After a domain name is added, CDN regards it as the host by default. If you do not want CDN to pull content from the acceleration domain name, set a host to specify the location of the requested content.
- If your origin server address is an IP address or a domain name, your host type is the acceleration domain name by default.
- The actual host of a wildcard domain name is the domain name accessed by users, even though the default host is listed as the wildcard domain name itself.
- Do not set the host to a wildcard domain name for an acceleration domain that is not a wildcard domain name, as this will result in an invalid host.
- When a Huawei Cloud OBS bucket is used as an origin server, the bucket's domain name is used as the host by default. To use a custom host, ensure that the host has been added as a **user domain name** of the bucket. Or, bucket access will fail.
- If you set your origin server address as a domain name, and specify the domain name as that of an object storage bucket 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 4-11 Editing the origin server



5. Enter the domain name of the host and click **OK**.

   Each label of a domain name (for example, *** in ***.***.**com**) can contain up to 63 characters.

6. To edit host headers in a batch, click **Edit** above the origin server list.

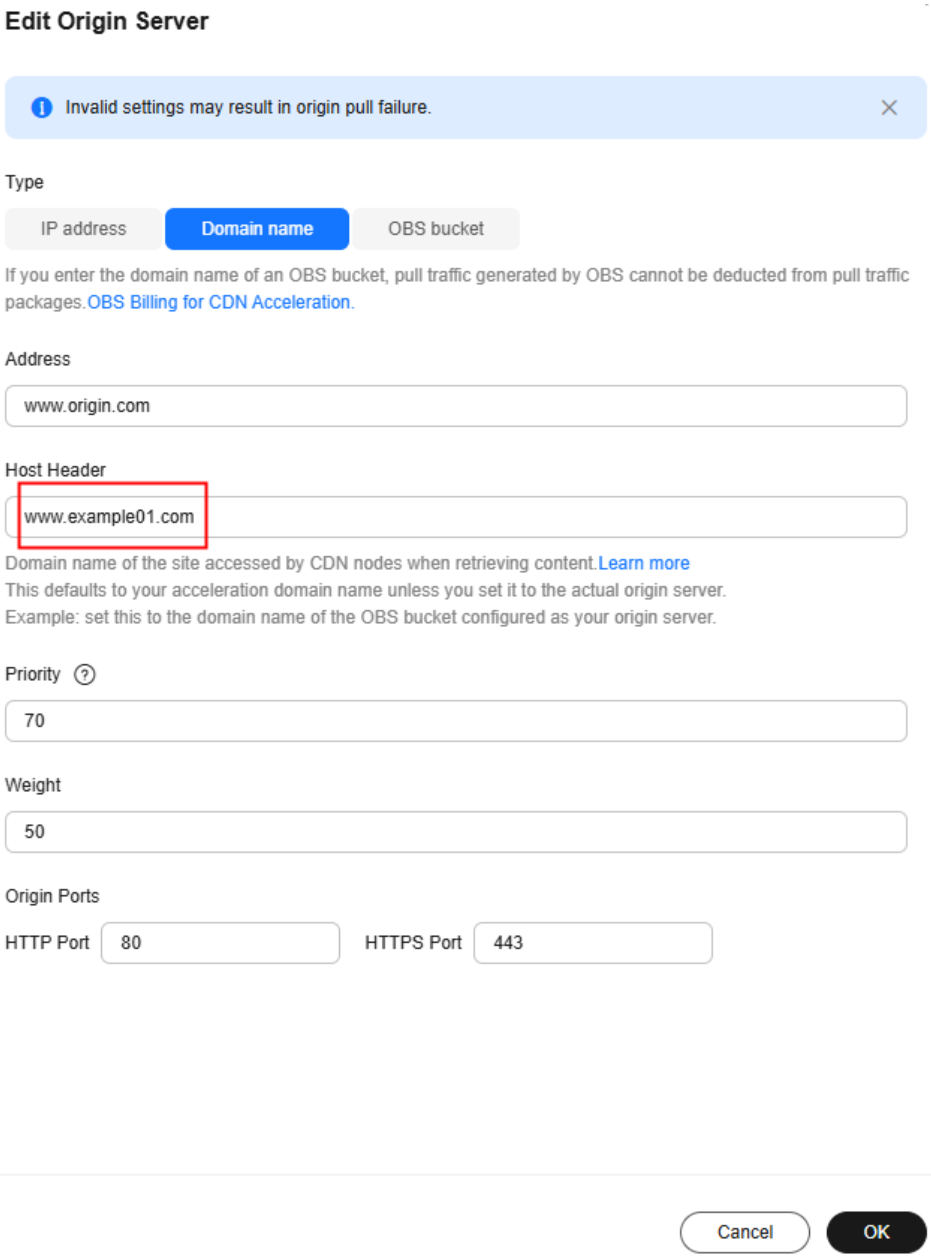
   In the **Host Header** column, modify the information and click **Save**.

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.

4.5.6 Allowing Clients to Access CDN Using IPv6

You can enable IPv6 to allow clients to access CDN PoPs using the IPv6 protocol. Most CDN PoPs support IPv6. After IPv6 is enabled, if a user uses IPv6 to access

CDN but the optimal PoP does not support IPv6, the user can still use IPv4 to access the PoP.

NOTE

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 list, click the target domain name or click **Configure** in the **Operation** column.

   Figure 4-12 IPv6

   NOTE

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

4.6 Origin Settings

4.6.1 Overview

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

CDN Origin Pull Principle

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

Supported Configuration Items

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

Function	Description
Origin Protocol	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, set the SNI to specify the domain to be visited by CDN during origin pull.
Origin URL Rewrite	If the URLs of origin pull requests do not match the origin server URLs, rewrite the request URLs to improve the origin pull hit ratio.
Advanced Origins	Configure advanced origins to allow CDN to pull content of different resource types or paths from different origin servers.
Range Requests	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, 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, enable ETag verification.
Origin Response Timeout	Adjust the origin response timeout based on the features and service scenarios of your origin server.
Origin Request Headers	Rewrite headers in users' request URLs for origin pull.
Dynamic Content Pull Mode	By default, CDN pulls dynamic content from the origin server with the best performance. Choose to pull content from origin servers based on their weights.

4.6.2 Origin Protocol

You can configure the protocol used for origin pull.

Precautions

- By default, CDN uses HTTP for origin pulls.
- If you have enabled **HTTP/2** and set the origin protocol to **Same as user**, CDN uses HTTPS/1.1 for origin pull.

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 4-13 Origin protocol

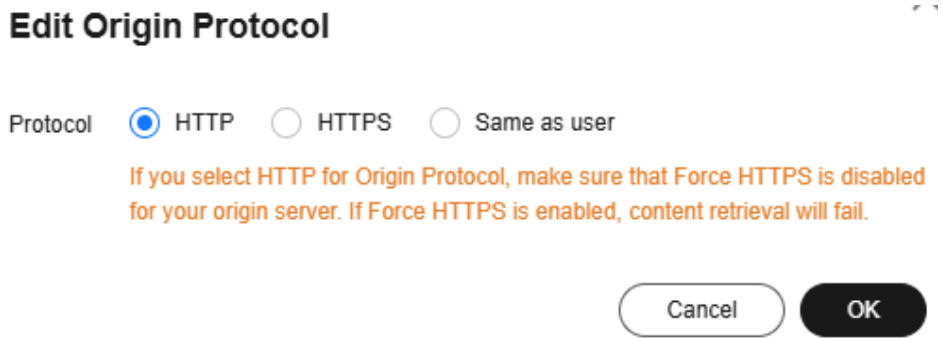


   Table 4-4 Parameter description

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.

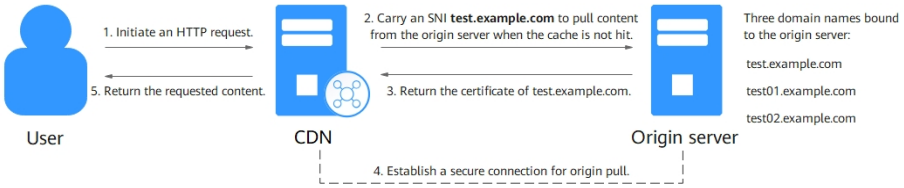
6. Select an origin protocol and click **OK**.

4.6.3 Origin SNI

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

Working Principles

This diagram shows the CDN origin pull process when there is an origin SNI.



1. A user initiates a request.
2. The CDN PoP cache is not hit. The PoP carries SNI test.example.com to pull content from the origin server.
3. The origin server returns the certificate of domain name test.example.com to the PoP.
4. The PoP receives the certificate and sets up a secure connection with the origin server.
5. The PoP receives content from the origin server, returns it to the user, and caches it.

Constraints

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

Procedure

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

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

Figure 4-14 Origin SNI

Table 4-5 Parameters

Parameter	Description
Origin SNI	Origin domain name to be accessed by CDN during origin pull, for example, **test.example.com**. • Wildcard domains are not supported. • The value contains up to 75 characters, including letters, digits, hyphens (-), and periods (.). It cannot start with a hyphen (-) or period (.). • Each label of a domain name (for example, ***** in ***.***.com**) can contain up to 63 characters.

6. Click **OK**.

4.6.4 Origin URL Rewrite

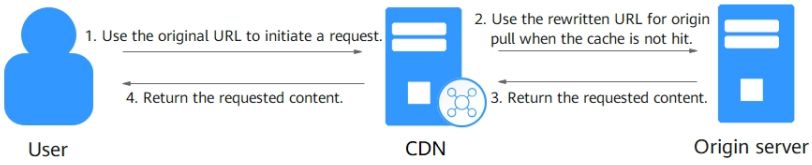
If the URLs of origin pull requests do not match the origin server URLs, origin pull fails. You can rewrite origin URLs to origin server URLs, improving the origin pull hit ratio.

Scenarios

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

Working Principles

This diagram shows the origin pull process when a user request matches an origin URL rewrite rule.



1. A user requests content from a PoP. The request does not hit the cache, but its original URL, for example, example.com/test/index.html, matches an origin URL rewrite rule.
2. The PoP uses the rewritten URL, for example, example.com/newtest/index.html, to send a request to the origin server.
3. The origin server returns the content to the PoP.
4. The PoP caches the content and sends it to the user.

Constraints

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

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 4-15 Rewriting origin URLs

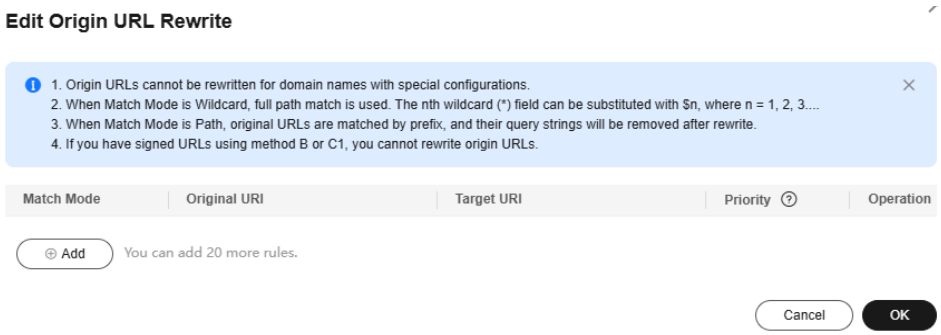


Table 4-6 Parameter description

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

Parameter	Description
	Full path: Rewrites the entire URL. The original URI must be a specific path, for example, **/test/01/abc.mp4**.
Original URI	URI to be rewritten. • A URI starts with a slash (/) and does not contain **http://**, **https://**, or the domain name. • A URI contains up to 512 characters. • Wildcards (*) are supported, for example, **/test/*/*.mp4**. • When **Match Mode** is **Path**, 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.

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

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.

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

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.

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

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.

Match Mode	Original URI	Target URI	Priority
Wildcard	/*.html*	/thread0/$1.html$2	1

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**

4.6.5 Advanced Origins

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

Differences Between Advanced and Basic Origin Servers

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

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

Constraints

- You can configure up to 20 rules.
- 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.

Precautions

When CDN pulls content, **the origin server provider charges the bandwidth or traffic fees generated by the origin server**. For example, the traffic generated when CDN pulls content from OBS is charged by OBS.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. In the **Advanced Origin** area, click **Edit**.
6. Click **Add** to add an advanced origin rule

Figure 4-16 Advanced origins

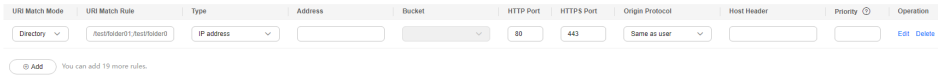


Table 4-7 Parameter description

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

Parameter	Description
Address	**IP address** • Enter an IPv4 address. **Domain name** • Start with a letter or digit. Enter up to 255 characters, including letters, digits, hyphens (-), and periods (.). • Each label of a domain name (for example, ***** in ***.***.com**) can contain up to 63 characters. • Third-party public object storage buckets can be accessed using their domain names. **OBS bucket** • Only OBS buckets of the current account can be accessed. • To access OBS private buckets, allow CDN to read OBS private buckets. For details, see **OBS Authorization**. **NOTE** You cannot add an OBS bucket if the domain name has special configuration.
HTTP Port	Port number for origin pull using HTTP. • The port number ranges from 1 to 65535. The default port is 80. • If **Type** is set to **OBS bucket**, this parameter cannot be modified.
HTTPS Port	Port number for origin pull using HTTPS. • The port number ranges from 1 to 65535. The default port is 443. • If **Type** is set to **OBS bucket**, this parameter cannot be modified.
Origin Protocol	Protocol used by CDN PoPs to pull content from the origin server. **HTTP**: CDN uses HTTP for origin pull. **HTTPS**: CDN uses HTTPS for origin pull. (Ensure that the origin server supports HTTPS access.) **Same as user**: The origin protocol is the same as the client access protocol. For example, if a client accesses CDN using HTTP, CDN also uses HTTP for origin pull.

Parameter	Description
Host Header	Host information of the advanced origin. For details, see **Modifying the Host Header**. • If **Type** is set to **IP address** or **Domain name**, the host is the acceleration domain name by default. • If **Type** is set to **OBS bucket**, the host is the OBS bucket domain name by default.
Bucket	This parameter is mandatory when **Type** is set to **OBS bucket**. • **Public bucket**: Select this option when the OBS bucket policy is public read or public read and write. • **Private bucket**: Select this option when the OBS bucket policy is private.
Priority	The priority value ranges from 1 to 100. The larger the value, the higher the priority.
Operation	**Delete**: Delete the rule.

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

Examples

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

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

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

4.6.6 Range Requests

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

Background

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

Precautions

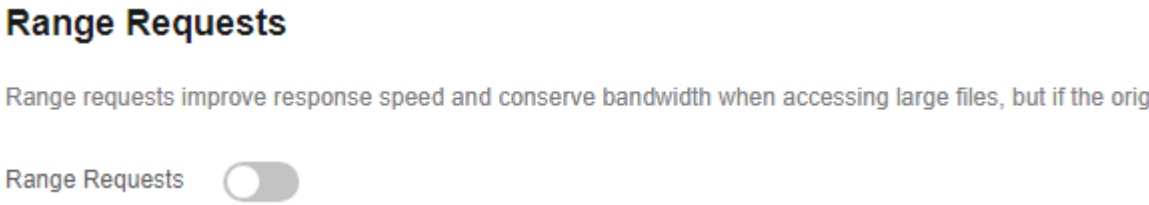
- To enable range requests for origin pull, the origin server must support range requests, that is, requests with the **Range** field in the headers. Otherwise, origin pull may fail.
- By default, range requests are enabled for file download acceleration and on-demand service acceleration.
- If an origin server resource exceeds 1 GB and range requests are not enabled, origin pull for such resource will fail.
- This function does not take effect when a resource requested by a client is not cached on CDN PoPs. CDN will not pull the resource using the range rules set on CDN. In this case, CDN pulls the resource by transparently transmitting the range rules in the client request.
- If a client request contains the **Range** field, the request does not hit the cache, and this function is not enabled on CDN, CDN pulls the complete content from the origin server. As a result, the pull traffic may be greater than the request traffic.
- If the service type of your domain name is whole site acceleration, this function takes effect only for static resources.

Procedure

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

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

   Figure 4-17 Range requests

Examples

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.

4.6.7 Redirect from Origin

Background

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

- Disabled

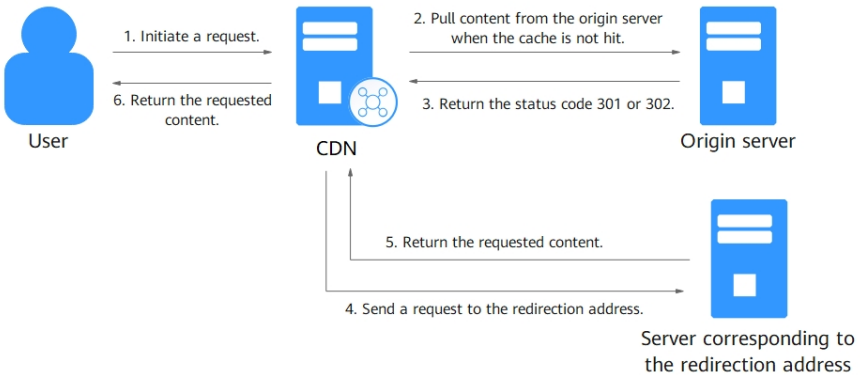
  The CDN PoP returns the redirect address to the user and leaves the user to finish the request process. If the domain name of the redirect address is not added to CDN, the subsequent request process will not be accelerated by CDN.

- Enabled

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

Working Principles

With redirect from origin, if a user request does not hit the cache and a CDN PoP receives status code 301 or 302 during origin pull, the PoP can follow the new address to obtain the content and cache and return it to the user. This diagram shows the detailed process.



1. A user sends a request to a CDN PoP. Assume that the access URL is http://example.com/test/index.html.
2. The request misses the cache. The CDN PoP requests the content from the origin server. Assume that the origin pull URL is http://example.com/test/index.html.
3. The origin server responds with 301 or 302 and includes **http://example.com/newtest/index.html** in the **Location** header.

4. After receiving the response, the PoP sends a request to http://example.com/newtest/index.html.
5. The PoP obtains the content, caches it, and returns it to the user.

Precautions

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

Procedure

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

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

   Figure 4-18 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.

4.6.8 ETag Verification

Background

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

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

If ETag verification is enabled, CDN verifies the **ETag** value. If the values of **ETag**, **Last-Modified**, and **Content-Length** do not change, CDN returns the cached content to the user, reducing the origin pull ratio and relieving the pressure on the origin server. If the value of **ETag**, **Last-Modified**, or **Content-Length** changes, CDN pulls content from the origin server.

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

Precautions

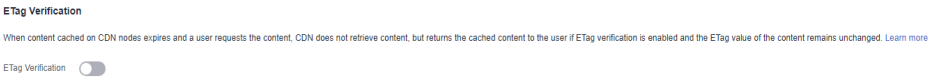
- By default, ETag verification is enabled.
- If range requests are enabled for an acceleration domain name, when the **Last-Modified** values of different segments of an origin resource pulled by CDN PoPs are different, CDN determines that the resource has changed. To avoid returning incorrect resources to clients, CDN interrupts the connection and client access. If similar problems occur, take the following measures:
  a. Disable **range requests**.
  b. If resource segments are stored on different origin servers, move them to the same origin server.
  c. Submit a service ticket to disable the verification of the **Last-Modified** value during origin pull.
- If the service type of your domain name is whole site acceleration, this function takes effect only for static resources.

Procedure

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

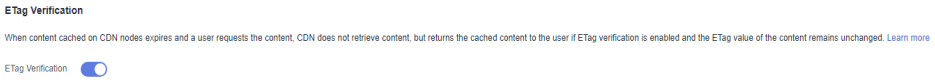
   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Origin Settings** tab.
5. Configure **ETag Verification** as required.

   Figure 4-19 ETag verification



Examples

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



Configuration result: 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.

4.6.9 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

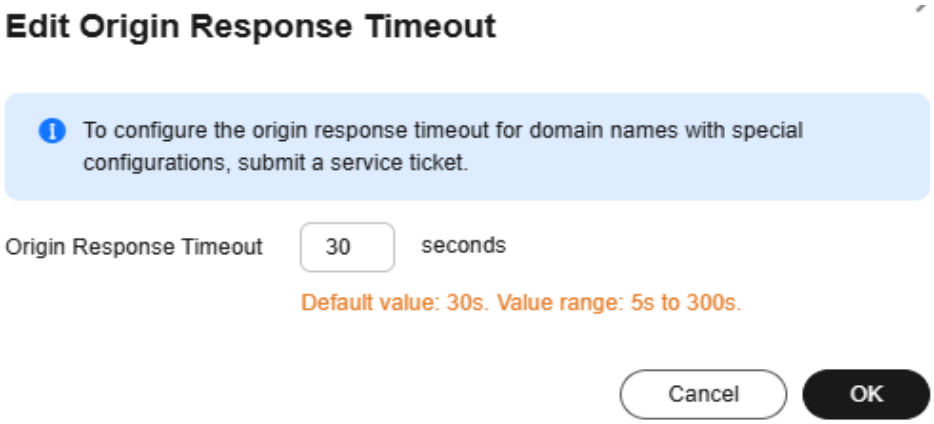
To modify the origin response timeout interval for domain names with special configurations, submit a service ticket.

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 4-20 Origin response timeout



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

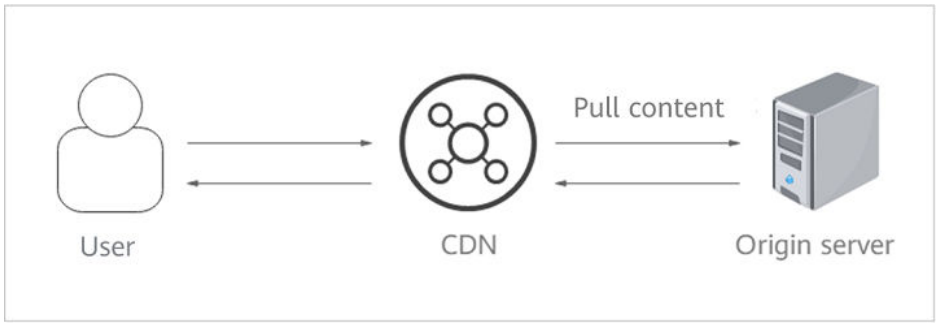
4.6.10 Origin Request Headers

You can configure HTTP headers in origin pull URLs.

Background

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

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



Precautions

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

Procedure

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

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

Figure 4-21 Adding an origin request header

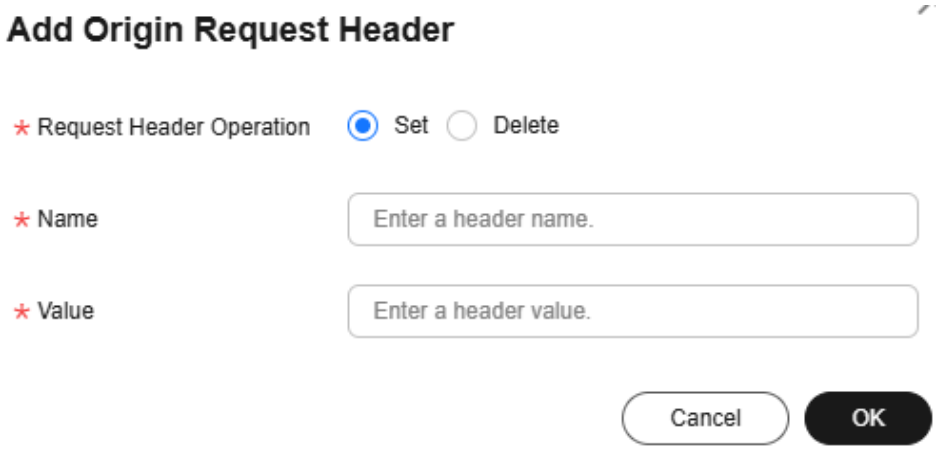


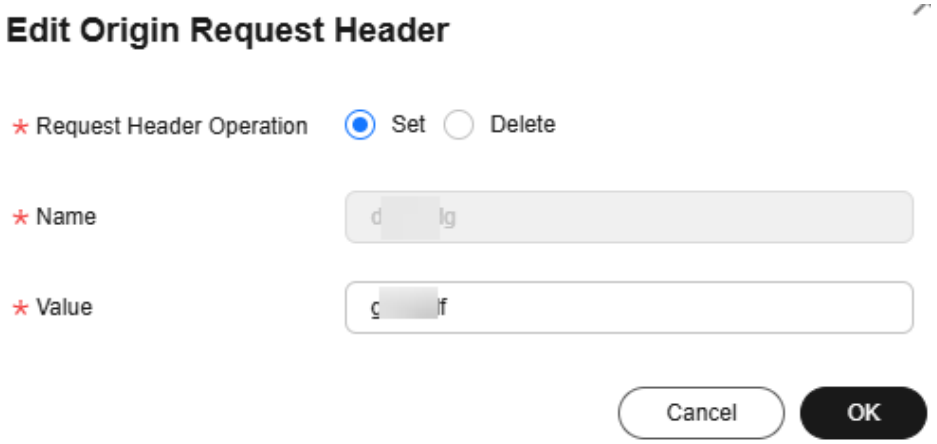
Table 4-8 Parameter description

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.

Parameter	Example	Description
	Delete	Delete the HTTP header that exists in a user request URL. ● If a request URL contains the **X-test** header, it will be deleted during origin pull.
Name	X-test	● Enter 1 to 100 characters. ● Start with a letter and use only letters, digits, and hyphens (-).
Value	aaa	● Enter 1 to 1,000 characters. ● Use only letters, digits, and these special characters: .-_*#!&+|^~'"/::,=@?<>${} ● ${ and } must be used in pairs. ● Supported variables: – **${arg_*xxx*}**: obtains the value of request parameter *xxx*. *xxx* can contain letters, digits, hyphens (-), underscores (_), periods (.), and tildes (~). *xxx* is case sensitive. That is, **${arg_test}** and **${arg_TEST}** are different. – **${http_*xxx*}**: obtains the value of request header *xxx*. *xxx* can contain letters, digits, underscores (_), and periods (.). – *xxx* is case insensitive. That is, **${http_test}** and **${http_TEST}** are the same. – To obtain the value of request header *xxx* using a variable, replace the hyphen (-) with an underscore (_) when configuring the request header. For example, to obtain the value of request header **X-CCDN-Test**, set this parameter to **${http_X_CCDN_Test}**. – **${request_method}**: obtains the request method. – **${host}**: obtains the acceleration domain name. – **${remote_addr}**: obtains the client IP address. ● You can concatenate variables, such as **${host}and${arg_name}**, but you cannot nest them, such as **${${host}}**.

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

Figure 4-22 Editing an origin request header



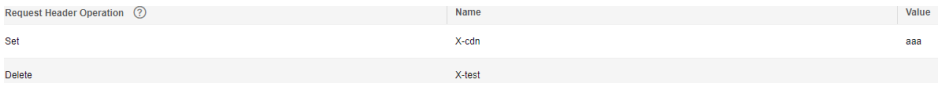
Parameter	Example	Description
Request Header Operation	Set	Add a specific header to an HTTP request of origin pull. • If a request URL contains the **X-test** header and its value is **111**, CDN will set **X-test** to **aaa** during origin pull. • If a request URL does not contain the **X-test** header, 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.

Parameter	Example	Description
Value	aaa	• Enter 1 to 1,000 characters. • Use only letters, digits, and these special characters: .-_*#!&+|^~'"/:;,=@?<>$%{} • ${ and } must be used in pairs. • Supported variables: – **${arg_name}**: obtains the value of request parameter **name** (changeable). – **${http_name}**: obtains the value of request header **name** (changeable). – **${request_method}**: obtains the request method. – **${host}**: obtains the acceleration domain name. – **${remote_addr}**: obtains the client IP address. • Variables can be concatenated but cannot be nested. For example, **${host}and${arg_name}** is supported, but **${${host}}** is not.

  - **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**.

Examples

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



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

Constraints

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

Expires	Content-Disposition

Content-Type	Content-Language
Cache-Control	-

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

a_dynamic	cross-origin-embedder-policy	origin	strict-transport-security
accept	cross-origin-opener-policy	ping-from	te
accept-ch	cross-origin-resource-policy	ping-to	timing-allow-origin
accept-charset	date	pragma	tk
accept-ch-lifetime	device-memory	proxy-authenticate	trailer
accept-push-policy	dnt	proxy-authorization	transfer-encoding
accept-ranges	dpr	public-key-pins	upgrade
accept-signature	early-data	public-key-pins-report-only	upgrade-insecure-requests
access-control-allow-credentials	etag	push-policy	vary
access-control-allow-headers	expect	range	via
access-control-allow-methods	expect-ct	referer-policy	viewport-width
access-control-allow-origin	feature-policy	report-to	warning
access-control-expose-headers	forwarded	retry-after	width
access-control-max-age	from	save-data	www-authenticate
access-control-request-headers	host	sec-fetch-dest	x-client-ip
access-control-request-method	if-match	sec-fetch-mode	x-content-type-options
age	if-modified-since	sec-fetch-site	x-dns-prefetch-control

allow	if-none-match	sec-fetch-user	x-download-options
alt-svc	if-range	sec-websocket-accept	x-firefox-spdy
authorization	if-unmodified-since	sec-websocket-extensions	x-forwarded-for
clear-site-data	keep-alive	sec-websocket-key	x-forwarded-host
connection	large-allocation	sec-websocket-protocol	x-frame-options(xfo)
content-dpr	last-event-id	sec-websocket-version	x-permitted-cross-domain-policies
content-encoding	last-modified	server	x-pingback
content-length	link	server-timing	x-powered-by
content-location	location	service-worker-allowed	x-requested-with
content-range	max-age	signature	x-robots-tag
content-security-policy	max-forwards	signed-headers	x-ua-compatible
content-security-policy-report-only	nel	sourcemap	x-xss-protection

4.6.11 Dynamic Content Pull Mode

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

Precautions

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

Procedure

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

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

4. Click the **Origin Settings** tab.
5. In the **Dynamic Content Pull Mode** area, click **Edit**.

Figure 4-23 Dynamic content pull mode

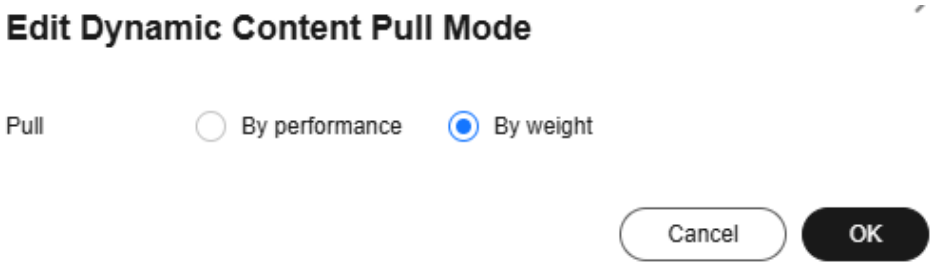


Table 4-9 Parameters

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

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

4.7 HTTPS Settings

4.7.1 Overview

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

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

Function	Description
SCM Authorization	An SCM agency is required for SCM certificate configuration, so that you can directly obtain the certificate content when configuring SCM certifications in CDN.
Configuring an HTTPS Certificate	Add a certificate on CDN PoPs to allow clients to access PoPs using HTTPS.

Function	Description
HTTPS Certificate Requirements	Learn how to combine and upload certificates issued by different authorities.
HTTPS Certificate Format Conversion	Convert certificates in other formats to the PEM format that CDN supports.
TLS Versions	Enable or disable Transport Layer Security (TLS) versions as required.
OCSP Stapling	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	Configure force redirect to HTTP or HTTPS for requests from clients to CDN PoPs.
HSTS	Configure HSTS to force clients (such as browsers) to use HTTPS to access your server, improving access security.
HTTP/2	Understand the background and advantages of HTTP/2.
QUIC	Configure the QUIC protocol to improve transmission security, reduce transmission and connection latency, and prevent network congestion.
Client Certificates	Configure a client certificate to enforce mutual certificate authentication between clients and CDN PoPs, securing website communication.

4.7.2 SCM Authorization

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

CAUTION

Do not delete the agency for authorizing CDN to access CCM. Otherwise, CDN cannot obtain certificate content when you configure HTTPS certificates.

Constraints

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

Associated Cloud Service	Permission
IAM	• Listing permissions: **iam:roles:listRoles** • Creating a custom policy: **iam:roles:createRole** • Listing agencies: **iam:agencies:listAgencies** • Creating an agency: **iam:agencies:createAgency** • Granting global service permissions to an agency: **iam:permissions:grantRoleToAgencyOnDomain**
CDN	• Changing the billing option: **cdn:configuration:modifyChargeMode** • Granting CDN read-only permissions: **CDN ReadOnlyAccess**
SCM	Listing certificates: **scm:cert:list**

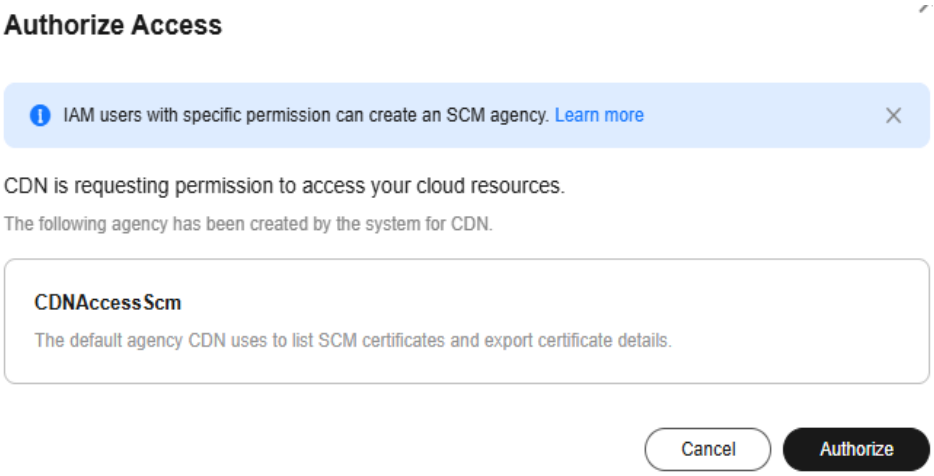
2. After creating an agency, IAM users can configure certificates for domain names when they have the following permissions.
   - Modifying HTTPS settings: **cdn:configuration:modifyHttpsConf**
   - Modify origin pull settings: **cdn:configuration:modifyOriginConfInfo**

Enabling SCM Authorization

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the upper right corner of the page, click **Enable SCM Authorization**.

Figure 4-24 Cloud resource authorization



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

4.7.3 Configuring an HTTPS Certificate

Background

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

- **HTTP**

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

- **HTTPS**

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

Constraints

- CDN supports your own certificates or SSL Certificate Manager (SCM) certificates. The format of your own certificates must meet the requirements described in **HTTPS Certificate Requirements**.
- Only certificates and private keys in PEM format are supported. If a certificate is not in PEM format, convert the certificate by referring to **HTTPS Certificate Requirements**.
- 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 change the certificate type from **International** to **Chinese (SM2)**, **QUIC** should be disabled first.

