CDN

Troubleshooting

Issue	01
Date	2023-08-30



HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. 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 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 Why Can't I Access a Web Page or Play a Video After I Enable CDN?..... 1
2 Why Is It Still Slow to Access a Domain Name That Has Been Added for CDN Acceleration?..... 3
3 Why Is the Displayed or Downloaded Content Incorrect After CDN Acceleration Is Used?..... 6
4 Common Faults on WAF Resources Accelerated by CDN..... 9
5 Why Is a 4XX Status Code Returned When I Request Resources from My Acceleration Domain Name?..... 10
6 Why Is a 5XX Status Code Returned When I Request Resources from My Acceleration Domain Name?..... 13
7 Why Does a 301/302 Redirect Loop Occur When I Request Resources from My Acceleration Domain Name?..... 16
8 Status Code and Handling Suggestions..... 17
9 Why Am I Getting a Permission Error Message?..... 20
10 Why Can't I Log In to My Domain Name or Why Is the Information of Other Users Displayed?..... 22
11 How Do I Check Whether an Access Fault Is Caused by the CDN PoP or Origin Server?..... 23
12 Why Is the Cache of a Resource Inconsistent on Different PoPs?..... 25
13 Why Does the Configured Cache Rule Not Take Effect?..... 27
14 What Do I Do If the Browser Displays a Message Indicating that a Cross-domain Exception Occurs After CDN Is Enabled?..... 29

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1 Why Can't I Access a Web Page or Play a Video After I Enable CDN?

Symptom

After CDN is enabled, a web page cannot be accessed or a video cannot be played.

Check Items

- Whether the CDN origin server is faulty
- Whether CDN acceleration is enabled for the domain name
- Status code and domain name configuration
- Whether your HUAWEI ID is in arrears

Procedure

1. Check whether the fault is caused by the origin server or CDN points of presence (PoP). For details, see **How Do I Check Whether an Access Fault Is Caused by the CDN PoP or Origin Server?**.
2. Check whether CDN acceleration is enabled for the domain name.

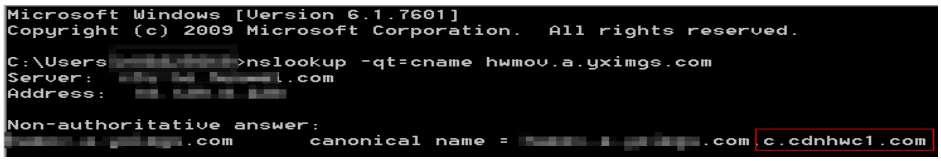
   NOTE

   If you have just added an acceleration domain name on the CDN console and are testing the domain name before adding a CNAME record, skip this step and configure the domain name as instructed in **Getting Started**.

   Check whether the domain name is resolved to CDN. Take the Windows operating system as an example. Open the Command Prompt and run the following command:

   ```
   nslookup -qt=cname Domain name
   ```

   If the command output contains **.c.cdnhwc1.com**, the CNAME record has taken effect.

a. If the command output does not contain **.c.cdnhwc1.com**, the domain name has not been resolved to CDN. You can **test the domain name** after adding it on the CDN console. After the test is successful, add the CNAME record provided by CDN to the record set of the DNS provider. For details, see **Configuring a CNAME Record**.

b. If the CNAME record has been correctly configured, check the time-to-live (TTL) of the previous resolution record of the domain name on the same resolution line. The TTL specifies the cache duration of a resolution record on the local DNS server. The newly added CDN CNAME record takes effect only after the TTL of the previous record expires.

If the domain name resolution is normal, proceed to the next step.

3. Check the CDN status code and domain name configuration.
   - If status code 4*xx*, 5*xx*, 301, or 302 is returned when you attempt to access a web page or video, fix the fault by following the instructions in the links below:
     i. 4*xx*: **Why Is a 4XX Status Code Returned When I Request Resources from My Acceleration Domain Name?**
     ii. 5*xx*: **Why Is a 5XX Status Code Returned When I Request Resources from My Acceleration Domain Name?**
     iii. 301/302: **Why Does a 301/302 Redirect Loop Occur When I Request Resources from My Acceleration Domain Name?**
   - Check whether the origin server configuration is correct. Log in to the CDN console and check whether the origin server is configured correctly on the **Basic Settings** tab of the domain name. Correct the IP address or domain name of the origin server if necessary.
4. **Check the account balance.**

   If your account is in arrears and is in the retention period, the system will disable your acceleration domain names and you cannot use CDN. View the outstanding amount of your account in the **Billing Center** and top up the account to offset the outstanding amount.

If the fault persists, contact customer service or **submit a service ticket**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2 Why Is It Still Slow to Access a Domain Name That Has Been Added for CDN Acceleration?

Symptom

After CDN acceleration is enabled, access to a web page or app resources is still slow.

