

# Content Delivery Network

## FAQs

**Issue** 01  
**Date** 2024-04-16



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

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

## **Trademarks and Permissions**



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

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

## **Notice**

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

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

# Security Declaration

## Vulnerability

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

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

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

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

---

# Contents

---

<b>1 Functions and Usage</b>	<b>1</b>
1.1 Functions	1
1.1.1 What Service Types Does CDN Support?	1
1.1.2 Which Protocols Does CDN Support?	1
1.1.3 Does On-Demand Service Acceleration Support HLS and RTMP?	1
1.1.4 Can CDN Identify Whether a User Is on a Desktop or Mobile Device?	2
1.1.5 Does CDN Support Acceleration for a Single Web Page?	2
1.1.6 Does CDN Support Binary File Acceleration?	2
1.1.7 Does CDN Support Level-2 Domain Name Acceleration?	2
1.1.8 Does CDN Accelerate POST Requests?	2
1.1.9 What Origin Types Does CDN Support?	2
1.1.10 Does Huawei Cloud CDN Support HTTP/3?	2
1.1.11 Does Huawei Cloud CDN Support Content Encryption Before Distribution?	2
1.1.12 Does Huawei Cloud CDN Support Intranet Acceleration?	2
1.2 Usage	3
1.2.1 How Do I Grant CDN Permissions to IAM Users?	3
1.2.2 How Do I Obtain the IP Address of a User?	3
1.2.3 Does CDN Support Acceleration by Region?	3
1.2.4 What Is the Conversion Rule for Traffic and Bandwidth?	3
1.2.5 Does CDN Accelerate the Origin Server of a Website, or Accelerate the Domain Name?	3
1.2.6 Can Wildcards Be Used as Part of an Acceleration Domain Name?	3
1.2.7 Is CDN Necessary If My Services Are Deployed Within a City?	4
1.2.8 How Does CDN Determine the Region to Which a User Belongs?	4
1.2.9 How Do I Direct Traffic from a Third-party Platform to CDN?	4
1.2.10 Can an Acceleration Domain Name Be Configured with Multiple Origin Servers?	4
1.2.11 Can I Use CDN If the Origin Port Is Not 80?	4
1.2.12 How Do I Configure an Origin Server When It Is a Non-Huawei Cloud Object Storage Bucket?	4
1.2.13 Does CDN Accelerate User Access from a Specified Line?	5
1.2.14 What Are the Differences Between an Acceleration Domain Name and an Origin Domain?	5
1.2.15 Can CDN Provide Acceleration for a Domain Name That Houses Different Types of Services (Website, VOD, and File Download)?	5
<b>2 Purchase and Billing</b>	<b>6</b>
2.1 What Will I Billed For?	6

2.2 Will I Be Billed If My Domain Name Is Under Attack?.....	6
2.3 Is Billing for On-Demand Service Acceleration the Same as That for File Download Acceleration?.....	7
2.4 What Is a Retention Period?.....	7
<b>3 Domain Name Settings.....</b>	<b>8</b>
3.1 Does CDN Support the Configuration of Domain Names with Ports?.....	8
3.2 Can a Subdomain Name Be Used as an Acceleration Domain Name?.....	8
3.3 Can the CNAME of an Acceleration Domain Name Be Directly Accessed?.....	8
3.4 Do I Need to Configure a Certificate for the Origin Server After Adding a Security Certificate to CDN? .....	9
3.5 How Do I Check Whether the CNAME Record Has Taken Effect?.....	9
3.6 Can I Limit Access to Domain Names Based on QPS?.....	9
3.7 Does Huawei Cloud CDN Accelerate Content Redirected from VPN?.....	9
3.8 Does My Domain Name Have to Be Resolved on Huawei Cloud?.....	9
3.9 Why Do My Domain Requests Still Go to CDN PoPs After My Domain Name Has Been Disabled and Domain Resolution Has Been Changed?.....	10
3.10 How Do I Configure a Certificate If My Domain Name Is a Wildcard Domain?.....	10
3.11 Does CDN Support Modification to Acceleration Service Types?.....	10
3.12 Why Am I Seeing the "Incomplete certificate chain" Message?.....	11
3.13 Why Am I Seeing a Message Indicating that the Certificate Format Is Incorrect?.....	11
3.14 Are Self-Signed HTTPS Certificates Supported?.....	11
3.15 Does CDN Support Force HTTPS?.....	11
3.16 Can I Use HTTP After HTTPS Is Configured?.....	11
<b>4 Cache Settings.....</b>	<b>12</b>
4.1 Will the Cache on CDN PoPs Be Updated in Real Time?.....	12
4.2 Does CDN Cache Status Codes 404 and 403?.....	12
4.3 What Are the Default Cache Rules? Can I Modify the Cache Age?.....	12
4.4 Does the Path in Cache Settings Refer to a Web Address or File Path on the Server?.....	13
4.5 Why Is the CDN Cache Hit Ratio Low?.....	13
4.6 How Do I Cache the Homepage (Root Directory)?.....	13
4.7 How Do I Check Whether a Cache Is Hit?.....	13
4.8 Why Is the Latest Content Inaccessible Even When the Maximum Cache Age Is Set to 0?.....	14
4.9 Does Huawei Cloud CDN Support Caching octet-stream Stream Files?.....	14
4.10 Why Are Certain Files Not Downloadable Even Though They Have Not Expired (365 Days)?.....	14
4.11 How Do I Configure Cache for Resources That Do Not Need to Be Cached?.....	14
4.12 How Do I Synchronize Content Cached on CDN PoPs with That on the Origin Server?.....	14
4.13 Why Does a Cache Rule Not Take Effect?.....	15
<b>5 Troubleshooting.....</b>	<b>16</b>
5.1 Why Am I Seeing a Message Indicating that the Domain Name Already Exists When I Add a Domain Name for CDN Acceleration?.....	16
5.2 Why Is My Domain Name Inaccessible After HTTPS Secure Acceleration Is Configured?.....	16
5.3 Why Is Data Obtained from a CDN PoP Not the Updated Data?.....	16
5.4 Why Is 304 Returned When a User Accesses a Resource Under My Acceleration Domain Name?.....	17