Precautions

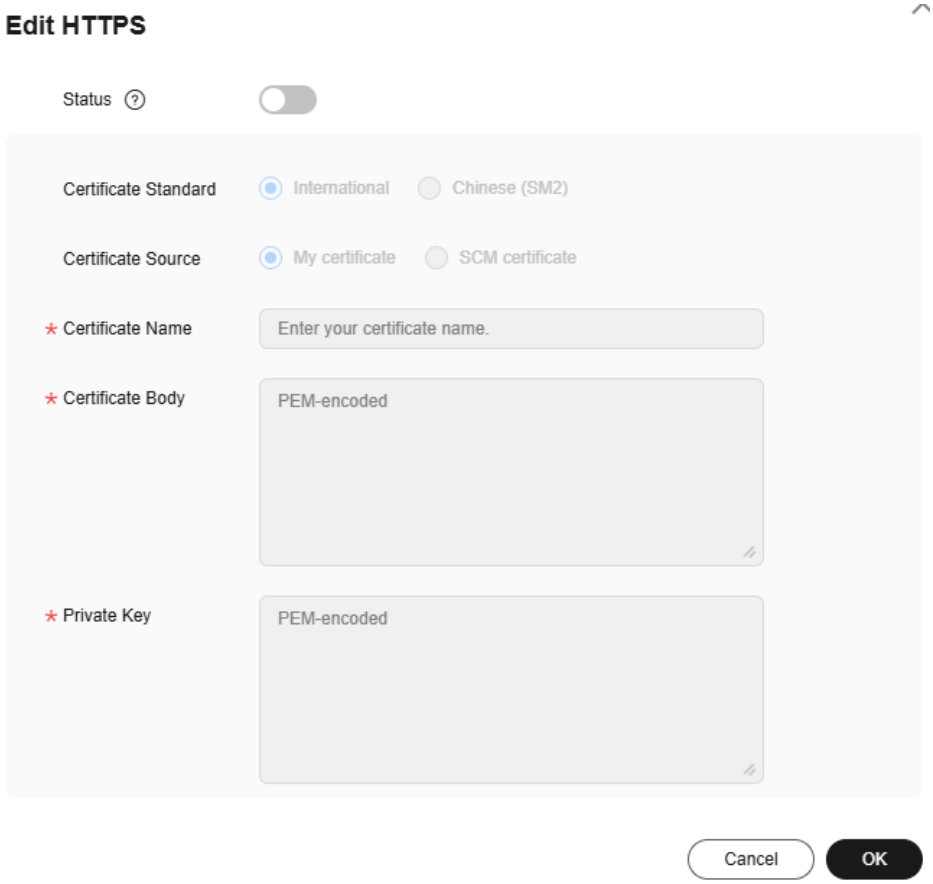
- An acceleration domain name has its associated certificate. They must match. If your domain name is a wildcard domain, configure a certificate for it by referring to **How Do I Configure a Certificate If My Domain Name Is a Wildcard Domain?**
- Certificate settings will be automatically deleted once HTTPS acceleration is disabled. To enable HTTPS acceleration again, you need to re-configure the certificate.
- If your certificate has changed, update certificate information on the CDN console in a timely manner.
  - For details about how to update your own certificate, see **Updating an HTTPS Certificate**.
  - For details about how to use the latest SCM certificate, see **Configuring an HTTPS 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**.
- When HTTPS is disabled, all HTTPS requests from clients cannot complete SSL handshakes and will fail.

Configuring an HTTPS Certificate

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

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

Figure 4-25 Configuring an HTTPS certificate



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

Table 4-10 Parameters of an international certificate

Parameter	Description
Certificate Standard	**International**: SSL certificate that complies with international standards.
Certificate Source	Either **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. • The size of the certificate body cannot exceed 20 KB.
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. • The size of the private key cannot exceed 20 KB.

Table 4-11 Parameters of a Chinese SM series cryptographic certificate

Parameter	Description
Certificate Standard	Chinese (SM2)
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
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. ● The size of the signature certificate cannot exceed 20 KB.
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. ● The size of the signature private key cannot exceed 20 KB.
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. ● The size of the encryption certificate cannot exceed 20 KB.
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. ● The size of the encryption private key cannot exceed 20 KB.

8. (Optional) To set another certificate, click **Add** at the bottom and set related parameters.

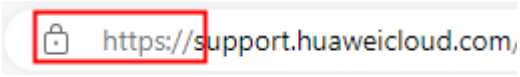
   Standards of the **two certificates** must be different. For example, if you have set an international certificate, you can add a Chinese (SM2) certificate.

9. Click **OK**.

Checking Whether a Certificate Has Taken Effect

A certificate works across the entire network about 5 minutes after it is configured. Then **you can access resources of the acceleration domain name**

via HTTPS and check the website authentication information by clicking in the address box of the browser.



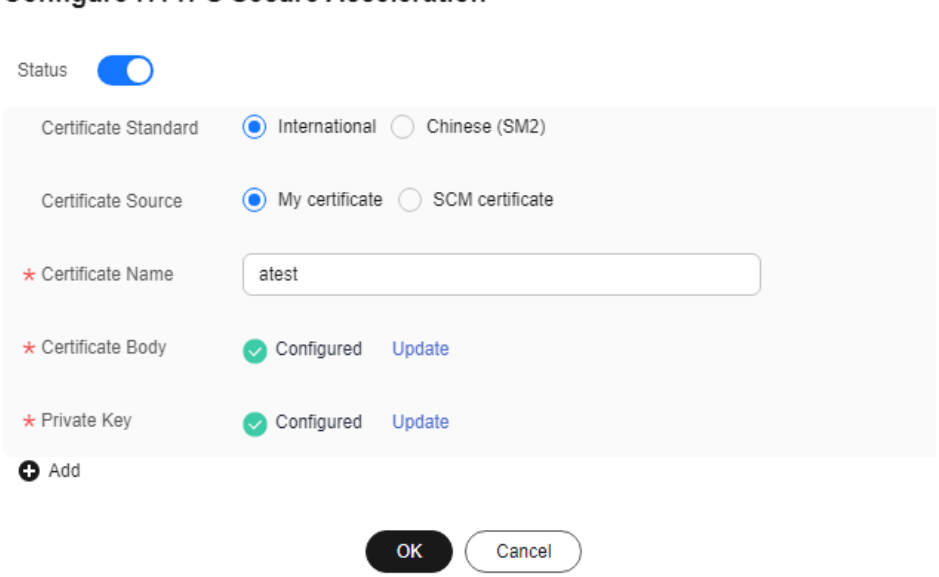
Updating an HTTPS Certificate

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

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

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

   Figure 4-26 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.

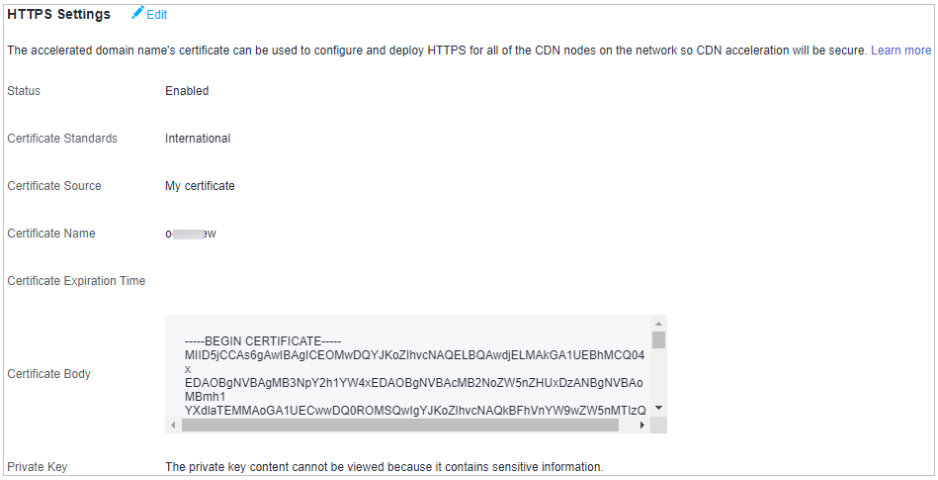
Viewing HTTPS Certificate Information

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.



Disabling a Certificate

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

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

   The **Configure HTTPS Secure Acceleration** dialog box is displayed.
6. Disable the **Status** switch and click **OK**.
   - Disable QUIC before disabling the certificate.

Certificate Expiration Time

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

Huawei Cloud CDN sends an SMS or email notification to the mobile number or email address bound to your account 30 days, 15 days, and seven days before the certificate expires. However, no notification is sent when the domain name is in the disabled, banned, deleting, or reviewing state. 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**. To view the **mobile**

number and email address of the recipient, see **What Are the Parameters and How Can I Use Them in the Account Center?**

Helpful Links

1. **Are Self-Signed HTTPS Certificates Supported?**
2. **Why Is My Domain Name Inaccessible After HTTPS Secure Acceleration Is Configured?**

4.7.4 Configuring a Certificate for a Batch of Domain Names

Background

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

- **HTTP**

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

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

Scenarios

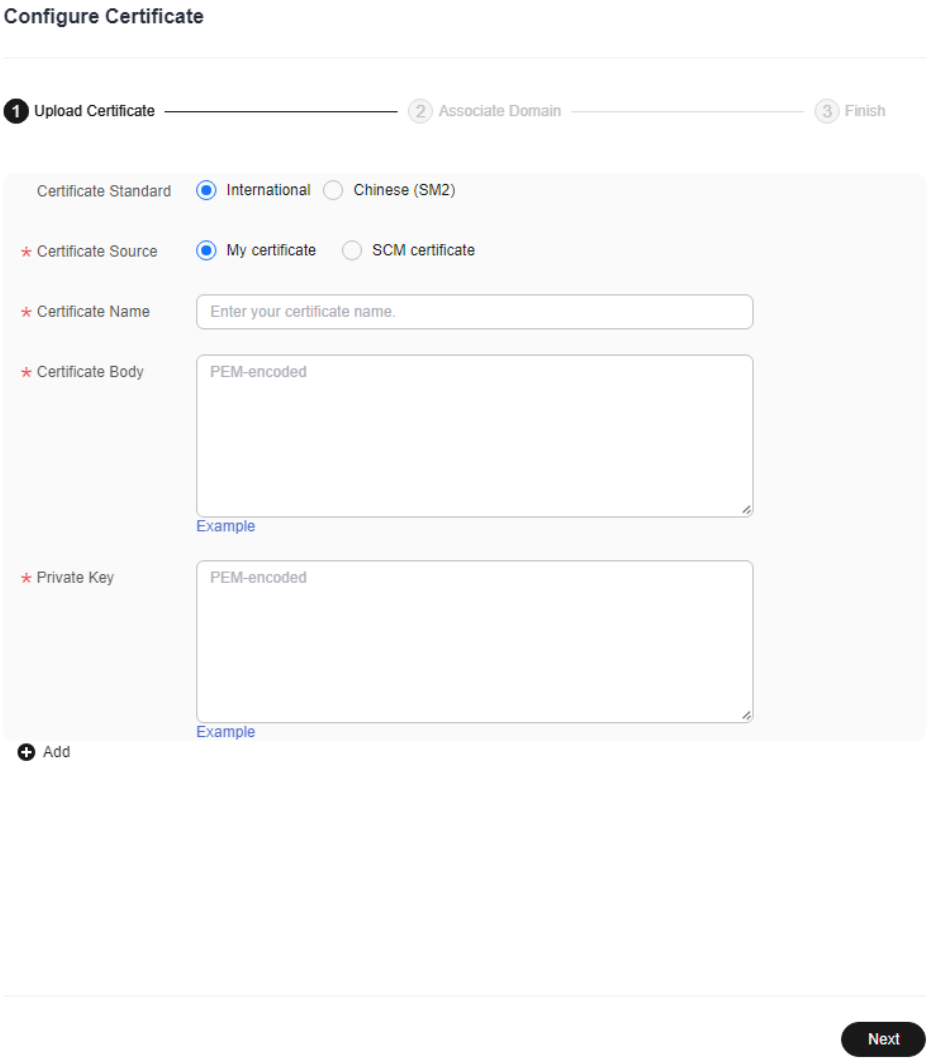
- If you have a certificate, you can directly upload it. You can also view and delete existing certificates.
- You can update certificates in batches. The new certificates will overwrite the original ones.
- You can buy certificates on **CCM**.

Configuring a Certificate

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

   The CDN console is displayed.
2. In the navigation pane, choose **O&M Tools** > **Certificates**.
3. Click **Configure Certificate** in the upper left corner.

Figure 4-27 Configuring a certificate



4. Set related parameters.

Table 4-12 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.

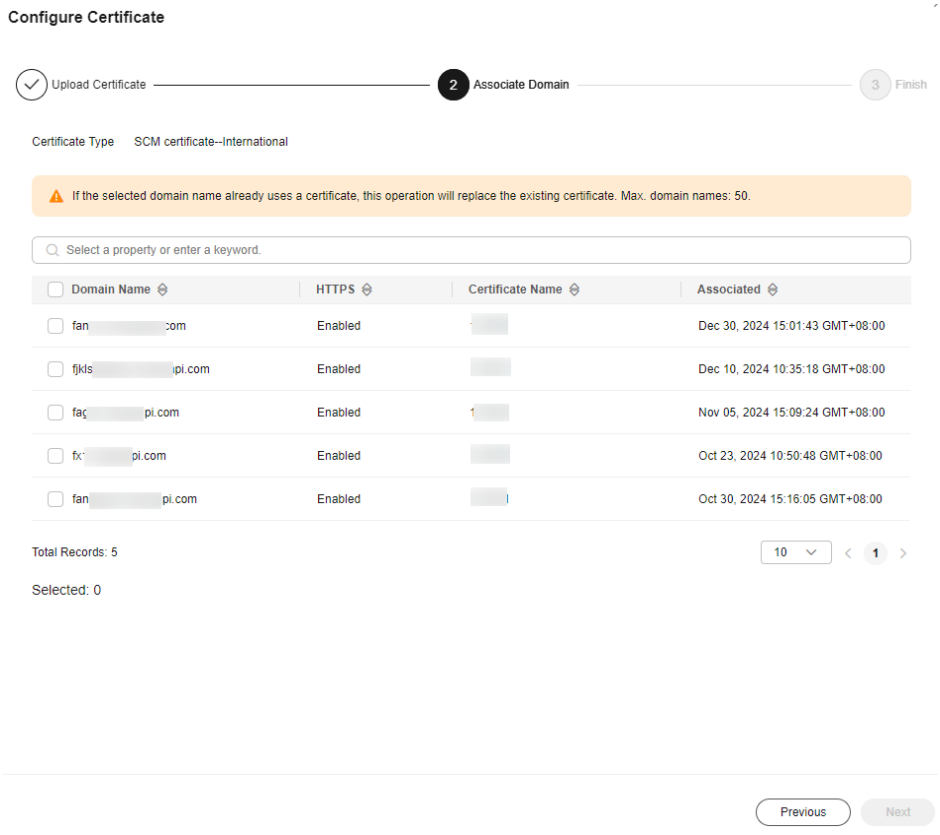
Parameter	Description
Certificate Body	• If you select **My certificate**, use a local text editor to open the certificate and copy the certificate content to the text box. For details about the certificate format, see **HTTPS Certificate Requirements**. • If you select **SCM certificate**, the content 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 4-13 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 domain names to be associated 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.

   The status of delivering the domain certificate configuration is displayed. If the delivery fails, you can rectify the fault based on the cause and submit the certificate configuration task again.

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**.
2. On the displayed drawer, select the certificates to be deleted and click **OK**.

   NOTE

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

4.7.5 HTTPS Certificate Requirements

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

Certificates Issued by Root CA

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

Use a text editor to open the certificate. The certificate content should be something similar to what is in **Figure 4-28**.

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 4-28 PEM certificate

Certificates Issued by Intermediate Agencies

A certificate file issued by an intermediate agency contains several certificates. You need to combine the certificates into a single, complete certificate for upload when configuring HTTPS acceleration. A combined certificate is shown as **Figure 4-29**.

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

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

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

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

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

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

Figure 4-29 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 4-30**.