Check Items

- Whether CDN acceleration is enabled for the domain name
- Whether the CDN cache is hit
- Whether inter-carrier or cross-province access is involved
- Whether cache rules are properly configured
- Whether the content is preheated
- Whether the client network is faulty

Procedure

1. Check whether CDN acceleration is enabled for the domain name.

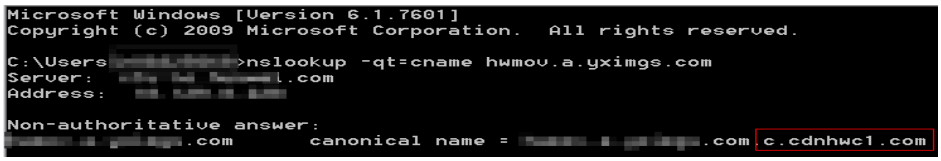
   NOTE

   If you have just added an acceleration domain name on the CDN console and are **testing the domain name** before adding a CNAME record, skip this step and configure the domain name as instructed in **Getting Started**.

   Check whether the domain name is resolved to CDN. Take the Windows operating system as an example. Open the Command Prompt and run the following command:

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

   If the command output contains **.c.cdnhwc1.com**, the CNAME record has taken effect.

- If the command output does not contain **.c.cdnhwc1.com**, CDN acceleration has not taken effect for the added domain name. The CNAME record has not been added to your domain's DNS records. Contact your DNS service provider to configure the CNAME record as instructed in **Configuring a CNAME Record**.
- If the CNAME record has been correctly configured, check the time to live (TTL) of the previous resolution record of the domain name on the same resolution line. The TTL specifies the cache duration of a resolution record on the local DNS server. The newly added CDN CNAME record takes effect only after the TTL of the previous record expires.

2. Check whether the CDN cache is hit.

   On the Google Chrome browser, press **F12** and click the **Network** tab. View the response headers of the URL of a specific resource and perform the following operations:

   - Check the value of the **x-hcs-proxy-type** header. The value **1** indicates that the cache is hit, and the value **0** indicates that the cache is not hit.
   - If the **x-hcs-proxy-type** header does not exist, check the value of the **X-Cache-Lookup** header. Value **Hit From MemCache**, **Hit From Disktank**, or **Hit From Upstream** indicates that the cache is hit, whereas other values indicate that the cache is not hit.
   - If neither the **x-hcs-proxy-type** nor **X-Cache-Lookup** header exists, check the value of the **age** header. Values greater than 0 indicate that the cache is hit, and the value **0** indicates that the cache is not hit.

   If no cache is hit, go to **4** to check the cache rule settings.

   If the cache is hit, proceed to the next step.

3. Check whether inter-carrier or cross-province access is involved.

   Perform the following steps:

   a. Check the client IP address and local DNS to see whether a proxy is used. If a proxy is used, inter-carrier and cross-province access may occur, affecting the access speed.

      Example 1: A user in the Hebei province uses the Broadcasting Network to access the acceleration domain name. The client IP address is assigned by Beijing Unicom but the local DNS is assigned by Shijiazhuang Telecom. The access speed is greatly affected by inter-carrier access.

      Example 2: A user in Beijing uses the Broadcasting Network to access the acceleration domain name. The client IP address is assigned by Beijing Unicom but the local DNS is assigned by Guangdong Telecom, so the CDN scheduling system assigns the nearest point of presence (PoP) in Guangdong to return resources based on the local DNS. As a result, the access is slow.

   b. Currently, Huawei Cloud CDN supports China Telecom, China Unicom, China Mobile, China Tietong, CERNET, and Dr. Peng.

4. Check cache rules.

   - Check whether the configured TTL is 0 or a small value. If CDN does not cache content or the TTL is too short, CDN has to frequently pull content from the origin server, and the origin pull cannot be accelerated.
   - Check the cache settings on the origin server. If **no-cache**, **private**, or **no-store** is configured on the origin server and **Origin Cache Control** is

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

enabled on the CDN console (this function is disabled by default), CDN cannot cache content. CDN needs to pull content from the origin server, and the origin pull cannot be accelerated.

- Check the priority of cache rules. The greater the value, the higher the priority.
- Check whether URL parameter filtering is enabled. If URL parameter filtering is disabled, when users request a file using URLs containing different parameters, CDN considers that each request is new, and pulls the file from the origin server for each request. For details, see **Cache Rules**.
- For more cache settings, see **Setting the Maximum Cache Age**.

5. Check whether the content is prefetched.

   If the content has not been prefetched and is requested for the first time, CDN PoPs will pull it from the origin server. In this case, slow access to the content is normal.

   NOTE

   When enabling CDN for the first time, you can prefetch large files or videos.

6. Check the client network.

   Ping the domain name to which access is still slow after CDN acceleration to check the network delay and packet loss. If the network delay is long or severe packet loss occurs, check the network connection of the client.