5.5 Why Is the Accelerated Page Incorrect Even Though I Can Access the Origin Server?.....	18
5.6 Why Can't a Web Page Be Properly Displayed After the Origin Server's IP Address Is Changed?.....	18
5.7 Why Do I Get an Access Failure and Access-Control-Allow-Origin Error?.....	18
5.8 Why Does the System Always Display "301" After HTTPS Is Configured for a Domain Name?.....	19
5.9 Why Do I Get Request Timed Out When Trying to Ping an Acceleration Domain Name?.....	19
5.10 Why Are Incorrect Resources Being Pulled from My Origin Server?.....	19
5.11 Why Is My Site Slow the First Time I Access It After CDN Is Configured?.....	19
<b>6 Cache Purge and Prefetch.....</b>	<b>20</b>
6.1 What Are the Differences Between Cache Purge and Cache Prefetch?.....	20
6.2 Why Am I Seeing Insufficient Permission for Cache Purge and Prefetch?.....	20
6.3 Why Does a Cache Prefetch Operation Fail?.....	20
6.4 Does Cache Purge Refresh Content Cached on All PoPs?.....	21
6.5 Should I Enter an Origin URL or Domain Name URL for Cache Purge and Prefetch?.....	21
6.6 Why Does a Prefetch Task Remain in the Being Processed Status for a Long Time?.....	21
6.7 How Do I Purge the CDN Cache Where the Domain Name Includes a Wildcard?.....	21
6.8 Why Is the Content Not Updated Even After I Prefetched and Purged the Cache?.....	22
6.9 Does CDN Support Directory Prefetch?.....	22
6.10 Are Cache Purge and Prefetch Mandatory?.....	22
6.11 Do I Need to Purge or Prefetch the Cache of Both HTTP and HTTPS URLs?.....	22
6.12 Can I Prefetch M3U8 Files?.....	22
6.13 Which Should I Do First, Purge or Prefetch, When I Want to Update Cache?.....	22
<b>7 Security.....</b>	<b>24</b>
7.1 What Security Capabilities Does CDN Provide?.....	24
7.2 Can I Configure Referer Validation to Prevent Hotlinking?.....	24
7.3 Does CDN Support IP Address Filtering?.....	24
7.4 How Does CDN Respond to CC Attacks?.....	24
7.5 Does CDN Have Anti-DDoS Capabilities?.....	25
7.6 Can Certificates Be Updated Without Service Interruption?.....	25
7.7 Does CDN Detect Viruses in an Acceleration File?.....	25
7.8 Can Multiple Certificates Be Configured for a Domain Name?.....	25
<b>8 Statistics and Logs.....</b>	<b>26</b>
8.1 What Could Fall Into the "Other" Category in the Visitor Region Statistics?.....	26
8.2 What Are the Meanings of HEAD, HIT, and MISS in CDN Logs?.....	26
8.3 What Does User-Agent OkHttp in CDN Logs Mean?.....	26
8.4 How Many Days of Data Can Be Queried?.....	27
8.5 Why Is There No Data in Analytics?.....	27
<b>9 Origin Pull.....</b>	<b>28</b>
9.1 In What Scenarios Does CDN Pull Content from an Origin Server?.....	28
9.2 What Do I Fix Origin Pull Failures?.....	28
9.3 How Do I Check Whether Range Requests Are Supported for Origin Pull?.....	28
9.4 If a Domain Name Is Attacked, Will Access Requests Be Directed to the Origin Server?.....	29

---

9.5 What Are the Benefits of Configuring a Standby Origin Server?.....	29
9.6 Does CDN Support Direct Origin Pull Through Crawler Access?.....	29
9.7 What Is the Difference Between a Host and an Origin Server?.....	29
9.8 How Is Origin Pull If the Origin Server Has Multiple IP Addresses?.....	29
9.9 Why Are Incorrect Resources Being Pulled?.....	30
9.10 How Do I View Origin Pull Records?.....	30
9.11 Will CDN Download All Files If I Send a Status Code 206 to Request 100-Byte Content?.....	30
<b>A Change History.....</b>	<b>31</b>

# 1 Functions and Usage

---

## 1.1 Functions

### 1.1.1 What Service Types Does CDN Support?

- Website acceleration  
CDN is perfect for web portals, e-commerce platforms, information apps, and UGC-focused apps. It can accelerate the delivery of images and small HTML, CSS, and JS files.
- File download acceleration  
CDN is suitable for websites, game clients, and app stores that provide file download services, and download tools. It is used in scenarios such as downloading game installation packages and application packages, and updating the ROM on mobile phones.
- On-demand service acceleration  
For customers providing on-demand audiovisual services, CDN is a must. On-demand services include online education, video sharing, music or video on demand, and other audiovisual content.
- Example:
  - If both on-demand service acceleration and file download acceleration are required, only one service type can be selected for an acceleration domain name. You need to create two domain names, one for on-demand service acceleration and the other for file download acceleration.

### 1.1.2 Which Protocols Does CDN Support?

CDN supports HTTP and HTTPS. It does not support FTP, TCP, UDP, WebSocket, or WSS.

### 1.1.3 Does On-Demand Service Acceleration Support HLS and RTMP?

On-demand service acceleration supports the HLS protocol but does not support the RTMP or FLV protocol.



## 1.1.4 Can CDN Identify Whether a User Is on a Desktop or Mobile Device?

No.

If a CDN point of presence (PoP) caches the content for mobile devices, when a user accesses that content, the CDN PoP directly serves the content. If a CDN PoP caches the content for desktop devices, when a user accesses that content, the CDN PoP also directly serves the content. Therefore, the content for mobile devices and that for desktop devices need to be distinguished on the origin server.

## 1.1.5 Does CDN Support Acceleration for a Single Web Page?

Yes.

If you want to accelerate some resources on a website, you can set an independent domain name for these resources and then configure CDN acceleration for the domain name.

## 1.1.6 Does CDN Support Binary File Acceleration?

Yes. You can select download acceleration for such requirements.