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 4-30 RSA private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909eYlvLCqow
wEPqs6vyqQM3gKo8qCkNkmS5QgMPOFI4fx2G22mHvT0x8PHjm6GTQDPDniWaIuky
lufqVPD/zqK0oBl2AeAvbzKxWwRqf4JTLa3136B4l5yZVoDjRfU5EKY6LW1sD/00
5uF0qE3td5KQwQc6ZzbnkAof0Oyp5PbMfajM9My2mcvQJzWPLRxET3eWHYdBUtEg
1rxdrWxLheKjENzW3P7Mz/7KycIRxAlurl/Z9s8ytj3l24AQY7NElt1iL9wwA47k
0EumxTaLz8H/vHB1fLMouvYfsSDEr3Snf6eSSwIDAQABAoIBAQDCNmxC3qHXPgvI
EzBOtIPVl1PyzizXWi+U4U6WwUBjCQ6ijfoYOKLaHHnnCEIm4V2N8KV4prAkQjcM
[redacted]
xxrq/vizzNh6K1dBrZKmrWrAqGifkHqx2M3wwssfSzG3WhS0UT1nrUnONg9XLbl5
WeBd2Zp/Fn+tk2T9SsTotAgJAoGAOvmo5APBVRLILHwungLno8ZOYJopOtEPGFDp
v0bHNfgGIrfMcoKIx2xuX5cUe9MihRdyPV8aHYvd4ciE6yOGGq2ypVAt0SSS+TSL
GXJpezX9AjeWtQV8iWoEojIKKPs9FAHftS2aCbXXVJxwR1kbp8clyDxQ9yNNCr7o
OBG9XHECgYEA0xuJhoD8HMmoLJockHeMvHY9DqjcncFLwXyuKORKzRT5SiUy7tDJ
VV8cqljV95gNbae6tUp9zNO7mwlwD2ztjyjDc1gtW+Kpfj7VXImtURHrxKfZflNx
uQ/fbf/zaVpJ7QPcL7y671BGevC/JIZ/i2jBGQkQtn8d4rhk72C1kyw=
-----END RSA PRIVATE KEY-----
```

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

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

FAQ

Why Am I Seeing the "Incomplete certificate chain" Message?

4.7.6 HTTPS Certificate Format Conversion

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

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

- **Converting DER to PEM**
  ```
  openssl x509 -inform der -in old_certificate.cer -out new_certificate.pem
  openssl rsa -inform DER -outform pem -in old_key.der -out new_key.key
  ```
- **Converting P7B to PEM**
  ```
  openssl pkcs7 -print_certs -in old_certificate.p7b -out new_certificate.cer
  ```
- **Converting PFX to PEM**
  ```
  openssl pkcs12 -in old_certificate.pfx -nokeys -out new_certificate.pem
  openssl pkcs12 -in old_certificate.pfx -nocerts -out new_key.key
  ```

You can also use an online third-party certificate conversion tool.

4.7.7 TLS Versions

You can configure TLS versions as required.

Background

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

Table 4-14 TLS versions supported by mainstream browsers

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

Constraints

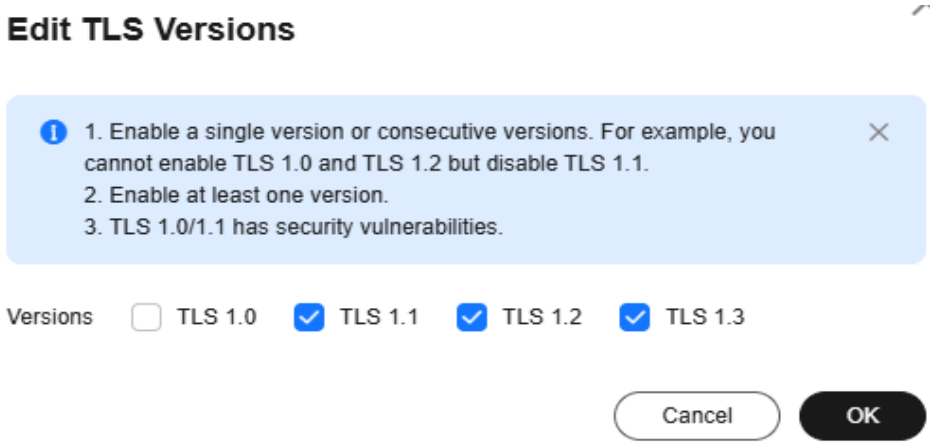
- Before configuring the TLS versions, configure an international HTTPS certificate first. For details, see **Configuring an HTTPS Certificate**.
- If the domain name is bound to a certificate with Chinese cryptographic algorithm, TLS versions cannot be configured.
- If you change the certificate type 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 4-31 Configuring the TLS versions



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

4.7.8 Force Redirect

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

Scenarios

Force redirect to HTTP: If you do not have high security requirements, use 301/302/307 to forcibly redirect all client requests to HTTP.

Force redirect to HTTPS: If you have set a certificate for your domain name on CDN and you pay more attention to security, use 301/302/307 to forcibly redirect all client requests to HTTPS.

Precautions

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

Procedure

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

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

Figure 4-32 Force redirect

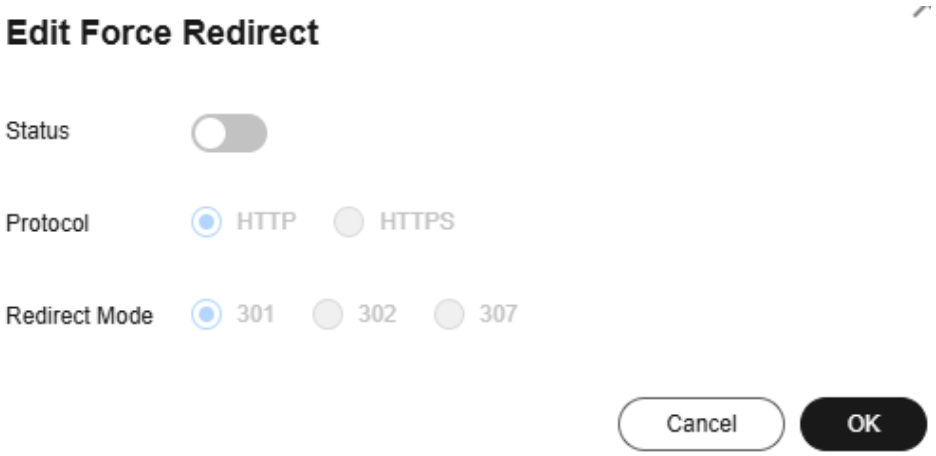


Table 4-15 Parameter description

Parameter	Description
Status	Whether to enable this function. Enabled: Specify whether to redirect requests from clients to HTTP or HTTPS. Disabled: Both HTTP and HTTPS requests from clients are supported.
Protocol	**HTTP**: Requests from clients to CDN PoPs are forcibly redirected to HTTP. **HTTPS**: Requests from clients to CDN PoPs are forcibly redirected to HTTPS.
Redirect Mode	301 302 307

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

4.7.9 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

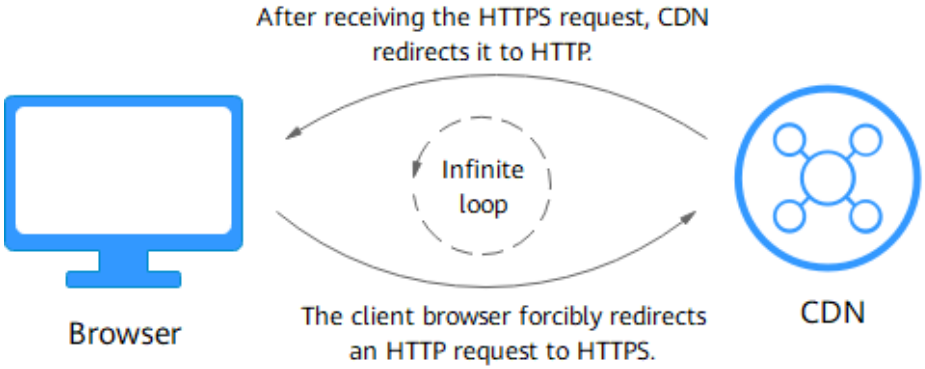
If HSTS is configured on CDN, when a client (such as a browser) uses HTTPS to access a CDN PoP for the first time, the PoP responds to the browser with the **Strict-Transport-Security** header. The browser caches this header if it supports HSTS and uses HTTPS to access CDN PoPs until the cache expires. The structure of the HSTS response header is **Strict-Transport-Security:max-age=expireTime [;includeSubDomains]**. The following table describes the parameters.

Parameter	Description
max-age	Validity period of the HSTS header, in seconds. During this period, clients must use HTTPS for access.
includeSubDomains	(Optional) Enables HSTS for all subdomain names of this domain name.

Precautions

- HSTS is valid when an international HTTPS certificate is configured.
- Use **force redirect** to redirect the first HTTP client request to HTTPS.
- To disable the HTTPS certificate, disable HSTS as well.

- When HSTS is enabled and a browser caches the **Strict-Transport-Security** header, force redirect to HTTP will lead to an infinite loop. As a result, the domain name cannot be accessed.



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

Procedure

1. Log in to **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.
   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **HTTPS Settings** tab.
5. In the **HSTS** area, click **Edit**.
6. Turn on the **Status** switch and set parameters.

Figure 4-33 HSTS

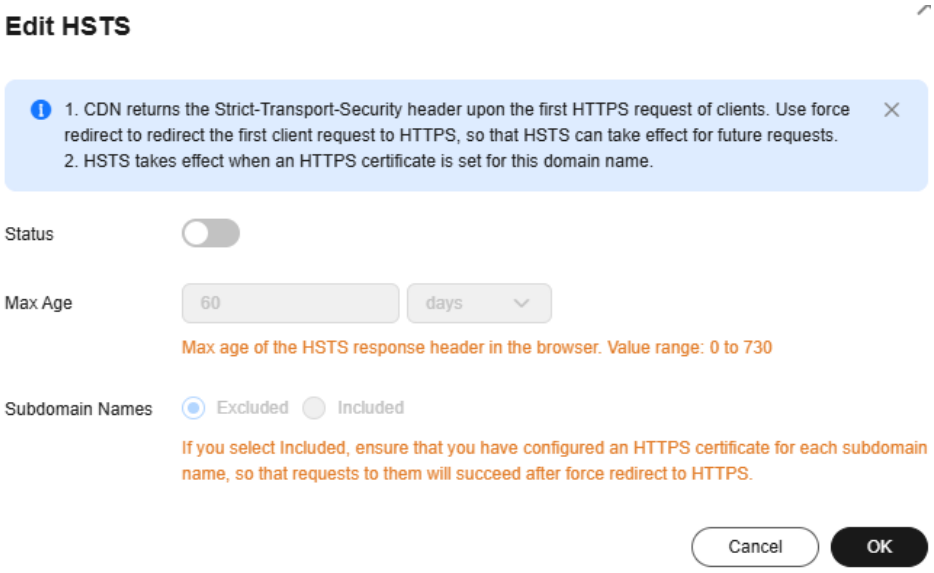


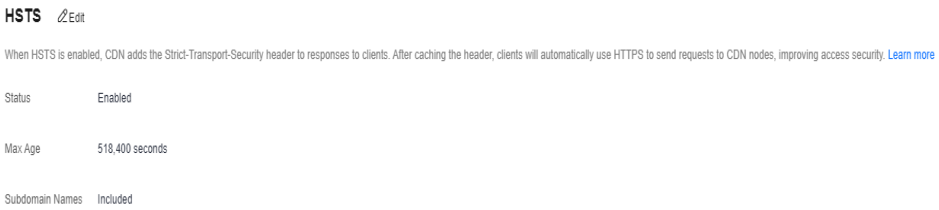
Table 4-16 Parameters

Parameter	Description
Max Age	TTL of the response header **Strict-Transport-Security** on clients. • The value ranges from 0 to 63,072,000, in seconds. • If the TTL is too short, the client cache frequently expires, affecting HSTS. If the TTL is too long and the HTTPS certificate is canceled within the TTL, the domain name cannot be accessed, affecting businesses. The recommended TTL is 5,184,000 seconds, that is, 60 days.
Subdomain Names	Whether to enable HSTS for subdomain names. • **Excluded**: HSTS is disabled for subdomain names. • **Included**: HSTS is enabled for subdomain names. Check whether HTTPS certificates have been configured for all subdomain names. Subdomain names without a certificate cannot be accessed.

7. Click **OK**.

Examples

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



Result:

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

4.7.10 HTTP/2

Background

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

Prerequisites

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

Precautions

- 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.
- 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

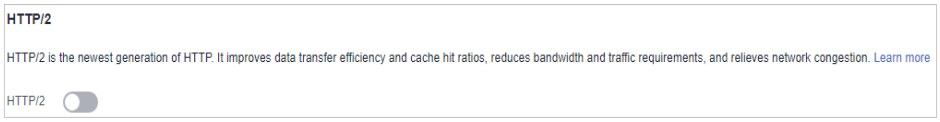
  HTTP/2 multiplexes multiple requests or responses over a single TCP connection. While HTTP/1.1 establishes a TCP connection for each request or response in order. By sending requests concurrently, HTTP/2 lessens the pressure on server connection and alleviates the network blocking problem.

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**.



4.7.11 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.

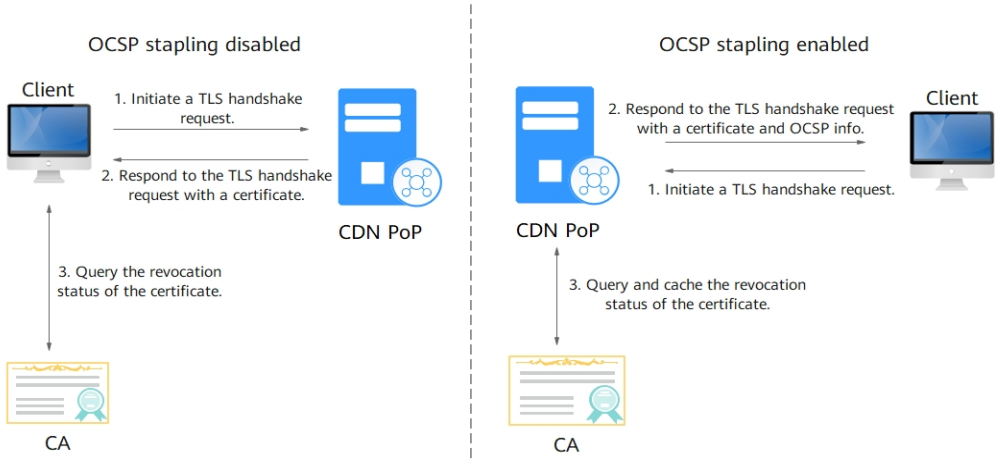
NOTE

By default, OCSP stapling is disabled.

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

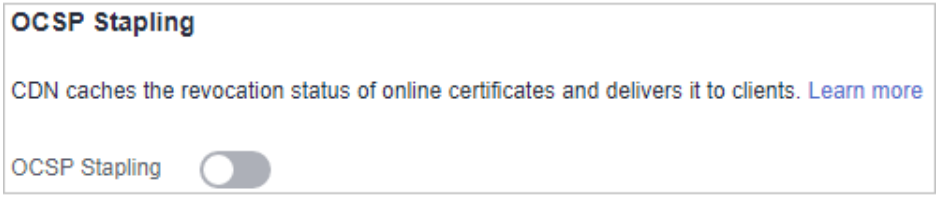
- An international HTTPS certificate has been configured. For details, see **Configuring an HTTPS Certificate**.
  - Disabling the HTTPS certificate will disable OCSP stapling.
  - After configuring the HTTPS certificate, wait about 5 minutes for the configuration to complete and then enable OCSP stapling.
- 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 4-34 OCSP stapling

5. Switch on **OCSP Stapling**.

4.7.12 QUIC

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

What Is QUIC?

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

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

Supported Version

IETF-v1 (H3)

Prerequisites

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

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

Precautions

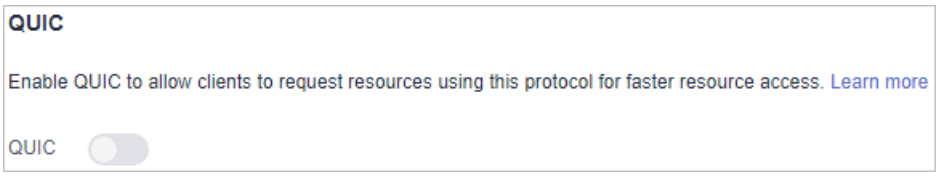
- QUIC cannot be enabled for domain names with special configurations.
- QUIC cannot be used for origin pull.
- This function is in OBT and is available for free trial.
- To change the certificate type from **International** to **Chinese (SM2)**, QUIC should be disabled first.
- If you configure two 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 4-35 QUIC

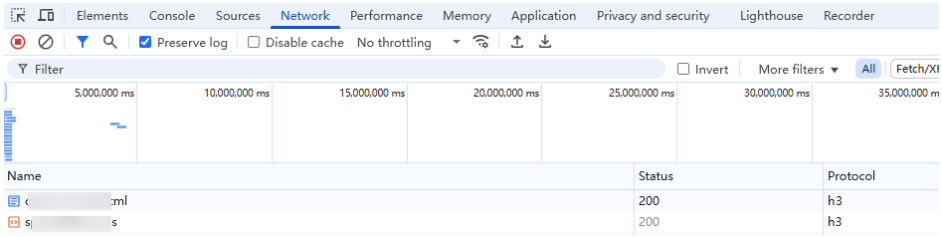
   

How Do I Check Whether a Client Request Uses the QUIC or HTTP Protocol?

After you enable QUIC, clients can use it to access your acceleration domain name. The following uses the Chrome browser as an example to describe how to check the client access protocol.

1. Open the Chrome browser and access the acceleration domain name for which QUIC has been enabled.
2. Press **F12** or right-click the page and choose **Inspect**. Then click the **Network** tab.

   If **h3** is displayed in the **Protocol** column, the request uses QUIC. If the **Protocol** column is invisible, refresh the page, right-click on a resource, and choose **Header Options** > **Protocol**.



4.7.13 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 **Configuring an HTTPS Certificate**.
- You have applied for a client CA certificate.

Precautions

- A client certificate cannot be configured for domain names with special configurations.
- After a client certificate is configured, if the domain name in the SNI of a client request is not the acceleration domain name, the client request may be blocked and status code 403 will be returned.

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 4-36 Configuring a client certificate

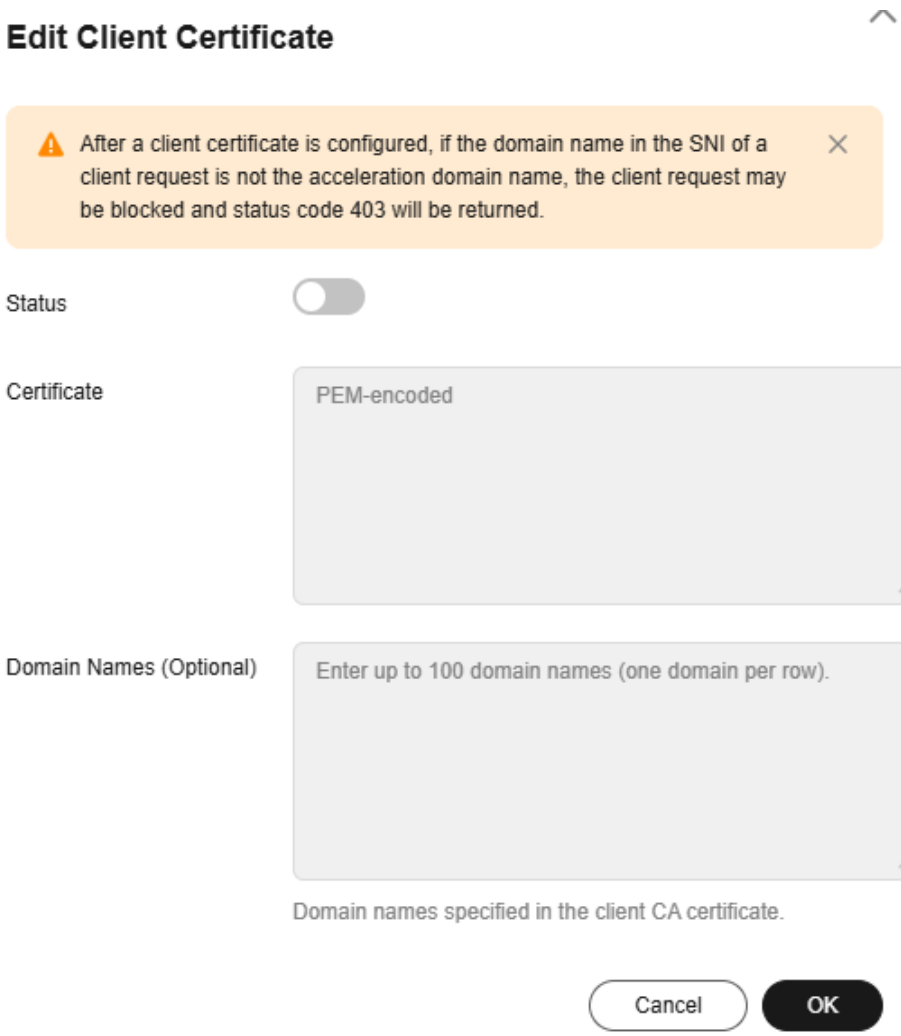


Table 4-17 Parameters

Parameter	Description
Certificate	Content of the client CA certificate. Only the PEM format is supported. • You can configure up to 20 CA certificates. Each certificate chain can contain up to four levels. • The common name (CN) of a certificate must be unique.
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. • If you configure multiple certificates, all certificates share the domain names.

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.

4.8 Cache Settings

4.8.1 Overview

CDN caches origin content on PoPs across the globe so that users can obtain content from nearby PoPs. You can modify rules and relevant settings of caches on CDN PoPs.

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

Function	Description
PoP Cache Rules	Set the cache TTL and priority for different resources to increase the hit ratio and reduce the back-to-source rate.
Browser Cache TTL	Set a browser cache TTL, during which users can obtain content directly from their browser cache (if available), reducing origin pulls.
Status Code Cache TTL	Cache error status codes returned by the origin server to CDN PoPs for a specified TTL. CDN returns the error codes to users when they request resources within this TTL, reducing the origin pull ratio and origin server pressure.
Access URL Rewrite	Set access URL rewrite rules to redirect user requests to the URLs of cached content.
Shared Cache Groups	Configure a shared cache group with a primary domain name to share its cache with other domain names. This improves the cache hit ratio when these domain names host the same resources.

NOTE

If you have modified the cache rules and origin cache control settings,

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

4.8.2 PoP Cache Rules

You can configure the TTL for one or more cached resources on CDN PoPs. If the TTL of a file expires, CDN fetches its latest version from the origin server when a user requests the file. CDN returns the content to the user and caches it on PoPs. You can cache the homepage, all files, or desired content by directory, file type,

and full path. In addition, you can ignore query parameters 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 periods can increase the hit ratio and reduce the origin pull rate, which reduces bandwidth utilization.

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

Precautions

- Up to 60 cache rules can be added to each domain name.
- The cache TTL affects the origin pull rate directly. If the TTL is short, cached content on CDN PoPs becomes invalid in a short time, resulting in frequent origin pulls, which increases the origin server load and prolongs the access latency. However, if the TTL is too long, cached content may be outdated as a result.
- If the TTL is set to 0, CDN pulls content from the origin server for all user requests, which may interrupt the acceleration service.
- Resources cached on PoPs may be deleted due to infrequent access.
- If you have modified a cache rule,
  - Your modifications are effective for new content cached.
  - You can purge to apply modifications to all resources (including the existing PoP cache).

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Cache Settings** tab.
5. In the **Cache Rules** area, click **Edit**. The **Configure Cache Rule** dialog box is displayed.
6. Click **Add** to add a cache rule. **Table 4-18** describes the parameters. You can click **Suggested Rules** to view the recommended configuration.

Figure 4-37 Configuring a cache rule

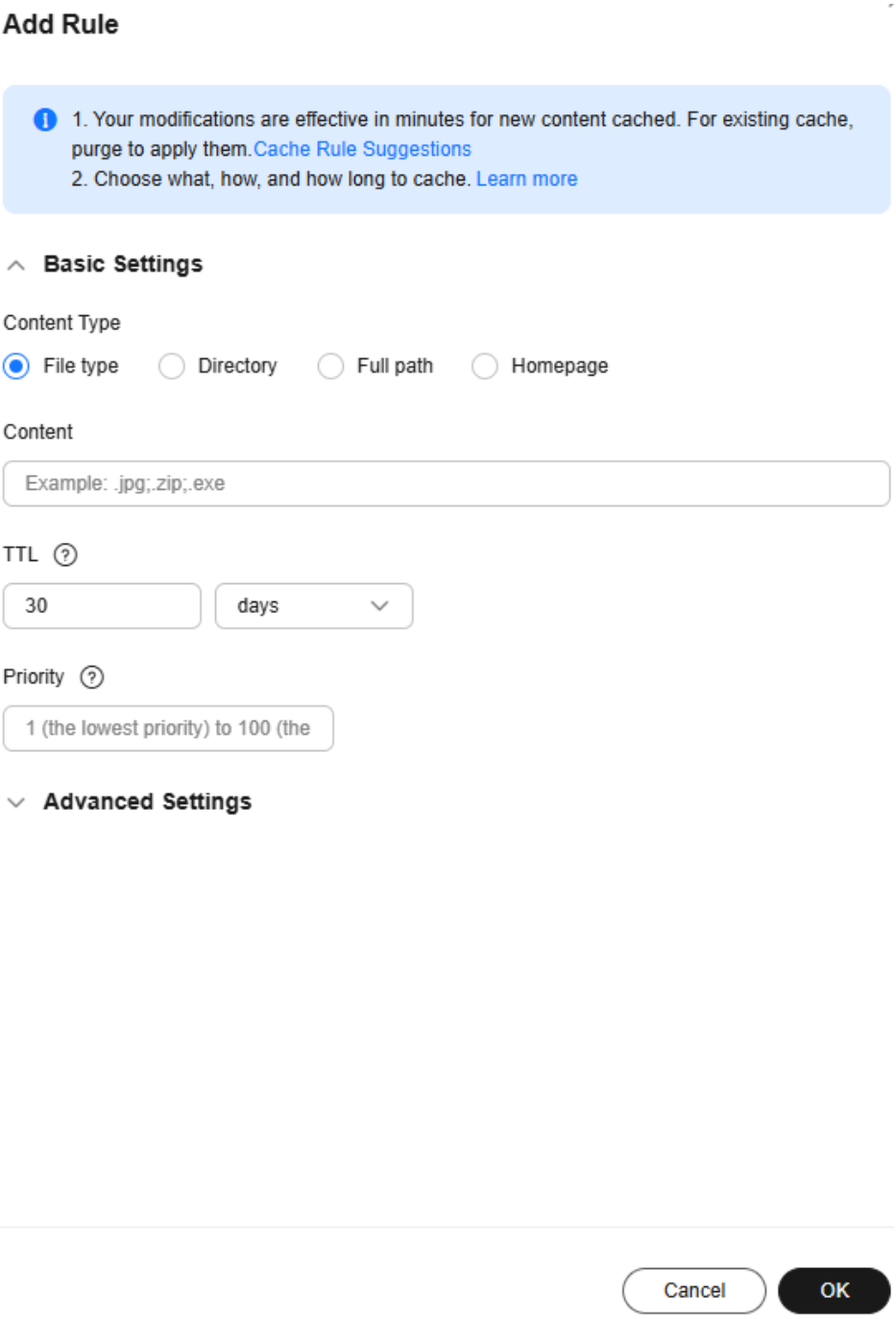


Table 4-18 Cache rule parameters

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 specific types. If the service type of a new domain name is **Website**, **File download**, or **On-demand services** and its origin server type is **IP address** or **Domain name**, CDN adds a rule to it by default. The rule specifies that the cache 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 100 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	Directories are matched by prefix. Start a directory with a slash (/), and separate multiple directories with semicolons (;). Enter up to 20 directories and up to 255 characters. Example: **/test/folder01;/test/folder02** • Wildcard matching is supported. Rules for using wildcards (*): – Only one directory with one wildcard can be set for each rule. Example: **/test/*** – CDN uses prefix match. For example, when the path in a cache rule is **/test/***, **/test/abc** and **/test/abc/001** also use this rule. – Wildcards cannot be set for domain names with special configurations. – Wildcards cannot match slashes (/). For example, **/test/*/abc** cannot match **/test/folder01/folder02/abc**. – A wildcard can match one or more characters but cannot match zero characters. For example, **/test*** cannot match **/test**. – **/*** cannot be set as a path. • You can use consecutive slashes (/) to specify a different path. For example, **/test** and **//test** indicate different paths.

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** and **/test/*.jpg** • You can use consecutive slashes (/) to specify a different path. For example, **/test** and **//test** indicate different paths.
Homepage	Root directory	The root directory of a website is the top-level directory of the website folder, which contains all subfolders of the website. • You can configure only one cache rule for the homepage.
Priority	Priority of a cache rule Each cache rule must have a unique priority. If a resource is specified in multiple cache rules, the rule with the highest priority is applied.	Enter an integer ranging from 1 to 100. A greater number indicates a higher priority.

Parameter	Description	Configuration Rule
TTL	Duration that a file can be cached. If the TTL has reached, CDN pulls the most recent content of the file from the origin server when a user requests the file from a CDN PoP. Then, CDN caches that content on the PoP and serves it to the user.	The TTL of a cached file cannot exceed 365 days. You are advised to set the time according to the following rules: • For static files (such as .jpg and .zip files) that are not frequently updated, set the TTL to more than one month. • For static files (such as .js and .css files) that are frequently updated, set the TTL based on service requirements. • For dynamic content (such as .php, .jsp, and .asp files and dynamic APIs), set the TTL to 0 seconds.
Query Parameters	Most web page requests carry URL parameters starting with a question mark (?). If parameters do not contain important information (such as version), you can ignore them to improve the cache hit ratio and speed up delivery. **Configuration rules:** • If resources do not change with URL parameters, ignore query parameters. • If resources change with URL parameters, retain query parameters. • If you have enabled video seek, set **Query Parameters** to **Ignore all** for your video resources.	• **Retain all**: CDN retains all parameters following the question mark (?). • **Ignore all**: CDN ignores all parameters following the question mark (?) in request URLs, improving the cache hit ratio. • **Ignore specific**: CDN ignores the specified parameters in request URLs but retains other parameters. • **Retain specific**: CDN retains the specified parameters in request URLs but ignores other parameters.
URL Parameters	Parameters to be ignored or retained. Leave this parameter blank when **Query Parameters** is set to **Retain all** or **Ignore all**.	• Enter up to 30 parameter names separated by semicolons (;). • Only letters, digits, periods (.), underscores (_), and tildes (~) are supported.

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

Parameter	Description	Configuration Rule
Forcible Cache	Whether to ignore the **no-cache**, **private**, and **no-store** fields in the **Cache-Control** response header of the origin server. When this function is enabled, these fields are ignored. Forcible cache supplements TTL source. The rules are as follows: 1. When **TTL Source** is set to **Origin server** and **Forcible Cache** is disabled: • If **no-cache**, **private**, or **no-store** is set in the **Cache-Control** response header, CDN PoPs do not cache resources. • If other response headers are set, the priority is **s-maxage** > **max-age** > **expires**. For example, if **Cache-Control: max-age=500, s-maxage=400** is set on the origin server, the cache TTL on CDN PoPs is 400s. • If the preceding response headers are not set, the cache TTL configured on the CDN console is used. 2. When **TTL Source** is set to **Origin server** and **Forcible Cache** is enabled: • If cache directives are set in the response header of the origin server, the priority is **s-maxage** > **max-age** > **expires**. For example, if **Cache-Control: max-age=500, s-maxage=400** is set on the origin server, the cache TTL on CDN PoPs is 400s. • If the preceding response headers are not set, the cache TTL configured on the CDN console is used.	By default, this function is enabled.

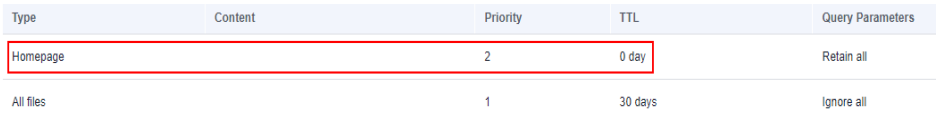
Parameter	Description	Configuration Rule
	3. When **TTL Source** is set to **CDN** and **Forcible Cache** is enabled: • CDN ignores response headers from the origin server and uses the cache TTL configured on the CDN console. 4. When **TTL Source** is set to **CDN** and **Forcible Cache** is disabled: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

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

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

Examples

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

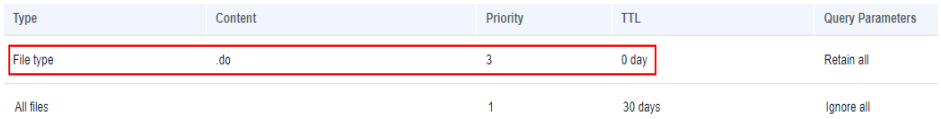


The homepage of the website is not cached, and URL parameters are not ignored in requests for all pages.

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, purge the cached URL or directory where the .do file is located on the CDN console so that the new rule can take effect for all .do files.

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

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

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

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

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

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

Helpful Links

- **Basic Concepts** of query parameters and SWR
- **Will the Cache on CDN PoPs Be Updated in Real Time?**
- **How Do I Check Whether a Cache Is Hit?**
- **Why Does a Cache Rule Not Take Effect?**
- **How Do I Synchronize Content Cached on CDN PoPs with That on the Origin Server?**

4.8.3 Browser Cache TTL

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

Precautions

- Add up to 10 rules for each domain name.
- Add only one rule for **All files** or **Homepage** for each domain name.

Procedure

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

   The CDN console is displayed.

2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Cache Settings** tab.
5. In the **Browser Cache TTL** area, click **Edit**.
6. In the displayed dialog box, click **Add** and set the browser cache policy as required.

Figure 4-38 Browser cache TTL

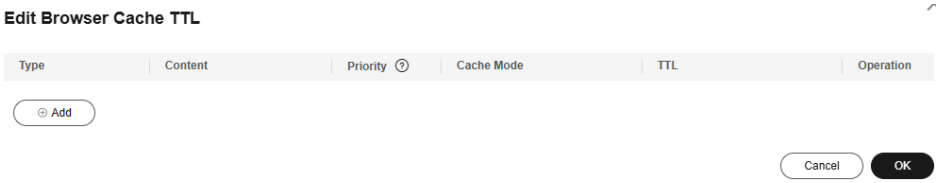


Table 4-19 Parameters

Parameter	Description
Type	**All files** **File type**: files with the specified extension names **Directory**: files under the specified directory **Full path**: file of the complete path **Homepage**

Parameter	Description
Content	When **Type** is set to **All files**, you do not need to set this parameter. When **Type** is set to **File type**: • Start with a period (.) and separate file name extensions by commas (,). Do not end with a comma (,) or enter consecutive commas (,). • Enter up to 20 file name extensions. • Enter up to 255 characters. • File name extensions are case-insensitive. • Example: **.JPG,.zip,.exe** When **Type** is set to **Directory**: • Start with a slash (/) and separate directories by commas (,). Do not end with a comma (,) or enter consecutive commas (,). • Enter up to 20 directories. • Enter up to 255 characters. • Do not enter wildcards (*). • Example: **/test/folder01,/test/folder02** When **Type** is set to **Full path**: • Start with a slash (/). • A wildcard (*) can only follow the last slash (/). • Enter only one full path. • Enter up to 255 characters. The following special characters are not allowed: ,;|:"\ • Examples: **/test/index.html** and **/test/*.jpg** When **Type** is set to **Homepage**, the root directory of a website is used. It is the top-level directory of the website folder, which contains all subfolders of the website. For example, for **www.example.com/abc/file01/2.png**, **abc/** is the root directory.
Priority	Priority of the rule. Enter an integer ranging from 1 to 100. A greater number indicates a higher priority. Each rule must have a unique priority.

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

7. Click **OK**.

4.8.4 Status Code Cache TTL

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

Scenarios

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

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

Precautions

- If a resource is not cached on CDN PoPs, the status code generated when a client requests the resource cannot be cached even if a cache TTL has been set for this status code.
- The status code cache TTL cannot be configured for domain names with special configurations.
- If the service type of your domain name is whole site acceleration, this function takes effect only for static resources.

- By default, CDN caches status codes 404, 500, 502, and 504 for 3 seconds and does not cache other status codes.
  - The header settings determine whether the 404 status code is cached by default. If the **X-HTTP-Method-Override**, **X-HTTP-Method**, or **X-Method-Override** header is carried, the 404 status code is not cached by default. If not, the 404 status code is cached for 3 seconds.
- When **Query Parameters** is set to **Ignore all** for a resource, and a status code (for example, 400) returned for a client request is cached, the status code (400 in this example) will be returned for all requests for the resource within the cache TTL.
- You can modify the cache TTL of the following status codes:
  - 4*XX*: 400, 401, 403, 404, 405, 407, 414, 416, and 451
  - 5*XX*: 500, 501, 502, 503, 504, 509, and 514
  - 3*XX*: 301 and 302

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Cache Settings** tab.
5. Click **Add** under **Status Code Cache TTL**.

Figure 4-39 Adding a status code cache TTL

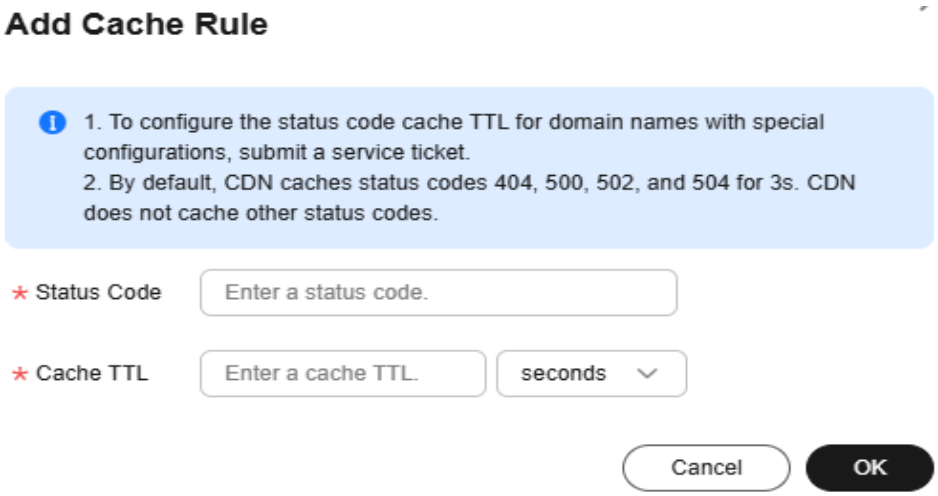


Table 4-20 Parameters

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

Parameter	Description	Example
Cache TTL	Duration for caching the status codes on CDN PoPs. • If it is set to **0**, the status code is not cached. • The value ranges from 0 to 365 days. **NOTE** Status codes 3*XX* and 416 can be cached for 0 to 20 seconds.	3 days

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

Examples

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.

4.8.5 Access URL Rewrite

You can set access URL rewrite rules to redirect or rewrite user requests to the URLs of cached content.

Scenarios

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.

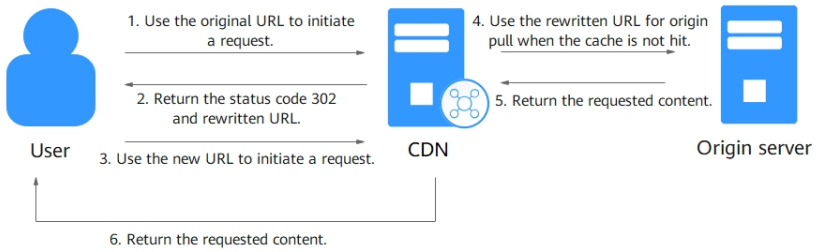
If a URL rewrite rule has been configured, CDN matches URLs in redirection mode and uses the HTTP 302 status code (**302 Found**) to indicate that the requested resource has been temporarily moved to another location. Specifically, CDN PoPs add the new URL to the HTTP **Location** header in the 302 response to the client. After receiving the response, the client sends a request to the new URL. **Table 4-21** lists the redirection status codes and their meanings.

Table 4-21 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.

Working Principles

This diagram shows the request process when a request hits a URL rewrite rule.



1. A user requests content from a CDN PoP. Assume that the access URL is example.com/test/index.html, which matches an access URL rewrite rule.
2. The PoP responds with 302 (specified during URL rewrite configuration) and includes the new URL, example.com/newtest/index.html, in the HTTP **Location** response header.
3. After receiving status code 302, the user uses the new URL to send a request again.

4. If the new request hits the cache, the PoP returns the content. If the cache misses, the PoP uses the new URL to request the content from the origin server.
5. The origin server returns the content to the PoP.
6. The PoP caches the content and sends it to the user.

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 **Access URL Rewrite** area, click **Add**.

Figure 4-40 Adding an access URL rewrite rule

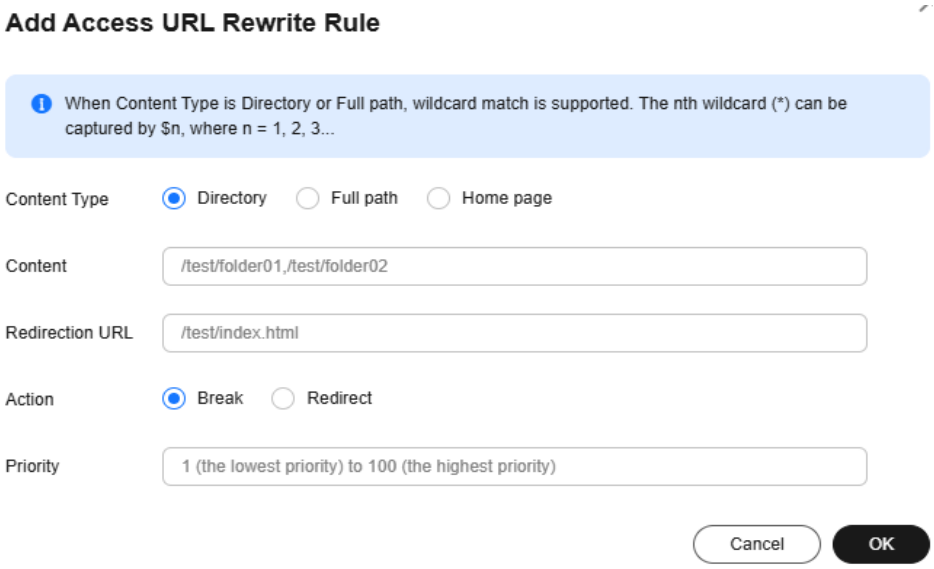


Table 4-22 Parameters

Parameter	Description
Content Type	**Directory**: Execute the rule for files in the specified directory. **Full path**: Execute the rule for the file under the specified path. **Home page**: Execute the rule when the homepage of the domain name is visited.

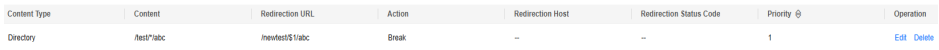
Parameter	Description
Content	When **Content Type** is set to **Directory**, enter up to 20 directories and separate them by commas (,). A directory starts with a slash (/). Wildcards (*) are supported. Enter only one directory with up to five wildcards (*) for wildcard matching. Example: **/test/folder01,/test/folder02** When **Content Type** is set to **Full path**, enter the path of a file or a path with wildcards (*). Question marks (?) are not allowed. A path must start with a slash (/) and cannot end with a wildcard (*). Only one wildcard (*) can be entered. Examples: **/test/index.html** and **/test/*.jpg** When **Content Type** is set to **Home page**, this parameter is left blank. You can configure only one rule for the homepage. **Regular expression match is not supported.**
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**, **$1** is replaced by **11**, so the requested URL after redirection is **/newtest/11.jpg**. • When **Content Type** is set to **Directory**, wildcards (*) can be captured by **$***n* (*n* = 1, 2, 3..., no larger than the total number of wildcards). That is, **$1** captures the first wildcard (*), **$2** captures the second wildcard (*), and **$n** captures the *nth* wildcard. – Example 1: If **Content** is set to **/test/*/abc*** and **Redirection URL** is set to **/newtest/abc$2**, when a user requests **/test/test1/abc01/02/1.jpg**, **$2** captures the content corresponding to the second wildcard, that is, **01/02/1.jpg**. In this case, the requested URL after redirection is **/newtest/abc01/02/1.jpg**. – Example 2: If **Content** is set to **/test/*/abc** and **Redirection URL** is set to **/newtest/$1/abc**, when a user requests **/test/test1/abc/abc02/1.jpg**, **$1** captures **test1**. In this case, the requested URL after redirection is **/newtest/test1/abc**.

Parameter	Description
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 rewritten as the target URL. After this rule is executed, CDN does not execute any other rules. You cannot set the redirection host or status code. If the redirected request hits the CDN cache, status code 200 is returned. If the CDN cache is not hit, CDN pulls the content from the origin server and transparently transmits the status code returned by the origin server to the client.
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 4-21**.
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.**

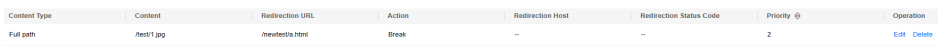
6. Click **OK**.

Examples

Example 1: When the client requests **http://www.example.com/test/test1/abc/abc02/1.jpg**, the directory rule **/test/*/abc** is matched. In this case, the URL accessed by the client is **http://www.example.com/newtest/test1/abc**.



Example 2: When the client requests **http://www.example.com/test/1.jpg**, the full path rule **test/1.jpg** is matched. In this case, the URL accessed by the client is **http://www.example.com/newtest/a.html**.



4.8.6 Shared Cache Groups

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 50 associated domain names.
- An account can have up to 500 shared cache groups.
- Before deleting a cache group, you need to remove associated domain names from 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 4-41 Creating a shared cache group

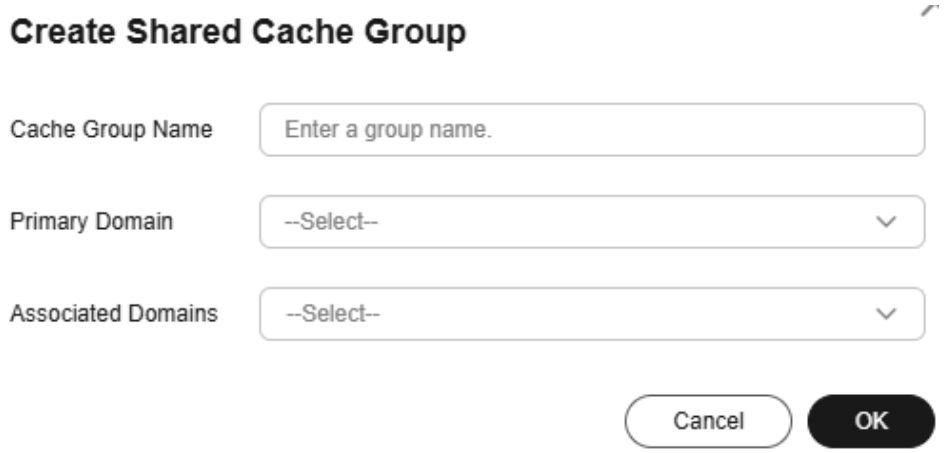


Table 4-23 Parameters

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**.

4.9 Access Control

4.9.1 Overview

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

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

Function	Description
Referer Validation	Configure a referer blacklist or whitelist to identify and filter out users from specific access sources.
IP ACL	Filter out requests from specific IP addresses.
User-Agent ACL	Filter out requests from specific user agents.
Geo-blocking	Prevent users in certain geographical locations from accessing your content.
Token Authentication	Protect your website resources from being downloaded by malicious users.
Remote Authentication	Allow CDN to forward user requests to a specific server for authentication, to prevent malicious resource download.

Function	Description
IP Access Frequency	Restrict the number of times that a single IP address requests a URL from a PoP per second to defend against CC attacks and malicious theft.

4.9.2 Referer Validation

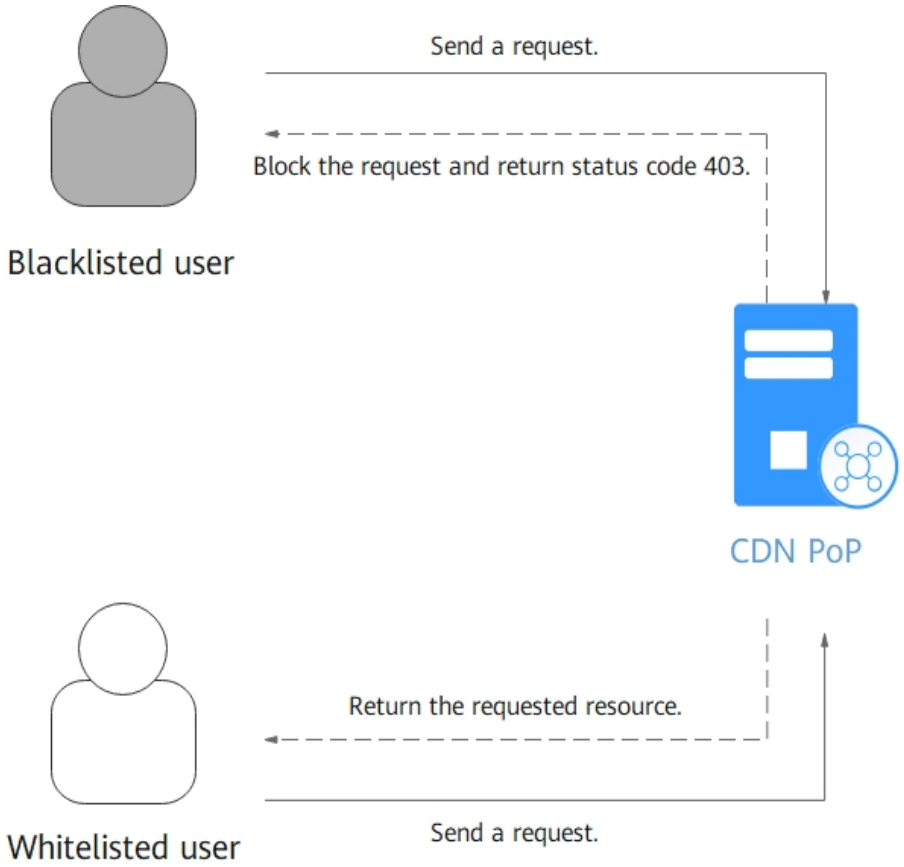
You can set a referer blacklist or whitelist to identify and filter out values of the **Referer** header in HTTP requests, controlling access sources.

Background

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

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

Figure 4-42 How referers work



Precautions

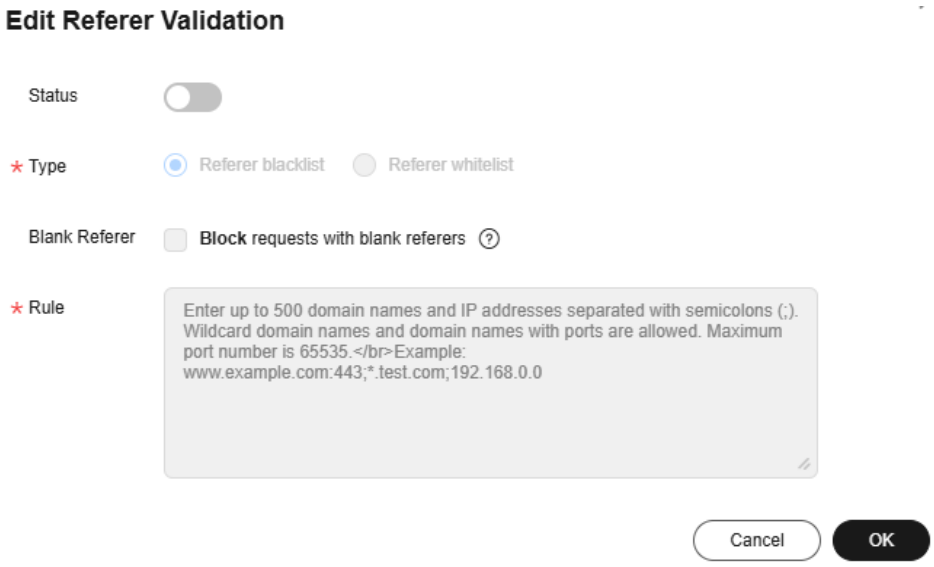
- This function is disabled by default.
- Either a referer blacklist or whitelist can be configured.
- This function sets access control rules based on the **Referer** header in HTTP requests. When a client request hits the blacklist and is blocked, a small amount of traffic or bandwidth fees are generated. If the service type of the domain name is whole site acceleration, the client request is also charged for the request fees.

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**.

   Figure 4-43 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 4-24 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 you select **Block requests with blank referers** when configuring a blacklist, CDN will block requests with blank referers. If you select **Allow requests with blank referers** when configuring the whitelist, CDN will allow requests with blank referers. **NOTE** A blank referer indicates that the referer field is left blank or is not included in an HTTP request. The referer field with value **null** is not a blank referer.	/

Parameter	Description	Filling Rule
Referer whitelist	• If the referer field of an access request matches the whitelist rules, the requester can access the requested content. Otherwise, CDN returns a 403 error response code, indicating that access is forbidden. • If **Include blank referer** is selected and an access request contains a blank referer, the requester can access the requested content.	• Enter domain names (excluding the protocol, path, and parameters) and IP addresses and separate them by semicolons (;). • Wildcard domain names are supported. • Enter up to two asterisks (*). They cannot be consecutive or at the end. • Domain names and IP addresses with ports are supported. The maximum port number is 65535. • Enter up to 500 domain names and IP addresses. Example: **www.example.com:443;*.test.com;192.168.0.0** **NOTE** Domain names with special configurations support only one asterisk (*).

Parameter	Description	Filling Rule
Referer blacklist	• If the referer field in an access request matches the blacklist rules, the requester cannot access the requested content, and **403 Forbidden** will be returned. Otherwise, the requester can access the requested content. • If **Include blank referer** is selected and an access request contains a blank referer, the access request will be rejected, and **403 Forbidden** will be returned.	• Enter **domain names** (excluding the protocol, path, and parameters) and **IP addresses** and separate them by semicolons (;). • Do not enter a specific URL, for example, **example.com/abc/01.jpg**. • Wildcard domain names are supported. • Enter up to two asterisks (*). They cannot be consecutive or at the end. • Domain names and IP addresses with ports are supported. The maximum port number is 65535. • Enter up to 500 domain names and IP addresses. Example: **www.example.com:443;*.test.com;192.168.0.0** **NOTE** Domain names with special configurations support only one asterisk (*).

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

Verification

After you configure a referer rule, CDN allows or blocks client requests based on the rule. You can run **curl** commands to check whether the configuration works.

Scenario: Assume that you have configured a referer blacklist to block requests coming from referer example.com and you have disabled **Include blank referer**.

Expected result: CDN blocks requests containing http://example.com or https://example.com in the referer field, but it accepts other requests.

1. To test access from the primary domain name, run **curl -e http://example.com -I** *CDN acceleration domain name*.

```
[root@Server-5 conf]# curl -I http://referer-te                    :xt -e http://example.com
HTTP/1.1 403 Forbidden
Server: openresty
```

2. To test access from a sub-domain name, for example, http://abc.example.com, run **curl -e http://abc.example.com -I** *CDN acceleration domain name*.

```
[root@Server-5 conf]# curl -I http://referer                    :xt -e http://abc.example.com
HTTP/1.1 200 OK
```

3. To test access from another domain name, for example, http://axample.com, run **curl -e http://axample.com -I** *CDN acceleration domain name*.

```
[root@Server-5 conf]# curl -I http://referer-                    txt -e http://axample.com
HTTP/1.1 200 OK
```

4. To test access with a blank referer, run **curl -e " " -I** *CDN acceleration domain name*.

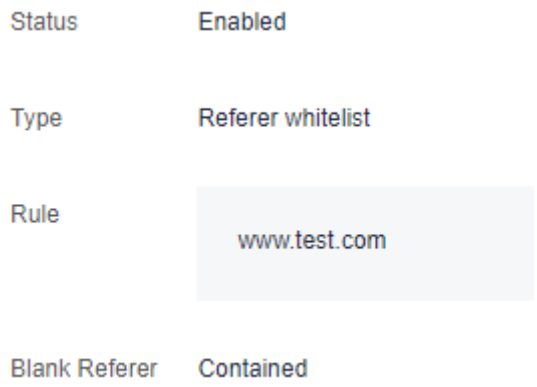
```
[root@Server-5 conf]# curl -I http://referer                    txt -e ""
HTTP/1.1 200 OK
```

5. To test access from a domain name without protocol, for example, axample.com, run **curl -e axample.com -I***CDN acceleration domain name*.

