Content Delivery Network

Troubleshooting Methods

Product Documentation

Tencent Cloud

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

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 blocklist/allowlist, IP blocklist/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.
499	The client closes the connection	Check the client status and timeout configuration.
502	Gateway Error	Check whether the business origin server is normal.

Status Code	Meaning	Suggestion
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.
537	Origin server data reception timeout in the HTTPS request	Check the stability of the business origin server.

Status Code	Meaning	Suggestion
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.
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

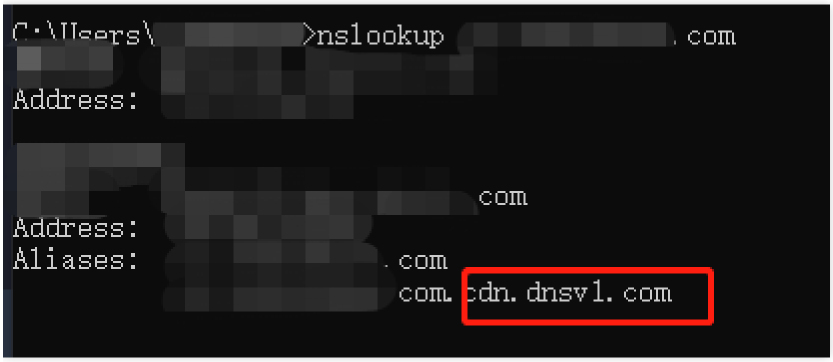
- i. You have not configured a CNAME record for the connected domain name at a DNS service provider, so the CDN acceleration service for the domain name is not in effect. Please check DNS.
- ii. The node cache validity is not configured properly. Please check the node cache validity configuration.
- 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
```



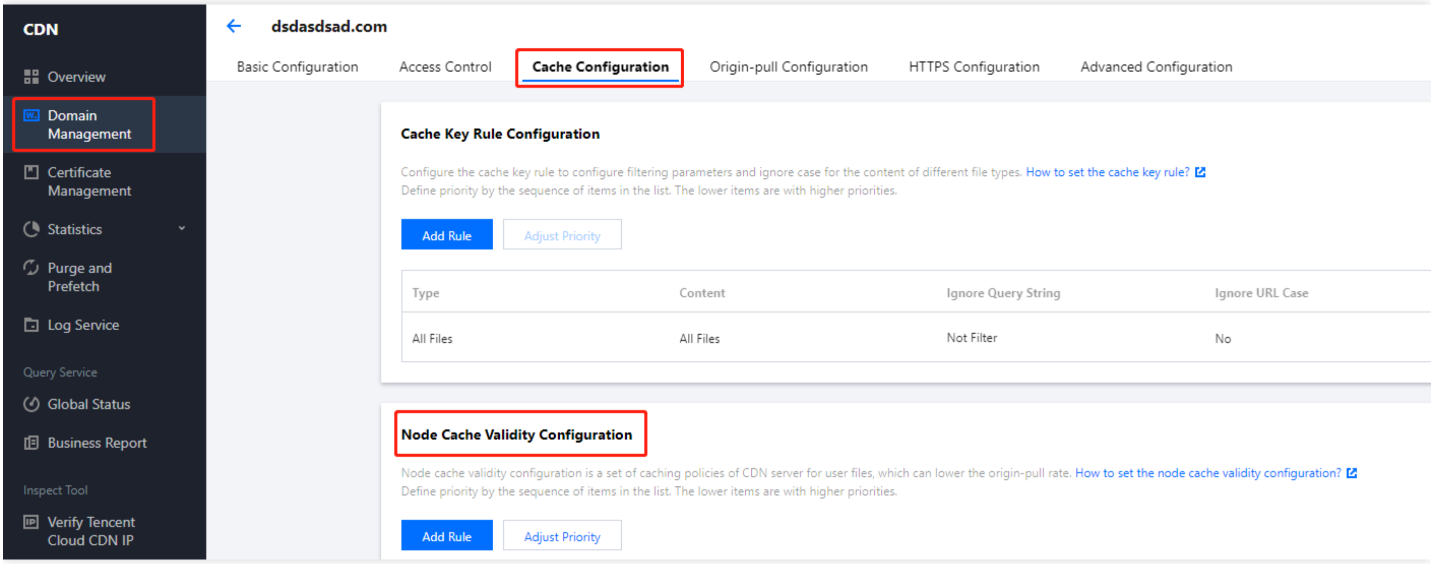
```
C:\Users\[redacted]>nslookup [redacted].com
[redacted]
Address:  [redacted]

[redacted]com
Address:  [redacted]
Aliases:  [redacted].com
          [redacted]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.



Cache Key Rule Configuration

Configure the cache key rule to configure filtering parameters and ignore case for the content of different file types. How to set the cache key rule?
Define priority by the sequence of items in the list. The lower items are with higher priorities.

