

Content Delivery Network Troubleshooting Methods Product Documentation



Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Troubleshooting Methods

- Status Codes and Solutions

- Node Cache Inconsistency

- Slow Access Speed After CDN Activation

- Page Display - CORS error

Troubleshooting Methods

Status Codes and Solutions

Last updated : 2021-09-23 14:58:19

The table below explains the status codes of CDN.

Status Code	Meaning	Suggestion
400	HTTP request syntax error and the server cannot parse the request	Check whether the request syntax is correct.
403	Request is rejected	Check whether the request is blocked by access controls such as referer blacklist/allowlist, IP blacklist/allowlist, and authentication.
404	Server cannot return correct information	Check whether the original server is running normally, and whether the original server information or origin domain configurations are changed.
413	Content length of the POST request exceeds the limit	Check the content size of the POST request from the client (the maximum size is 32 MB by default).
414	URL length exceeds the limit	The maximum URL size is 2 KB by default.
423	Looping request	Check the 301/302 configuration, HTTPS origin-pull, and rewriting method of the origin server.

Status Code	Meaning	Suggestion
499	The client closes the connection	Check the client status and timeout configuration.
502	Gateway Error	Check whether the business origin server is normal.
503	COS frequency control is triggered	Check the cache configuration or whether the COS origin server returns no-cache/no-store.
509	Blocked due to CC attack	Please submit a ticket
514	IP access frequency exceeds the limit	Check the IP access frequency control configuration in the CDN Console.
531	Error resolving the origin-pull domain name in the HTTP request	Check the domain name resolution configuration of the origin server.
532	Failed to establish a connection with the origin server in the HTTPS request	Check the port 443 status of the origin server, certificate configuration, or availability of the origin server.
533	Origin-pull connection timeout in the HTTPS request	Check the port 443 status of the origin server, certificate configuration, or availability of the origin server.

Status Code	Meaning	Suggestion
537	Origin server data reception timeout in the HTTPS request	Check the stability of the business origin server.
538	SSL handshake of HTTPS request failed	Check the compatibility between the origin server protocol and algorithm.
539	Certificate validation of HTTPS request failed	Check whether the certificate of the origin server is correctly configured (validity period and completeness of the certificate chain).
540	Certificate domain name validation of HTTPS request failed	Check whether the certificate of the origin server is correctly configured.
562	Failed to establish a connection in the HTTPS request	Please submit a ticket and provide the X-NWS-LOG-UUID information for troubleshooting.
563	Connection timeout in the HTTPS request	Please submit a ticket and provide the X-NWS-LOG-UUID information for troubleshooting.

Status Code	Meaning	Suggestion
564	HTTP origin request failed	If HTTP is configured as the origin request protocol, check the load and bandwidth utilization or access limit of the origin server. If the protocol is set to Follow Request , check the port 443 status and certificate configuration of the origin server. If no error is found in the origin server, please submit a ticket and provide the X-NWS-LOG-UUID information for troubleshooting.

Node Cache Inconsistency

Last updated : 2021-05-24 17:01:22

Error Description

Users in different regions receive different contents for the same resource URL.

Possible Reasons

- Reason 1: The cache key is configured to **Filter All** for the domain name, and the origin server is set to return different resources according to the parameters.
In this case, different nodes may cache different contents due to the different parameters of their first-received access requests. When the same request accesses a different node, the returned contents will be different.
- Reason 2: The requested resource is not purged after being updated on the origin server.
CDN caches resources based on the URL. If the content on the origin server is updated but the URL is not changed, when a user sends a request to the URL, the content cached on the node previously will be returned. Also, the access frequency varies by region, so the resource cache validity may be different in each region. When a user request accesses a cache node, if the requested resource on the node is expired, the request will be forwarded to the origin server, and the latest content is pulled and returned. Some nodes have the latest content, and some have the legacy content.

Solutions

1. Do not set the origin server to return different resources according to URL parameters if the "Filter All" cache key is used.
2. Purge the URL resource after it is updated on the origin server.

Troubleshooting Procedure

Step 1. Check whether your origin server returns different resources according to URL parameters.

- If it does, please go to [Step 2](#).
- If it does not, please go to [Step 4](#).

Step 2. Log in to the [CDN console](#), select **Domain Management** on the left sidebar, click **Manage** on the right of a domain name to enter its configuration page. Open the **Cache Configuration** tab to find the **Cache Key Configuration** section, and check whether the **Ignore Query String** is configured as **Not Filter**.