If the fault persists even after taking the previous steps, contact customer service or **submit a service ticket**.

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3 Why Is the Displayed or Downloaded Content Incorrect After CDN Acceleration Is Used?

Symptom

After CDN acceleration is enabled, when a user accesses a website or app, the displayed or downloaded content is incorrect.

Check Items

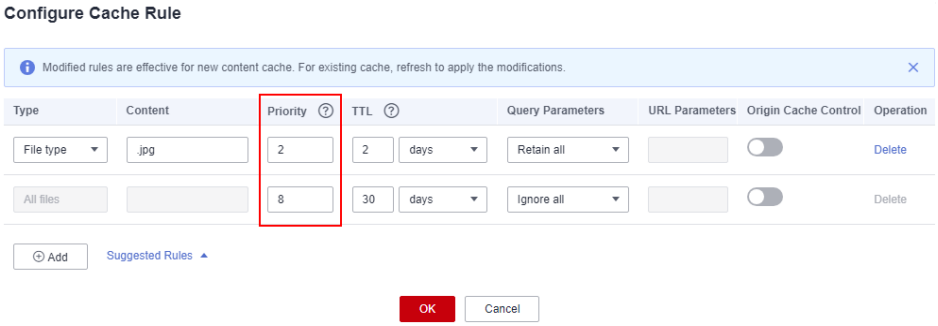
- Cache rules
- Local cache
- Whether CDN points of presence (PoPs) still store stale versions of your content
- Whether the origin server stores different versions of files
- Whether content access is hijacked

Procedure

1. Check cache rules.
   a. Cache rules may be incorrect.
      - For dynamic files (such as PHP, JSP, and ASP files), set the cache time to live (TTL) to 0, so these files are not cached and are pulled from the origin server for each request.
      - For static files (such as JPG and ZIP files) that are not frequently updated, set the cache TTL to more than one month.
      - For static files (such as JS and CSS files) that are frequently updated, set the cache TTL based on service requirements.
   b. The cache rule priority may be incorrect. As a result, the cache rules do not take effect. The priority value ranges from 1 to 100. The larger the value, the higher the priority.

      Assume that you have set a rule with the cache TTL as two days for JPG files.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



As shown in the preceding figure, the first rule indicates that the cache TTL of all files is 30 days, and its priority is 8. The second rule indicates the cache TTL of JPG files is 2 days, and its priority is 2. When a user requests a JPG file, the first rule is matched because its priority is higher. Therefore, the JPG file will be cached on CDN PoPs for 30 days instead of 2 days.

c. For more cache settings, see **Setting the Maximum Cache Age**.

2. Check whether the fault is caused by the local cache.

   Clear the browser cache and request content again to check whether the fault has been solved.

3. Check whether CDN PoPs still store stale versions of your content.

   If the content on the origin server is updated, but the cache on CDN PoPs is not refreshed and is still valid, the cache will be returned to users. You can manually refresh the cache in either of the following ways:

   a. Log in to the **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**. In the navigation pane, choose **Prefetch & Purge**. On the **Purge** tab, refresh the cache.

   b. Call the cache purge or prefetch API to refresh the cache. For details, see **API Reference**.

4. Check whether the origin server stores different versions of files.

   - Your origin server uses load balancing. There are multiple servers at the backend, and they store different versions of files.
   - A standby origin server is added on the CDN console, but files stored on the primary server and the standby server are different.

   If the fault is caused by either of the preceding reasons, store the same version of files on your origin servers.

5. Check whether content access is hijacked.

   If content access is hijacked, configure HTTPS to enhance security. Common hijacks are as follows:

   - When you visit a website, 302 is returned, but the address specified by **location** in the response is not the desired one. Enter the URL to be accessed in the address bar of Google Chrome, press **F12**, click the **Network** tab, and click a resource. On the displayed **Headers** tab, find **location** under **Response Headers** to check its value.
   - When you visit a website, the content displayed is not the desired content.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

If the fault persists even after taking the previous steps, contact customer service or **submit a service ticket**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4 Common Faults on WAF Resources Accelerated by CDN

Error: Website is under maintenance (Protected by WAF)

If the error message **Website is under maintenance (Protected by WAF)** is displayed when you use Web Application Firewall (WAF) as the origin server, check whether the service bandwidth limit of WAF is exceeded. For details about the impact of this error, see **What Happens If Website Traffic Exceeds the Service Bandwidth Limit?**

NOTE

After the fault is rectified, refresh the corresponding resource to prevent the existing cache from affecting your services.

Error: 418

Check whether an IP address blacklist is configured for WAF. If a CDN origin IP address is added to the blacklist, origin pull requests from this IP address will be blocked and error 418 will be reported.