## 1.1.7 Does CDN Support Level-2 Domain Name Acceleration?

Yes.

## 1.1.8 Does CDN Accelerate POST Requests?

POST requests are dynamic interaction requests. If you have only configured website acceleration, download acceleration, or on-demand service acceleration, CDN does not accelerate these requests.

## 1.1.9 What Origin Types Does CDN Support?

CDN supports the following origin types: origin IP addresses and origin domain names. An origin server can be deployed on Huawei Cloud, other clouds, or Internet Data Centers (IDCs). There is no requirement on the location of the origin server. For details about how to access CDN, see [Adding a Domain Name](#).

## 1.1.10 Does Huawei Cloud CDN Support HTTP/3?

No.

## 1.1.11 Does Huawei Cloud CDN Support Content Encryption Before Distribution?

No. CDN only provides content distribution.

## 1.1.12 Does Huawei Cloud CDN Support Intranet Acceleration?

No.

## 1.2 Usage

### 1.2.1 How Do I Grant CDN Permissions to IAM Users?

You can use IAM to implement fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely access your Huawei Cloud resources. For details about all CDN permissions and how to grant permissions to IAM users, see [Permissions Management](#).

### 1.2.2 How Do I Obtain the IP Address of a User?

You can obtain the IP address of a user from the value of the **X-Forwarded-For** header.

### 1.2.3 Does CDN Support Acceleration by Region?

No. However, you can configure DNS settings at the domain name provider to redirect requests from a certain region to CDN points of presence (PoPs), so that acceleration can be implemented only for this region.

### 1.2.4 What Is the Conversion Rule for Traffic and Bandwidth?

- 1 GB = 1,024 MB
- 1 Mbit/s = 1,000 kbit/s

### 1.2.5 Does CDN Accelerate the Origin Server of a Website, or Accelerate the Domain Name?

CDN accelerates domain names. When CDN is enabled, access requests to all files under an acceleration domain name will be directed to CDN points of presence (PoPs).

### 1.2.6 Can Wildcards Be Used as Part of an Acceleration Domain Name?

Yes. A wildcard, \*, allows multiple secondary domain names to be included by the same value. All these secondary domain names point to the same IP address. For example, if you add \*.test.com to CDN as an acceleration domain name and have it resolved to the CNAME record provided by CDN, CDN acceleration will apply to all level-2 domain names under \*.test.com, such as a.test.com, by default. However, CDN acceleration will not apply to level-3 domain names such as b.a.test.com.

The following are the rules for adding wildcards to domain names:

- If you add a wildcard to a domain name for a particular account, you cannot add any of the level-2 domain names under that domain name to other accounts.

- 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 domain name with the wildcard, not on each of the level-2 domain names.

You can log in to the CDN console, choose **Domains** in the navigation pane, and click **Add Domain Names** to configure a wildcard domain name.

### 1.2.7 Is CDN Necessary If My Services Are Deployed Within a City?

Yes. CDN has different lines. Its carrier partners have their own points of presence (PoPs). Using CDN to cache static resources on different PoPs can relieve the pressure on your origin server and improve user experience.

### 1.2.8 How Does CDN Determine the Region to Which a User Belongs?

Huawei Cloud CDN uses Local Domain Name Server (LDNS) to determine the region to which a user belongs.

### 1.2.9 How Do I Direct Traffic from a Third-party Platform to CDN?

Add your domain name to CDN. Test your domain name before adding a CNAME record. For details, see [Testing the Domain Name](#). After the test is successful, add the CNAME record provided by CDN to your domain's DNS records. For details, see [Configuring a CNAME Record](#).

### 1.2.10 Can an Acceleration Domain Name Be Configured with Multiple Origin Servers?

Yes.

You can configure two origin servers in primary/standby mode. One origin server is selected as the primary origin server, and the other as a standby one. For details, see [Origin Server Settings](#).

### 1.2.11 Can I Use CDN If the Origin Port Is Not 80?

Yes. The origin port is customizable. You can modify the origin port on the CDN console. For details, see [Modifying Origin Server Details](#).

### 1.2.12 How Do I Configure an Origin Server When It Is a Non-Huawei Cloud Object Storage Bucket?

1. Obtain the domain name of your bucket. Add a domain name on the CDN console, set the origin server type to **Domain name**, and enter the obtained bucket domain name.
2. By default, the host for origin pull is your acceleration domain name. If you configure an object storage bucket as your origin server, change the host to

the domain name of that object storage bucket. Otherwise, origin pull will fail.

### **1.2.13 Does CDN Accelerate User Access from a Specified Line?**

No.

Among all the requests for your domain name, CDN cannot accelerate access from a specific line.

### **1.2.14 What Are the Differences Between an Acceleration Domain Name and an Origin Domain?**

- An acceleration domain name is provided for acceleration, that is, the domain name accessed by users.
- An origin domain corresponds to the server IP address. It is accessed by CDN during origin pull.

The acceleration domain name and origin domain cannot be the same. When a user accesses the acceleration domain name for a website resource but it is not cached, CDN will need to pull the resource from the origin server. If the origin domain is the same as the acceleration domain name, the user's request will be repeatedly directed to CDN points of presence (PoPs), and CDN PoPs will not be able to pull content from the origin server.

### **1.2.15 Can CDN Provide Acceleration for a Domain Name That Houses Different Types of Services (Website, VOD, and File Download)?**

Yes, but the acceleration will not be noticeable. It is recommended that different types of pages use different domain names for acceleration.

For example, place the VOD content in <http://video.example.com> and video content in <http://file.example.com>, and then apply CDN separately to the two different domains.

# 2 Purchase and Billing

---

## 2.1 What Will I Billed For?

You will be billed for:

- Traffic generated by user access to CDN points of presence (PoPs). CDN does not charge any origin pull requests.
- Traffic for obtaining content from the origin server that is an object storage bucket.

Billing on the CDN side:

- You can choose to be billed by traffic, peak bandwidth, 95th percentile bandwidth, or average daily peak bandwidth. You can also purchase economical traffic packages. For details, see [Billing](#).