- If it is not, please go to [Step 3](#).
- If it is, please go to [Step 4](#).

Step 3. Click **Modify** on the right of the rule, tick **Not Filter**, and click **Save**.

Note :

If this operation is not suitable for your business, you can use the **Reserve Specified Parameter** feature as needed. For more information, please see [Cache Key Configuration](#).

Step 4. Click **Purge and Prefetch** on the left sidebar to purge the resource that is updated on the origin server.

Note :

You can also bind the API for resource purge, so that resources can be purged across the entire network immediately once updated, guaranteeing the content consistency for access. For more information, please see [PurgeUrlsCache](#) and [PurgePathCache](#).

Slow Access Speed After CDN Activation

Last updated : 2021-06-23 11:51:07

Problem Description

My website is still slow after it's connected to Tencent Cloud CDN.

Possible Reasons

- i. You have not configured a CNAME record for the connected domain name at a DNS service provider, so the CDN acceleration service for the domain name is not in effect. Please [check DNS](#).
- ii. The node cache validity is not configured properly. Please [check the node cache validity configuration](#).
- iii. The resource URL is accessed for the first time after CDN activation, and it has not been prefetched before. Please [prefetch the URL](#).
- iv. The website architecture has defects. Please [optimize the website architecture](#).

Solutions

Check DNS

This example shows you how to run `nslookup` to check the DNS record of a CDN acceleration domain name:

```
Run `nslookup` for the acceleration domain name
```

```
C:\Users\ >nslookup .com
Address:
Address:
Aliases:
.com
.com
.com. cdn. dnsv1. com
```

If the result domain name is not suffixed with `dnsv1.com` as shown above, then the CDN acceleration service for your domain name is not in effect. Please check the CNAME record of the domain name at the DNS service provider as instructed in [CNAME Configuration](#).

Check the node cache validity configuration

Log in to the [CDN console](#), select **Domain Management** on the left sidebar, click **Manage** on the right of a domain name to enter its configuration page, and switch to the **Cache Configuration** tab to find the **Node Cache Validity Configuration** section.

The screenshot shows the CDN console interface for a domain named 'dsdasdsad.com'. The left sidebar has 'Domain Management' selected. The main content area is under the 'Cache Configuration' tab. It features two sections: 'Cache Key Rule Configuration' and 'Node Cache Validity Configuration', both highlighted with red boxes. The 'Node Cache Validity Configuration' section includes a table with one rule:

Type	Content	Ignore Query String	Ignore URL Case
All Files	All Files	Not Filter	No

- Check the node cache rules of the resource: whether the validity is "0", too short, or is configured as "No Cache".

Access requests will be forwarded to the origin server if the request resources are not cached on nodes, in which case the acceleration is not effective. Please configure the cache validity as required by your business.

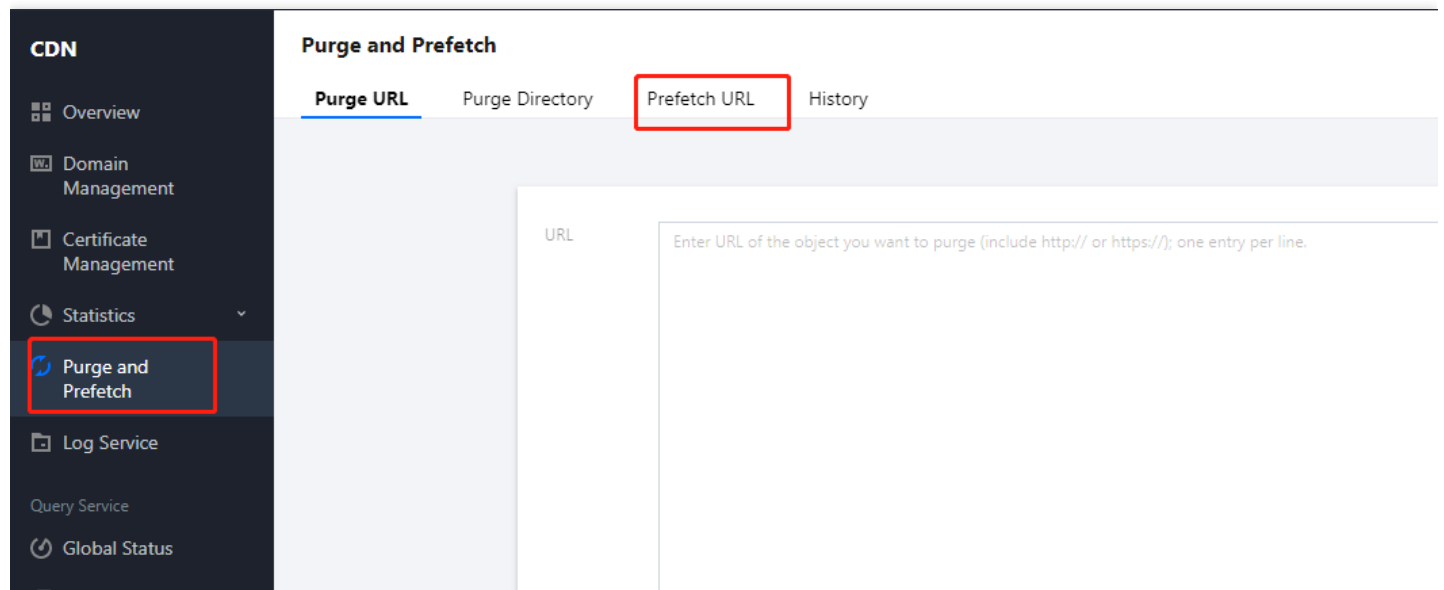
- Check whether the header `Cache-Control` is set as `no-store/no-cache/private` for your origin server.
 - If it is, you need to enable **Force Cache** for the CDN nodes to cache resources as configured.