```
[root@Server-5 conf]# curl -I http://referer-                    .txt -e example.com
HTTP/1.1 403 Forbidden
```

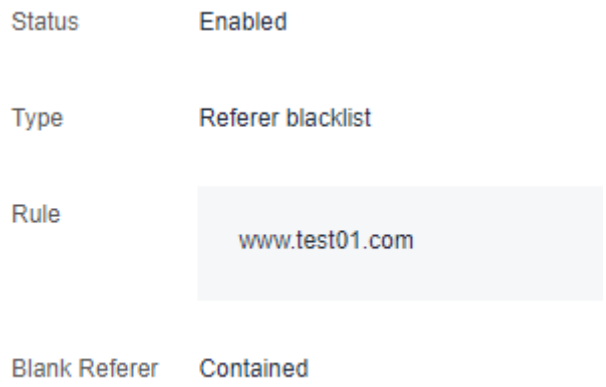
Examples

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.

4.9.3 IP ACL

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

Precautions

- This function is disabled by default.
- Either an IP address blacklist or IP address whitelist can be configured.
- 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.
- This function uses the Layer 7 HTTP IP address identification technology. When a client request hits the blacklist and is blocked, a small amount of traffic or bandwidth fees are generated. If the service type of the domain name is whole site acceleration, the client request is also charged for the request fees.

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 **Edit IP ACL** dialog box is displayed.

Figure 4-44 Configuring an IP ACL

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

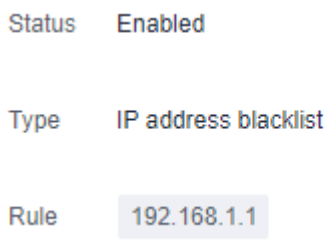
Parameter	Description
Type	**IP address blacklist**: If the IP address of a user is included in the blacklist, status code 403 will be returned when the user accesses a CDN PoP. **IP address whitelist**: If the IP address of a user is not included in the whitelist, status code 403 will be returned when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

Parameter	Description
Rule	• Enter up to 500 IPv4 and IPv6 addresses and CIDR blocks, one per row. The prefix length ranges from 1 to 32 bits for IPv4 and 1 to 128 bits for IPv6. • A CIDR block is in the format of *First host IP address*/*Prefix length*. • Duplicate IP addresses and IP address segments will be removed. • Wildcards are not supported, for example, 192.168.0.*. **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.

Helpful Links

- **How Do I Obtain Real IP Addresses of Users?**
- **Does CDN Support IP Address Filtering?**

4.9.4 User-Agent ACL

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

Background

You can filter requests to your domain name based on the **User-Agent** field.

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

Precautions

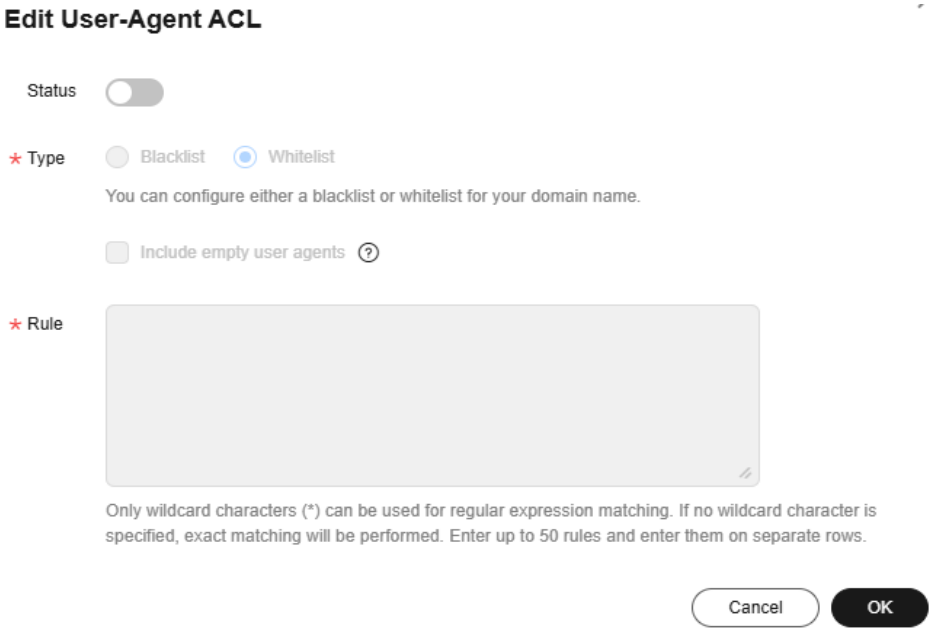
- This function is disabled by default.
- Either a User-Agent blacklist or whitelist can be configured.
- When a client request hits the blacklist and is blocked, PoP resources are consumed, generating a small amount of traffic or bandwidth fees. If the service type of the domain name is whole site acceleration, the client request is also charged for the request fees.

Procedure

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

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

Figure 4-45 Configuring a User-Agent ACL



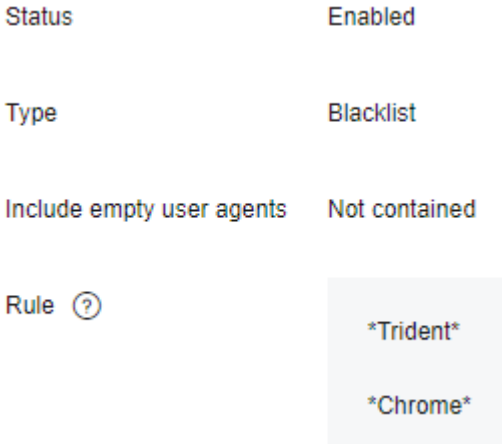
6. Switch on **Status** to enable this configuration item.
7. Select a type and enter rules.

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.
Include empty user agents	An empty user agent indicates that the User-Agent field is left blank or is not included in an HTTP request. If this option is selected, such requests will also be accepted (whitelist) or rejected (blacklist). **NOTE** The **User-Agent** field with value **null** is not an empty user agent.
Rule	• Enter letters, digits, spaces, and the following special characters: *.-_();,/'#!@$^&+=~?"[]{}\:% **NOTE** For domain names with special configurations, (), {}, or [] must be both entered. • Only wildcard characters (*) can be used for regular expression matching. If no wildcard character is included, exact matching will be used. • Enter up to 100 characters for a rule. • Enter up to 50 rules, one per row.

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.

Examples

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.

4.9.5 Geo-blocking

You can prevent users in certain geographical locations from accessing your content.

Scenarios

You can use geo-blocking when users in specific geographic areas need to be restricted from accessing your businesses due to local laws and regulations or business attributes. CDN identifies client IP addresses to determine the user access source. The working principle is as follows:

1. Assume that your domain name www.example.com does not serve users in region W, and you have configured a blacklist for region W on the CDN console.
2. CDN receives a request to access www.example.com from an IP address in region W. The DNS resolves the request to a CDN PoP in region W.
3. The PoP detects that this IP address is not allowed to download resources under your domain name.
4. CDN returns HTTP status code 403 (Forbidden) to the user.

Precautions

- You can configure up to 20 rules.
- If a blacklist and whitelist are configured for the same resource, when a user in both lists accesses the resource, the blacklist takes effect and status code 403 is returned.
- If a blacklist and whitelist are configured for the same resource, when a user outside both lists accesses the resource, status code 403 is returned.
- When a client request hits the blacklist and is blocked, PoP resources are consumed, generating a small amount of traffic or bandwidth fees. If the

service type of the domain name is whole site acceleration, the client request is also charged for the request fees.

- Huawei Cloud periodically updates the IP address library. The locations of IP addresses that are not in the library cannot be identified. CDN allows requests from such IP addresses and returns resources to the users.
- If your domain name is connected to **EdgeSec** and a geo-blocking 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 **Geo-blocking** area, click **Add**.

Figure 4-46 Adding a geo-blocking rule

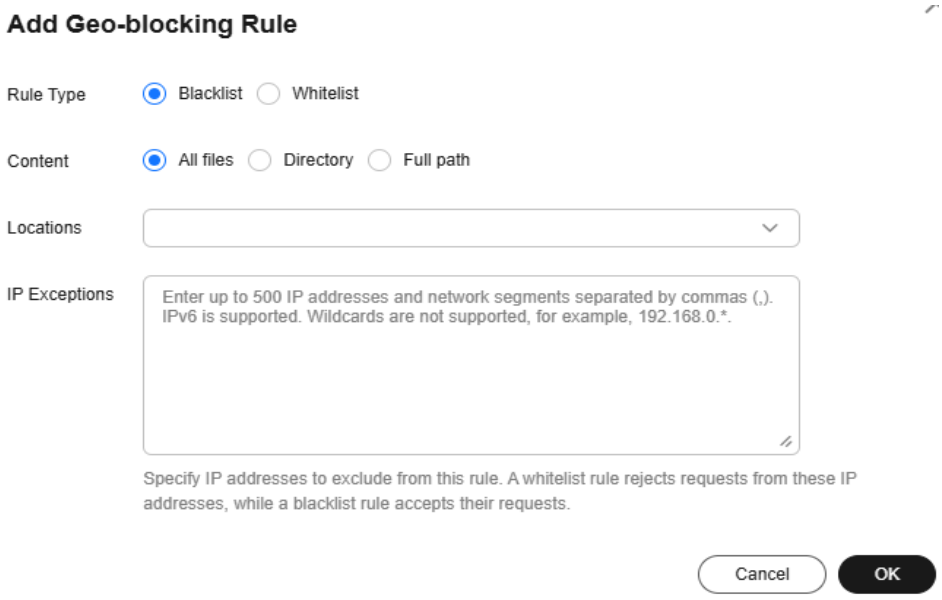


Table 4-25 Parameter details

Parameter	Description	Example
Rule Type	**Blacklist**: Users in regions specified in the blacklist cannot access resources and status code 403 is returned. **Whitelist**: Only users in regions specified in the whitelist can access resources. Status code 403 is returned for other users.	Blacklist
Content	**All files**: The rule takes effect for all files. **Directory**: The rule takes effect for resources in the specified directory. **Full path**: The rule takes effect for resources corresponding to the paths.	All files
Rule	**Directory**: • Start with a slash (/) and separate directories by commas (,). • Enter up to 100 directories. • Do not enter wildcard characters (*). **Full path**: • Start with a slash (/) or wildcard (*). Wildcards (*) can be used for match. – Do not enter two consecutive wildcard characters (*). – Enter up to two wildcard characters (*). • Enter up to 100 paths and separate them by comma (,). **NOTE** • Each whitelist or blacklist rule must be unique. • You can configure only one rule for all files.	/test/folder01,/test/folder02

Parameter	Description	Example
Locations	User locations to which the rule applies. That is, users in the specified locations cannot access the resources (blacklist) or only they can access the resources (whitelist). For details about the supported regions, see **Table 4-26**.	Chinese mainland
IP Exceptions	IP addresses excluded from this rule. For example, if you have configured a blacklist whose **Content** is **All files** and added an exception IP address 0.0.0.0, this IP address is not restricted by this blacklist rule and requests from this IP address are accepted. • IP addresses and CIDR blocks in the *IP address*/*Subnet mask* format are supported. • Enter up to 500 IP addresses and CIDR blocks separated by commas (,). • Wildcards are not supported, for example, 192.168.0.*. • IPv6 is supported.	0.0.0.0

6. Configure related information and click **OK**.

Supported Regions

Table 4-26 Supported regions

Geographic Region	User Location
Asia	Afghanistan, Armenia, Azerbaijan, Bahrain, Bangladesh, Bhutan, Cambodia, Chinese mainland, Georgia, Hong Kong (China), India, Indonesia, Iraq, Israel, Japan, Jordan, Kazakhstan, Kuwait, Kyrgyzstan, Lao People's Democratic Republic, Lebanon, Macao (China), Malaysia, Maldives, Mongolia, Myanmar, Nepal, Oman, Pakistan, Palestine, Philippines, Qatar, Republic of Korea, Saudi Arabia, Singapore, Sri Lanka, Taiwan (China), Tajikistan, Thailand, Timor-Leste, Türkiye, Turkmenistan, United Arab Emirates, Uzbekistan, Vietnam, and Yemen
Europe	Albania, Andorra, Austria, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Faroe Islands, Finland, France, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Republic of Moldova, Romania, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, and United Kingdom of Great Britain and Northern Ireland
South Africa	Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Central African Republic, Chad, Comoros, Côte d'Ivoire, Democratic Republic of the Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Kenya, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Republic of the Congo, Rwanda, Sao Tome and Principe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, Togo, Tunisia, Uganda, United Republic of Tanzania, Zambia, and Zimbabwe
North America	Antigua and Barbuda, Bahamas, Barbados, Belize, Canada, Costa Rica, Dominica, Dominican Republic, El Salvador, Grenada, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Trinidad and Tobago, and United States of America
Oceania	Australia, Cook Islands, Fiji, Micronesia, Kiribati, Marshall Islands, Nauru, Niue, New Zealand, Papua New Guinea, Solomon Islands, Tokelau, Tonga, Tuvalu, Vanuatu, and Samoa
South America	Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Guyana, Paraguay, Peru, Suriname, and Venezuela

Examples

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

Rule Type	Content	Rule	Locations	Operation
Whitelist	Directory	/test	Chinese mainland	Edit | Delete
Blacklist	Directory	/test	Chinese mainland	Edit | Delete

Result:

- The blacklist takes precedence over the whitelist. Therefore, the blacklist takes effect. When a user in the Chinese mainland accesses a resource in the **/test** folder (for example, **www.example.com/test/abc.jpg**), status code 403 is returned.
- When a user in Hong Kong (China) accesses the same resource, neither the blacklist nor the whitelist is hit. In this case, the access is denied and status code 403 is returned.

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

Rule Type	Content	Rule	Locations	Operation
Blacklist	Directory	/test	Hong Kong	Edit | Delete
Whitelist	Directory	/test	Chinese mainland	Edit | Delete

Result:

- When a user in Hong Kong (China) accesses a resource in the **/test** folder (for example, **www.example.com/test/abc.jpg**), the blacklist is hit and status code 403 is returned.
- When a user in the Chinese mainland accesses the same resource, the whitelist is hit and the resource is returned to the user.
- When a user in Macao (China) accesses the same resource, neither the blacklist nor the whitelist is hit. In this case, the access is denied by default and status code 403 is returned.

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

Rule Type	Content	Rule	Locations	Operation
Blacklist	Directory	/test/abc	Hong Kong	Edit | Delete
Whitelist	Directory	/test	Chinese mainland	Edit | Delete

Result:

- When a user in Hong Kong (China) accesses a resource in the **/test/abc** folder (for example, **www.example.com/test/abc/1.jpg**), the blacklist is hit and status code 403 is returned.
- When a user in the Chinese mainland accesses a resource in the **/test** folder (for example, **www.example.com/test/cat.jpg**), the whitelist is hit and the corresponding resource is returned to the user.
- When a user in Hong Kong (China) accesses a resource in the **/test** folder (for example, **www.example.com/test/cat.jpg**), neither the blacklist nor the whitelist is hit. In this case, the access is denied by default and status code 403 is returned.

- When a user in Macao (China) accesses a resource in the **/test** folder (for example, **www.example.com/test/cat.jpg**), neither the blacklist nor the whitelist is hit. In this case, the access is denied by default and status code 403 is returned.

4.9.6 Token Authentication

4.9.6.1 Signing Method A

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

CAUTION

- Token authentication is disabled by default.
- When a client request fails the authentication and is blocked, PoP resources are consumed, generating a small amount of traffic or bandwidth fees. If the service type of the domain name is whole site acceleration, the client request is also charged for the request fee.
- You cannot configure this function for domain names with special configurations on the CDN console.
- When token authentication is configured, user requests will include authentication parameters. If **Ignore specific parameters** is not configured:
  - Origin pull will become frequent.
  - If your origin server is an OBS bucket, fees for bucket outbound traffic will incur.

How It Works

Example signed URLs look like:

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

The following table describes the parameters in a signed URL.

Table 4-27 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.

Parameter	Description
Validity period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s. Example: If the validity period is set to 1,800s, users can access CDN only when the current time is earlier than or equal to **timestamp** + 1,800s. Or, the signed URL is considered invalid.
rand	Random number. The recommended value is a UUID, which cannot contain hyphens (-), for example, **202cb962ac59075b964b07152d234b70**.
uid	User ID. This parameter is not used now. You can set it to **0**.
md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of lowercase letters and digits.
sha256	A string of 64 characters calculated using the SHA256 algorithm. The string consists of lowercase letters and digits.
Filename	Back-to-origin URL. Its value must start with a slash (/) and does not include the parameters following the question mark (?).
PrivateKey	Signing key, which is used to generate a signed URL, for example, **huaweicloud12345**. A key contains 6 to 32 characters, including letters and digits.
Authentication parameter	Authentication parameter carried in a URL. The default value is **auth_key**.

Verification Method

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

1. Checks whether the authentication parameter is included in the request. If not, the request is considered invalid and an HTTP 403 error code is returned.
2. Checks whether the value of **timestamp** plus the validity period specified in the signed URL is later than the current time.
   - If not, the signed URL is considered invalid and the HTTP 403 error is returned.
   - If yes, the time verification passes and CDN goes to step **3**.
3. Constructs **sstring**, calculates **HashValue** using this string and the MD5 or SHA256 algorithm, and compares **HashValue** with the **md5hash** or **sha256** value in the request. If the **md5hash** or **sha256** value is the same as **HashValue**, the authentication is successful and the requested file is returned. Or, the authentication fails and an HTTP 403 error code is returned.
   HashValue is calculated as follows:

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

   Or

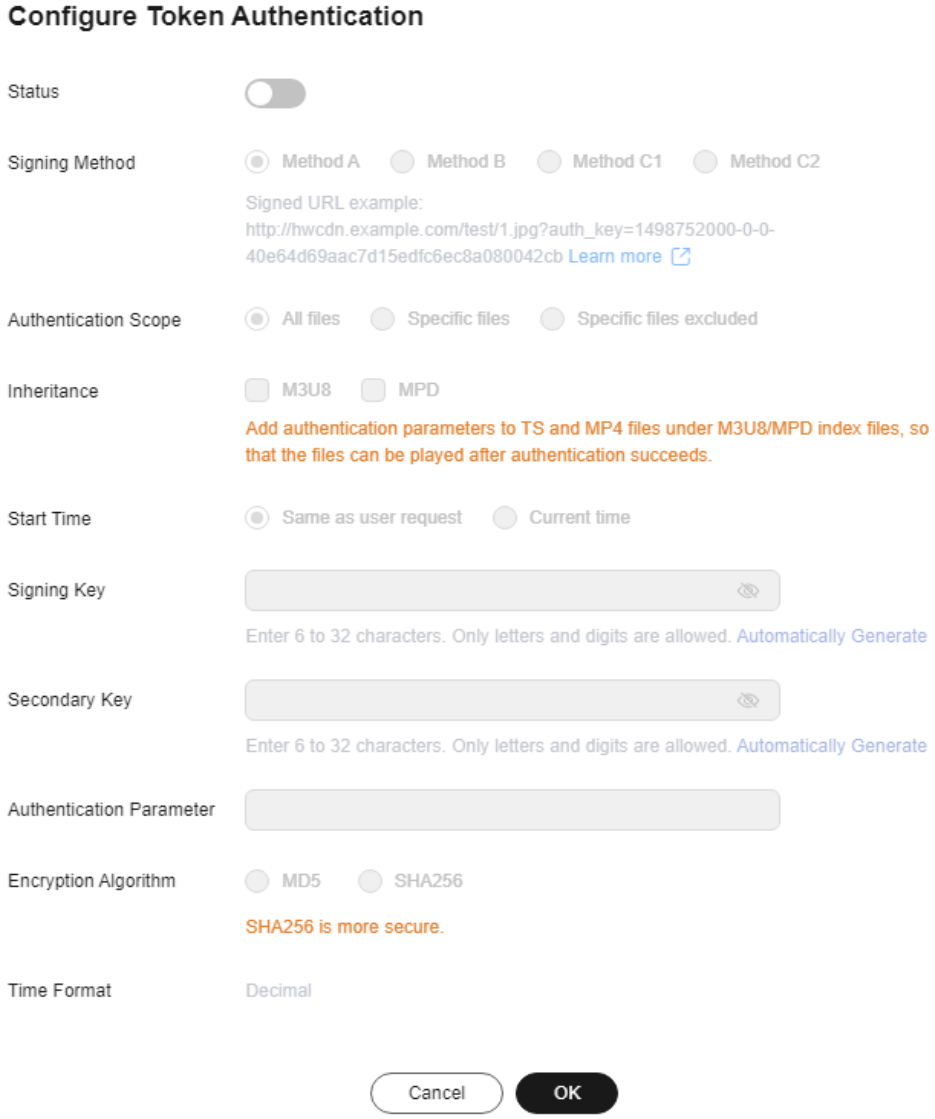
   ```
   sstring = "Filename-Timestamp-rand-uid-PrivateKey"
   HashValue = sha256sum(sstring)
   ```


Procedure

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

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

   Figure 4-47 Configuring token authentication

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

Table 4-28 Parameter description

Parameter	Description
Signing Method	Select **Method A**.
Authentication Scope	Files to be authenticated. Select **All files**, **Specific files**, or **Specific files excluded**.
Inheritance	Add the authentication parameter to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds. **NOTE** • If there are multi-layer M3U8/MPD files, only the first-layer M3U8/MPD files are parsed, and the TS/MP4 streams of M3U8/MPD files in other layers are not expanded. • The standard M3U8 format is supported. M3U8 files are parsed by line. If the parsing fails, responses from the origin server are returned to users. URIs starting with the **#EXT-X-MAP** tag and URLs/URIs not starting with the pound key (#) are supported. • The standard MPD format is supported. MPD files are parsed by line. If the parsing fails, responses from the origin server are returned to users. The URI between tags **<BaseURL>** and **</BaseURL>** is identified. The **SegmentTemplate** tag is not supported. • If your M3U8/MPD index files contain special characters, CDN does not automatically transcode the characters during authentication calculation. If clients have the logic for automatically transcoding special characters, the access may fail due to the authentication failure. • If the origin server returns resources compressed using gzip or Brotli to CDN PoPs, the authentication inheritance settings become invalid.
Start Time	• **Same as user request**: time when a user accesses the M3U8/MPD file. • **Current time**: current time of the authentication server.
File Name Extensions	Set this parameter when you select **Specific files** or **Specific files excluded** for **Authentication Scope**. Only requests for files with the specified file name extensions are authenticated or not authenticated. • Only lowercase letters and digits are supported. Use semicolons (;) to separate multiple file name extensions.
Signing Key	Authentication password. The value contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.

Parameter	Description
Secondary Key	(Optional) Secondary password for authentication. If you want the old and new keys to take effect, you can set the old key as the secondary key. Users can access content only after CDN verifies the primary or secondary key. • A key contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.
Authentication Parameter	Authentication parameter carried in a URL. The default value is **auth_key**. • Enter up to 100 characters. • Start with a letter. Enter letters, digits, and underscores (_).
Encryption Algorithm	**MD5** or **SHA256**.
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s.

Authentication Calculator

Using the authentication calculator, you can generate a signed URL for users. Set parameters according to **Table 4-28** and **Table 4-29**, 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 4-29 Parameter description

Parameter	Description
Signing Key	Authentication password. Enter 6 to 32 characters, including letters and digits. The value must be the same as the signing key specified in the token authentication configuration.
Access Path	Path of the content, which starts with a slash (/) and does not carry a query string.
Encryption Algorithm	**MD5** or **SHA256**.
Start Time	Time when the signed URL will take effect.

Parameter	Description
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s. If this value is greater than the validity period set in the token authentication settings, the latter will be used. Example: If you set this parameter to 2,000s, but the validity period set in the token authentication settings is 1,800s, the validity period of signed URLs will be 1,800s.

Disabling Token Authentication

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

Example

The following uses the MD5 algorithm as an example:

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

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

4.9.6.2 Signing Method B

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

CAUTION

- Token authentication is disabled by default.
- When a client request fails the authentication and is blocked, PoP resources are consumed, generating a small amount of traffic or bandwidth fees. If the service type of the domain name is whole site acceleration, the client request is also charged for the request fee.
- You cannot configure this function for domain names with special configurations on the CDN console.
- Domain names whose service type is **whole site acceleration** do not support **signing method B**.

How It Works

Example signed URLs look like:

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

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

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

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

The following table describes the parameters in a signed URL.

Table 4-30 Parameter description

Parameter	Description
DomainName	Acceleration domain name.
timestamp	Time when the authentication server generates a signed URL, that is, the authentication start time. The UTC+08:00 time of the authentication server is used. The format is YYYYMMDDHHMM, for example, 201706301000.
Validity period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s. Example: If the validity period is set to 1,800s, users can access CDN only when the current time is earlier than or equal to **timestamp** + 1,800s. Or, the signed URL is considered invalid.
md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of lowercase letters and digits.
sha256	A string of 64 characters calculated using the SHA256 algorithm. The string consists of lowercase letters and digits.
Filename	Back-to-origin URL. Its value must start with a slash (/) and does not include the parameters following the question mark (?).

Parameter	Description
PrivateKey	Signing key, which is used to generate a signed URL, for example, **huaweicloud12345**. A key contains 6 to 32 characters, including letters and digits.

Verification Method

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

1. Checks whether the authentication parameter is included in the request. If not, the request is considered invalid and an HTTP 403 error code is returned.
2. Checks whether the value of **timestamp** plus the validity period specified in the signed URL is later than the current time.
   - If not, the signed URL is considered invalid and the HTTP 403 error is returned.
   - If yes, the time verification passes and CDN goes to step **3**.
3. Constructs **sstring**, calculates **HashValue** using this string and the MD5 or SHA256 algorithm, and compares **HashValue** with the **md5hash** or **sha256** value in the request. If the **md5hash** or **sha256** value is the same as **HashValue**, the authentication is successful and the requested file is returned. Or, the authentication fails and an HTTP 403 error code is returned.
   HashValue is calculated as follows:

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

   Or

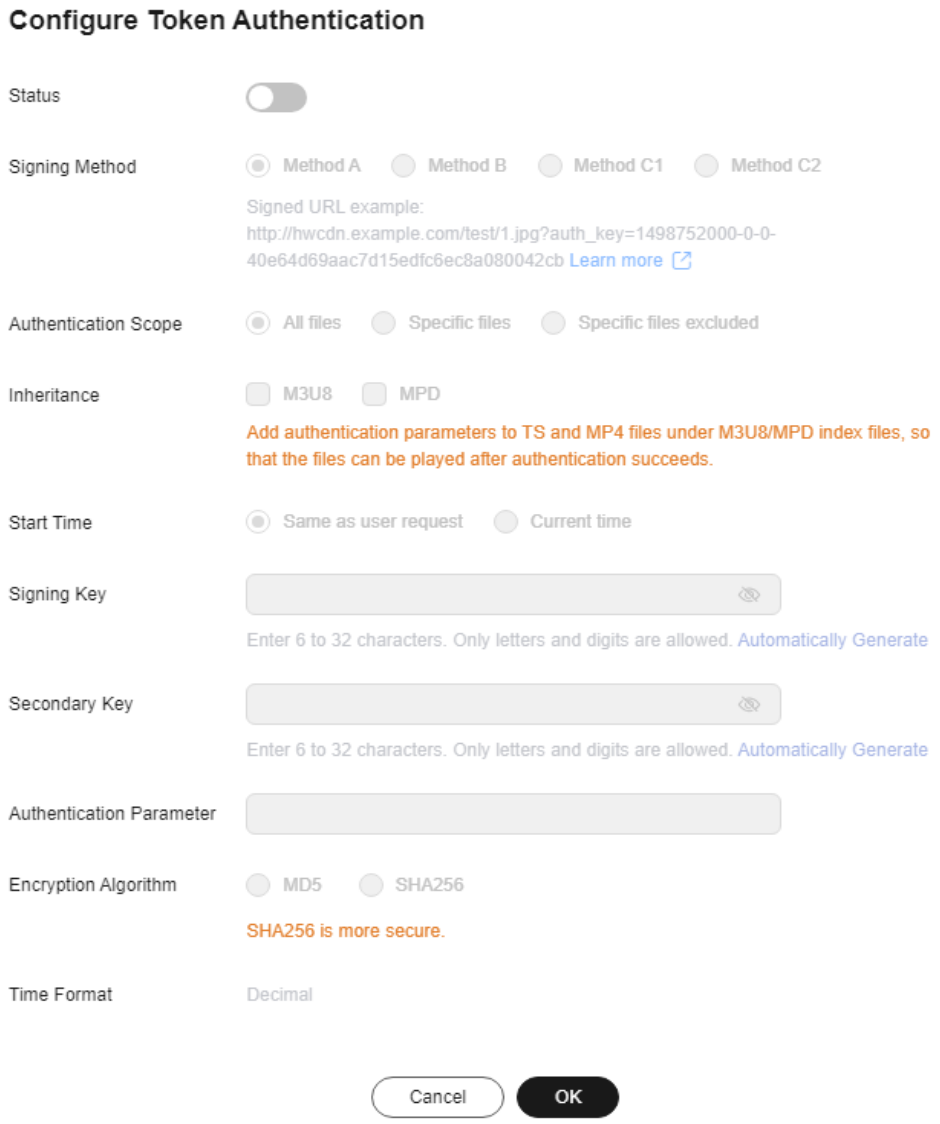
   ```
   sstring = "PrivateKeytimestampFilename"
   HashValue = md5sum(sstring)
   ```

Procedure

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

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

Figure 4-48 Configuring token authentication



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

Table 4-31 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 the authentication parameter to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds. **NOTE** • If there are multi-layer M3U8/MPD files, only the first-layer M3U8/MPD files are parsed, and the TS/MP4 streams of M3U8/MPD files in other layers are not expanded. • The standard M3U8 format is supported. M3U8 files are parsed by line. If the parsing fails, responses from the origin server are returned to users. URIs starting with the **#EXT-X-MAP** tag and URLs/URIs not starting with the pound key (#) are supported. • The standard MPD format is supported. MPD files are parsed by line. If the parsing fails, responses from the origin server are returned to users. The URI between tags **<BaseURL>** and **</BaseURL>** is identified. The **SegmentTemplate** tag is not supported. • If your M3U8/MPD index files contain special characters, CDN does not automatically transcode the characters during authentication calculation. If clients have the logic for automatically transcoding special characters, the access may fail due to the authentication failure. • If the origin server returns resources compressed using gzip or Brotli to CDN PoPs, the authentication inheritance settings become invalid.
Start Time	• **Same as user request**: time when a user accesses the M3U8/MPD file. • **Current time**: current time of the authentication server.
File Name Extensions	Set this parameter when you select **Specific files** or **Specific files excluded** for **Authentication Scope**. Only requests for files with the specified file name extensions are authenticated or not authenticated. • Only lowercase letters and digits are supported. Use semicolons (;) to separate multiple file name extensions.
Signing Key	Authentication password. The value contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.
Secondary Key	(Optional) Secondary password for authentication. If you want the old and new keys to take effect, you can set the old key as the secondary key. Users can access content only after CDN verifies the primary or secondary key. • A key contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.
Encryption Algorithm	**MD5** or **SHA256**.

Parameter	Description
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 4-31** and **Table 4-32**, and click **Generate** to generate a signed URL that will expire at a specific time.

Table 4-32 Parameter description

Parameter	Description
Signing Key	Authentication password. Enter 6 to 32 characters, including letters and digits. The value must be the same as the signing key specified in the token authentication configuration.
Access Path	Path of the content, which starts with a slash (/) and does not carry a query string.
Encryption Algorithm	**MD5** or **SHA256**.
Start Time	Time when the signed URL will take effect.
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s. If this value is greater than the validity period set in the token authentication settings, the latter will be used. Example: If you set this parameter to 2,000s, but the validity period set in the token authentication settings is 1,800s, the validity period of signed URLs will be 1,800s.

NOTE

Escape special characters in the signed URL if any.

Disabling Token Authentication

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

Example

The following uses the MD5 algorithm as an example:

1. The back-to-origin URL is as follows:


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

2. The signing key is **huaweicloud12345** (customizable).
3. **timestamp** is **201706301000**.
4. The CDN server constructs a string for calculating **md5hash**.
   ```
   huaweicloud12345201706301000/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3
   ```
5. The CDN server calculates **md5hash** according to the string.
   ```
   md5hash = md5sum("huaweicloud12345201706301000/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3")
   =668f28d134ec6446a8ae83a43d0a554b
   ```
6. The request URL is:
   ```
   http://hwcdn.example.com/201706301000/668f28d134ec6446a8ae83a43d0a554b/T128_2_1_0_sdk/
   0210/M00/82/3E/test.mp3
   ```

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

4.9.6.3 Signing Method C1

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

CAUTION

- Token authentication is disabled by default.
- You cannot configure this function for domain names with special configurations on the CDN console.
- When a client request fails the authentication and is blocked, PoP resources are consumed, generating a small amount of traffic or bandwidth fees. If the service type of the domain name is whole site acceleration, the client request is also charged for the request fee.
- Domain names whose service type is **whole site acceleration** do not support **signing method C1**.

How It Works

Example signed URLs look like:

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

The following table describes the parameters in a signed URL.

Table 4-33 Parameter description

Parameter	Description
DomainName	Acceleration domain name.

Parameter	Description
timestamp	Time when the authentication server generates a signed URL, that is, the authentication start time. The value is a hexadecimal integer, indicating the total number of seconds that have elapsed since 00:00:00 January 1, 1970.