Cache prefetch:

- Cache prefetch is simulation of origin pull. Traffic or bandwidth consumed during cache prefetch is not billed by CDN, but billed by other services based on your origin server configuration. For example, if your origin server is an OBS bucket, you will be billed by OBS for traffic generated during origin pull.

CDN services will be suspended if you have outstanding unpaid balance. Top up your account in a timely manner to ensure that your services are not interrupted.

## 2.2 Will I Be Billed If My Domain Name Is Under Attack?

Yes. The consumed traffic or bandwidth will be billed.

If a domain name is under attack and the attacks affect other CDN users or pose risks to CDN, CDN will ban the domain name, change its status to **Disabled**, and disable the acceleration service for it. The domain name cannot be accessed but its configuration is retained. When the attack stops, contact customer service to unban the domain name.

- Solutions

Solution	Description
Access control	You can use access control functions such as referer validation, IP address access control lists (ACLs), and token authentication for domain names to avoid unnecessary traffic or bandwidth consumption. For details, see <a href="#">Access Control</a> .

#### NOTE

To ensure data integrity and accuracy of bills, a bill is usually generated after a billing cycle ends. Therefore, the bill time is later than the time when resources are consumed, and resource consumption cannot be reflected in real time through bills. This is due to the distributed architecture of CDN points of presence (PoPs).

## 2.3 Is Billing for On-Demand Service Acceleration the Same as That for File Download Acceleration?

CDN is billed based on the used traffic or bandwidth, regardless of the acceleration service types. For details, see [Billing](#).

## 2.4 What Is a Retention Period?

It is the time Huawei Cloud provides for a customer to renew or repay when the yearly/monthly resources are still not renewed, the pay-per-use resources are still in arrears, or the overdue bills are still not paid off. Within the retention period, you cannot access or use your cloud service but your data stored in the cloud service is still retained. After a resource enters a retention period, Huawei Cloud will notify you of this by email or text message. If you still do not complete the renewal or payment after the retention period has ended, your data stored in the cloud service will be deleted and the resource will be released.

For details about the retention period, see [Retention Period](#).

# 3 Domain Name Settings

---

## 3.1 Does CDN Support the Configuration of Domain Names with Ports?

Yes.

- Acceleration domain name: The default port numbers are 80 and 443. If you have special ports, change them to port 80 and 443.
- Origin server: You can add a port for origin pull in the **Origin Server Settings** area under the **Basic Settings** tab of the CDN console. For details, see [Origin Server Settings](#).

## 3.2 Can a Subdomain Name Be Used as an Acceleration Domain Name?

Yes.

## 3.3 Can the CNAME of an Acceleration Domain Name Be Directly Accessed?

No.

After a domain name is added, the system will assign a CNAME record to the domain name. Then, you need to configure a CNAME record with your domain provider, specifying that the CNAME record is an alias for your domain name. After the CNAME record takes effect, all requests for your domain name will be sent to CDN points of presence (PoPs).

### 3.4 Do I Need to Configure a Certificate for the Origin Server After Adding a Security Certificate to CDN?

The security certificate configured on the CDN side is used for encrypted transmission when users access CDN points of presence (PoPs). If you want to encrypt the transmission from CDN PoPs to your origin server, you are advised to configure the security certificate on the origin server.

### 3.5 How Do I Check Whether the CNAME Record Has Taken Effect?

The time it takes for the CNAME record to take effect depends on the DNS provider. To check whether a CNAME record has taken effect:

Open the command line interface that comes with Windows and run the following command:

```
nslookup -qt=cname Acceleration domain name
```

If the CNAME record is displayed, the CNAME record has taken effect.

### 3.6 Can I Limit Access to Domain Names Based on QPS?

No.

You are advised to check access logs for any suspicious access. If you find suspicious accesses from any IP addresses, configure an IP address blacklist to block them.

### 3.7 Does Huawei Cloud CDN Accelerate Content Redirected from VPN?

No.

### 3.8 Does My Domain Name Have to Be Resolved on Huawei Cloud?

No.

CDN only accelerates content delivery. No matter where your domain name is resolved, make sure it resolves to the CNAME record provided by CDN.



## 3.9 Why Do My Domain Requests Still Go to CDN PoPs After My Domain Name Has Been Disabled and Domain Resolution Has Been Changed?

Possible causes:

- The carrier and users have cached the DNS resolution result locally. Before the cache expires, domain requests are still sent to CDN points of presence (PoPs). They will be sent to the new DNS record only after the cache expires.
- Before the domain name is disabled, a user pings the domain name to obtain the IP addresses of CDN PoPs, and then binds the domain name with the PoP IP addresses in the local **hosts** file. It means that the user specifies a resolution to bypass normal DNS resolution. As a result, requests from the user are sent to CDN PoPs.

Solutions:

- If the problem is caused by local cache, wait until the cache expires.
- If a user binds the domain name with CDN PoPs in the local **hosts** file, the user needs to unbind them.

## 3.10 How Do I Configure a Certificate If My Domain Name Is a Wildcard Domain?

When you configure a wildcard-domain certificate, the wildcard domain must match the certificate at the same level. For example:

1. If your domain name is a.b.example.com or \*.b.example.com, the wildcard-domain certificate must be \*.b.example.com rather than \*.example.com or \*.a.b.example.com.
2. If your domain name is a.example.com or \*.example.com, the wildcard-domain certificate must be \*.example.com rather than \*.b.example.com.

### Configuration Method

- To configure a certificate for a domain name:  
In the navigation pane of the CDN console, choose **Domains**. Click **Configure** in the row containing the target domain name, click the **HTTPS Settings** tab, and configure a certificate.

## 3.11 Does CDN Support Modification to Acceleration Service Types?

No. You cannot change the service type on the CDN console.

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

This is maybe because:

- Certificates are installed in the wrong order.

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

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

### 3.13 Why Am I Seeing a Message Indicating that the Certificate Format Is Incorrect?

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

### 3.14 Are Self-Signed HTTPS Certificates Supported?

No.

You are advised to buy trusted root certificates. For details about HTTPS certificates, see [HTTPS Certificate Requirements](#).