- If **Force Cache** is not enabled and the header is configured as so, CDN nodes will not cache resources even the cache validity is configured.

For more configuration rules, please see [Node Cache Validity Configuration \(New\)](#).

Prefetch the URL

It is normal that the speed is slow when accessing a resource for the first time which has not been prefetched before. Please log in to the [CDN console](#), click **Purge and Prefetch** on the left sidebar, and then submit the URL for prefetch. For more information, please see [Prefetch Cache](#).



Optimize the website architecture

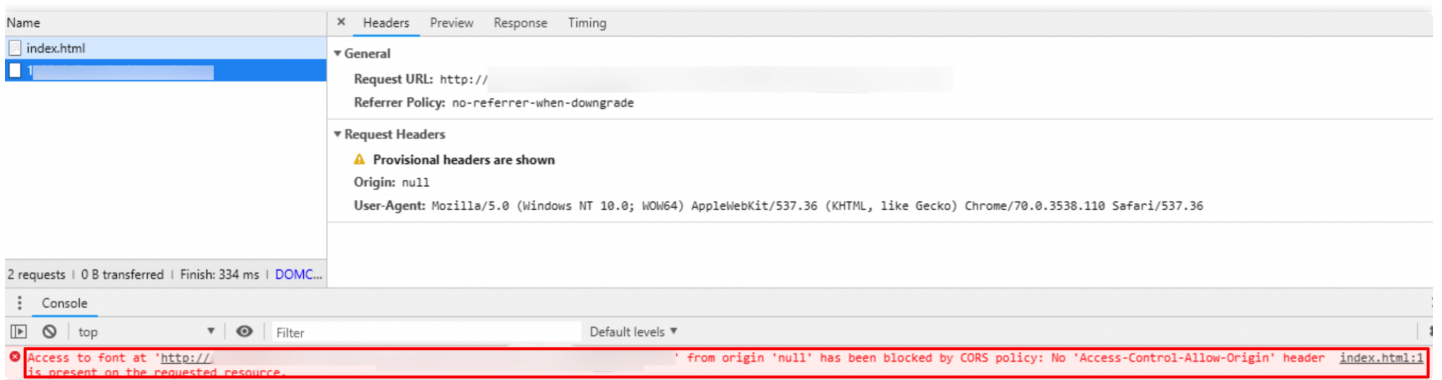
Requests for dynamic resources are always forwarded to the origin server to pull the latest resources, slowing the access speed. If your website has many dynamic resources, we recommend separating them from static resources and using CDN for your static resources only.

Page Display - CORS error

Last updated : 2021-09-23 15:09:58

Error Description

A CORS error is reported, which results in page error or exceptional page display. See the figure below:

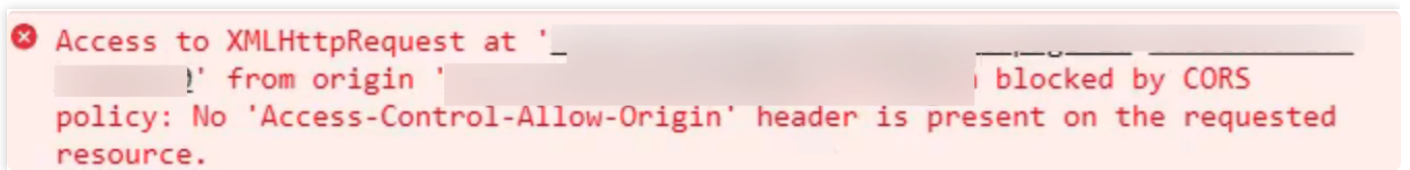


Possible Reasons

CORS error are caused by the same-origin policy of the browser. For the webpage security, when the response for this request will be blocked by the browser, which will result in frontend error or exceptional page display. When the protocol, domain name or port of the request URL is different with that of the URL of requested page, the request is considered a cross-site request.