Examples of configuration errors and solutions:

1. Private IP addresses starting with 10 or 100 are added to the blacklist. As a result, requests from education network customers may be blocked. Remove the IP addresses from the blacklist on WAF.
2. A CDN origin IP address is added to the blacklist. As a result, CDN origin pull error code 418 is displayed. Check the WAF block logs and rules.
3. Requests from specific geographical locations are blocked on the customer side. For example, if a customer blocks requests from users outside the Chinese mainland, some CDN IP addresses may be blocked.

An HTTPS certificate is configured only on CDN or WAF.

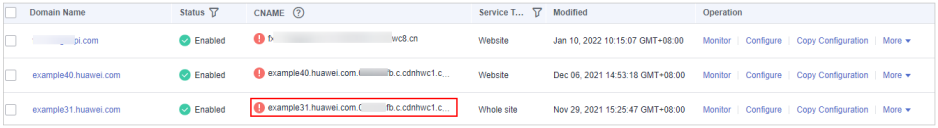
Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5 Why Is a 4XX Status Code Returned When I Request Resources from My Acceleration Domain Name?

Status Code 403

If the status code 403 is returned, locate the fault as follows:

1. Check whether your origin server can be accessed. For details, see **How Do I Check Whether an Access Fault Is Caused by the CDN PoP or Origin Server?**.
2. Check whether the CNAME record matches your acceleration domain name. For details about how to configure the CNAME record, see **Configuring a CNAME Record**.



3. If you have configured referer validation, check whether your request URL is allowed by the referer validation rule. CDN identifies and filters out visitors based on a referer blacklist or whitelist. Unqualified users will receive a 403 error response. For details about the rules, see **Configuring Referer Validation**.
4. If your origin server is an OBS bucket, check whether you have configured a referer whitelist on the origin server and specified that blank referer is not allowed, but no referer validation settings are configured in CDN. If the original request does not carry referer information, CDN will not carry any referer information during origin pull. In this case, origin pull fails and the origin server returns status code 403. To fix this fault, modify the referer validation rule in OBS. For details, see **Configuring Referer Validation**.
5. If your origin server is an OBS private bucket and OBS authorization is not enabled on CDN, 403 will be returned. Enable OBS authorization on CDN. For details, see **OBS Authorization**.
6. If you have configured an IP address whitelist or blacklist, check if your IP address is in the blacklist or is not in the whitelist. If it is in the blacklist or is

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

not in the whitelist, your request will be rejected and a 403 status code will be returned. For details, see **IP ACL**.

7. If you have configured a User-Agent blacklist or whitelist, check if your request URL is in the blacklist or is not in the whitelist. If it is in the blacklist or is not in the whitelist, your request will be rejected and a 403 status code will be returned. For details, see **User-Agent ACL**.
8. If you have configured token authentication, check the validity period of the signed URL. If the URL has expired, your access to it will be rejected and a 403 status code will be returned. For details, see **Token Authentication**.

Status Code 404

If the status code 404 is returned, locate the fault as follows:

1. Access the URL of the origin server and check whether 404 is returned. For details, see **How Do I Check Whether an Access Fault Is Caused by the CDN PoP or Origin Server?**.
2. If the origin server can be accessed, log in to the CDN console and check whether the host header is correct on the **Basic Settings** tab of the domain name. For details, see **Host Header**.

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

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

     Let's assume that the origin server IP address is **x.x.x.x**, the acceleration domain name is **www.example.com**, and sites www.a.com and www.b.com are deployed on the origin server.

     - If you want CDN to pull content from the origin server, set the origin server to **x.x.x.x** on CDN.
     - By default, the host is the acceleration domain name **www.example.com**. If you want CDN to pull content from the **www.a.com** or **www.b.com** site, set the host host to **www.a.com** or **www.b.com**.

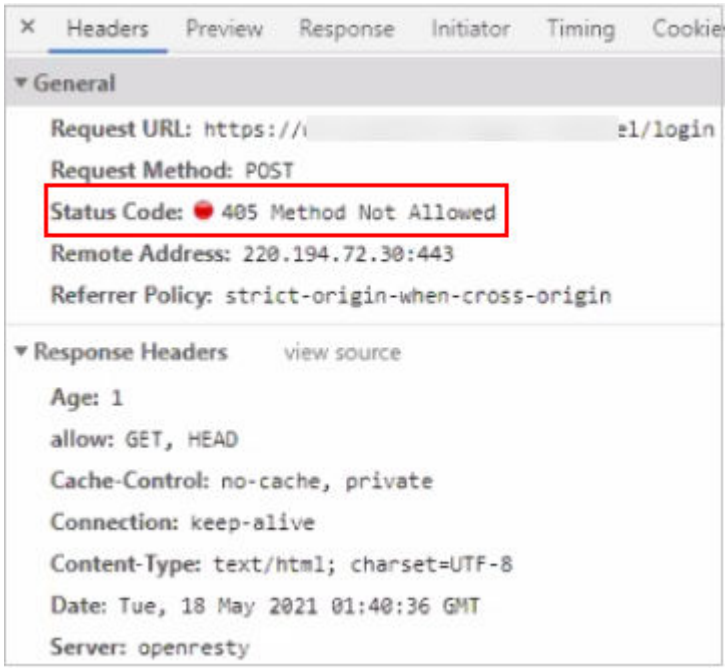
   NOTE

   - If the origin server is an OBS bucket, the host must be the domain name of the OBS bucket.
   - If your origin server is an object storage bucket of a third party, change the host to the bucket domain name.
3. Check whether the origin server configuration is correct on the **Basic Settings** tab of the domain name on the CDN console. If not, change the IP address or domain name of the origin server to the correct one.