### 3.15 Does CDN Support Force HTTPS?

Yes. Log in to the CDN console and choose **Domains > Configure > HTTPS Settings** to configure force HTTPS.

### 3.16 Can I Use HTTP After HTTPS Is Configured?

Yes. Both HTTP and HTTPS requests are supported.

# 4 Cache Settings

---

## 4.1 Will the Cache on CDN PoPs Be Updated in Real Time?

Cached content on CDN points of presence (PoPs) is not updated in real time. CDN PoPs only obtain new content from the origin server when the previously cached content expires. If you want to update content cached on CDN PoPs, configure cache rules.

## 4.2 Does CDN Cache Status Codes 404 and 403?

By default, CDN caches status codes 400, 404, 416, 500, 502, and 504 for 3 seconds and does not cache other 4XX and 5XX status codes.

## 4.3 What Are the Default Cache Rules? Can I Modify the Cache Age?

Each domain name is configured with one or more default cache rules.

- If the service type is website acceleration, file download acceleration, or on-demand service acceleration, and the origin server address is an origin IP address or origin domain, two default cache rules are available.
  - The default maximum cache age for common dynamic files (for example, .php, .jsp, .asp, and .aspx files) is 0. CDN pulls content from the origin server directly when receiving requests for such dynamic files. You can modify and delete this rule.
  - The default maximum cache age for all files is 30 days. You can modify but cannot delete this rule.

If you want to change the maximum cache age, choose **Domains > Configure > Cache Settings** on the CDN console to change it.

## 4.4 Does the Path in Cache Settings Refer to a Web Address or File Path on the Server?

It refers to a web address.

## 4.5 Why Is the CDN Cache Hit Ratio Low?

Possible causes:

- The HTTP header has been incorrectly configured. As a result, the content cannot be cached. Check the Cache-Control settings of your origin server. If **cache-control** is set to **no-cache**, **no-store**, **max-age=0**, or **private** on the origin server and **Origin Cache Control** is enabled on CDN, CDN cannot cache resources, resulting in a low hit ratio.
- The maximum cache age you have configured is too short. In this case, CDN points of presence (PoPs) will not be able to cache data. They will frequently pull the fresh content from the origin server. As a result, the CDN cache hit ratio will be low.
- A large portion of the content on your origin server is dynamic. CDN mainly accelerates static content (such as CSS, JS, HTML, TXT files, pictures, and video). Dynamic content (such as ASP, JSP, PHP files, APIs, and dynamic interaction requests) is typically pulled from the origin server.
- If your origin server has a large number of resources and does not support range requests, CDN PoPs will pull complete resources, increasing the pull traffic and affecting the traffic hit ratio.
- The website is not accessed very frequently. Content cached on the CDN PoPs may be deleted due to infrequent access. As a result, the fresh content is pulled when it is accessed, and the CDN cache hit ratio will decrease.
- An exception occurred on your origin server. In this case, troubleshoot your origin server first.
- HEAD requests are sent. By default, CDN does not cache HEAD requests. Even if cache prefetch is performed, HEAD requests are not cached.

## 4.6 How Do I Cache the Homepage (Root Directory)?

On the CDN console, choose **Domains > Configure > Cache Settings**. In the **Configure Cache Rule** dialog box, set **Type** to **Homepage** and set the cache rule for the root directory.

## 4.7 How Do I Check Whether a Cache Is Hit?

1. Open Google Chrome and press **F12**.
2. Choose **Network**.
3. Enter the website to be accessed in the address box and press **Enter**. View the response headers of the URL of a specific resource and perform the following operations:

- If the value of the **x-hcs-proxy-type** header is **1**, the cache is hit. If the value is **0**, the cache is not hit.

## 4.8 Why Is the Latest Content Inaccessible Even When the Maximum Cache Age Is Set to 0?

If the maximum cache age is set to 0, CDN pulls the requested content from the origin server. After the maximum cache age is reset, the new setting does not take effect immediately. Wait for a few minutes and try again. You can also manually refresh the cache to force the cache to expire.

## 4.9 Does Huawei Cloud CDN Support Caching octet-stream Stream Files?

Yes.

## 4.10 Why Are Certain Files Not Downloadable Even Though They Have Not Expired (365 Days)?

Although their maximum cache age is 365 days, CDN points of presence (PoPs) regularly delete cached content that has not recently been accessed, regardless of the content's expiration time.

You can preheat resources so that users can obtain the most recent resources from CDN PoPs upon first access.

## 4.11 How Do I Configure Cache for Resources That Do Not Need to Be Cached?

You can set the maximum cache age of these resources to **0** in a cache rule.

## 4.12 How Do I Synchronize Content Cached on CDN PoPs with That on the Origin Server?

- You can set cache rules. For content that is frequently updated, you can set a cache rule with a short maximum cache age. For content that is not frequently updated, you can set a cache rule with a long maximum cache age to reduce the pressure on the origin server.
- If the configured cache age is not reached but new content is released or content is deleted on the origin server, you can manually refresh the cache.
  - Log in to the console and choose **Service List > Content Delivery & Edge Computing > Content Delivery Network**. In the navigation pane, choose **Prefetch & Purge**. On the **Cache Purge** tab, refresh the cache.

## 4.13 Why Does a Cache Rule Not Take Effect?

Possible causes and solutions:

1. You have just completed configuring the cache rule and it takes about 5 minutes for the rule to take effect. Verify cache configuration after the rule takes effect.
2. You have modified the cache rule. The new rule does not apply to content that has been cached but only applies to new content. If you want the new rule to take effect on the cached content, purge the cache on points of presence (PoPs).
3. Cache rules have priorities. The cache rule with a higher priority (large value) is matched first. Check the priority of your cache rules.

**Example:** You have configured a **File type** cache rule for domain name **www.example.com** to cache JPG files for only one day. The priority of the cache rule is set to **2**.

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

**Result:** When a user accesses the **www.example.com/test/cdn.jpg** file, two cache rules, **Full path** and **File type**, can be applied to this file. The priority of the **Full path** rule is **8**, which is higher than that of the **File type** rule. Therefore, the system follows the **Full path** rule **/test/\*.jpg** and caches the file for three days.