Solutions

1. Check whether the issue is caused by cross-site request. See the figure below:



2. Configure corresponding HTTP response header in CDN console and define domains allowed to access this resource.

Troubleshooting Procedure

1. Log in to [CDN console](#), go to **Domain Name Management - Advanced Configuration - HTTP Response Header**, complete the setting of **Access-Control-Allow-Origin** parameter as below to allow cross-site requests from all domains. For more information, see [Access-Control-Allow-Origin match mode description](#).
2. You can also configure to allow cross-region requests from a single or multiple specified domain names/IPs.
You can also configure header parameters such as Access-Control-Request-Method, Access-Control-Request-Headers, and Access-Control-Max-Age to specify the allowed request methods and headers and how long the results of a preflight request can be cached. For more information, see [List of Supported Parameters](#).

Note :

If you have configured cross-region access on the COS bucket, please configure cross-region rules in [HTTP Response Header](#) in the CDN console.

List of Supported Parameters

Header Parameter	Description
Access-Control-Allow-Origin	Specifies which origins are allowed to access the resource. For requests from the allowed origins, the host is added to the request header. You can also configure it to <code>*</code> to allow requests from all origins. For more information, see [Access-Control-Allow-Origin match mode description]
Access-Control-Allow-Methods	Indicates the HTTP methods allowed for cross-origin requests. You can configure one or more methods, as shown below: Access-Control-Allow-Methods: <code>POST, GET, OPTIONS</code> .

Header Parameter	Description
Access-Control-Max-Age	Specifies the validity period (in seconds) of a preflight request. For a non-simple cross-origin request, an HTTP query request, namely the preflight request, is needed before the official communication to check whether the cross-origin request is secure to be accepted. A cross-origin request is non-simple if it is: not a GET, HEAD, or POST request, or it is a POST request but its request data type is application/xml, text/xml or any other data type except application/x-www-form-urlencoded, multipart/form-data, and text/plain. For example, if a custom request header is Access-Control-Max-Age: 1728000 , there will not be another preflight request sent for this CORS within 1,728,000 seconds (20 days).
Access-Control-Expose-Headers	This specifies which headers can be exposed to clients as a part of responses. By default, these 6 headers can be exposed to clients: Cache-Control, Content-Language, Content-Type, Expires, Last-Modified, and Pragma. If you want to make other headers accessible to clients, you can separate multiple headers with a comma, e.g., Access-Control-Expose-Headers: Content-Length,X-My-Header. In this way, clients can access the two headers Content-Length and X-My-Header.

Access-Control-Allow-Origin Configuration

Mode	Value/Example	Description
Allow all	*	When it is set to * , the header Access-Control-Allow-Origin:* will be added to the response, which means to allow requests from all origins.
Specified domain	http://cloud.tencent.com https://cloud.tencent.com http://www.b.com	When a request is initiated from https://cloud.tencent.com , which hits the rule, the header Access-Control-Allow-Origin: https://cloud.tencent.com is added to the response. However when there is a request from https://www.qq.com , which does not hit the rule, the response is not changed.
Specified second-level domain name	https://*.tencent.com	When a request is initiated from https://cloud.tencent.com , which hits the rule, the header Access-Control-Allow-Origin: https://cloud.tencent.com is added to the response. However when there is a request from https://cloud.qq.com , which does not hit the rule, the response is not changed.

Mode	Value/Example	Description
Specified port	<code>https://cloud.tencent.com:8080</code>	When a request is initiated from <code>https://cloud.tencent.com:8080</code> , which hits the rule, the header <code>Access-Control-Allow-Origin:https://cloud.tencent.com:8080</code> is added to the response. However when there is a request from <code>https://cloud.tencent.com</code> , which does not hit the rule, the response is not change.

Note :

If there are special ports, you need to enter the relevant information in the list. You must specify the port as arbitrary port match is not supported.