Validity period	How long a signed URL remains effective. The value ranges from 0s to 31,536,000s. Example: If the validity period is set to 1,800s, users can access CDN only when the current time is earlier than or equal to **timestamp** + 1,800s. Or, the signed URL is considered invalid.
md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of lowercase letters and digits.
sha256	A string of 64 characters calculated using the SHA256 algorithm. The string consists of lowercase letters and digits.
Filename	Back-to-origin URL. Its value must start with a slash (/) and does not include the parameters following the question mark (?).
PrivateKey	Signing key, which is used to generate a signed URL, for example, **huaweicloud12345**. A key contains 6 to 32 characters, including letters and digits.

Verification Method

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

1. Checks whether the authentication parameter is included in the request. If not, the request is considered invalid and an HTTP 403 error code is returned.
2. Checks whether the value of **timestamp** plus the validity period specified in the signed URL is later than the current time.
   - If not, the signed URL is considered invalid and the HTTP 403 error is returned.
   - If yes, the time verification passes and CDN goes to step **3**.
3. Constructs **sstring**, calculates **HashValue** using this string and the MD5 or SHA256 algorithm, and compares **HashValue** with the **md5hash** or **sha256** value in the request. If the **md5hash** or **sha256** value is the same as **HashValue**, the authentication is successful and the requested file is returned. Or, the authentication fails and an HTTP 403 error code is returned.
   HashValue is calculated as follows:

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

   Or

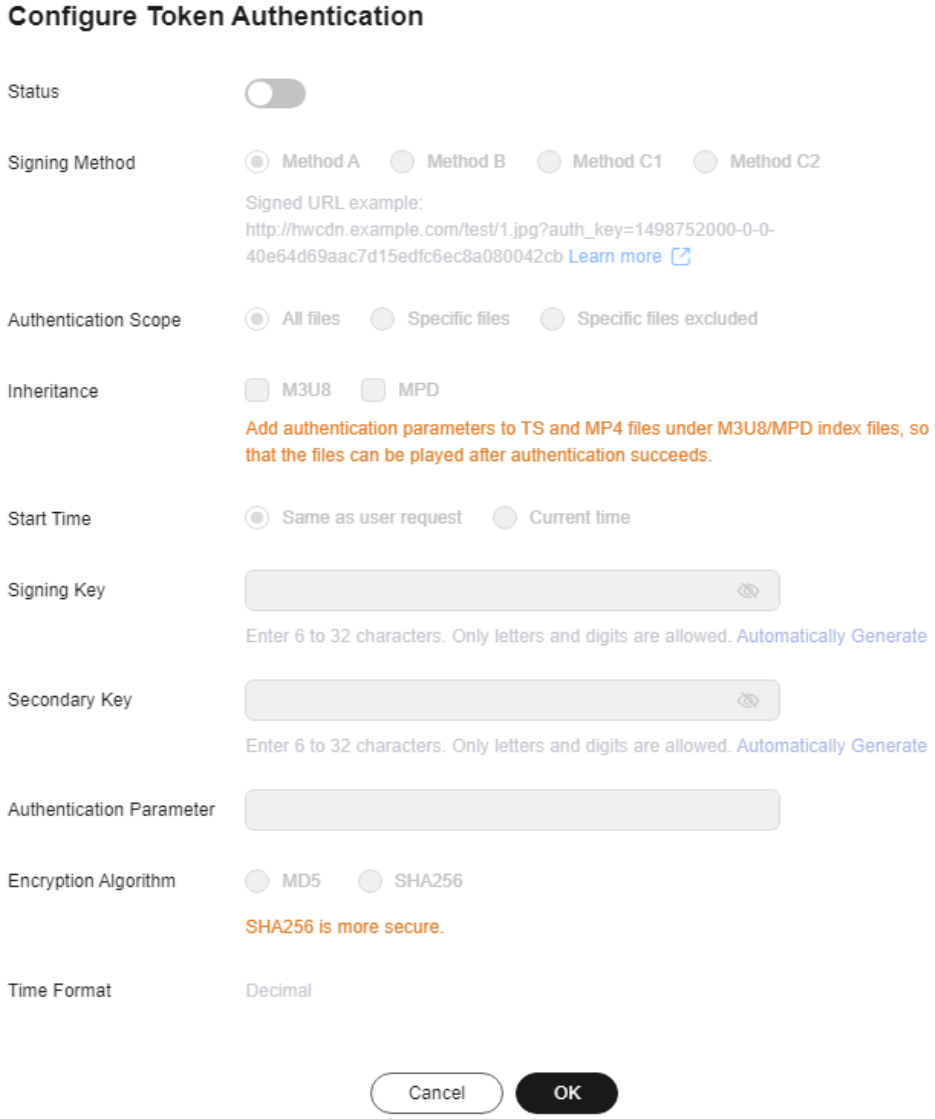
   ```
   sstring = "PrivateKeyFilenameTimestamp"
   HashValue = sha256sum(sstring)
   ```


Procedure

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

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

   Figure 4-49 Configuring token authentication

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

Table 4-34 Parameter description

Parameter	Description
Signing Method	Select **Method C1**.
Authentication Scope	Files to be authenticated. Select **All files**, **Specific files**, or **Specific files excluded**.
Inheritance	Add the authentication parameter to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds. **NOTE** • If there are multi-layer M3U8/MPD files, only the first-layer M3U8/MPD files are parsed, and the TS/MP4 streams of M3U8/MPD files in other layers are not expanded. • The standard M3U8 format is supported. M3U8 files are parsed by line. If the parsing fails, responses from the origin server are returned to users. URIs starting with the **#EXT-X-MAP** tag and URLs/URIs not starting with the pound key (#) are supported. • The standard MPD format is supported. MPD files are parsed by line. If the parsing fails, responses from the origin server are returned to users. The URI between tags **<BaseURL>** and **</BaseURL>** is identified. The **SegmentTemplate** tag is not supported. • If your M3U8/MPD index files contain special characters, CDN does not automatically transcode the characters during authentication calculation. If clients have the logic for automatically transcoding special characters, the access may fail due to the authentication failure. • If the origin server returns resources compressed using gzip or Brotli to CDN PoPs, the authentication inheritance settings become invalid.
Start Time	• **Same as user request**: time when a user accesses the M3U8/MPD file. • **Current time**: current time of the authentication server.
File Name Extensions	Set this parameter when you select **Specific files** or **Specific files excluded** for **Authentication Scope**. Only requests for files with the specified file name extensions are authenticated or not authenticated. • Only lowercase letters and digits are supported. Use semicolons (;) to separate multiple file name extensions.
Signing Key	Authentication password. The value contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.

Parameter	Description
Secondary Key	(Optional) Secondary password for authentication. If you want the old and new keys to take effect, you can set the old key as the secondary key. Users can access content only after CDN verifies the primary or secondary key. • A key contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.
Encryption Algorithm	**MD5** or **SHA256**.
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s.

Authentication Calculator

Using the authentication calculator, you can generate a signed URL for users. Set parameters according to **Table 4-34** and **Table 4-35**, 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 4-35 Parameter description

Parameter	Description
Signing Key	Authentication password. Enter 6 to 32 characters, including letters and digits. The value must be the same as the signing key specified in the token authentication configuration.
Access Path	Path of the content, which starts with a slash (/) and does not carry a query string.
Encryption Algorithm	**MD5** or **SHA256**.
Start Time	Time when the signed URL will take effect.
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s. If this value is greater than the validity period set in the token authentication settings, the latter will be used. Example: If you set this parameter to 2,000s, but the validity period set in the token authentication settings is 1,800s, the validity period of signed URLs will be 1,800s.

Disabling Token Authentication

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

Example

The following uses the MD5 algorithm as an example:

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

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

4.9.6.4 Signing Method C2

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

CAUTION

- Token authentication is disabled by default.
- You cannot configure this function for domain names with special configurations on the CDN console.
- When a client request fails the authentication and is blocked, PoP resources are consumed, generating a small amount of traffic or bandwidth fees. If the service type of the domain name is whole site acceleration, the client request is also charged for the request fee.
- When token authentication is configured, user requests will include authentication parameters. If **Ignore specific parameters** is not configured:
  - Origin pull will become frequent.
  - If your origin server is an OBS bucket, fees for bucket outbound traffic will incur.

How It Works

Example signed URLs look like:

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

The following table describes the parameters in a signed URL.

Table 4-36 Parameter description

Parameter	Description
DomainName	Acceleration domain name.
timestamp	Time when the authentication server generates a signed URL, that is, the authentication start time. The value is the total number of seconds that have elapsed since 00:00:00 January 1, 1970. It is a decimal or hexadecimal integer.
Validity period	How long a signed URL remains effective. The value ranges from 0s to 31,536,000s. Example: If the validity period is set to 1,800s, users can access CDN only when the current time is earlier than or equal to **timestamp** + 1,800s. Or, the signed URL is considered invalid.
md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of lowercase letters and digits.
sha256	A string of 64 characters calculated using the SHA256 algorithm. The string consists of lowercase letters and digits.
Filename	Back-to-origin URL. Its value must start with a slash (/) and does not include the parameters following the question mark (?).
PrivateKey	Signing key, which is used to generate a signed URL, for example, **huaweicloud12345**. A key contains 6 to 32 characters, including letters and digits.
Authentication parameter	Authentication parameter carried in a URL. The default value is **auth_key**.
Time parameter	Name of the timestamp parameter carried in the request URL.

Verification Method

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

1. Checks whether the authentication parameter is included in the request. If not, the request is considered invalid and an HTTP 403 error code is returned.
2. Checks whether the value of **timestamp** plus the validity period specified in the signed URL is later than the current time.

- If not, the signed URL is considered invalid and the HTTP 403 error is returned.
- If yes, the time verification passes and CDN goes to step **3**.

3. Constructs **sstring**, calculates **HashValue** using this string and the MD5 or SHA256 algorithm, and compares **HashValue** with the **md5hash** or **sha256** value in the request. If the **md5hash** or **sha256** value is the same as **HashValue**, the authentication is successful and the requested file is returned. Or, the authentication fails and an HTTP 403 error code is returned.
   HashValue is calculated as follows:

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

   Or

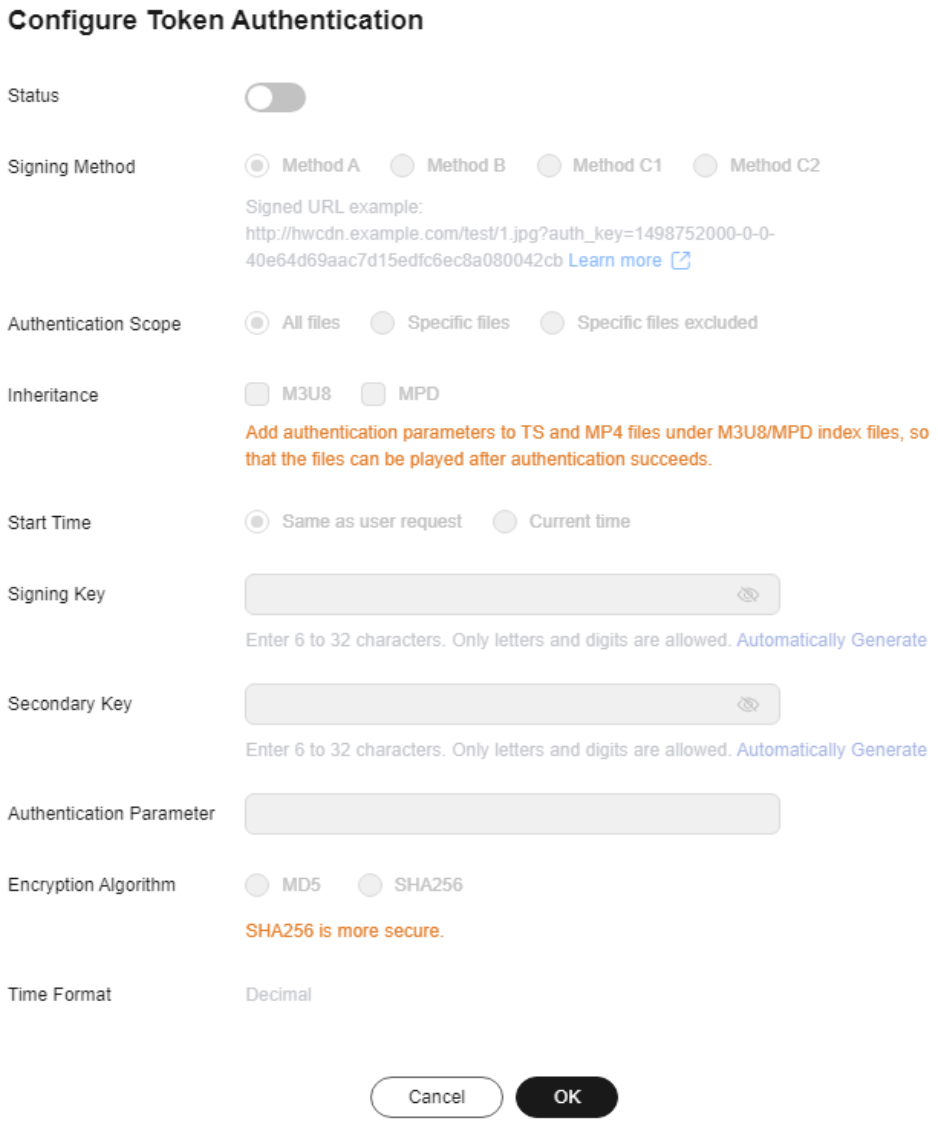
```
sstring = "PrivateKeyFilenameTimestamp"
HashValue = sha256sum(sstring)
```

Procedure

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

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

Figure 4-50 Configuring token authentication



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

Table 4-37 Parameter description

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

Parameter	Description
Inheritance	Add the authentication parameter to TS and MP4 files under M3U8/MPD index files, so that the files can be played after authentication succeeds. **NOTE** • If there are multi-layer M3U8/MPD files, only the first-layer M3U8/MPD files are parsed, and the TS/MP4 streams of M3U8/MPD files in other layers are not expanded. • The standard M3U8 format is supported. M3U8 files are parsed by line. If the parsing fails, responses from the origin server are returned to users. URIs starting with the **#EXT-X-MAP** tag and URLs/URIs not starting with the pound key (#) are supported. • The standard MPD format is supported. MPD files are parsed by line. If the parsing fails, responses from the origin server are returned to users. The URI between tags **<BaseURL>** and **</BaseURL>** is identified. The **SegmentTemplate** tag is not supported. • If your M3U8/MPD index files contain special characters, CDN does not automatically transcode the characters during authentication calculation. If clients have the logic for automatically transcoding special characters, the access may fail due to the authentication failure. • If the origin server returns resources compressed using gzip or Brotli to CDN PoPs, the authentication inheritance settings become invalid.
Start Time	• **Same as user request**: time when a user accesses the M3U8/MPD file. • **Current time**: current time of the authentication server.
File Name Extensions	Set this parameter when you select **Specific files** or **Specific files excluded** for **Authentication Scope**. Only requests for files with the specified file name extensions are authenticated or not authenticated. • Only lowercase letters and digits are supported. Use semicolons (;) to separate multiple file name extensions.
Signing Key	Authentication password. The value contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.
Secondary Key	(Optional) Secondary password for authentication. If you want the old and new keys to take effect, you can set the old key as the secondary key. Users can access content only after CDN verifies the primary or secondary key. • A key contains 6 to 32 characters, including letters and digits. **NOTE** For security purposes, you are advised to use 8 to 32 characters.

Parameter	Description
Authentication Parameter	Authentication parameter carried in a URL. The default value is **auth_key**. • Enter up to 100 characters. • Start with a letter. Enter letters, digits, and underscores (_).
Time Parameter	Authentication time parameter. The default value is **timestamp**. This parameter affects the signed URL. For details, see **How It Works**. • Start with a letter. Enter up to 100 characters, including letters, digits, and underscores (_).
Time Format	Format of the time in the signed URL.
Encryption Algorithm	**MD5** or **SHA256**.
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s.

Authentication Calculator

Using the authentication calculator, you can generate a signed URL for users. Set parameters according to **Table 4-37** and **Table 4-38**, 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 4-38 Parameter description

Parameter	Description
Signing Key	Authentication password. Enter 6 to 32 characters, including letters and digits. The value must be the same as the signing key specified in the token authentication configuration.
Access Path	Path of the content, which starts with a slash (/) and does not carry a query string.
Encryption Algorithm	**MD5** or **SHA256**.
Start Time	Time when the signed URL will take effect.
Time Format	Format of the time in the signed URL. Time format of the signed URL, which must be the same as that specified in the token authentication settings.

Parameter	Description
Validity Period	How long the signed URL remains effective. The value ranges from 0s to 31,536,000s. If this value is greater than the validity period set in the token authentication settings, the latter will be used. Example: If you set this parameter to 2,000s, but the validity period set in the token authentication settings is 1,800s, the validity period of signed URLs will be 1,800s.

Disabling Token Authentication

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

Example

The following uses the MD5 algorithm as an example:

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

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

4.9.7 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: CDN PoPs perform authentication.

Remote authentication: CDN PoPs forward user requests to a server you specify for authentication.

The remote authentication process is as follows.

Figure 4-51 Remote authentication process

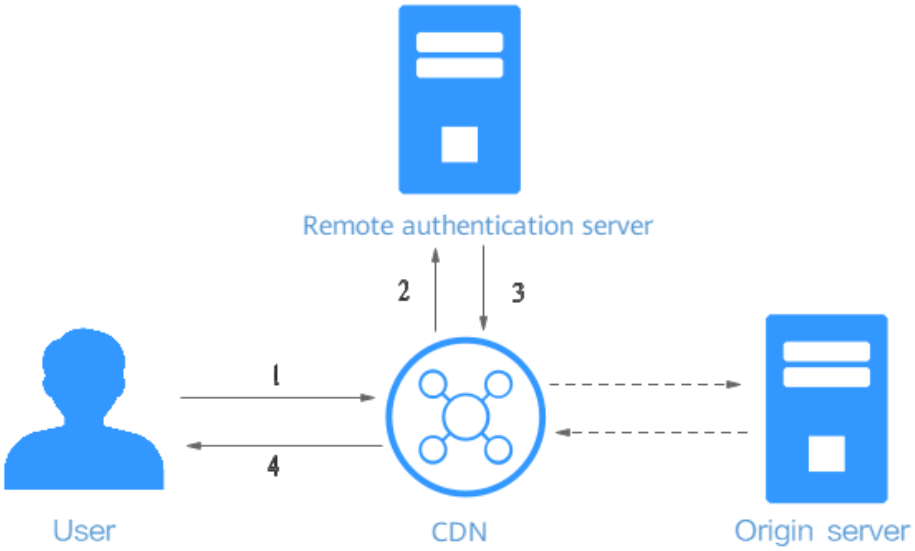


Table 4-39 Process description

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.
- When a client request fails the authentication and is blocked, PoP resources are consumed, generating a small amount of traffic or bandwidth fees. If the service type of the domain name is whole site acceleration, the client request is also charged for the request fee.

Procedure

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

The CDN console is displayed.

2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Access Control** tab and click **Edit** next to **Remote Authentication**.

Figure 4-52 Configuring remote authentication

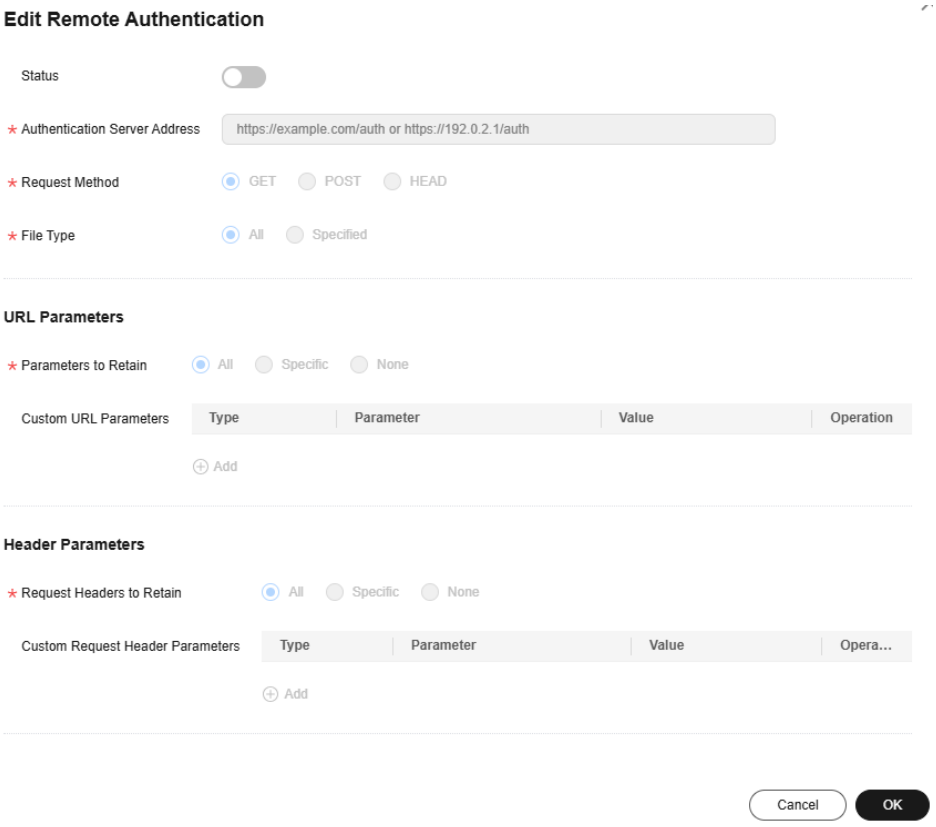


Table 4-40 Parameter description

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

Parameter	Description	Example
Request Method	Request method supported by the authentication server. GET, POST, and HEAD are supported.	GET
File Type	• **All**: Requests for all files are authenticated. • **Specific file types**: Requests for files of specified types are authenticated. Separate types by vertical bars (|), for example, **jpg|MP4**. – Enter up to 512 characters, including letters and digits. • File types are case insensitive. For example, **jpg** and **JPG** indicate the same file type.	All
Parameters to Retain	Parameters that need to be authenticated in user requests. You can retain or ignore all URL parameters or retain specific URL parameters. • Parameters are case insensitive. Use vertical bars (|) to separate them.	All
Custom URL Parameters	Parameters to be added when CDN PoPs forward user requests to the remote authentication server. You can select **preset parameters** or customize parameters (parameters and values are case insensitive). • **Custom**: Customize a parameter and set the value to a string. • **Select**: Select a preset or customized parameter and select a variable as the value.	Select **http_host**. Value: **$http_host**.
Request Headers to Retain	Headers to be authenticated in user requests. You can retain or ignore all request headers or retain specific request headers. Headers are case insensitive. Use vertical bars (|) to separate them.	All

Parameter	Description	Example
Custom Request Header Parameters	Request headers to be added when CDN PoPs forward user requests to the remote authentication server. You can select **preset request headers** or customize request headers (headers and values are case insensitive). • **Custom**: Customize a parameter and set the value to a string. • **Select**: Select a preset or customized parameter and select a preset variable as the value.	Select **http_referer**. Value: **$http_referer**.
Success Status Code	Status code returned by the remote authentication server to CDN PoPs when authentication is successful. Value range: 2*xx* and 3*xx*.	200
Failure Status Code	Status code returned by the remote authentication server to CDN PoPs when authentication fails. Value range: 4*xx* and 5*xx*.	403
Custom Response Status Code	Status code returned by CDN PoPs to users when authentication fails. Value range: 2*xx*, 3*xx*, 4*xx*, and 5*xx*.	403
Timeout Interval	Duration from the time when a CDN PoP forwards an authentication request to the time when the CDN PoP receives the result returned by the remote authentication server. Enter **0** or a value ranging from 50 to 3,000. The unit is millisecond.	60
Action After Timeout	How CDN PoPs process a user request after authentication times out. • **Accept**: The user request will be accepted and the requested resource will be returned. • **Reject**: The user request will be rejected and the configured custom response status code will be returned.	Reject

Table 4-41 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.

Examples

Assume that you have enabled remote authentication for **example.com** and configured settings shown in **Figure 4-53**.

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

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

Figure 4-53 Remote authentication

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

4.9.8 IP Access Frequency

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

Precautions

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

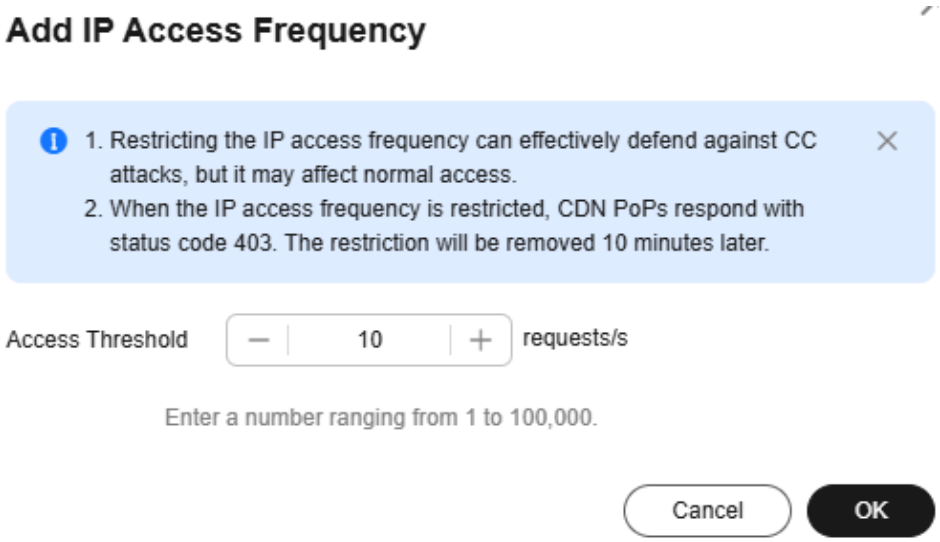
- When the IP access frequency limit is triggered, client requests are blocked and PoP resources are consumed, generating a small amount of traffic or bandwidth fees. If the service type of the domain name is whole site acceleration, the client request is also charged for the request fees.
- By default, 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 4-54 IP access frequency

5. Set **Access Threshold** and click **OK**.

   When the number of times that a single client 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.

   - Value range: 1 to 100,000 requests/second
   - A low threshold can cause frequent blocking. For example, setting it to **1** means that CDN will block a client IP address for 10 minutes after receiving just one request per second to a specific URL from that IP address.
   - If you change **Access Threshold** within the restriction duration, the change takes effect after the restriction is removed.
6. To disable this function, turn off the **IP Access Frequency** switch. This will clear related configuration.

Examples

Configuration: You have restricted the IP access frequency of domain name www.example.com to 10,000 requests/second.

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

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

4.10 Advanced Settings

4.10.1 Overview

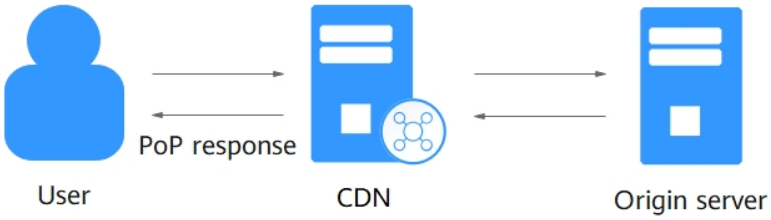
You can modify advanced settings of a domain name that is in the **Enabled** or **Configuring** state and is not locked or banned.

Item	Description
HTTP Header Settings (Cross-origin Requests)	Customize values of HTTP response headers for your website.
Custom Error Pages	Customize error pages returned to user clients.
Smart Compression	Compress static content on your websites by reducing file size. This speeds up file transfer and saves you a lot of bandwidth.
WebSocket	If you have enabled whole site acceleration in scenarios such as on-screen commenting, collaborative session, market data broadcast, sports live update, online education, and IoT, configure WebSocket to implement long-term bidirectional data transmission.
Request Rate Limiting	Limit the user request rate within a specific range to reduce costs and the risk of burst bandwidth.
Usage Cap	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, reducing high bills caused by traffic theft or attacks.

4.10.2 HTTP Header Settings (Cross-origin Requests)

Background

HTTP headers are part of an HTTP request or response message that define the operating parameters of an HTTP transaction. HTTP headers in this function refer to the information that PoPs send to clients. After you set HTTP headers for a domain name, CDN includes them in responses to user requests for resources within that domain name.



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

Precautions

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

Supported Response Headers

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

- **Content-Disposition**

  This header can start a download on clients and specify the name of the file to be downloaded.

  When a server sends a file to a browser, as long as the file format is supported (for example, TXT or JPG), the file is opened using the browser by default. You can use this header to treat the file as an attachment and let users save it with a specific file name.

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 OBS Objects in My Web Browser?**

- **Content-Language**

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

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

  This header carries the domain names that are allowed for CORS after server authentication. For a simple CORS request, the browser determines whether to return the requested content to the client based on this header. For a preflight request, the browser determines whether to initiate an actual CORS request to the server based on this header.

  NOTE

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

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

  This header carries the methods that are allowed for CORS after server authentication. For a simple CORS request, the browser determines whether to return the requested content to the client based on this header. For a preflight request, the browser determines whether to initiate an actual CORS request to the server based on this header.

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

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

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

  This header specifies the response headers that the browser can expose to the client. You can use this header to define the response headers visible to the client. The following response headers are visible to the client by default: **Cache-Control**, **Content-Language**, **Content-Type**, **Expires**, **Last-Modified**, and **Pragma**.

- **Custom**

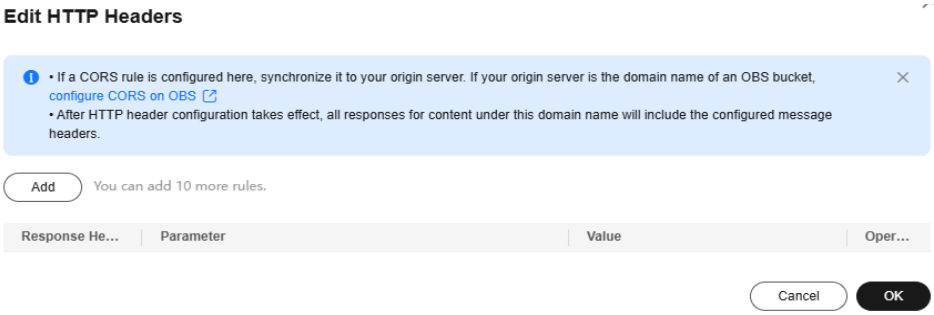
  If the preceding response headers cannot meet your needs, you can create response headers. A custom response header contains 1 to 100 characters, starting with a letter and consisting of letters, digits, and hyphens (-).

Procedure

1. Log in to the **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 **Edit HTTP Headers** dialog box is displayed.

Figure 4-55 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.
Delete	The header will be deleted from the response.

7. Set the header parameter and value.

Parameter	Description	Example Value
Content-Disposition	Starts a download on the client side and specifies the name of the file to be downloaded. **Value requirements**: Enter 1 to 1,000 characters. For a typical configuration, see the example on the right.	attachment;filename=FileName.xls
Content-Language	Specifies the language of the response page of the client. **Value requirements**: Enter 1 to 1,000 characters. For a typical configuration, see the example on the right.	zh-CN en-US

Parameter	Description	Example Value
Access-Control-Allow-Origin	Specifies the foreign domain URLs (request sources) that are allowed to access the resource in CORS. **Value requirements**: ● Enter up to 66 URLs. ● Wildcard domain names are supported. ● Enter up to 1,000 characters. ● Separate URLs with commas (,). ● Start with **http://** or **https://**. ● If this is set to *****, no URLs are allowed after the wildcard (*). ● Domain names with port numbers are supported. ● The value can be **null**, which is case-insensitive.	Example 1: https://www.example.com Example 2: * Example 3: https://www.example.com,https://www.example01.com,https://*.abc.com
Access-Control-Allow-Methods	Specifies the HTTP request methods that can be used in a CORS request. **Value requirements**: Enter 1 to 1,000 characters. Separate methods by commas (,).	GET,POST,HEAD
Access-Control-Max-Age	Specifies how long to cache the results of CORS preflight requests on specific resources. **Value requirements**: This value is expressed in seconds and ranges from 0 to 1,000,000,000.	86400

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 1,000 characters. Multiple headers can be configured at the same time. Separate them by commas (,).	Content-Length,Content-Encoding
Access-Control-Allow-Headers	Specifies the fields that can be carried in a cross-domain request. **Value requirements**: Enter 1 to 1,000 characters. Multiple fields can be configured at the same time. Separate them by commas (,).	X- Custom-Header

Parameter	Description	Example Value
Custom	Specifies the custom response header. A response header starts with a letter and contains 1 to 100 characters, including letters, digits, and hyphens (-). **Value requirements**: Enter 1 to 1,000 characters, which can contain letters, digits, spaces, and the following special characters: .-_*#!&+|^~'"/:;,=@?<> **NOTE** • If the custom parameter is **Cache-Control**, the value can be **public**, **private**, **no-cache**, **no-store**, **no-transform**, **only-if-cached**, **proxy-revalidate**, **must-revalidate**, **immutable**, **max-age=*******, **stale-while-revalidate=*******, **s-maxage=*******, **stale-if-error=*******, or **min-fresh=******* (***** is a number). Enter up to 10 values and separate them by commas (,). • The value of the **Cache-Control** header may affect the PoP cache.	x-testcdn

8. Click **OK**.

Constraints

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

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

- CDN does not support the following response headers.

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

Helpful Links

- **What Should I Do If the Browser Displays a Message Indicating that a Cross-domain Exception Occurs After CDN Is Enabled?**
- **Why Is a File in an OBS Bucket with CDN Acceleration Enabled Automatically Downloaded When I Access the File?**

4.10.3 Custom Error Pages

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

Precautions

- You can customize error pages for status codes 4*xx* and 5*xx*.
- If CDN acceleration is enabled for the custom error pages, you will be billed by CDN.
- You cannot customize error pages 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 4-56 Customizing an error page

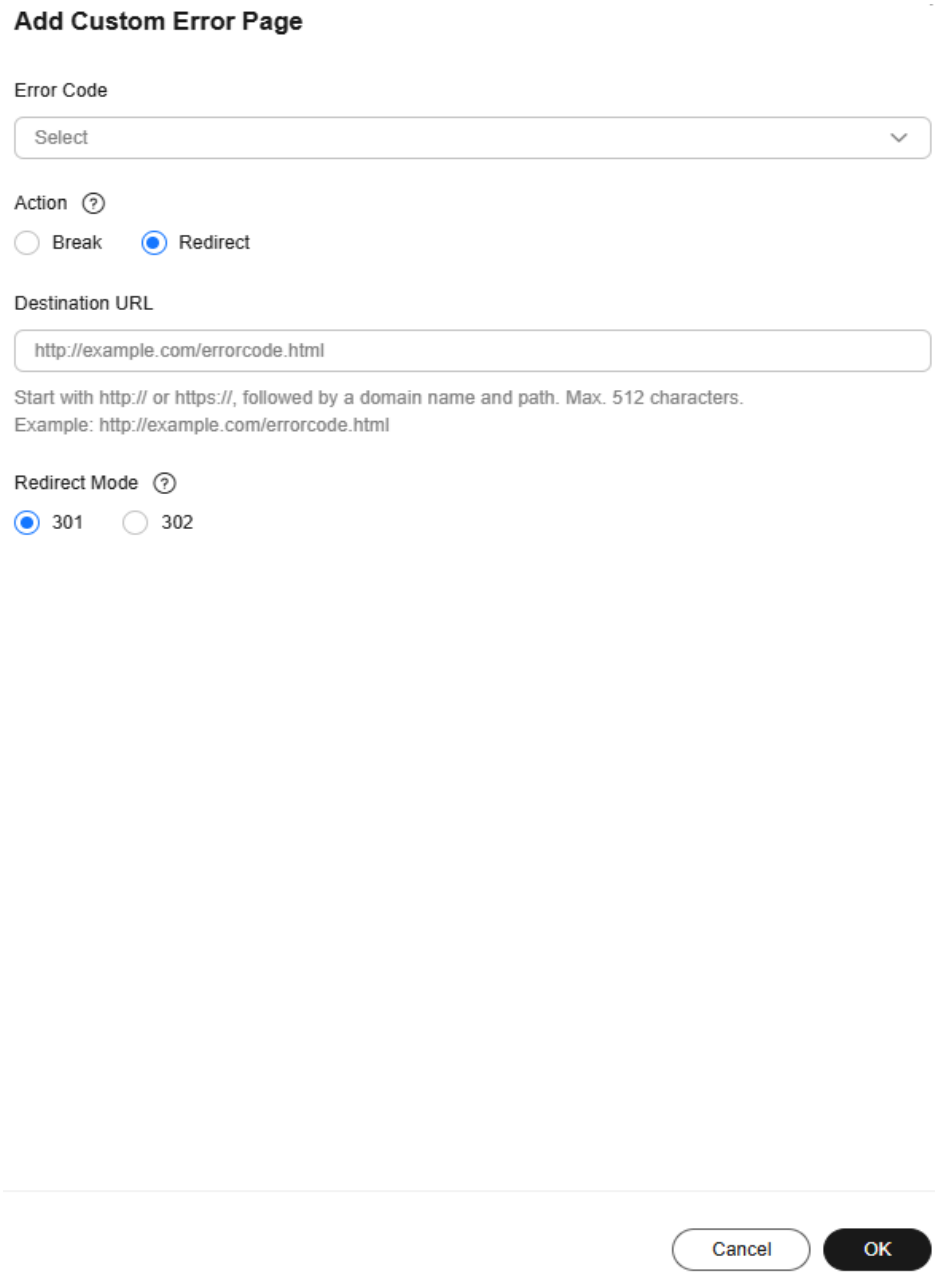


Table 4-42 Parameter description

Parameter	Description	Example
Error Code	Error code (4*xx* or 5*xx*) whose error page needs to be customized.	404

Parameter	Description	Example
Action	**Break**: CDN redirects requests with the specified error code returned to the destination URL. Once this rule runs, CDN skips all remaining rules. **Redirect**: CDN redirects requests with the specified error code returned to the destination URL. Once this rule runs, CDN will run any other matched rules.	Break