**Method:** To make the **File type** rule to take effect, set its priority to a value greater than **8**.

# 5 Troubleshooting

---

## 5.1 Why Am I Seeing a Message Indicating that the Domain Name Already Exists When I Add a Domain Name for CDN Acceleration?

If you have the permission to resolve the domain name, submit a service ticket.

## 5.2 Why Is My Domain Name Inaccessible After HTTPS Secure Acceleration Is Configured?

**Possible cause:** The origin protocol of the domain name is HTTP and force redirect from HTTP to HTTPS is configured on your origin server, so that the domain name cannot be accessed using HTTP or HTTPS.

In this case, a status code 301 is returned. CDN points of presence (PoPs) access the origin server using HTTP rather than HTTPS until the maximum number of retransmissions has been reached. As a result, the access will fail.

**Solution:** Go to the CDN console, choose **Domains** in the navigation pane, click **Configure** in the **Operation** column, click the **Origin Settings** tab, and set **Origin Protocol** to **Same as user**.

## 5.3 Why Is Data Obtained from a CDN PoP Not the Updated Data?

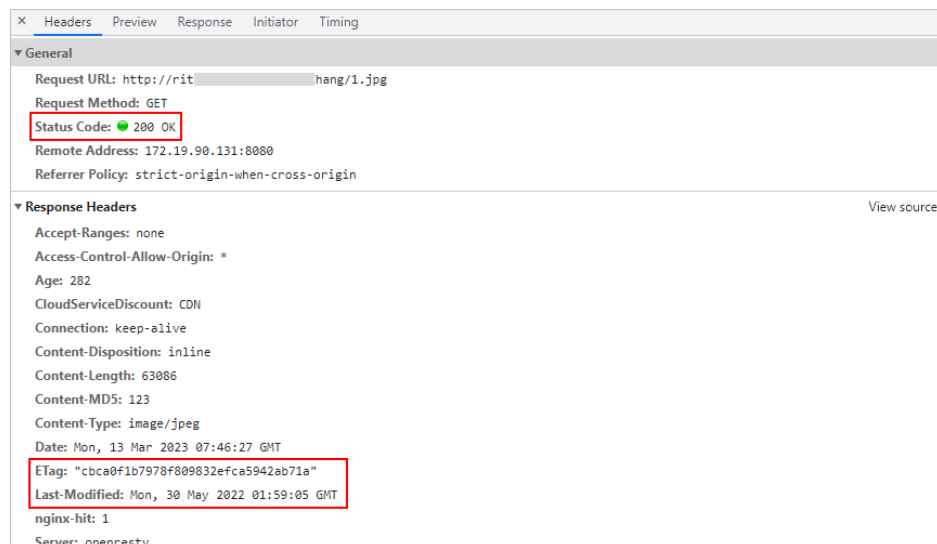
Cached content on CDN points of presence (PoPs) is not updated in real time. CDN PoPs only pull new content from the origin server when the previously cached content expires and then update the cache. After updating content on the origin server, you can submit cache purge requests to force the cached content on CDN PoPs to expire and ensure the latest content is updated. In this way, users can get the latest data when they access the website.

## 5.4 Why Is 304 Returned When a User Accesses a Resource Under My Acceleration Domain Name?

Status code 304 indicates that the resource has not changed since the last time CDN cached it.

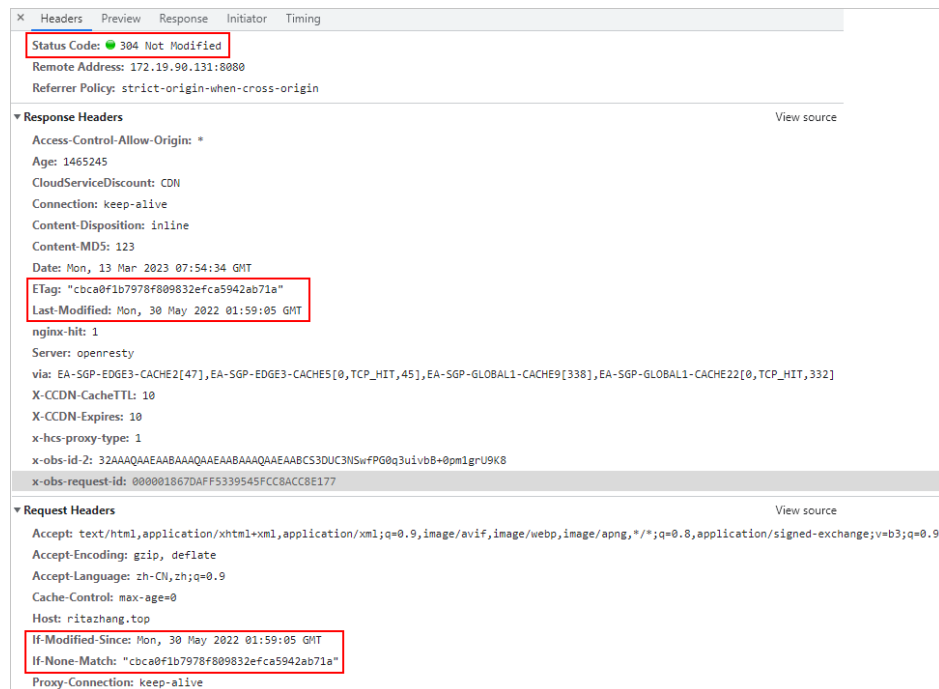
When a client requests the resource for the first time, CDN returns the resource in a 200 response to the client. The response includes **ETag** that marks the time when the resource was last modified. When the client requests the resource again, if the **ETag** value is not modified, 304 is returned and the client loads the cached content. If the **ETag** value differs, the modification time is marked and CDN returns the new resource to the client. Details are as follows:

1. When a client accesses **1.jpg** for the first time, CDN returns the image in a 200 response to the client. Response headers include **Last-Modified** (last modification time) and **ETag**.