Status Code 405

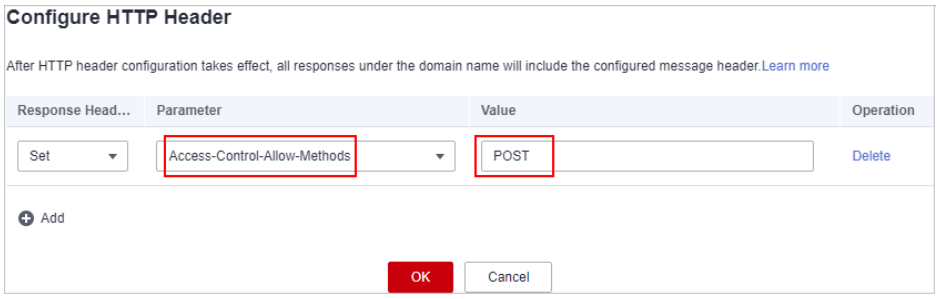
Symptom: Content of a domain name with CDN acceleration enabled cannot be accessed, and status code 405 is returned on the **Headers** tab under **Network** of the DevTools.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



Cause: The response header does not support the POST method.

Solution: Edit the HTTP header configuration. Add the header **Access-Control-Allow-Methods** and set its value to **POST**. For details, see **HTTP Header Settings (Cross-origin Requests)**.



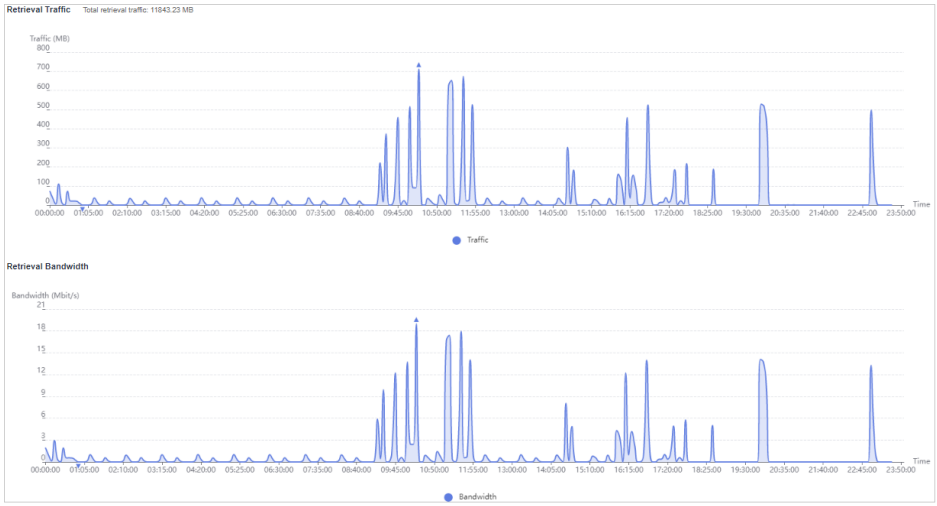
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

6 Why Is a 5XX Status Code Returned When I Request Resources from My Acceleration Domain Name?

1. Visit the origin server to check whether a 5XX error occurs. For details, see **How Do I Check Whether an Access Fault Is Caused by the CDN PoP or Origin Server?**.

   If the error occurs, check the origin server configuration. Data on the CDN console can help you troubleshoot certain origin server faults.

   - Log in to the CDN console. In the navigation pane, choose **Analytics** > **Origin**.

   - Check whether the bandwidth and traffic increase sharply. If the bandwidth and traffic increase sharply, the origin server will be overloaded and the response from the origin server will time out. Check whether resources are updated recently or new cache rules are configured for popular resources. When releasing new resources or functions, prefetch large files to CDN points of presence (PoPs) to prevent bandwidth bottlenecks caused by a large number of origin pull requests.
   - Check whether cache rules are configured on the origin server. If **no-cache**, **private**, or **no-store** is configured on the origin server and **Origin Cache Control** is enabled on the CDN console (this function is disabled

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

by default), CDN cannot cache content and needs to pull content from the origin server. When a large number of origin pull requests are sent to the origin server, the response from the origin server may time out. For details about how to set cache rules, see **Setting the Maximum Cache Age**.