Destination URL	When you set **Action** to **Break**, CDN uses full path match. Enter only one path, start with a slash (/), and enter up to 512 characters. Example: **/errorcode.html** When you set **Action** to **Redirect**, start the URL with http:// or https://, enter up to 512 characters, and include the complete domain name and path. Example: **http://example.com/errorcode.html**	/errorcode.html
Redirect Mode	Required when **Action** is set to **Redirect**. Mode of redirecting the error code page to a new page. Select **301** or **302**.	301

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.

4.10.4 Smart Compression

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

Precautions

- Starting in late January 2025, CDN will change the default file size for compression. If you do not specify a file size when enabling smart compression:
  - Before the change, all files are compressed by default.
  - After the change, files whose size ranges from 0 MB to 30 MB are compressed by default.
- Do not enable this function if MD5 verification has been configured for your origin server. When CDN compresses static files, the MD5 value is changed. As a result, the MD5 value of the compressed file is different from that of the file on the origin server.
- 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 4-57 Smart compression

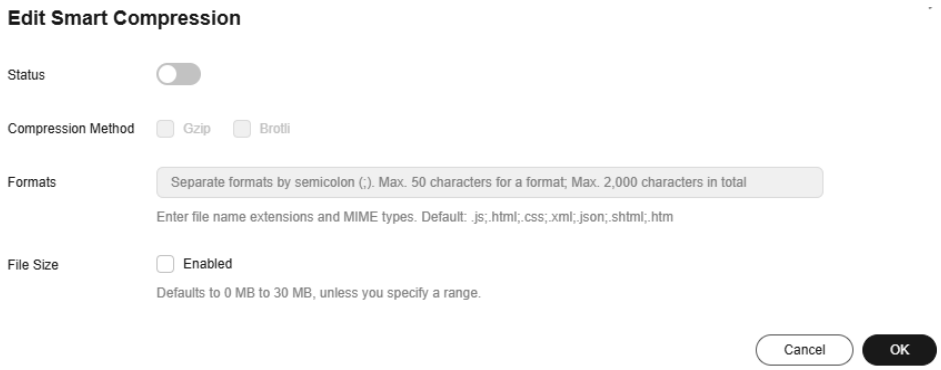


Table 4-43 Parameter description

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. Files in this range will be compressed. ● The maximum file size range is 0 MB to 30 MB. ● If no range is specified, files no larger than 30 MB will be compressed.

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

4.10.5 WebSocket

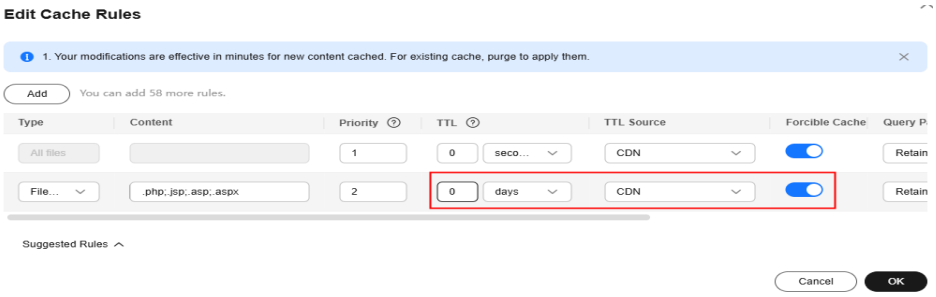
If you have added whole site acceleration domain names to CDN to meet requirements such as on-screen commenting, collaborative session, market data broadcast, sports live update, online education, and IoT connectivity, you can configure WebSocket to implement long-term bidirectional data transmission.

Background

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

Precautions

- This function applies only to domain names whose **Service Type** is **Whole site**. The domain resources are not cached on CDN PoPs. That is, **TTL** of these resources is set to **0**, **TTL Source** is set to **CDN**, and **Forcible Cache** is enabled.



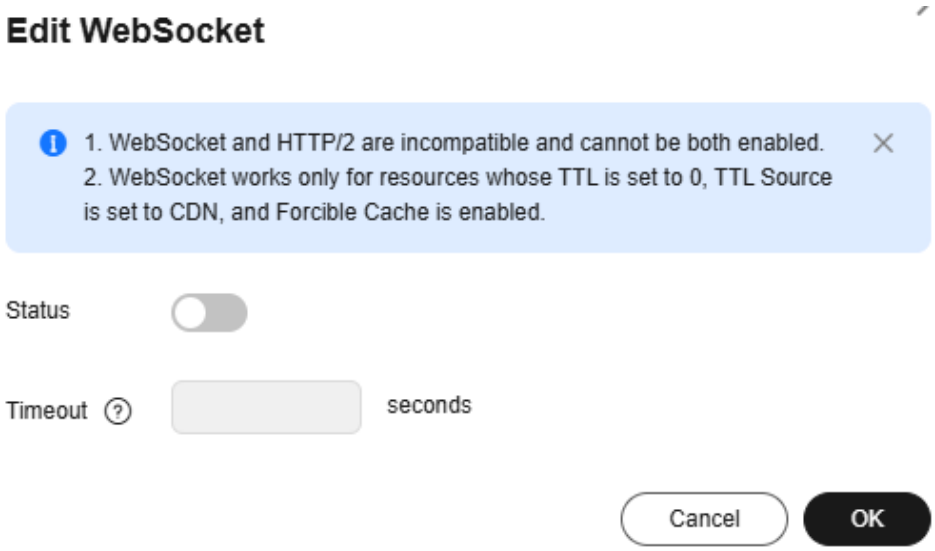
- This function is in OBT and is available for free trial.
- The maximum timeout interval is 300 seconds. If no message is transferred within the specified interval, the connection is closed.
- You cannot configure WebSocket for domain names with special configurations.
- Do not enable both WebSocket 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 4-58 WebSocket Settings



6. Turn on the **Status** switch, set a proper timeout period (1 to 300 seconds), and click **OK**. This timeout defines how long CDN maintains a session after establishing a connection. It will disconnect if no communication occurs during this period.

4.10.6 Request Rate Limiting

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

Precautions

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

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Advanced Settings** tab.
5. In the **Request Rate Limiting** area, click **Edit**.
6. Click **Add** to add a rule.

Figure 4-59 Configuring request rate limiting

Table 4-44 Parameters

Parameter	Description
Content Type	**All files** **Directory**: files in a specific directory
Content	• This parameter is left blank when **Content Type** is set to **All files**. • When **Content Type** is set to **Directory**, specify this parameter. 1. Start with a slash (/), for example, **/test/folder**. 2. Do not end with a slash (/). 3. Enter one directory per rule.
Rate Limit Type	Rate limiting by transmission traffic is supported. That is, when the traffic of a single HTTP request reaches the specified value, the access speed is limited. The access speed of subsequent requests cannot exceed the specified rate limit.

Parameter	Description
Rate Limit Condition	Volume of the transmitted traffic that triggers rate limiting. • The unit is byte. The maximum value is 1 GB, that is, 1,073,741,824 bytes.
Rate Limit	Maximum access speed when rate limiting starts. • The maximum value is 100 Mbit/s.
Periods	Periods when the rate is limited, in the 24-hour clock. Period format: HHMM-HHMM (in UTC+08:00). Periods are separated by commas (,). Example: **0100-0200,2200-2300**. Default value: **0000-2400**, indicating all day. • You can set up to 10 periods.
Priority	Priority of a rate limiting rule. Each cache rule must have a unique priority. If multiple rate limiting rules are configured for a resource, CDN uses the rate limiting rule with the highest priority. • Enter an integer ranging from 1 to 100. A greater number indicates a higher priority.

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

4.10.7 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, reducing high bills caused by traffic theft or attacks.

Scenarios

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 binds the domain name with a CDN PoP in the **hosts** file to forcibly resolve requests, CDN will refuse to provide services after receiving the requests.

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.
- You cannot set usage caps for domain names with special configurations.
- When a domain name reaches the usage cap and CDN is disabled, usage capping will be executed again 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, usage capping was not executed again 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 4-60 Setting the usage cap

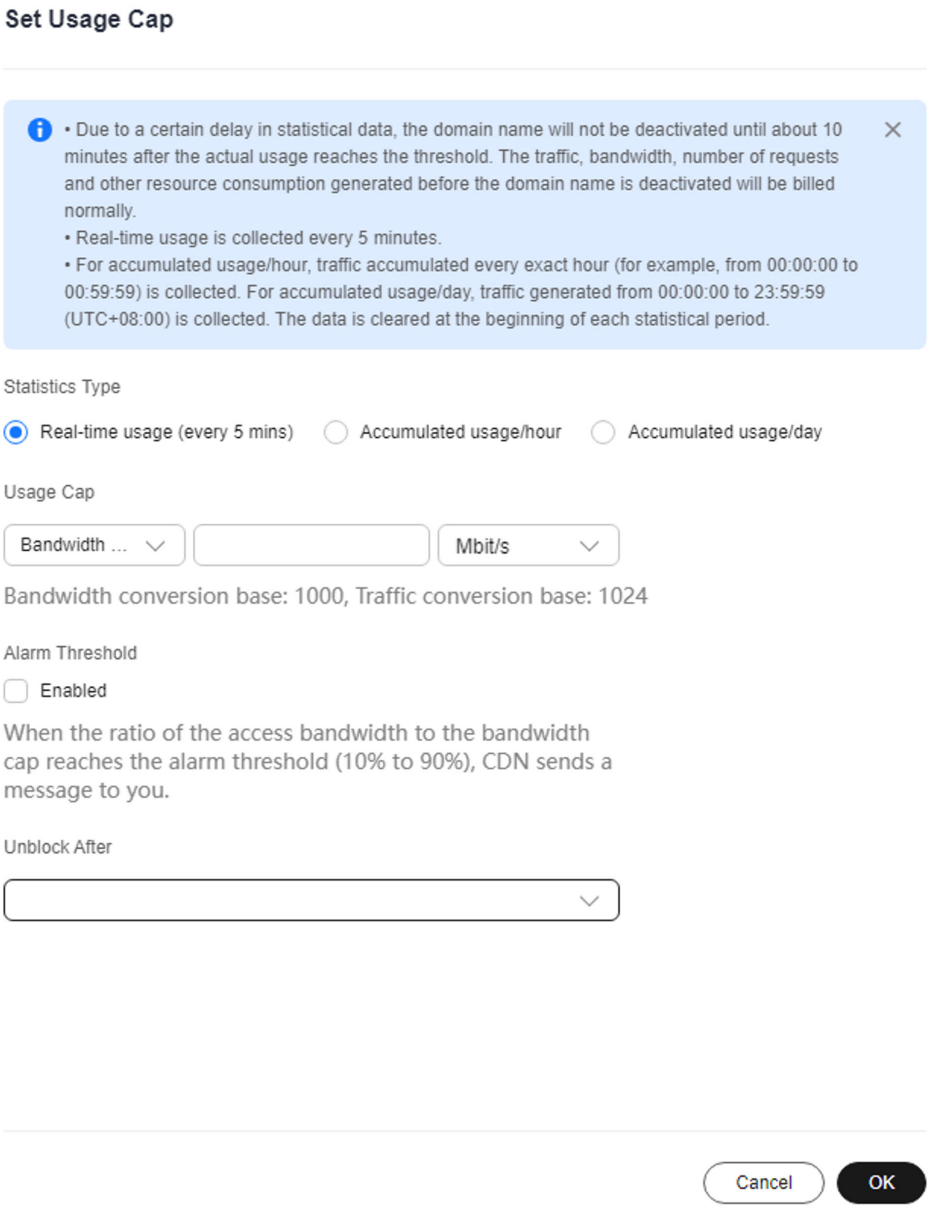


Table 4-45 Parameters

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. This customer added domain name **example.com** to CDN, enabled a bandwidth cap, and set the 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. This customer added domain name **example.com** to CDN, enabled a traffic cap, and set the 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.

4.10.8 Burst Bandwidth Alert

You can enable this function and set a bandwidth threshold. When the bandwidth of client requests reaches the threshold, CDN alerts you, helping you identify attacks promptly and prevent excess billing caused by bandwidth theft or attacks.

Scenarios

This function is suitable for domain names with stable bandwidth.

Assume that your domain name **example.com** consumes 500 Mbit/s to 2 Gbit/s per day and rarely uses over 2 Gbit/s. You can set the bandwidth threshold to 2 Gbit/s. When the bandwidth reaches 2 Gbit/s, alerts are sent to the mobile number and email address bound to your account. You can quickly check the domain access status to prevent high bandwidth caused by attacks and excess billing.

Precautions

- Set an appropriate threshold. Setting it lower than 100 Mbit/s may frequently trigger alerts.
- If major events are expected to generate high bandwidth, adjust the threshold or temporarily disable this function. Remember to adjust the threshold again after events.
- Monitoring alerts may be delayed by about 10 minutes.
- SMS messages and emails are sent to the mobile number and email address bound to your account. 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**. To view the **mobile number and email address of the recipient**, see **What Are the Parameters and How Can I Use Them in the Account Center?**

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 **Burst Bandwidth Alert**.

Figure 4-61 Setting a bandwidth threshold

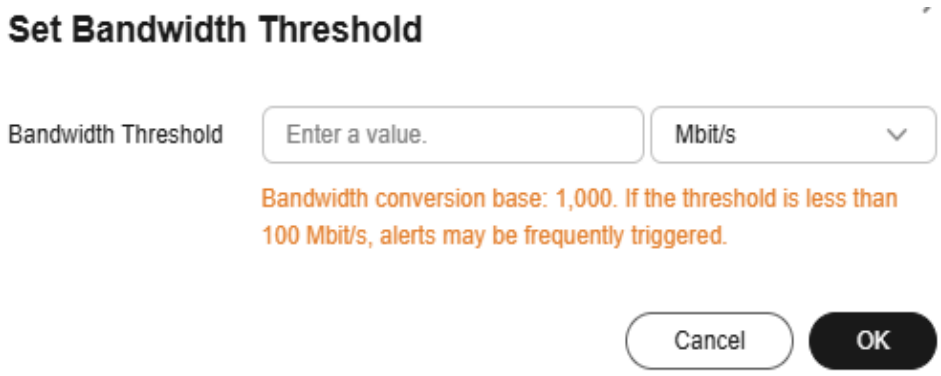


Table 4-46 Parameters

Parameter	Description
Bandwidth Threshold	When the total bandwidth of client requests reaches this threshold, an alert is triggered and sent to your account contact. • Range: 1 Mbit/s to 10 Tbit/s. Conversion base: 1,000 • Set an appropriate threshold. A high or low threshold reduces the alert effect.

5. Enter a threshold and click **OK**.

4.11 Video Settings

4.11.1 Video Seek

Background

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

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

Table 4-47 File formats

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

Precautions

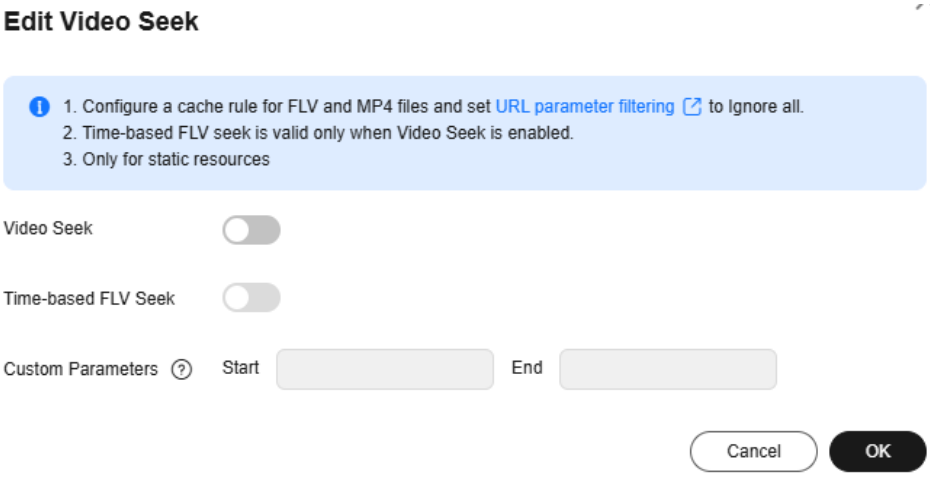
- You have configured a cache rule for FLV and MP4 files and set **Query Parameters** to **Ignore all**.
- If the service type of your domain name is whole site acceleration, this function takes effect only for static resources.

Procedure

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

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

Figure 4-62 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**.

4.12 Tag Management

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

Scenarios

Tags help you identify your cloud resources. When you have many cloud resources of the same type, you can use tags to classify them by dimension (for example, use, owner, or environment). You can quickly search for specific cloud resources based on the tags added to them. For example, you can define a set of tags for cloud resources in an account to track the owner and usage of each cloud resource, making resource management easier.

Constraints

- You can add up to 20 tags to each domain name.
- 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 4-63 Editing a tag

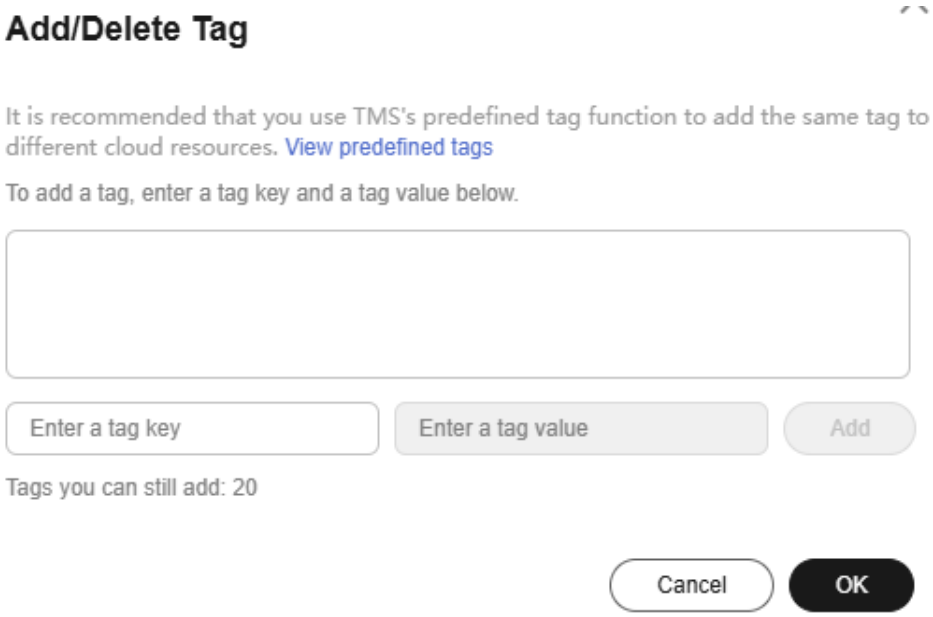


Table 4-48 Parameter description

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 4-64 Editing tags

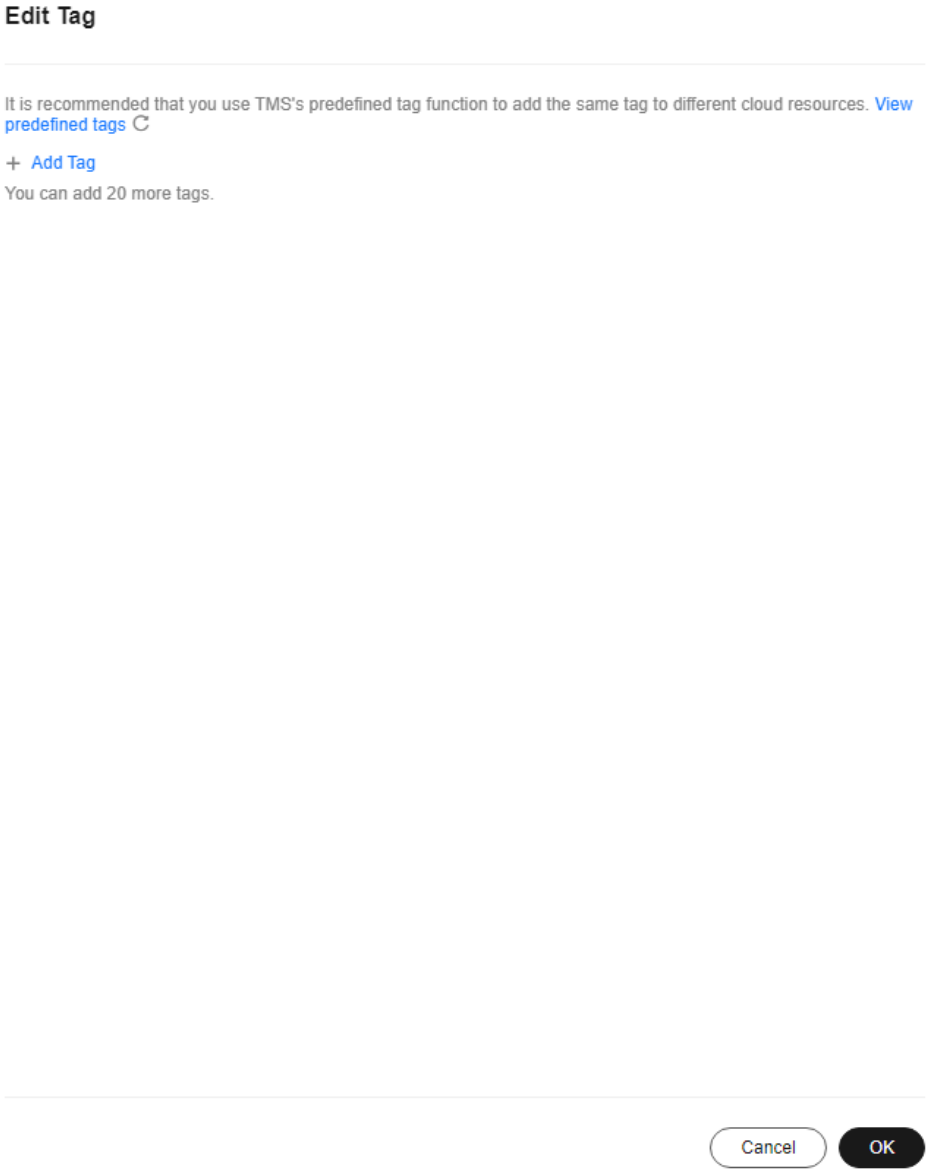


Table 4-49 Parameter description

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. 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.

4.13 Rules Engine

Scenarios

The rules engine allows you to configure rules in graphical mode, which is more flexible and fine-grained. By restricting trigger conditions, you can control the resource range for the configuration to take effect, meeting requirements in various scenarios, such as:

- When the CDN PoP configuration cannot apply to specific resources, for example, when the access control conditions of some resources are different from the global configuration.

Precautions

- To use the rules engine, submit a service ticket.
- You can add up to 10 rules for a domain name.
- Domain names whose **Service Type** is **Whole site** do not support rules engines.
- You cannot configure the rules engine for domain names with special configurations.
- The rules engine configuration takes precedence over settings under other tabs.
- By default, the newest rule is displayed at the top. When multiple rules exist, those listed higher have a higher priority than those listed lower. That is, if multiple rules are matched, the rule with the highest priority takes effect.
- A trigger condition supports up to three levels of nesting. The logical operator of all rules at the deepest level must be either **And** or **Or**.

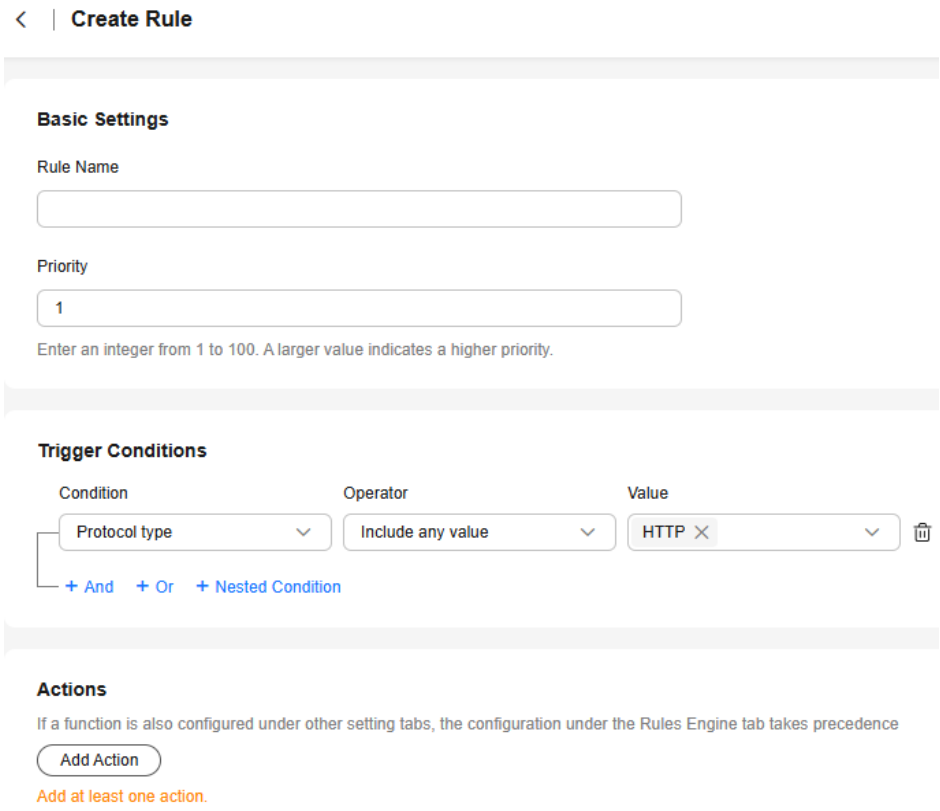
Procedure

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 **Rules Engine** tab and click **Create Rule**.

5. Set **Rule Name**, configure the rule based on **Trigger Conditions** and **Actions**, and click **OK**.
   - **Rule Name**: Enter 1 to 50 characters.
   - **Priority**: Enter a number ranging from 1 to 100. A larger number indicates a higher priority.

Figure 4-65 Creating a rule



Trigger Conditions

Each trigger condition consists of a logical operator and a condition rule.

Logical operator: **And** and **Or** are used to judge the logic of condition rules (including nested rules) at the same level.

- **And**: triggers actions only when all conditions of the current level are met.
- **Or**: triggers actions when a condition of the current level is met.

Condition rule: consists of a condition, operator, and value. The condition and value define requests to comply with the rule. The operator defines the use cases of the rule.

Operator:

- **Include any value**: The condition is met when user requests include any value of the condition.
- **Exclude any value**: The condition is met when user requests do not include any value of the condition.

- **Exist**: The condition is met when parameters configured in the condition (regardless of the value) exist in user requests.
- **Do not exist**: The condition is met when parameters configured in the condition (regardless of the value) do not exist in user requests.

Trigger condition parameters

When a user request matches a trigger condition, the specified actions are performed. **Table 4-50** lists the trigger condition parameters.

Table 4-50 Trigger condition parameters

Condition	Condition Description	Name	Operator	Value	Case Sensitive
Protocol type	Protocols used by client requests, for example, **HTTP** or **HTTPS**	N/A	• Include any value • Exclude any value	• HTTP • HTTPS	N/A
Request method	Methods used by client requests, for example, **GET** or **PUT**	N/A	• Include any value • Exclude any value	**GET**, **POST**, **HEAD**, **PUT**, **DELETE**, **OPTIONS**, **PATCH**, **TRACE**, and **CONNECT**	N/A

Condition	Condition Description	Name	Operator	Value	Case Sensitive
URL path	Paths in client request URLs, excluding query parameters, for example, **/favicon.ico**	N/A	• Include any value • Exclude any value	• Start a URL with a slash (/) and do not contain http://, https://, or the domain name, for example, **/test/index.html**. • Enter only one regular expression to match requests. Use the following characters in the regular expression: ^$* +|?:.\<=![]{}()-_;~/	By default, **Case sensitive** is enabled. When it is disabled, uppercase and lowercase values are considered equal.

Condition	Condition Description	Name	Operator	Value	Case Sensitive
HTTP request header	Headers carried in user requests	Request header name. • Enter only one request header name. • Use letters, digits, hyphens (-), periods (.), and underscores (_).	• Include any value • Exclude any value • Exist • Do not exist	• Set one or more header values. • Enter only one regular expression to match requests. Use the following characters in the regular expression: ^$*+|?:.\<=![]{}()-_;~/	By default, **Case sensitive** is enabled. When it is disabled, uppercase and lowercase values are considered equal.

Condition	Condition Description	Name	Operator	Value	Case Sensitive
Query parameter	Query parameters carried in user request URLs	Query parameter name	• Include any value • Exclude any value • Exist • Do not exist	• Set one or more parameter values. • Enter only one regular expression to match requests. Use the following characters in the regular expression: ^$*+|?:.\<=![]{}()-_;~/	By default, **Case sensitive** is enabled. When it is disabled, uppercase and lowercase values are considered equal.
File name	Names of files requested by clients, for example, **name1**.	N/A	• Include any value • Exclude any value	Set one or more file names.	By default, **Case sensitive** is enabled. When it is disabled, uppercase and lowercase values are considered equal.
File name extension	Types of files requested by clients. CDN scans a file name from right to left until it encounters the first period (.) to identify the file name extension, for example, **.txt**.	N/A	• Include any value • Exclude any value	Select or enter suffixes, such as .txt, .doc, .html, .jpg, .png, .svg, .zip, and .rar.	By default, **Case sensitive** is enabled. When it is disabled, uppercase and lowercase values are considered equal.

Condition	Condition Description	Name	Operator	Value	Case Sensitive
Client IP address	Client IP addresses	• Connecting IP • X-Forwarded-For header	• Include any value • Exclude any value	Enter IPv4 addresses (for example, **0.0.0.0**) and IPv6 addresses (for example, **240e:95c:3004:2:3:0:0:***XXX*). Enter CIDR blocks (for example, **192.168.***XXX.XXX***/31**). The prefix length ranges from 1 to 32 bits for IPv4 and 1 to 128 bits for IPv6.	N/A
Client IP version	IPv4 or IPv6	• Connecting IP • X-Forwarded-For header	• Include any value • Exclude any value	• IPv4 • IPv6	N/A

Condition	Condition Description	Name	Operator	Value	Case Sensitive
Nginx Var	If all the preceding conditions cannot meet your requirements, you can use these Nginx variables: **$protocol**, **$arg_**, **$http_**, **$scheme**, **$uri**, **$ssl_protocol**, **$ssl_server_name**, **$remote_addr**, **$http2**, **$sent_http_**, and **$request_method**. **CAUTION** After selecting the **$sent_http_** variable, you can only set **Actions** to **HTTP response headers**. Conversely, you can select **$sent_http_** only when you set **Actions** to **HTTP response headers**.	Nginx variable name • A variable name starts with a dollar sign ($), followed by letters, digits, and underscores (_).	• Include any value • Exclude any value • Exist • Do not exist	• Use letters, digits, and these special characters: .-_*#!&+|^~'"/:;,=@?<> • Enter one or more values. • Enter only one regular expression to match requests. Use the following characters in the regular expression: ^$*+|?:.\<=![]{}()-_:~/	By default, **Case sensitive** is enabled. When it is disabled, uppercase and lowercase values are considered equal.
User-Agent	User-Agent header in requests	N/A	• Include any value • Exclude any value	• Use letters, digits, spaces, and these special characters: *.-_();,/'#!@$^&+=~?"[]:{}\% • Enter one or more values.	By default, **Case sensitive** is enabled. When it is disabled, uppercase and lowercase values are considered equal.

Actions

When a client request matches a rule, the related actions are executed. **Table 4-51** lists the actions supported by the rules engine.

Table 4-51 Supported actions

Category	Name	Description
Basic settings	**HTTP response headers**	The configuration must be the same as that of **HTTP Headers** for CORS in the **Advanced Settings** tab, but their effective scopes are different. • HTTP response headers: take effect only for resources that match the rule. • **HTTP Headers** for CORS: take effect for all resources under the domain name.
	Advanced origins	Client requests that match the conditions in a rule must comply with the advanced origin configuration of this rule.
	Origin request headers	Client requests that match the conditions in a rule must comply with the origin request header configuration of this rule.
Higher access security	**Access control**	Client requests that match the conditions in a rule must comply with the access control configuration of this rule. The action can be **Permit** or **Reject**. • **Permit**: Requests that match the conditions can access resources. • **Reject**: Requests that match the conditions will be blocked and status code 403 will be returned.
Higher hit ratio	**Origin URL rewrite**	Client requests that match the conditions in a rule must comply with the origin URL rewrite configuration of this rule. **Rewrite Method**: Defines how to obtain the content to be rewritten. Select **Exact** or **Capturing**. **Exact** matches content whose **Match Mode** is set to **All files** or **Path** under the **Origin Settings** tab, while **Capturing** matches content whose **Match Mode** is set to **Wildcard** under that tab.
	Cache rules	Client requests that match the conditions in a rule must comply with the cache rule configuration of this rule.
	Access URL rewrite	Client requests that match the conditions in a rule must comply with the access URL rewrite configuration of this rule.

Category	Name	Description
Cache settings	Status Code Cache TTL	Client requests that match the conditions in a rule must comply with the status code cache TTL configuration of this rule.
	Browser Cache TTL	Client requests that match the conditions in a rule must comply with the browser cache TTL configuration of this rule.

IP Address Verification Modes

The rules engine has two IP address verification modes, affecting how CDN PoPs determine client IP addresses.

- Connecting IP: This mode matches the IP address used for connecting clients and CDN PoPs. If a proxy server is used, its IP address is the connecting IP address.
- **X-Forwarded-For** header: This mode matches the first IP address on the left carried in the **X-Forwarded-For** header of user requests. This IP address is the real IP address of clients, regardless of whether a proxy server is used between the clients and CDN PoPs.

Example: Assume that the real IP address of a client is 10.10.10.10 and the IP address of a proxy server is 192.168.0.1.

- If the proxy server is not used:
  - Value of **X-Forwarded-For** in the user request = 10.10.10.10
  - Real IP address of the client (the first IP address on the left carried in the **X-Forwarded-For** header) = IP address for connecting the client and CDN PoPs = 10.10.10.10
- If the proxy server is used:
  - Value of **X-Forwarded-For** in the user request = 10.10.10.10,192.168.0.1
  - Real IP address of the client (the first IP address on the left carried in the **X-Forwarded-For** header) = 10.10.10.10
  - IP address for connecting the client and CDN PoPs = IP address of the proxy server = 192.168.0.1
  - Real IP address of the client (the first IP address on the left carried in the **X-Forwarded-For** header) ≠ IP address for connecting the client and CDN PoPs

5 Resource Package Management

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

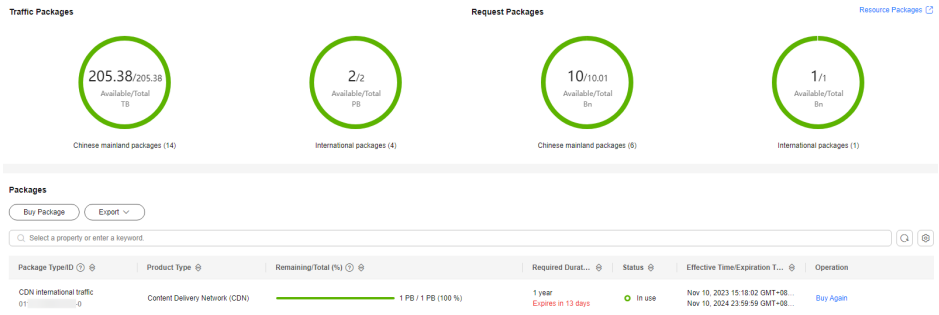
Procedure

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

   The CDN console is displayed.

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

   Figure 5-1 Managing resource packages



3. You can perform the following operations:
   - Viewing basic information about a package: Learn about your package consumption at any time.
   - Searching for resource packages: Filter traffic packages by region, status, required duration, and effective time. Different dimensions have the AND relationship, and similar dimensions have the OR relationship.
   - Buying packages again: Click **Buy Again** and buy packages based on your service requirements. 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.

6 Cache Prefetch and Purge

6.1 Overview

CDN can purge and prefetch content.

- **Cache Purge** forces cached content on CDN PoPs to expire. If a user requests that content, CDN has to pull fresh content from the origin server and then caches that new content.
- **Cache Prefetch** allows the origin server to proactively send the most current content to CDN PoPs. If users request the content, CDN PoPs immediately return the cached content. They do not need to pull any new content.

Prerequisites

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

6.2 Cache Prefetch

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

Typical Scenarios

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

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

Promotional activity: Before releasing a promotional campaign, you can prefetch the static content involved on the activity page to CDN PoPs. After the activity

starts, the CDN PoPs respond to user requests for accessing all static content, which ensures service availability and improves user experience.

Precautions

- Cache prefetch can be performed only for unbanned domain names in **Enabled** or **Configuring** state. For more information about the domain status, see **Viewing Basic Domain Information**.
- The time required to complete a prefetch task depends on the number and size of target files, and on network conditions.
- If the cache prefetch status of a URL is **Completed**, the prefetch is complete.
- Prefetching a large number of files may fully occupy the bandwidth resources of the origin server. Therefore, you are advised to prefetch files in batches.
- Dynamic files, such as ASP, JSP, and PHP files, cannot be prefetched.
- If you have disabled caching for a resource, prefetching it will fail.
- 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 import a TXT file.

Figure 6-1 Cache prefetch

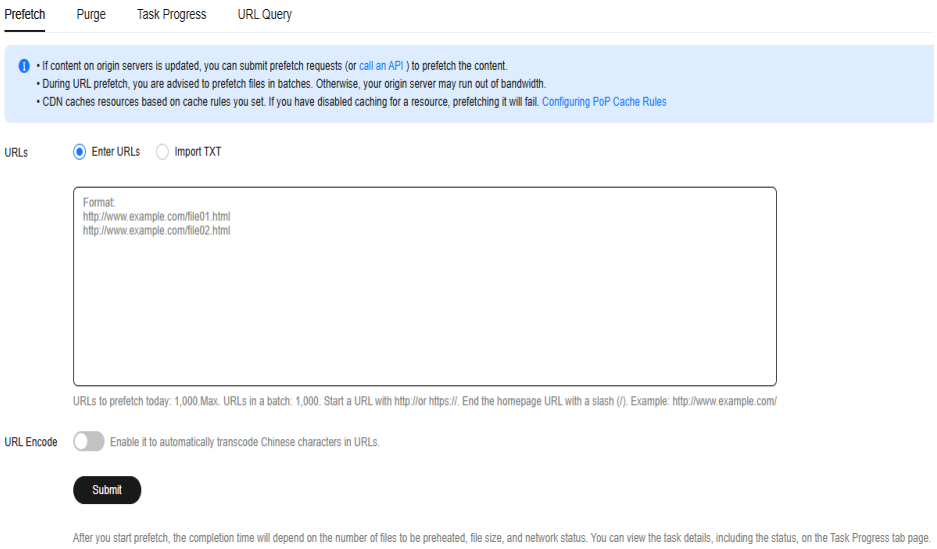


Table 6-1 Parameter description

Type	Description
URL prefetch • CDN prefetches a specific file.	Requirements of entered URLs: • http:// or https:// must be included. • Enter one URL per row. • End the homepage URL with a slash (/). Example: http://www.example.com/ • Each account can prefetch a maximum of 1,000 URLs per day or per task. Examples: http://www.example.com/file01.html http://www.example.com/file02.html https://example.huawei.com/download/app/abc.apk Requirements of URLs in imported TXT files: • Start a URL with **http://** or **https://** in the TXT file. • Enter one URL per row. • End the homepage URL with a slash (/). Example: **http://www.example.com/** • The number of URLs in the TXT file cannot exceed the remaining URL quota.
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.

6.3 Cache Purge

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

Typical Scenarios

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

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

Precautions

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

Figure 6-2 Cache purge

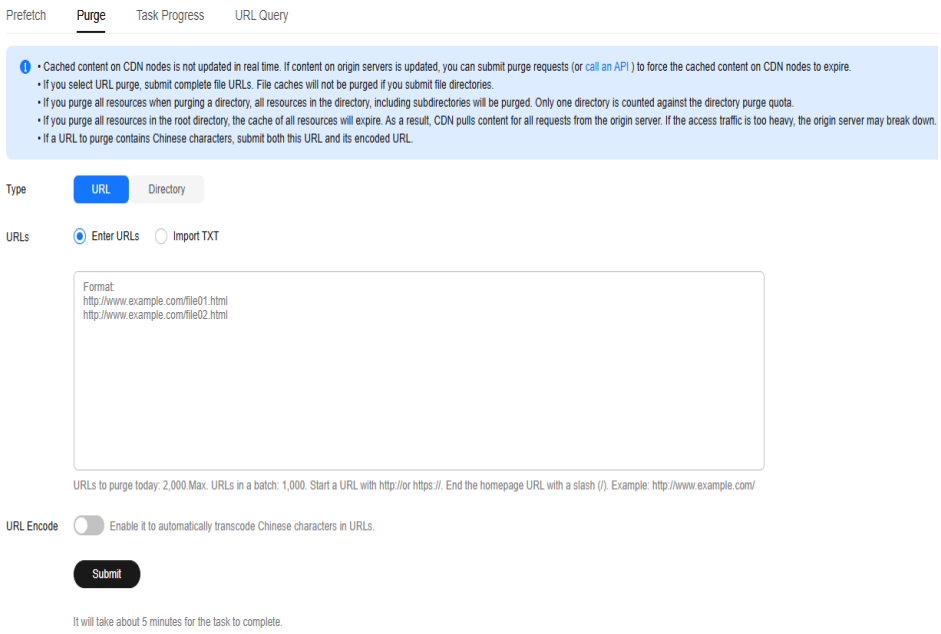


Table 6-2 Parameter description

Type	Description
URL • Refresh the cache of a single file.	Requirements of entered URLs: • Each account can refresh a maximum of 2,000 URLs per day and a maximum of 1,000 URLs per task. • http:// or https:// must be included. • End the homepage URL with a slash (/). Example: http://www.example.com/ • Enter one URL per row. **Examples:** http://www.example.com/file01.html http://www.example.com/file02.html https://example.huawei.com/download/app/abc.apk Requirements of URLs in imported TXT files: • Start a URL with **http://** or **https://** in the TXT file. • Enter one URL per row. • The number of URLs in the TXT file cannot exceed the remaining URL quota. **NOTE** • Submit complete file URLs. If you submit a directory, URL refreshing does not take effect. • If a URL contains spaces, escape spaces in the URL and disable **URL Encode**.

Type	Description
Directory	**Mode**: • **Purge updated resources**: Purge resources that have been updated in a directory (including subdirectories). • **Purge all resources**: Purge all resources in a directory, including resources in subdirectories. **Configuration rules:** • Each account can refresh a maximum of 100 directories per day at a time. • A URL must contain http:// or https:// and end with a slash (/). • Enter one URL per row. **Examples:** http://www.example01.com/folder01/ http://www.example01.com/folder02/ **NOTE** • URLs in the text box or in the TXT file have the same format. • If you select **Purge all resources** when refreshing the root directory, the cache of all resources will expire. As a result, CDN pulls content for all requests from the origin server. If the access traffic is too heavy, the origin server may break down. • If you select **Purge all resources** when refreshing a directory, all resources in the directory, including subdirectories will be refreshed. Only one directory is counted against the directory refreshing quota.
URL Encode	If enabled, Chinese characters in URLs are automatically transcoded and cache is purged only for transcoded URLs. • To purge an untranscoded URL with Chinese characters, enter this URL and disable **URL Encode**.

4. Click **Submit**.

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

6.4 Viewing Task Progresses

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

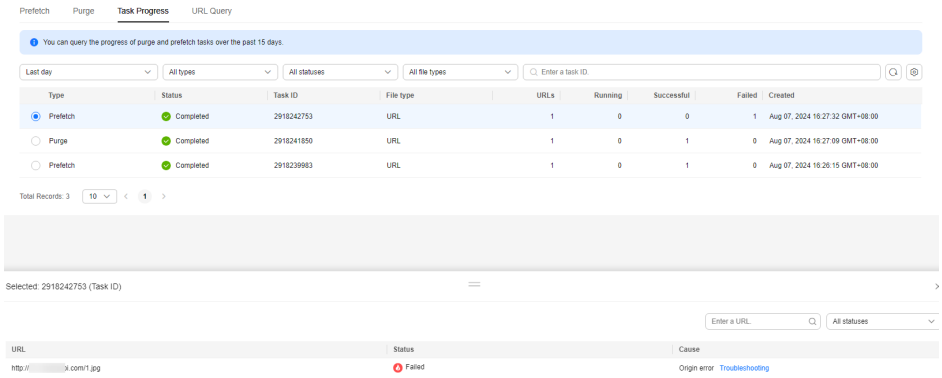
1. Log in to **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

   The CDN console is displayed.

2. In the navigation pane, choose **Prefetch & Purge**.
3. Click the **Task Progress** tab to check the task status.

   You can view the failure cause of a failed task.

Figure 6-3 Purge and prefetch history



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.

6.5 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 Should 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.

1. After updating a file on the origin server, purge the cache on CDN PoPs. Or, clients may obtain the stale version of the file, or encounter issues such as access failures, repeated redirections, white screens, or disordered page displays.