2. When the client accesses **1.jpg** again, the request headers carry the **Last-Modified** and **ETag** values. If the two values differ, CDN returns the latest image in a 200 response to the client. If not modified, the client loads the cached content.





3. The user can press **Ctrl+F5** to clear the client cache. When the user accesses the resource again, status code 200 will be returned.

## 5.5 Why Is the Accelerated Page Incorrect Even Though I Can Access the Origin Server?

It is possible that the origin server updated the content but points of presence (PoPs) of CDN are still caching outdated content. You are advised to purge or prefetch the cache on the CDN console.

## 5.6 Why Can't a Web Page Be Properly Displayed After the Origin Server's IP Address Is Changed?

If the IP address of an origin server is changed, you need to manually refresh the cache. If you do not refresh the cache, CDN points of presence (PoPs) still cache outdated content.

## 5.7 Why Do I Get an Access Failure and Access-Control-Allow-Origin Error?

This issue occurs due to the cross-origin setting.

Solution:

1. Click the target domain name on the **Domains** page.
2. On the **Advanced Settings** tab, click **Edit** next to **HTTP Headers**.
3. Select **Access-Control-Allow-Origin** and set its value to **\*** or a specified domain name.

## 5.8 Why Does the System Always Display "301" After HTTPS Is Configured for a Domain Name?

**Origin Protocol** is set to **HTTP** for the domain name on the CDN console but **Force HTTPS** is enabled on your origin server.

You need to set **Origin Protocol** to **Same as user** under the **Origin Settings** tab of your domain name on the CDN console.

## 5.9 Why Do I Get Request Timed Out When Trying to Ping an Acceleration Domain Name?

For security purposes, ping operations are not allowed. You can run the **nslookup** command to check whether CDN has taken effect. For details, see [How Do I Check Whether the CNAME Record Has Taken Effect?](#)

## 5.10 Why Are Incorrect Resources Being Pulled from My Origin Server?

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

### NOTE

- 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 the host to specify the location of the requested content.
- 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.

## 5.11 Why Is My Site Slow the First Time I Access It After CDN Is Configured?

The first time you access a site, CDN points of presence (PoPs) have not yet cached the resources. They still need to obtain resources from the origin server. To prevent such a situation, you can prefetch the cache.

# 6 Cache Purge and Prefetch

---

## 6.1 What Are the Differences Between Cache Purge and Cache Prefetch?

- **Cache purge**  
After you submit a cache purge request, cached content on CDN points of presence (PoPs) will be forcibly expired. If a user requests that content, CDN has to pull 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 for caching. If a user requests the content, the CDN PoP immediately returns the cached content. It does not pull any new content.

## 6.2 Why Am I Seeing Insufficient Permission for Cache Purge and Prefetch?

Perform the following operations to rectify the fault:

- If you log in as an IAM user, check whether you have the permissions required to perform cache purge and prefetch. If you do not have the required permissions, apply for them from your account administrator.
- If you have the permissions required to perform cache purge and prefetch, check whether your account is in arrears.

## 6.3 Why Does a Cache Prefetch Operation Fail?

It is possible that:

1. A large number of files are being prefetched at the same time, and this occupies all of the origin server's bandwidth. Perform prefetch in batches, or increase the bandwidth of the origin server to improve the efficiency.

2. The maximum cache age of your requested content is 0. Modify the cache setting.
3. **Cache-Control** is set to **private**, **no-cache**, or **no-store** on the origin server and **Origin Cache Control** is enabled on the CDN console.
4. You requested to prefetch directories or dynamic content.
5. Your origin content cannot be accessed.

## 6.4 Does Cache Purge Refresh Content Cached on All PoPs?

Yes.

## 6.5 Should I Enter an Origin URL or Domain Name URL for Cache Purge and Prefetch?

CDN can purge and prefetch URLs of domain names. Therefore, you need to enter a domain name URL.

## 6.6 Why Does a Prefetch Task Remain in the Being Processed Status for a Long Time?

Possible causes:

- 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 prefetching a large number of files may consume all of the bandwidth available for your origin server. You are advised to:
  - Divide the prefetch tasks 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.

## 6.7 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 whose CDN cache is 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/>.

## 6.8 Why Is the Content Not Updated Even After I Prefetched and Purged the Cache?

The interval between cache prefetch and purge may be too short. It is recommended that the interval be longer than 5 minutes.

## 6.9 Does CDN Support Directory Prefetch?

No. Only complete URLs can be prefetched.

## 6.10 Are Cache Purge and Prefetch Mandatory?

This depends on the scenario.

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

## 6.11 Do I Need to Purge or Prefetch the Cache of Both HTTP and HTTPS URLs?

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

## 6.12 Can I Prefetch M3U8 Files?

Yes. When you prefetch M3U8 files, TS files under the M3U8 files are also prefetched.

## 6.13 Which Should I Do First, Purge or Prefetch, When I Want to Update Cache?

If your origin server content is updated and you want to update the cache on CDN points of presence (PoPs):

- Purge the cache first. When cache purge is completed (about 5 minutes), prefetch the cache.
- If you directly perform cache prefetch, content that has been cached on CDN PoPs will not be updated.

If your domain name is added to CDN for the first time and no content is cached on CDN PoPs, you can directly perform cache prefetch to cache the content on PoPs.

# 7 Security

---

## 7.1 What Security Capabilities Does CDN Provide?

- By adding your domain name to CDN, you can have your origin IP address hidden to prevent the origin server from being exposed to attackers.
- CDN has more than 2,000 points of presence (PoPs) on the entire network. CDN effectively relieves the pressure of DDoS/CC attacks on the origin server and prevents the origin server from being paralyzed due to attacks. If CDN PoPs fail to provide services due to heavy attack traffic, CDN will temporarily ban the domain name, change its status to **Disabled**, and disable the acceleration service for it. The domain name cannot be accessed but its configuration is retained.
- CDN supports referer validation, IP address access control lists (ACLs), and token authentication. For details, see [Access Control](#).

## 7.2 Can I Configure Referrer Validation to Prevent Hotlinking?

Yes. Log in to the CDN console and choose **Domains > Access Control > Referrer Validation**.