- Check whether the network of the origin server fluctuates. If the carrier network of the origin server is faulty, origin pull times out.

If the origin server is normal, proceed to the next step.

2. If the status code 504 is returned, locate the fault as follows.



Cause: The origin server may not support the protocol used by CDN to pull content.

a. The origin protocol used by CDN is same as the client access protocol.

   - If a client uses HTTPS to access CDN, CDN will use HTTPS to pull content from the origin server. If the origin server does not support HTTPS, it will return a 504 response.
   - If a client uses HTTP to access CDN, CDN will use HTTP to obtain content from the origin server. If the origin server does not support HTTP, it will return a 504 response.
   - If a client uses HTTP to access CDN and you have configured force redirect to HTTPS on CDN, CDN will pull content from the origin server using HTTPS. If the origin server does not support HTTPS, it will return a 504 response.

b. The default origin protocol used by CDN is HTTP, but the origin server supports only HTTPS.

c. The origin protocol used by CDN is HTTPS, but the origin server supports only HTTP.

Solution: Modify the CDN configuration to match the access protocol supported by the origin server. The default origin protocol used by CDN is HTTP. Change it to a protocol supported by the origin server. For details, see **Origin Protocol**.

3. If the status code 502 is returned, locate the fault as follows:

   - Check whether security policies, such as Safedog and firewall, are configured on the origin server to block CDN origin IP addresses.
     - During origin pull, CDN intelligently schedules PoPs to access your origin server, and the IP addresses of the PoPs are not fixed. Configuring fixed PoP IP addresses in origin pull policies may cause origin pull failures.
     - If protection software such as Safedog is required, adjust security policies to avoid incorrect interception.

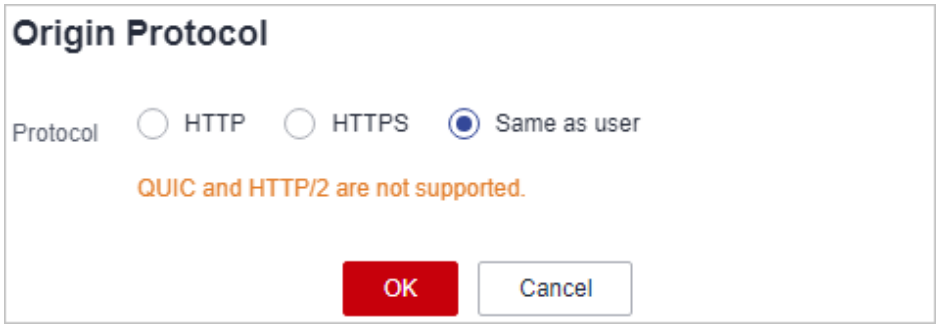
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4. If the fault persists, contact customer service or **submit a service ticket**.

7 Why Does a 301/302 Redirect Loop Occur When I Request Resources from My Acceleration Domain Name?

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

Solution: Set **Origin Protocol** to **Same as user** under the **HTTPS Settings** tab of your domain name on the CDN console.



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

8 Status Code and Handling Suggestions

Status Code	Description	Solution
200	The request is successful.	-
301	The requested resource has been assigned a new permanent URI, and the new URI is contained in the response.	-
302	The requested resource resides temporarily under a different URI.	-
304	The requested resource has not been modified. In such a case, there is no need to retransmit the resource since the client still has a previously-downloaded copy.	-
400	The server failed to process the request.	Check whether the request syntax or parameters are correct.
401	A username and password are required for access to the requested page.	Log in to the page first.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description	Solution
403	Access to the requested page is denied.	Check whether access controls such as the referer blacklist or whitelist, IP address blacklist or whitelist, and authentication are configured. For details, see **Why Is a 4XX Status Code Returned When I Request Resources from My Acceleration Domain Name?**.
404	The server failed to find the requested page.	• Check whether the origin server is normal, or whether the origin server information and host are correctly configured. • Check whether the requested resource exists on the origin server. For details, see **Why Is a 4XX Status Code Returned When I Request Resources from My Acceleration Domain Name?**.
405	The request method is not allowed.	Log in to the CDN console, click the acceleration domain name, click the **Advanced Settings** tab, add the HTTP header **Access-Control-Allow-Methods**, and set the header value to the required request method. For details, see **Why Is a 4XX Status Code Returned When I Request Resources from My Acceleration Domain Name?**.
406	The response from the server could not be received by the client.	Check whether the value of **Accept** in the header of the response from the origin server is allowed by the client.
407	Proxy authentication is required before the request is processed.	Check whether special authentication is configured.
408	The request timed out.	Check the request sending logic of the client.
409	The request could not be processed due to a conflict.	A conflict usually occurs during the processing of a PUT request. Check the uploaded file.
416	The requested range is invalid.	Check whether the range requested by the client exceeds the resource size.
499	The client closed the request.	Check the client status or timeout interval.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description	Solution
500	The request failed to be fulfilled because of a service error.	Check whether the origin server is normal. For details, see **How Do I Check Whether an Access Fault Is Caused by the CDN PoP or Origin Server?**.
501	The request failed to be fulfilled because the server does not support the required function.	Check whether the request method of the client is correct.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.	Check whether the origin server is normal. For details, see **Why Is a 5XX Status Code Returned When I Request Resources from My Acceleration Domain Name?**.
503	The request failed to be fulfilled because the system is temporarily abnormal.	Check whether the origin server is normal.
504	A gateway timed out.	Check whether the origin server is normal or overloaded. For details, see **Why Is a 5XX Status Code Returned When I Request Resources from My Acceleration Domain Name?**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