2. It is recommended that large files, especially video files, be prefetched to improve user experience.

3. Prefetch is not recommended for small files.

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

7 Analytics (Old)

7.1 Statistics Description

Table 7-1 displays reports provided by CDN. You can learn:

Table 7-1 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?

7.2 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.

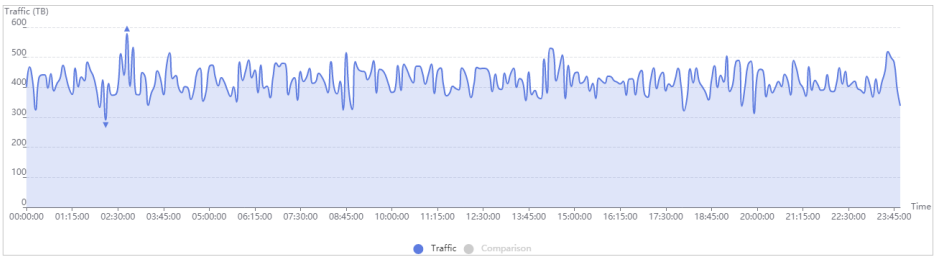
Constraints

- 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**.

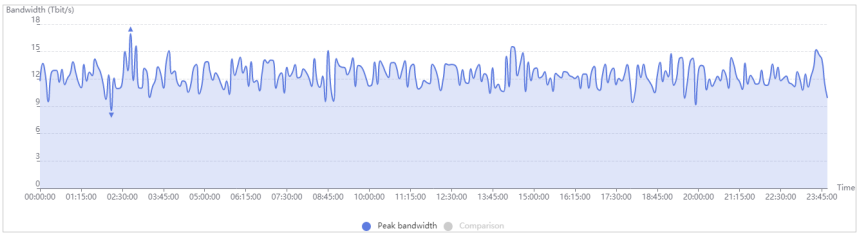
Procedure

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.

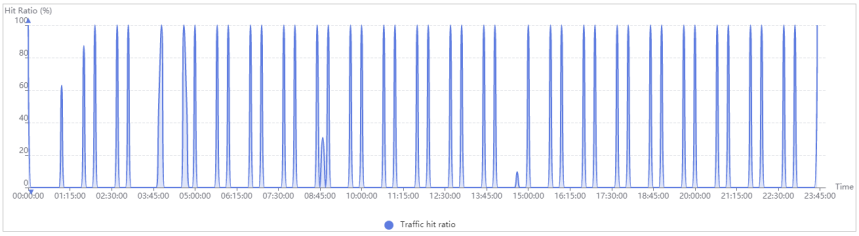
     

     NOTE

     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.

Domain Name	Traffic	Peak Bandwidth	Traffic Hit Ratio
tx- apl.com	110.50 MB	41.91 kbit/s	100.00 %
ww ite	10.69 KB	0.05 kbit/s	36.02 %

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

7.3 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.

Constraints

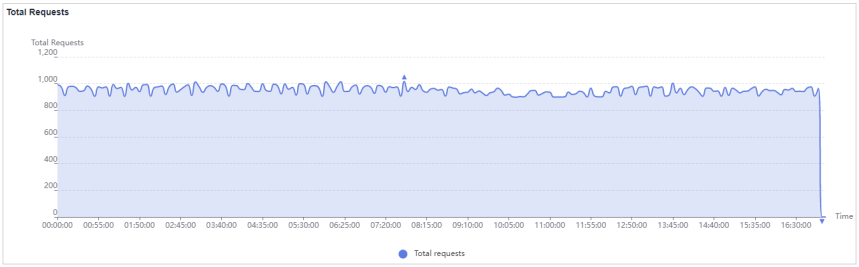
- If the service area of your domain name is global, you must query the statistics of this domain name by choosing **Chinese mainland** and **International** respectively.
- You can query the cache hit ratio only when setting **Region** to **Chinese mainland** or **International**.

Procedure

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

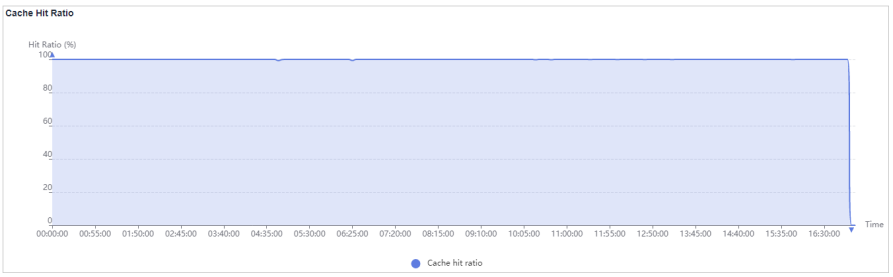
   The CDN console is displayed.
2. In the navigation pane, choose **Analytics** > **Requests**.

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

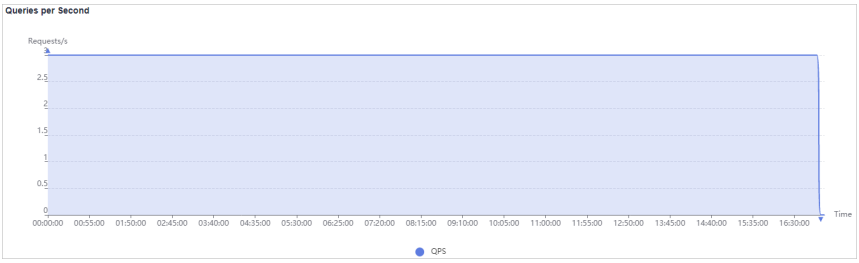
   - **Cache Hit Ratio**: displays the cache hit ratio of specific domain names over time.

     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

7.4 Origin

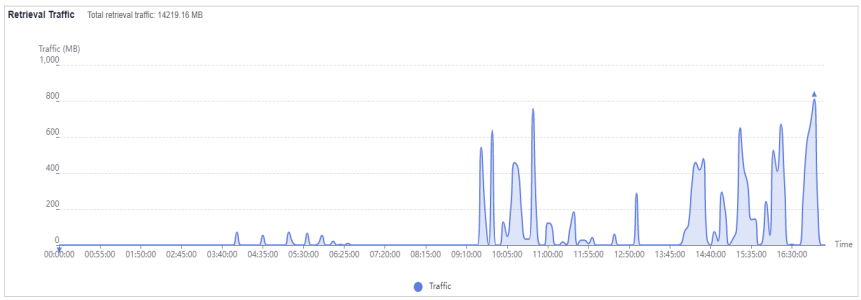
You can view the traffic, bandwidth, and failure rate of origin pulls for all your domain names (excluding those deleted if you have enabled the enterprise project function).

- 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.

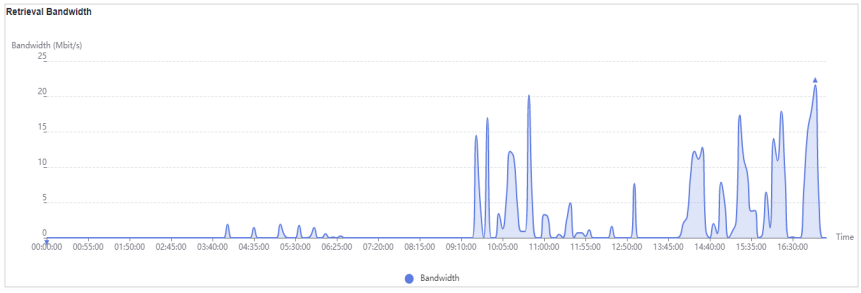
Procedure

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.

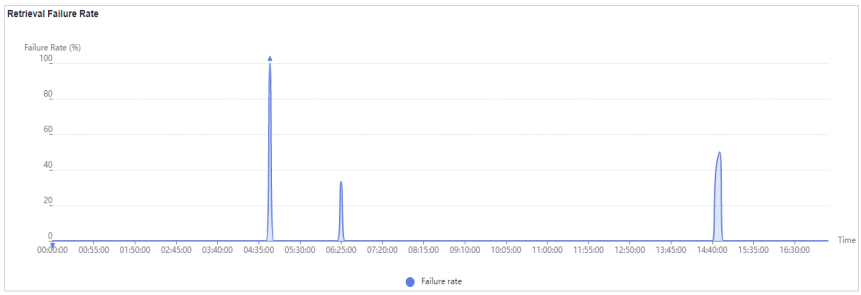
     

   - **Retrieval Bandwidth**: displays the origin pull bandwidth of specific domain names over time.

   - **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.

7.5 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.

Constraints

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 7-1 Customizing an operations report

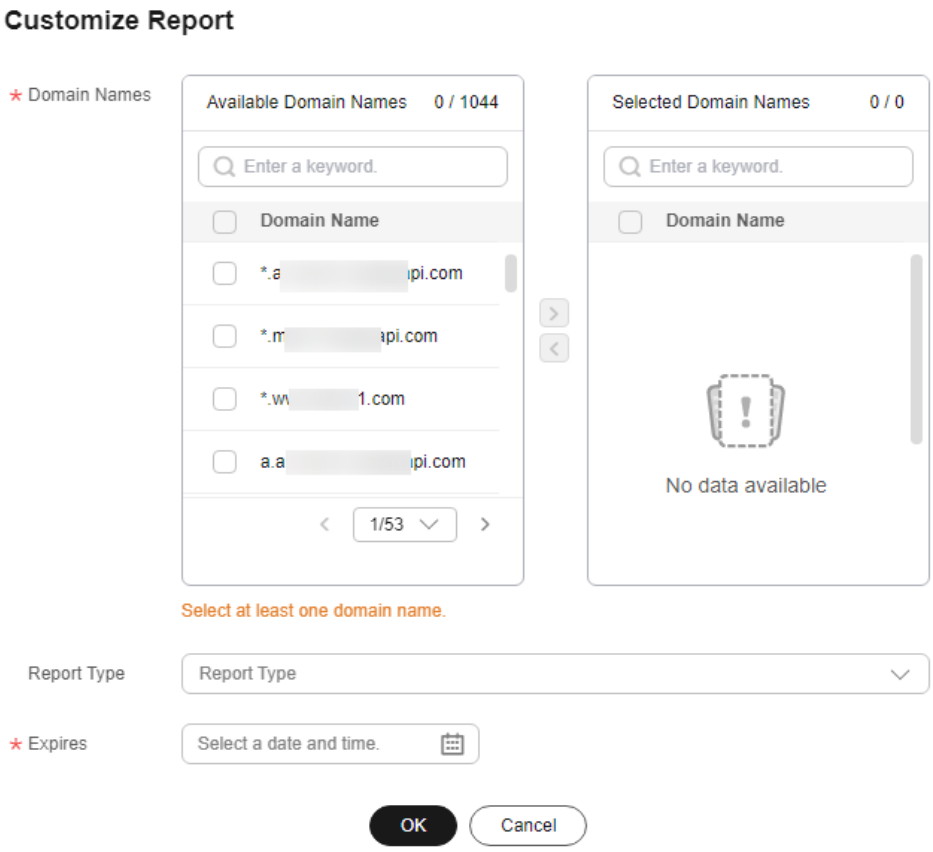


Table 7-2 Parameters

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.

7.6 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** > **Regions & Carriers**.
3. 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.

- **Carriers**: China Mobile, China Telecom, China Unicom, China Education and Research Network (CERNET), Dr. Peng, and China Mobile Tietong

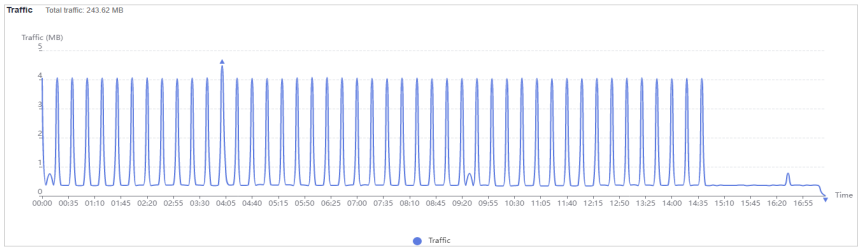
  i. **Carrier Index Distribution**: displays the proportion each carrier occupies in different index statistics.

  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.

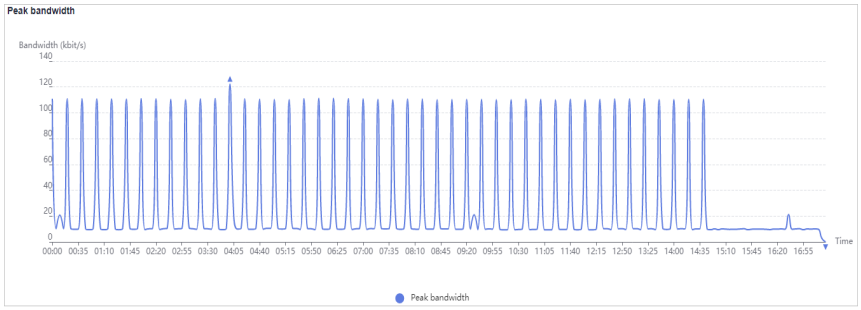
Carrier	Traffic (Percentage)	Peak Bandwidth (Percentage)	Total Requests (Percentage)	Avg. Response Time (ms)
China Telecom	589.13 KB (100.00%)	88.00 bit/s (100.00%)	543,000 (100.00%)	37

- **Utilization (Regions)**

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



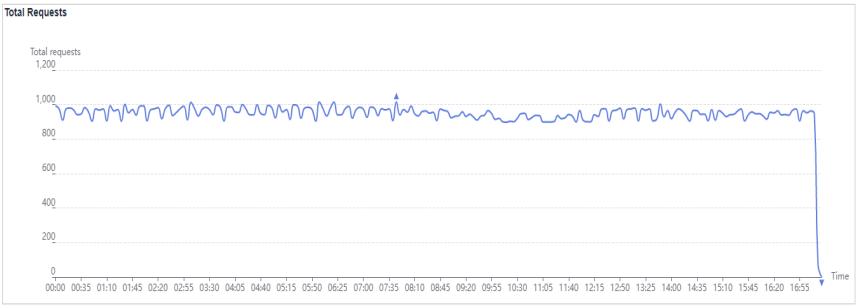
  ii. **Peak bandwidth**: displays the peak bandwidth of specific domain names by country/region or carriers.



  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.

7.7 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.

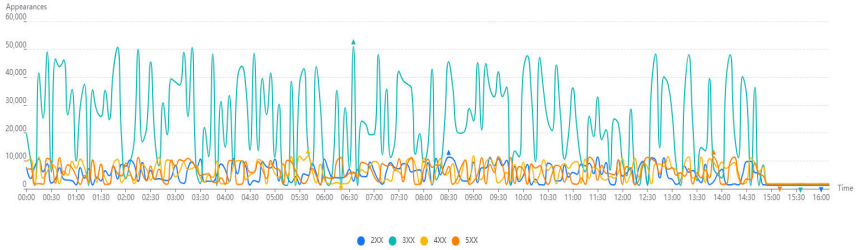
Constraints

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.

7.8 Whole Site Acceleration

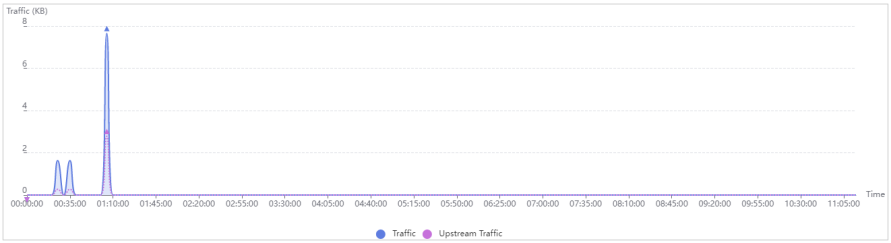
You can query traffic statistics of all domain names whose service type is whole site acceleration (excluding those deleted if you have enabled the enterprise project function).

- 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.

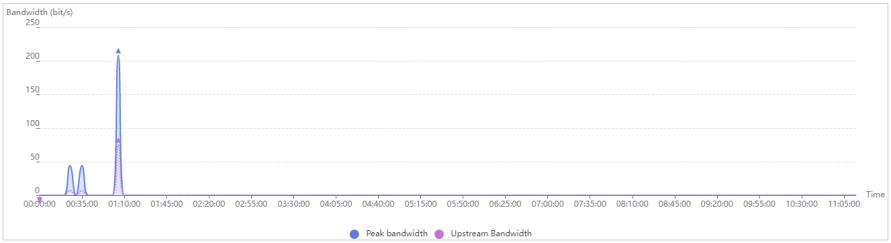
Procedure

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.

7.9 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 7-2 Creating an export task

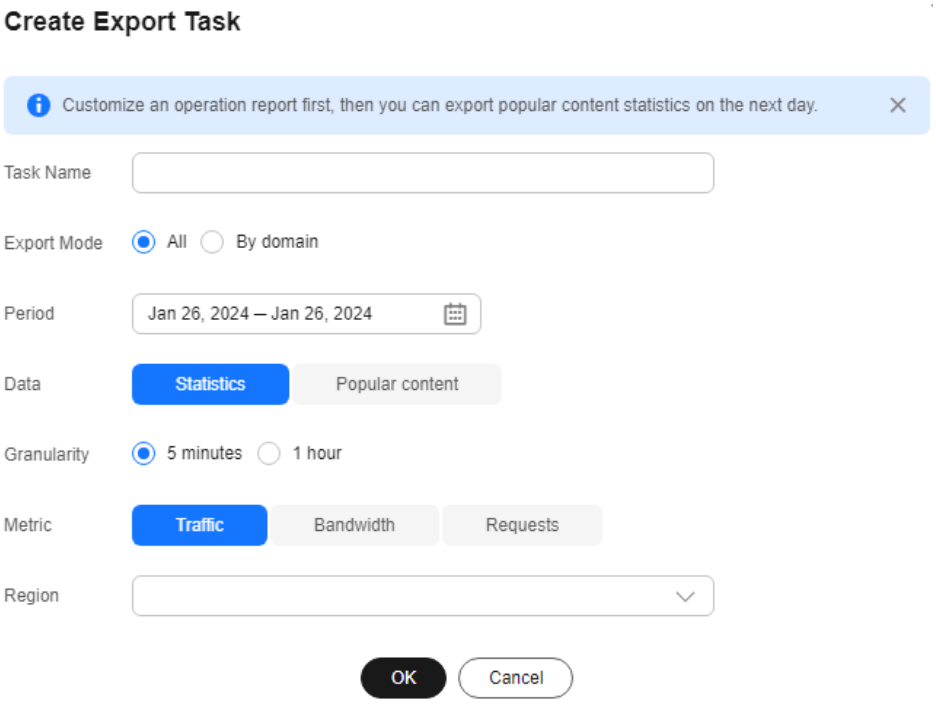


Table 7-3 Parameter description

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
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 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.

7.10 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 7-4 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 7-3 Creating a subscription task

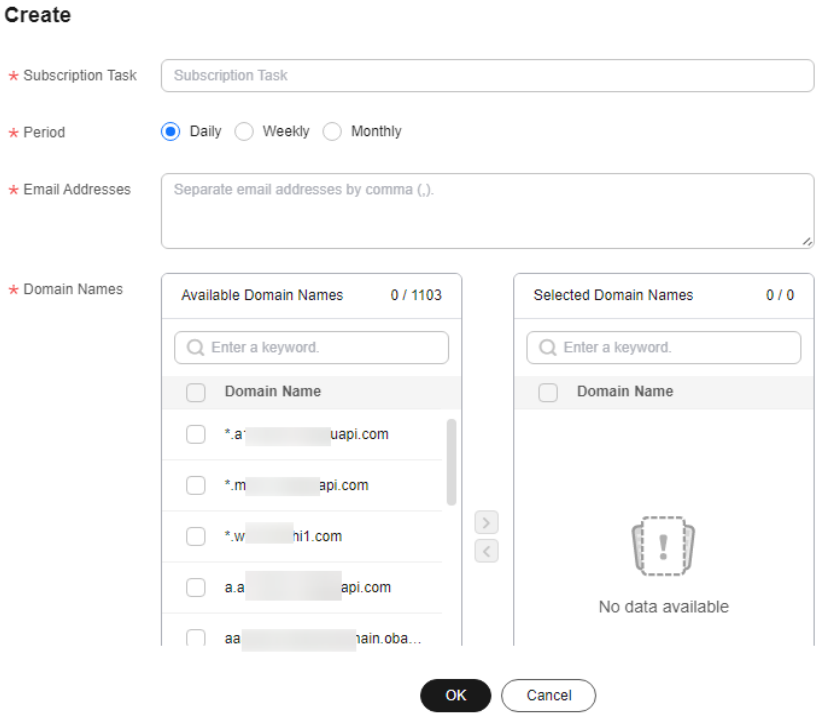


Table 7-5 Parameters

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.
Domain Names	Domain names whose statistics are collected. • Domain names cannot be filtered by enterprise project.

Parameter	Description
Report Type	Select the type of the report to be subscribed to. For details, see **Table 7-4**. **NOTE** To subscribe to the popular URL report, **customize a report** first.

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

7.11 Cloud Eye Monitoring

Scenarios

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

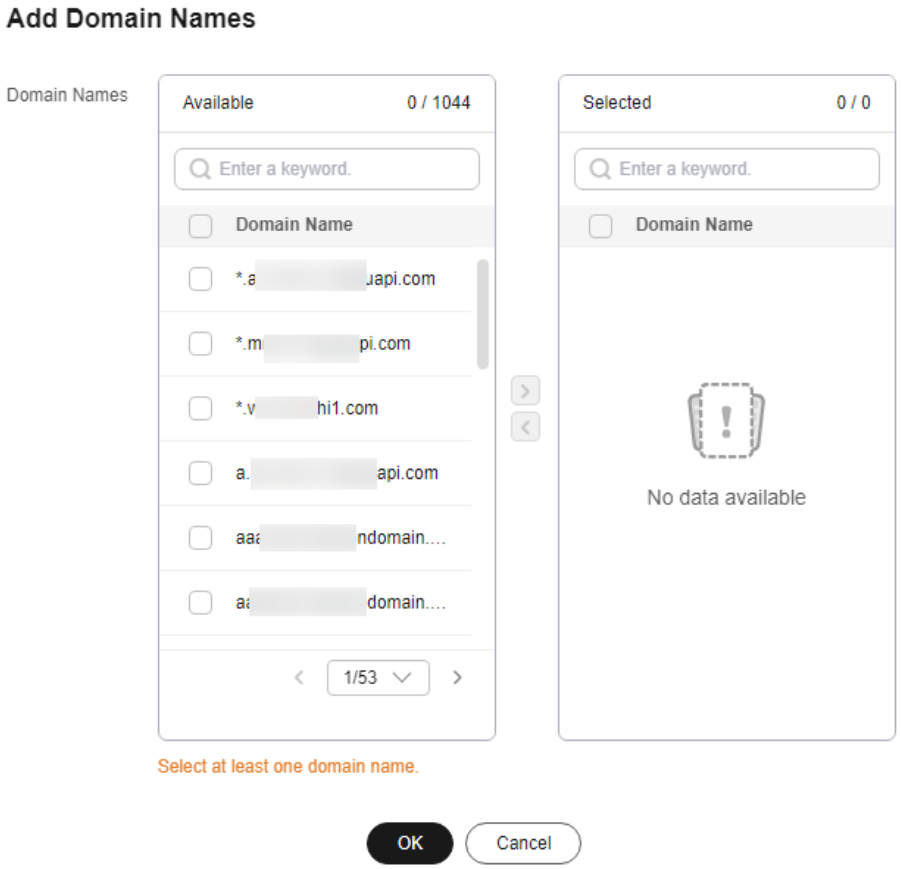
- You can add up to 100 domain names.
- Domain names with special configurations are not supported.
- The data reporting latency is about 4 minutes.
- Data is reported to Cloud Eye in the CN North-Beijing4 region.
- Cloud Eye monitoring is free of charge on CDN. If you configure alarms on Cloud Eye, 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 7-4 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.

7.12 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.

8 Analytics (New)

8.1 Analytics Description

Table 7-1 lists analytics reports and functions provided by CDN.

Table 8-1 Analytics description

Item	Description
Access Requests	Check the traffic/bandwidth usage, number of requests, and number of queries per second (QPS) of user requests to domain names, and export the detailed data.
Origin Pulls	Check the traffic/bandwidth usage, number of requests, and failure rates of origin pulls from domain names, and export the detailed data.
Hit Ratios	Check the traffic usage and request hit ratios of domain names, and export the hit ratio details.
Status Codes	Check the status codes of user requests to domain names, and export the status code details.
Cloud Eye Monitoring	Report domain name metrics to Cloud Eye for timely monitoring.
Monitoring Dashboard	Check details about metric reported to Cloud Eye to monitor metric anomalies and promptly adjust services.
Operations Reports	Customize operations reports for domain names to check statistics in different periods, monitor the domain status, and promptly adjust services.
Subscription Tasks	Check offline domain statistics in operations reports, analyze the domain status, and adjust operations policies properly.
Query	Check the traffic/bandwidth usage of domain names.

Item	Description
Summary	Check the total traffic/bandwidth usage and number of whole site acceleration requests of domain names on a specific day.
Whole Site Acceleration	Check the traffic/bandwidth usage and number of requests of domain names whose service type is whole site acceleration.
Data Export	Export statistics about all or specific domain names.

CAUTION

If you have **enabled the enterprise project function** for your account, note the following:

1. Deleted domain names are not counted.
2. If a domain name is migrated from enterprise project C to enterprise project D under the same account, its statistics are no longer available under enterprise project C. Its statistics before and after the migration are displayed in enterprise D.

If **the enterprise project function is not enabled**, you can view the historical statistics of deleted domain names generated in the past 90 days.

NOTE

- On the CDN console, there is a delay of about 1 hour for data on the **Analytics** and **Overview** pages.

8.2 Service Monitoring

8.2.1 Access Requests

Check the traffic/bandwidth usage and number of requests/QPS of domain names by **visitor region** or **carrier** on the CDN console.

CAUTION

If you have **enabled the enterprise project function** for your account, note the following:

1. Deleted domain names are not counted.
2. If a domain name is migrated from enterprise project C to enterprise project D under the same account, its access statistics are no longer available under enterprise project C. Its statistics before and after the migration are displayed in enterprise D.

If **the enterprise project function is not enabled**, you can view the historical access statistics of deleted domain names generated in the past 90 days.

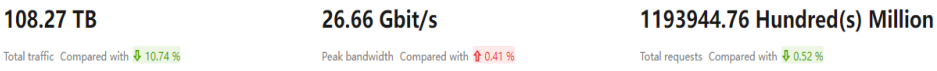
Precautions

- 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 eight days or longer, the minimum granularity is 1 hour.
- There is a delay of about one hour for data displayed on the **Access Requests** tab.
- You can export the query results.
- You can filter statistics by tag, service type, region, carrier, HTTP version, and Internet Protocol (IP) version.
- You can compare data.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Analytics** > **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 8-1 Data trend charts

8.2.2 Origin Pulls

Check the traffic/bandwidth usage, number of requests, and failure rate of origin pulls from domain names on the CDN console.

CAUTION

If you have **enabled the enterprise project function** for your account, note the following:

1. Deleted domain names are not counted.
2. If a domain name is migrated from enterprise project C to enterprise project D under the same account, its origin pull statistics are no longer available under enterprise project C. Its statistics before and after the migration are displayed in enterprise D.

If **the enterprise project function is not enabled**, you can view the historical origin pull statistics of deleted domain names generated in the past 90 days.

Precautions

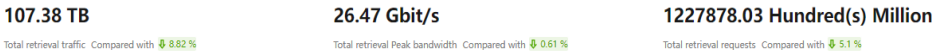
- Data of the past 90 days can be queried, and each query can include data of up to 31 days.
- If no data is available for the queried domain name within the specified time span, no data is displayed in the trend charts.
- The minimum granularity is 5 minutes. If the query time range is eight days or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

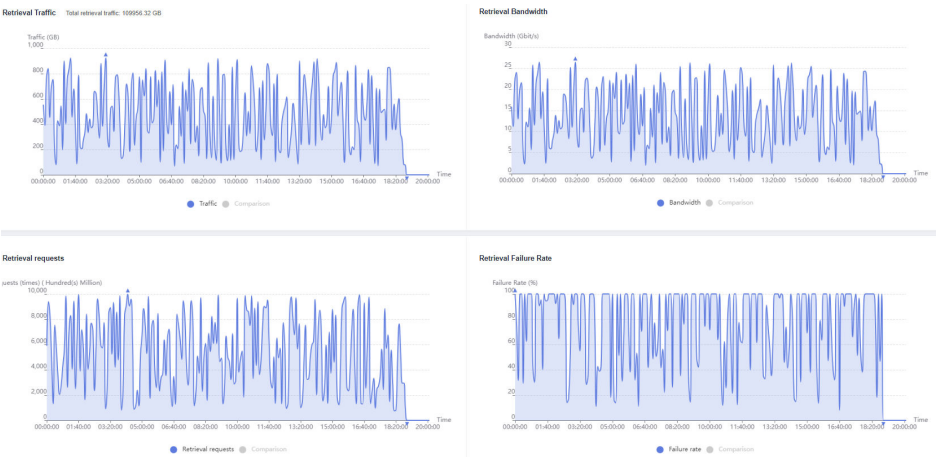
The CDN console is displayed.

2. In the navigation pane, choose **Analytics** > **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 8-2 Data trend charts



8.2.3 Hit Ratios

Check the traffic usage and request hit ratios of domain names on the CDN console.

CAUTION

If you have **enabled the enterprise project function** for your account, note the following:

1. Deleted domain names are not counted.
2. If a domain name is migrated from enterprise project C to enterprise project D under the same account, its hit ratio statistics are no longer available under enterprise project C. Its statistics before and after the migration are displayed in enterprise D.

If **the enterprise project function is not enabled**, you can view the historical hit ratio statistics of deleted domain names generated in the past 90 days.

Precautions

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

Procedure

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

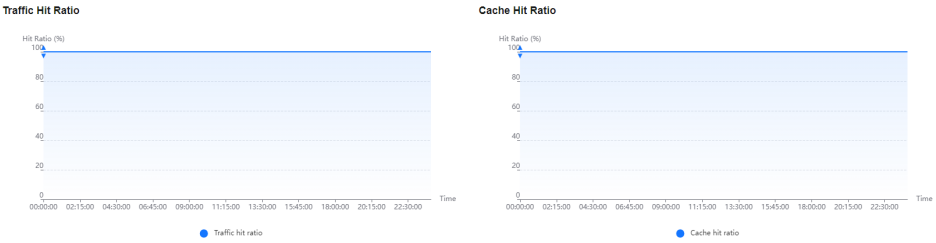
   The CDN console is displayed.
2. In the navigation pane, choose **Analytics** > **Service Monitoring**.
3. Click the **Hit Ratios** tab and set search criteria. You can query the following data:

   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 8-3 Hit ratio statistics



8.2.4 Status Codes

Check the status codes of domain names on the CDN console.

CAUTION

If you have **enabled the enterprise project function** for your account, note the following:

1. Deleted domain names are not counted.
2. If a domain name is migrated from enterprise project C to enterprise project D under the same account, its status code statistics are no longer available under enterprise project C. Its statistics before and after the migration are displayed in enterprise D.

If **the enterprise project function is not enabled**, you can view the historical status code statistics of deleted domain names generated in the past 90 days.

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 eight days or longer, the minimum granularity is 1 hour.
- There is a delay of about one hour for data displayed on the **Status Codes** tab.
- You can filter domain names by tag, service type, region, and enterprise project.
- You can export status code statistics.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Analytics** > **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 8-2**.

- **Overview**: displays the total number and proportion of appearances of each type of status codes in the query period.
- **Details**: displays the total number and proportion of each status code in the query period. You can also click **Check Details** to check domain names and top URLs of this status code.

Figure 8-4 Status code statistics

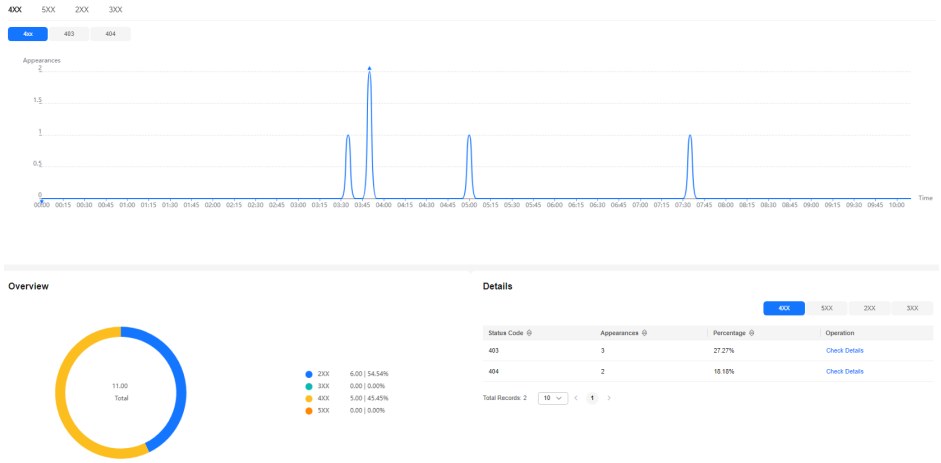


Table 8-2 Status code description

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.

8.2.5 Cloud Eye Monitoring

Scenarios

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 of accounts that enabled Cloud Eye monitoring before October 30, 2024 (UTC+08:00) will be reported to the CN North-Beijing4 region of Cloud Eye. Data of accounts that enabled Cloud Eye monitoring after October 30, 2024 (UTC+08:00) will be reported to the AP-Singapore region of Cloud Eye.

  NOTICE

  Enable Cloud Eye in the AP-Singapore region before reporting monitoring data there for the first time.

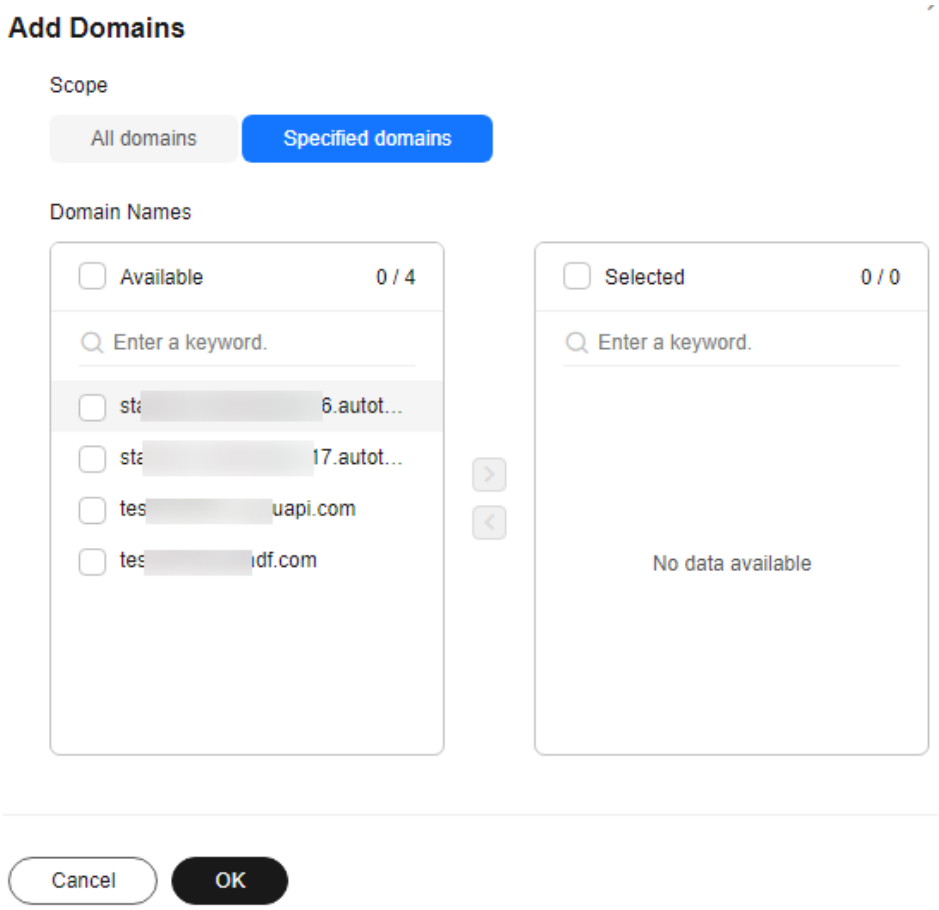
- Cloud Eye monitoring is free of charge on CDN. If you configure alarms on Cloud Eye, SMN will charge you for alarm notifications sent to you. For details about SMN pricing, see **SMN Pricing Details**.

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** > **Service Monitoring**.
3. Click the **Dashboard** tab.
4. In the **Cloud Eye Monitoring** area, click **Add Domains** and add domain names to report their metrics to Cloud Eye.
   - If **Scope** is set to **All domains**, all monitoring data for your domain names, including those added to CDN later, is reported to Cloud Eye.
   - If **Scope** is set to **Specified domains**, data of the domain names selected under **Domain Names** is reported to Cloud Eye.

Figure 8-5 Adding domain names



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

Stopping Monitoring

- If you set **Scope** to **All domains**, you cannot stop monitoring for a specific domain name.
- If you set **Scope** to **Specified domains**, you can delete a domain name to stop monitoring it.
  - Click **Delete Domain** in the **Operation** column of a domain name.
  - Select multiple domain names and click **Delete Domains** above the domain name list.

8.2.6 Monitoring Dashboard

If you have reported metrics related to acceleration domain names to Cloud Eye, you can view them on the monitoring dashboard.

Prerequisites

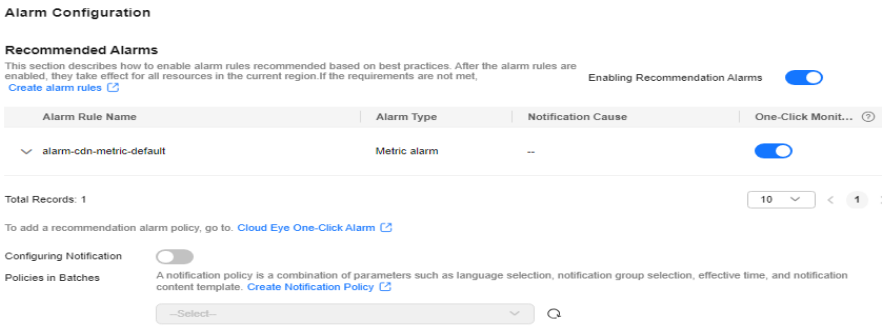
- You have added domain names to be monitored. For details, see **Cloud Eye Monitoring**.
- You have set **domain name alarm rules**.

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** > **Service Monitoring**.
3. Click the **Dashboard** tab to check monitoring information.
   - **Monitored Domains**: displays domain names whose metrics are reported to Cloud Eye.
   - **Alarms Today**: displays the severity distribution of alarms generated today. If no alarm rule is configured or no alarm is generated for the domain names, you can click **Create Now** to use recommended alarm rules or customize alarm rules.
     - The system provides the built-in one-click alarm function, including alarm rules for status codes 4*xx* and 5*xx*. You can enable **Enabling Recommendation Alarms** to use this function.
       - To adjust the default alarm rules, click **Cloud Eye One-Click Alarm** to go to the Cloud Eye console.
       - To adjust the notification policies, click **Create Notification Policy** to go to the Cloud Eye console.
       - If existing alarm rules cannot meet your needs, click **Create alarm rules** to **create one**.

     Figure 8-6 Recommended alarm configurations

   - **5 Domains with the Most Alarms**: displays five domain names with the most alarms.
     - If no alarm rule is configured or no alarm is generated for the domain names, you can click **Create Now** to use recommended alarm rules or customize alarm rules.
   - View metrics by domain name.

Creating an Alarm Rule

In the **Alarm Configuration** drawer, click **Create alarm rules**.

Figure 8-7 Creating an alarm rule

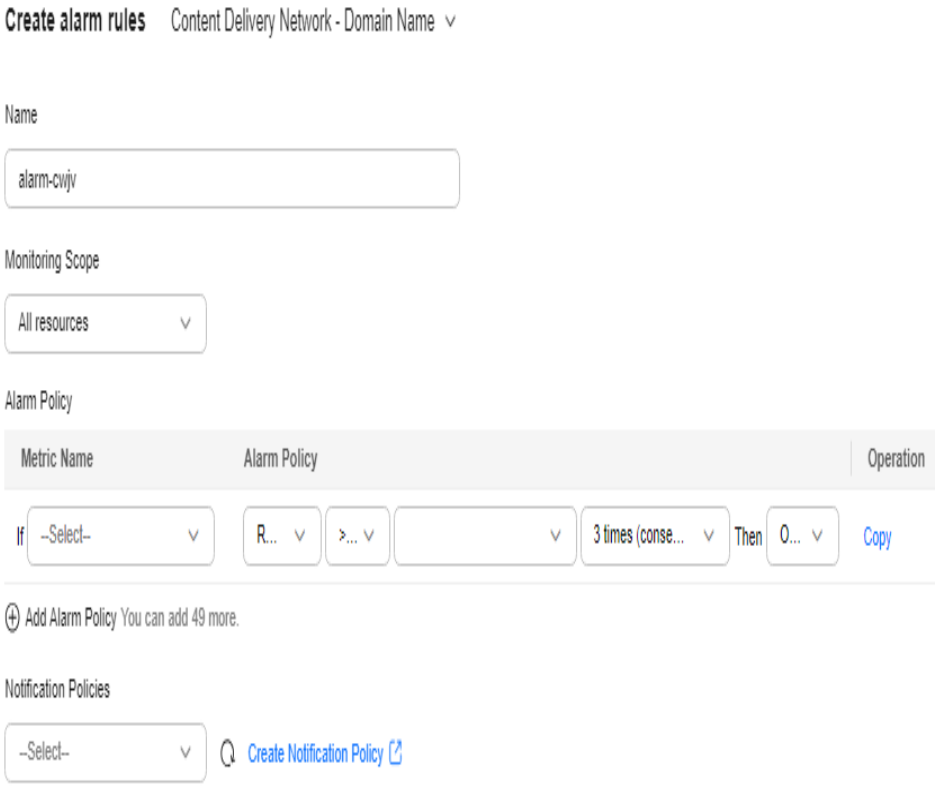


Table 8-3 Parameters

Parameter	Description
Name	Name of the alarm rule. The system generates a random name, which you can modify. Example value: **alarm-poxz**
Monitoring Scope	Resources to which the alarm rule applies. Only **All resources** can be selected.
Alarm Policy	Condition for triggering an alarm. When the specified event occurs, an alarm will be triggered.
Notification Policies	Combination of parameters, such as notification group, window, and template.

8.3 Data Analysis

8.3.1 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** > **Data Analysis**.
3. By default, CDN provides domain name rankings and region/carrier rankings.
   - **Domain Rankings**: displays domain names by the volume of user visit traffic and origin pull traffic in descending order by default. This report is displayed by default and does not need to be customized.
     - Data of the past 90 days can be queried, and each query can include data of up to 31 days.
   - **Regions & Carriers**: displays data about regions and carriers of users who access your domain names. This report is displayed by default and does not need to be customized.
     - You can filter domain names by service area (**All**, **Chinese mainland**, or **Outside Chinese mainland**).
     - You can filter domain names by service type.
     - You can filter statistics by tag, HTTP version, and IP version.
     - You can filter visitor data by region (global or China). China includes Chinese mainland, Hong Kong, Macao, and Taiwan.
     - Data of the past 90 days can be queried, and each query can include data of up to 31 days.
4. To customize an operations report, click **Customize Report**.

Figure 8-8 Customizing an operations report

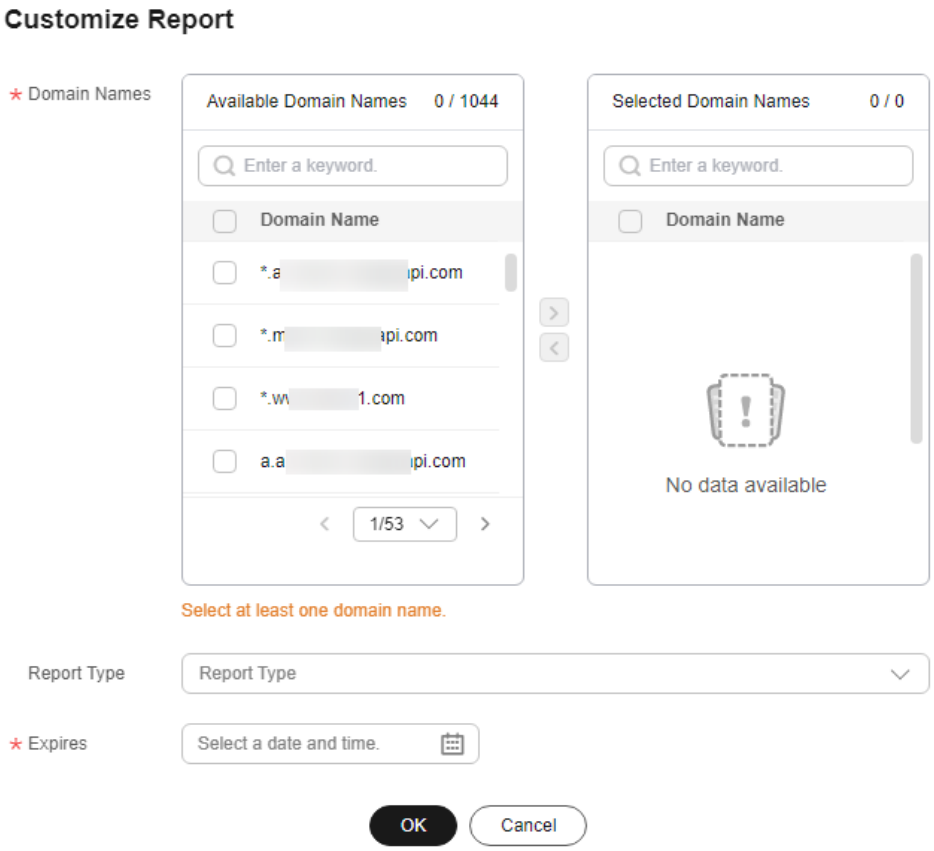


Table 8-4 Parameters

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.

8.3.2 Subscription Tasks

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 8-5 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** > **Data Analysis**.
3. On the **Subscription Tasks** tab, click **Create**.

Figure 8-9 Creating a subscription task

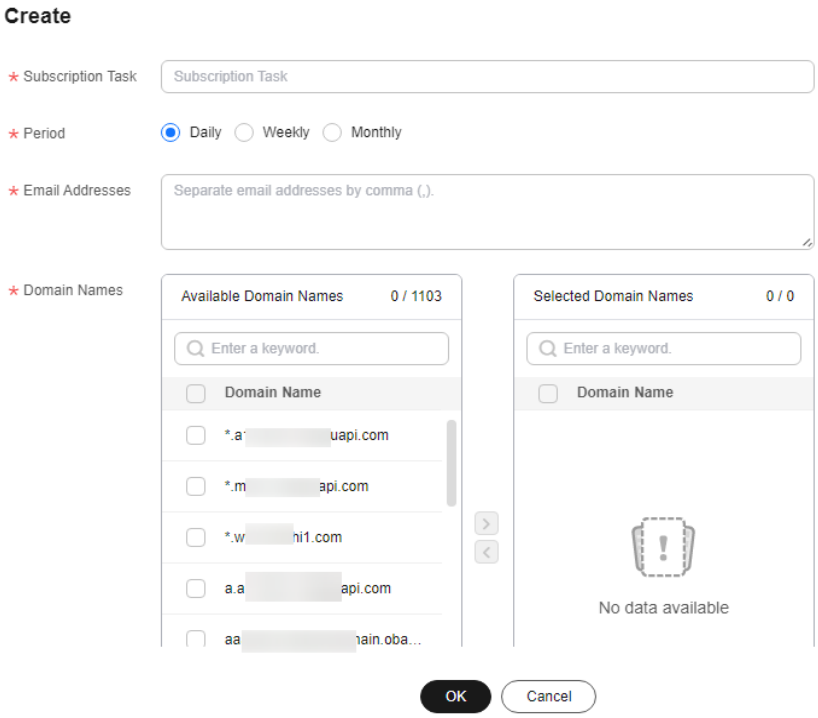


Table 8-6 Parameters

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 8-4**. **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 **Subscription Tasks** tab to export reports in XLSX format.

8.4 Traffic Query

8.4.1 Query

Check the traffic/bandwidth usage of domain names on the CDN console.

CAUTION

If you have **enabled the enterprise project function** for your account, note the following:

1. Deleted domain names are not counted.
2. If a domain name is migrated from enterprise project C to enterprise project D under the same account, its usage details are no longer available under enterprise project C. Its usage details before and after the migration are displayed in enterprise D.

If **the enterprise project function is not enabled**, you can view the historical usage details of deleted domain names generated in the past 90 days.

Constraints

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.

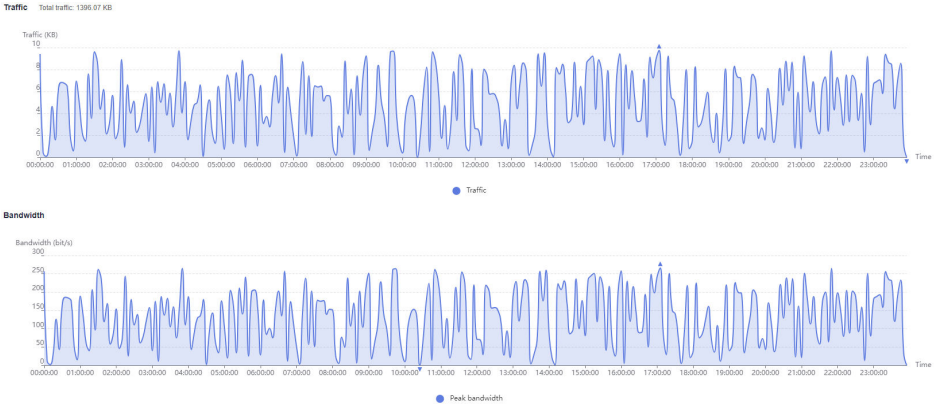
- If no data is available for the queried domain name within the specified time span, no data is displayed in the traffic or bandwidth trend chart.
- The minimum granularity is 5 minutes. If the query time range is eight days or longer, the minimum granularity is 1 hour.
- The logged traffic statistics 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** > **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 8-10 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.

8.4.2 Summary

Check the total traffic/bandwidth usage and number of whole site acceleration requests of domain names on a specific day on the CDN console.

CAUTION

If you have **enabled the enterprise project function** for your account, note the following:

1. Deleted domain names are not counted.
2. If a domain name is migrated from enterprise project C to enterprise project D under the same account, its usage summary is no longer available under enterprise project C. Its summary before and after the migration is displayed in enterprise D.

If **the enterprise project function is not enabled**, you can view the historical usage summary of deleted domain names generated in the past 90 days.

Precautions

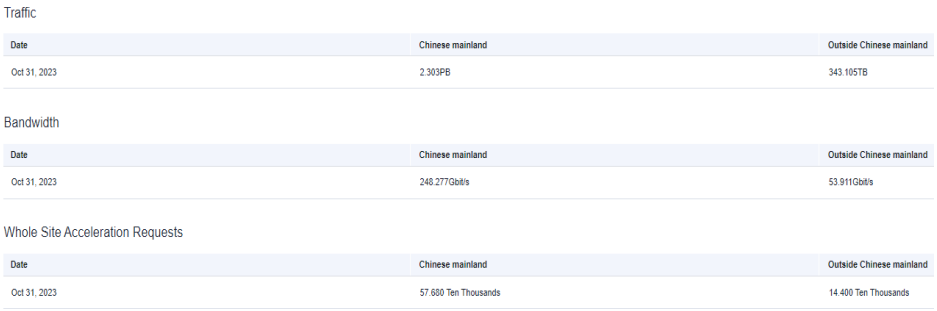
- You can view the usage data of a day in the last 90 days.
- By default, statistics about domain names are displayed by region (Chinese mainland and outside the Chinese mainland).

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

Figure 8-11 Summary



8.4.3 Whole Site Acceleration

Check the traffic/bandwidth usage and number of requests of domain names whose service type is whole site acceleration.

CAUTION

If you have **enabled the enterprise project function** for your account, note the following:

1. Deleted domain names are not counted.
2. If a domain name is migrated from enterprise project C to enterprise project D under the same account, its whole site acceleration statistics are no longer available under enterprise project C. Its statistics before and after the migration are displayed in enterprise D.

If **the enterprise project function is not enabled**, you can view the historical whole site acceleration statistics of deleted domain names generated in the past 90 days.

Constraints

- 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 eight days or longer, the minimum granularity is 1 hour.
- The logged traffic statistics are displayed. However, the billable traffic is 10% higher than the logged statistics because TCP/IP packet headers and TCP retransmissions also consume traffic.
- The current usage can be queried about one hour later.
- You can filter domain names by tag, service type, or enterprise project.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **Analytics** > **Traffic Query**.
3. Click the **Whole Site Acceleration** tab and set search criteria. You can query and export the following data:
   - **Traffic**: displays the traffic and upstream traffic of specific domain names over time.
   - **Bandwidth**: displays the peak bandwidth and upstream bandwidth of specific domain names over time.
   - **Request Appearances**: displays the number of dynamic and static requests sent to specific domain names over time.

Figure 8-12 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.

8.5 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** > **Data Export**.
3. On the **Data Export** page, click **Create Export Task**.

Figure 8-13 Creating an export task

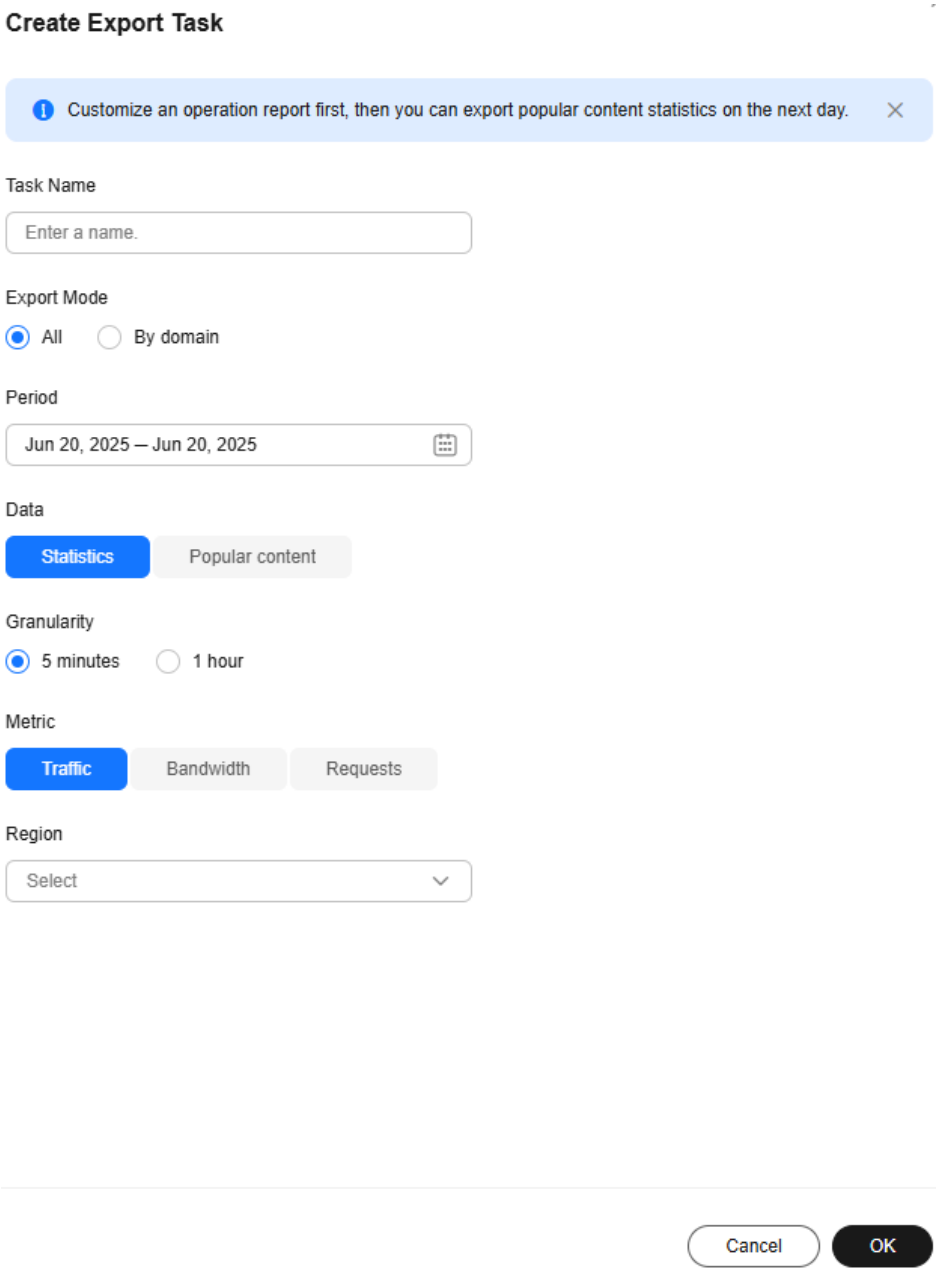


Table 8-7 Parameter description

Parameter	Description	Example
Task Name	Name of an export task. This parameter is user-defined.	test

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

Parameter	Description	Example
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.

9 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.

Precautions

CDN logs do not contain information about CC attacks.

Log Description

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

NOTE

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

Log naming: *Period start time-Acceleration domain name-Extended field*.**gz**. Example: 2018021123-www.example01.com-xx.gz

Log generation: By default, a log file is generated for each domain name every hour, and 24 log files are generated every day. The size of a log file is limited. If a log file generated within a period is too large, it will be divided into multiple files, with an extended field added to their names.

Example of log file content

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

Table 9-1 describes each field (from left to right) in the log.

Table 9-1 Description of a CDN log file

No.	Field Description	Example
1	Log generation time	[05/Feb/2018:07:54:52 +0800]
2	Access IP address (client IP address)	x.x.x.x
3	Time to last byte (ms)	1
4	Referer information	-
5	HTTP protocol identifier	HTTP/1.1
6	HTTP request method	GET
7	Acceleration domain name	www.test.com
8	Requested path (excluding URL parameters)	/test/1234.apk
9	HTTP status code	206
10	Response size (bytes)	720
11	Cache hit status	HIT
12	User-Agent information, which helps servers recognize the OS, OS version, CPU, browser, and browser version	Mozilla/5.0 (Linux; U; Android 6.0; en-us; EVA-AL10 Build/HUAWEIEVA-AL10) AppleWebKit/533.1 (KHTML, like Gecko) Mobile Safari/533.1
13	Range information. It specifies the positions of the first and last bytes for the data to be returned. **bytes** can be expressed by the following three methods: • bytes=x-y: requesting content from the *x*th to *y*th byte. • bytes=-y: requesting content from the last *y* bytes. • bytes=x-: requesting content from the *x*th to the last byte.	bytes=-256
14	Server IP address, that is, the IP address used by the CDN server to send responses	x.x.x.x

Downloading Logs

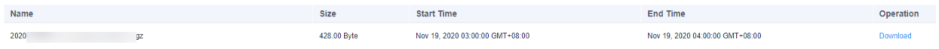
1. Log in to **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

   The CDN console is displayed.

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

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

   Figure 9-1 Log management

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

10 Diagnosis

10.1 IP Address Check

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

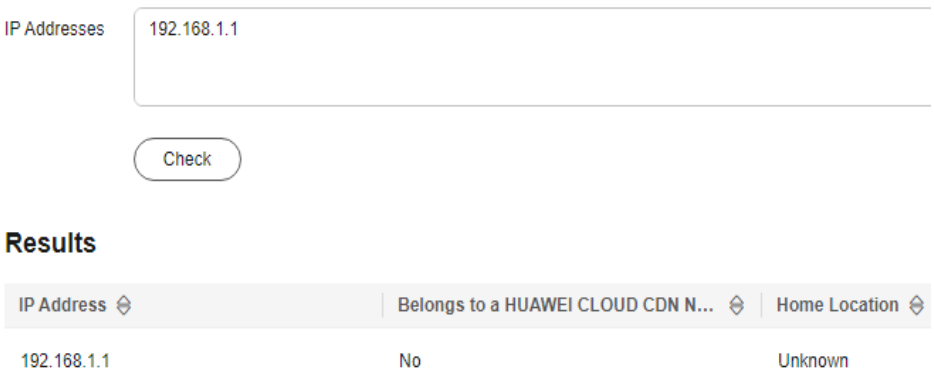
- If the check result shows that the IP address is not that of a Huawei Cloud CDN PoP, the problem may lie in the carrier network. In this case, contact your carrier.
- If the IP address belongs to a Huawei Cloud CDN PoP, rectify the fault by referring to **Troubleshooting**.

Procedure

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

   The CDN console is displayed.
2. In the navigation pane, choose **IP Address Check** to go to the PoP IP address check page.

   Figure 10-1 Checking PoP IP addresses



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.

11 Security

If your services require high security, enable and configure the security functions.

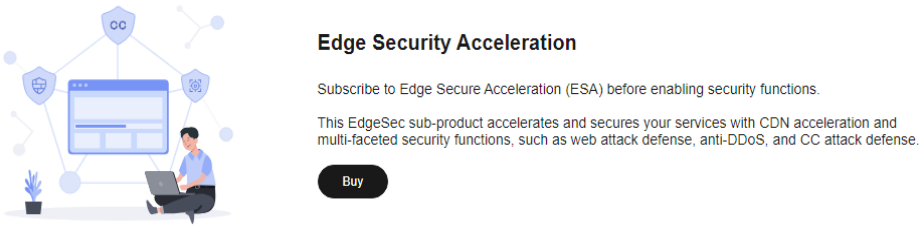
Procedure

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 **Security**.

   Figure 11-1 Enabling security

3. Click **Buy** and select a package.

   NOTE

   After the payment, professional technical personnel will contact you to confirm the order and assist you in enabling security.

Related Configurations

After security is enabled, configure related rules. For details, see *User Guide* of **Edge Security (EdgeSec)**.

Fee Description

- After security is enabled, the fees generated by the protected domain names are charged by EdgeSec. CDN does not charge any fees for these domain names.

- CDN resource packages (of traffic and requests) are used to deduct resources consumed by domain names that are not protected. For details about the billing rules for protected domain names, see **Billing Description** of EdgeSec.

12 Permissions Management

12.1 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"
        ]
      }
    ]
  }
  ```