## 7.3 Does CDN Support IP Address Filtering?

Yes.

To prevent attacks from specific IP addresses, you can set a blacklist to filter out requests from these addresses. Log in to the CDN console and choose **Domains > Access Control > IP ACL** to configure the IP address blacklist.

## 7.4 How Does CDN Respond to CC Attacks?

In a challenge collapsar (CC) attack, the attacker uses a proxy server to generate and send disguised requests to the target host. The attacker keeps sending a large

number of data packets to target servers to exhaust server resources and break them down. If a site is attacked, CDN points of presence (PoPs) will bear the attack traffic. Therefore, the origin server will not break down.

- If CDN PoPs fail to provide services due to heavy attack traffic, CDN will temporarily ban the domain name, change its status to **Disabled**, and disable the acceleration service for it. The domain name cannot be accessed but its configuration is retained. When the attack stops, contact customer service to unban the domain name.
- You will be billed for the traffic generated by CDN PoPs during attacks.
- If your acceleration domain name has burst traffic, for example, during new function release, the domain name may be considered to be under attack. Contact technical support in advance to avoid service loss.

## 7.5 Does CDN Have Anti-DDoS Capabilities?

Yes. CDN's anti-DDoS capabilities depend on the capacity of points of presence (PoPs). If CDN PoPs fail to provide services due to heavy attack traffic, CDN will temporarily ban the domain name, change its status to **Disabled**, and disable the acceleration service for it. The domain name cannot be accessed but its configuration is retained. The traffic generated by attacks will be charged.

## 7.6 Can Certificates Be Updated Without Service Interruption?

Yes.

You can choose **Domains > Configure > HTTPS Settings** on the CDN console to update SSL certificates.

## 7.7 Does CDN Detect Viruses in an Acceleration File?

No.

CDN does not check whether your file content contains viruses. If your file content contains viruses, the carrier will notify you so that you can take appropriate measures. If the risk is severe, the carrier will disable the URL and then notify you.

## 7.8 Can Multiple Certificates Be Configured for a Domain Name?

No.

Only one certificate can be configured for a domain name.



# 8 Statistics and Logs

---

## 8.1 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.

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

- **HEAD**  
The HEAD method is similar to the GET method. The only difference is that the server does not return a message body for a HEAD request. 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. This method can be used to obtain the metadata about an entity without transferring 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 point of presence (PoP) directly serves the content.
- **MISS**  
This indicates a cache miss. A PoP needs to pull content from the origin server.

## 8.3 What Does User-Agent OkHttp in CDN Logs Mean?

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

## 8.4 How Many Days of Data Can Be Queried?

- On the **Analytics** page  
You can query CDN data over the past 90 days. The maximum query time range is 7 days.
- On the **Logs** page  
You can query and download logs over the past 30 days.

## 8.5 Why Is There No Data in Analytics?

- The CNAME record configured for your domain name is incorrect.
- CDN statistics on the **Analytics** page are not available in real time. It is updated about 1 hour later.

# 9 Origin Pull

---

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

1. CDN points of presence (PoPs) pull content from an origin server when they do not cache requested content.
2. CDN PoPs pull content from an origin server when the cached content on CDN PoPs has expired.

## 9.2 What Do I Fix Origin Pull Failures?

Origin pull failures indicate that CDN points of presence (PoPs) fail to access your origin server or the origin server returns an error. If CDN fails to pull content, CDN will retry once. For details, see [How Is Origin Pull If the Origin Server Has Multiple IP Addresses?](#)

Check whether the origin server is normal. For details, see [How Do I Check Whether an Access Fault Is Caused by a CDN PoP or Origin Server?](#)

## 9.3 How Do I Check Whether Range Requests Are Supported for Origin Pull?

Check the response of the origin server. If the response contains the **Content-Range** field, range requests are supported for origin pull.

For example, **Content-Range: bytes 0-100/2600** indicates that bytes from 0 to 100 are requested and the total data size is 2,600 bytes.

The status code of range requests is 206 instead of 200.

## 9.4 If a Domain Name Is Attacked, Will Access Requests Be Directed to the Origin Server?

If a domain name is under attack and the attacks affect other CDN users or pose risks to CDN, CDN will ban the domain name, change its status to **Disabled**, and disable the acceleration service for it.

## 9.5 What Are the Benefits of Configuring a Standby Origin Server?

If the primary origin server fails, CDN can pull content from the standby one to prevent origin pull failures.

## 9.6 Does CDN Support Direct Origin Pull Through Crawler Access?

No.

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

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

- Origin server  
The origin server decides the address to be accessed during origin pull.
- Host  
The host decides the site that stores the origin content to be obtained.

## 9.8 How Is Origin Pull If the Origin Server Has Multiple IP Addresses?

If the origin servers have multiple IP addresses, the following load balancing mechanism is used for origin pull.

- An origin pull request can be forwarded to up to two IP addresses of the primary origin server. If origin pull from both IP addresses fails, the request is forwarded to the standby origin server. The request can be forwarded to up to two IP addresses of the standby origin server. If origin pull fails again, the request fails.
- Origin pull fails when the connection times out, the connection fails, or a 5xx error code is returned from the origin server.

## 9.9 Why Are Incorrect Resources Being Pulled?

The configuration for host may be incorrect. By default, the host is your acceleration domain name. If your acceleration domain name is not the one that you want CDN points of presence (PoPs) to pull content from, change the host to the origin domain.

## 9.10 How Do I View Origin Pull Records?

CDN does not have origin pull logs. You can use the following methods to view origin pull records:

- Check the request logs of your origin server.
- Check whether the CDN logs contain the **MISS** field. If yes, there are origin pull records.

You are advised to prefetch the cache before checking the origin pull traffic.

## 9.11 Will CDN Download All Files If I Send a Status Code 206 to Request 100-Byte Content?

No.

The status code 206 indicates CDN pulls the requested portion from the origin server.

If you constantly request remaining portions, all files will be fetched from the origin server.

# A Change History

---

Released On	Description
2023-03-30	This issue is the first official release.