9 Why Am I Getting a Permission Error Message?

Perform the following steps:

1. If you are using CDN as an IAM user with insufficient permissions, view each permission on **Permissions Management** and ask the account administrator to assign the required permissions to you by referring to **Creating a User and Granting CDN Permissions**.

   The following table lists the common CDN permissions.

Policy	Description	Type
CDN Administrator	All operations on CDN. Scope: Global-level service	System role
CDN DomainReadOnlyAccess	Read-only permissions on CDN acceleration domain names. Scope: Global-level service	System-defined policy
CDN StatisticsReadOnlyAccess	Read-only permissions on CDN statistics. Scope: Global-level service **NOTE** This policy does not include the permissions for querying operations reports.	System-defined policy
CDN LogsReadOnlyAccess	Read-only permissions on CDN logs. Scope: Global-level service	System-defined policy

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Policy	Description	Type
CDN DomainConfiguration	Permissions for configuring CDN acceleration domain names. Scope: Global-level service	System-defined policy
CDN RefreshAndPreheatAccess	Permissions for configuring CDN cache refreshing and preheating. Scope: Global-level service	System-defined policy
CDN FullAccess	All operations on CDN. Scope: Global-level service	System-defined policy
CDN ReadOnlyAccess	All read-only operations on CDN. Scope: Global-level service	System-defined policy

NOTE

When you want to acquire the CDN DomainConfiguration or CDN RefreshAndPreheatAccess permission, ensure that you also acquire the CDN DomainReadOnlyAccess permission. Otherwise, you cannot view the domain names, and thus cannot configure, or purge and prefetch cache for domain names.

2. Check whether your account is in arrears.
   - If your account is in arrears and is in the **retention period**, the system will ban your domain names and stop the acceleration service.
   - If your account is in arrears and the retention period expires, your domain names along with the associated resources will be deleted.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

10 Why Can't I Log In to My Domain Name or Why Is the Information of Other Users Displayed?

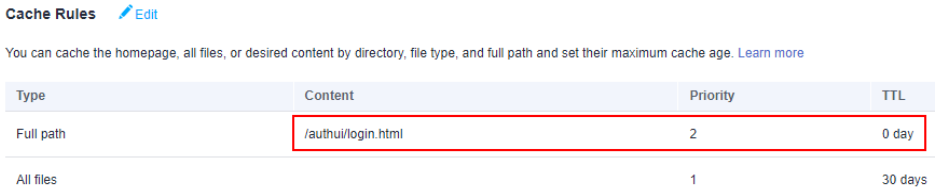
The login page is dynamic. To fix the fault, set the cache time to live (TTL) of the login page to 0 so that it will not be cached.

Perform the following steps:

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

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**, and click the domain name to be configured.
3. Click the **Cache Settings** tab, click **Edit** next to **Cache Rules**, and set the cache TTL of your login page to **0**.

The following figure uses the Huawei Cloud login page **https://auth.huaweicloud.com/authui/login.html#/login** as an example:



NOTE

If you have modified a cache rule, the new rule does not apply to content that has been cached but only applies to new content. If you want the modification to take effect immediately, refresh the cache after modifying the cache rule.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

11 How Do I Check Whether an Access Fault Is Caused by the CDN PoP or Origin Server?

1. Check whether you can visit other websites, for example, https://www.huaweicloud.com/ to make sure the fault is not caused by the client network.
2. Check whether the origin server is normal.

   The origin server can be a domain name, OBS bucket domain name, and IP address. Select a proper test method based on your settings.