12.2 Authorizing and Associating an Enterprise Project

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 **Supported Cloud Services**.

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**.

13 Monitoring and Auditing

13.1 CTS for Audit

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 13-1 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**.

13.2 Cloud Eye for Monitoring

13.2.1 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

Supported CDN Metrics

Table 13-2 CDN metrics that can be monitored

ID	Name	Description	Unit	Conversion Rule	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
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

ID	Name	Description	Unit	Conversion Rule	Monitoring Period (Original Value)
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
hit_flux_rate	Traffic hit ratio	Percentage of hit traffic of a domain name within one minute (Hit traffic/Traffic x 100)	%	-	1 minute
avg_req_time	Average request duration	Average request duration of a domain name within one minute (Total request duration/Number of requests)	ms	-	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

ID	Name	Description	Unit	Conversion Rule	Monitoring Period (Original Value)
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
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

ID	Name	Description	Unit	Conversion Rule	Monitoring Period (Original Value)
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
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

ID	Name	Description	Unit	Conversion Rule	Monitoring Period (Original Value)
bs_http_code_2xx_rate	Percentage of origin status codes 2*xx*	Percentage of origin HTTP status codes 2*xx* 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
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

ID	Name	Description	Unit	Conversion Rule	Monitoring Period (Original Value)
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
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

ID	Name	Description	Unit	Conversion Rule	Monitoring Period (Original Value)
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
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

ID	Name	Description	Unit	Conversion Rule	Monitoring Period (Original Value)
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
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

ID	Name	Description	Unit	Conversion Rule	Monitoring Period (Original Value)
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
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

ID	Name	Description	Unit	Conversion Rule	Monitoring Period (Original Value)
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
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

ID	Name	Description	Unit	Conversion Rule	Monitoring Period (Original Value)
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
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

ID	Name	Description	Unit	Conversion Rule	Monitoring Period (Original Value)
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
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

ID	Name	Description	Unit	Conversion Rule	Monitoring Period (Original Value)
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
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

13.2.2 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.

Prerequisites

You have configured **Cloud Eye Monitoring**.

Precautions

- Data of accounts that enabled Cloud Eye monitoring before October 30, 2024 (UTC+08:00) will be reported to the CN North-Beijing4 region of Cloud Eye. Data of accounts that enabled Cloud Eye monitoring after October 30, 2024 (UTC+08:00) will be reported to the AP-Singapore region of Cloud Eye.

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 **AP-Singapore** or **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.
   - **Alarm Type**: **Metric**
   - **Cloud product**: **Content Delivery Network - Domain Name**
   - **Resource Level**: **Specific dimension**
   - **Monitoring Scope**: Select **All resources**, **Resource groups**, or **Specific resources**.
6. After the configuration is complete, click **Create**.

13.2.3 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.

Precautions

- Data of accounts that enabled Cloud Eye monitoring before October 30, 2024 (UTC+08:00) will be reported to the CN North-Beijing4 region of Cloud Eye. Data of accounts that enabled Cloud Eye monitoring after October 30, 2024 (UTC+08:00) will be reported to the AP-Singapore region of Cloud Eye.

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 **AP-Singapore** or **CN North-Beijing4**.
3. In the navigation pane, choose **Cloud Service Monitoring**.
4. Click **Content Delivery Network CDN**.
5. 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.