   NOTE

   - If the origin server, for example, the domain name of an OBS bucket or the CNAME domain name of WAF, cannot be directly accessed, use the method **b**.

   a. Origin server domain name: Assume that the acceleration domain name is www.a.com, the origin server domain name is www.source.com, and the URL that cannot be accessed is http://www.a.com/a.html.

      i. Replace the acceleration domain name in the URL with the origin server domain name, that is, change http://www.a.com/a.html to http://www.source.com/a.html.

      ii. Open the new URL in the browser. Clear the browser cache before each test.

      iii. If the access fails, the origin server is abnormal. Check your origin server.

      iv. If the access succeeds, the origin server is normal.

   b. Origin server IP address: Assume that the acceleration domain name is www.example.com, the origin server IP address is 49.4.3.125, and the OS is Windows.

      i. In the **C:\Windows\System32\drivers\etc\hosts** file, bind the acceleration domain name www.example.com with the IP address 49.4.3.125.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

      49.4.3.125      www.example.com
```

ii. Open the URL that cannot be accessed in the browser. Clear the browser cache before each test.

iii. If the access fails, the origin server is abnormal. Check your origin server.

iv. If the access succeeds, the origin server is normal.

3. Check whether the CDN point of presence (PoP) is faulty.
   - Open the URL that cannot be accessed in Google Chrome, press **F12**, choose **Network** > **Headers**, and obtain the PoP IP address next to **Remote Address**.
   - In the **C:\Windows\System32\drivers\etc\hosts** file, bind the acceleration domain name with the PoP IP address.
     - Ping the acceleration domain name. If the ping fails, the CDN PoP is abnormal. Contact Huawei technical support.
     - If the ping succeeds, the CDN PoP is normal.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

12 Why Is the Cache of a Resource Inconsistent on Different PoPs?

Symptom

When users in different regions access a resource of your domain name with CDN acceleration enabled, CDN points of presence (PoPs) return different resource versions to them.

Possible Causes

- You have enabled URL parameter filtering on the CDN console and configured the origin server to return resources based on URL parameters.

  Resources cached on CDN PoPs may be different when the URL parameters carried in the first request to the PoPs are different. When requests for the same resource are sent to different PoPs, the returned data is different.

- The cache is not refreshed after the resource on the origin server is updated.

  If the resource is updated on the origin server but the access URL of the resource does not change, when a user accesses the resource, the PoP returns the cache. The PoP will pull the updated resource from the origin server and cache it only when the original cache expires. In addition, the cache eviction time varies by the access popularity in different regions. If the cache on some PoPs has been evicted, when a user accesses the resource, the PoP will pull the resource of the latest version from the origin server. If the cache on some PoPs is still available, the cache is directly returned to the user. As a result, the old and new versions may coexist in the cache of PoPs.

Solutions

1. Do not use URL parameter filtering of CDN and the function of returning different resource versions based on URL parameters of the origin server at the same time.

   Check whether the origin server is configured to return different resource versions based on URL parameters. If yes, perform the following operations:

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

      The CDN console is displayed.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

c. Click the target domain name, click the **Cache Settings** tab, and check whether URL parameter filtering is enabled.

d. If URL parameter filtering is enabled for the resource, disable it.

2. If the resource is updated on the origin server, refresh the cache on CDN.

   Perform the following steps:

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

      The CDN console is displayed.

   b. Choose **Prefetch & Purge** in the navigation pane, click the **Purge** tab, and enter the URL or directory of the resource.

      NOTE

      You can also use the cache purge or prefetch API provided by CDN to refresh the CDN cache. For details, see **API Reference**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

13 Why Does the Configured Cache Rule Not Take Effect?

Symptom

A cache rule has been configured for JPG files with a time to live (TTL) of 90 days. After **image 1.jpg** is prefetched, a client accesses **image 1.jpg** and finds that the cache is not hit.

Possible Causes and Countermeasures

1. It takes about 5 minutes for the cache rule to take effect. Prefetch the resource after the rule takes effect and check whether the cache is hit.
2. The cache TTL is too short, causing frequent origin pull. Set a proper cache TTL. For details ,see **Setting the Maximum Cache Age**.

   Figure 13-1 Short cache TTL

Type	Content	Priority	Maximum Age
File type	.jpg	2	1 second
All files		1	30 days

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**.

   Figure 13-2 Cache rule settings

Type	Content	Priority	Maximum Age
Full path	/test/*.jpg	3	3 seconds
File type	.jpg	2	1 day
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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

the **Full path** rule is **3**, 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 3 seconds.

Method: To make the **File type** rule to take effect, set its priority to a value greater than **3**.

4. If **Origin Cache Control** is enabled for the cache rule of JPG files and **no-cache**, **private**, or **no-store** is set on the origin server, CDN does not cache resources from the origin server. It pulls content from the origin server for each user request. In this case, disable **Origin Cache Control**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

14 What Do I Do If the Browser Displays a Message Indicating that a Cross-domain Exception Occurs After CDN Is Enabled?

Symptom

The page is abnormal when a client accesses resources. The following figure shows the error information.



Possible Causes and Countermeasures

Some resources in the cross-domain request do not respond to the header **Access-Control-Allow-Origin**. In this case, configure the response header information on CDN. For details, see **HTTP Header Settings (Cross-origin Requests)**.

NOTE

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.