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

Node Cache Validity Configuration

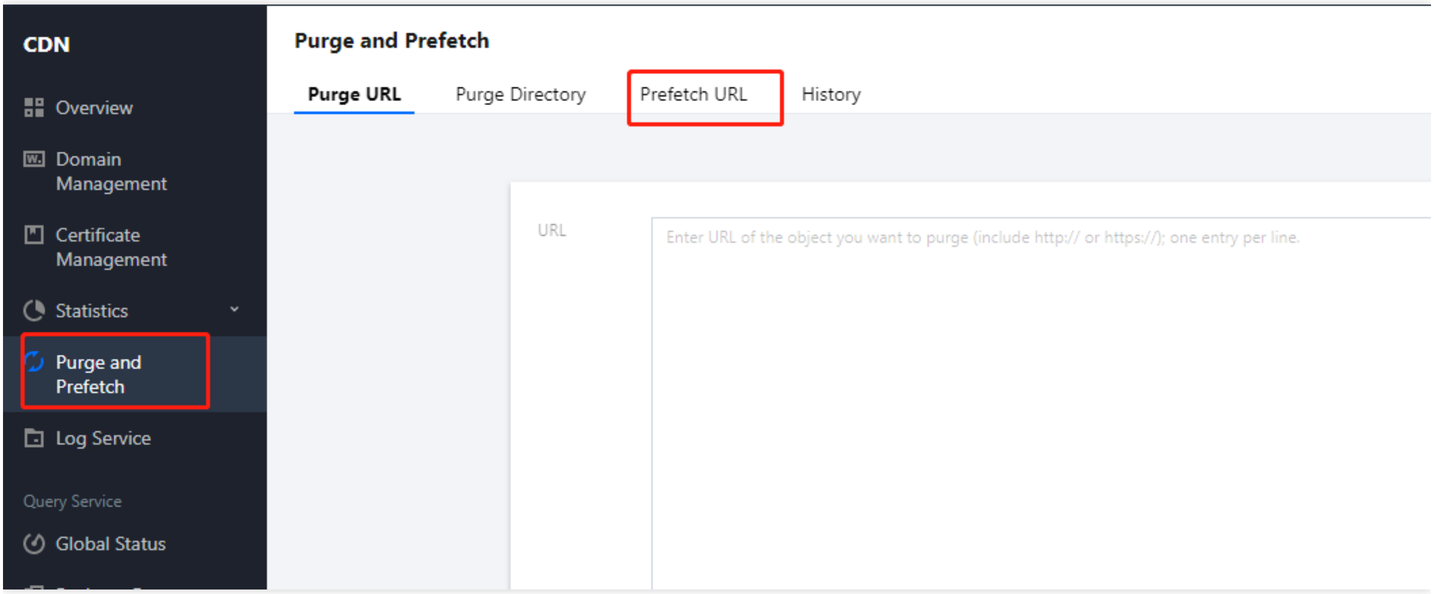
Node cache validity configuration is a set of caching policies of CDN server for user files, which can lower the origin-pull rate. How to set the node cache validity configuration?
Define priority by the sequence of items in the list. The lower items are with higher priorities.

- 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.

Low Traffic Hit Rate

Last updated：2022-02-26 13:42:33

Error Description

The real-time traffic hit rate is well below your expectation.

Possible Reasons

- The cache is purged.
  Cache purge will clear the specified content on the node, leading to a temporarily low traffic hit rate.
- There are new contents on the origin server.
  Large numbers of new contents will cause origin-pulls by CDN nodes, resulting in a low traffic hit rate.
- There are exceptions on the origin server.
  - If it is malfunctioning with multiple 4XX or 5XX errors, the traffic hit rate will be affected.
- The caching policy is not configured properly.
  You should configure it based on your business needs.
- Range GETs is disabled.
  In this case, files will be pulled in their entirety instead of multiple parts as requested during origin-pull, which increases the origin-pull traffic and lowers the hit rate.
- The requests hit the **Ignore all** cache key rule configured for the domain name while the origin server is set to return different contents according to the parameters.
  In this case, all contents will be cached and a specific content requested by the corresponding parameter cannot be matched, thus lowering the traffic hit rate.

Solutions

1. Check to ensure your origin server works properly.
2. It is normal to see a decrease in traffic hit rate when you purge the cache or have new contents on the origin server.
3. Do not set the origin server to return different resources according to URL parameters if the **Ignore all** cache key rule is used.
4. Set the caching rule based on your business needs.

Troubleshooting Procedure

Step 1. Check whether your origin server is exceptional or the cache is purged.

- If it is, the hit rate will be low.
- If it is not, go to Step 2.

Step 2. Check whether your origin server returns different contents according to URL parameters.

- If it does, go to Step 3.
- If it does not, go to Step 5.

Step 3. Log in to the CDN Console, select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. Open the **Cache Configuration** tab to find the **Cache Key Rule Configuration** section. Then check whether the **Ignore parameter** is configured as **Not ignore**.

- If it is not, go to Step 4.
- If it is, go to Step 5.

Step 4. Click **Modify** on the right of the rule, tick **Not ignore**, 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 Rule Configuration.

Step 5. Log in to the CDN Console, select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. Open the **Cache Configuration** tab to find the **Node Cache Validity Configuration** section and check whether the caching rules configured comply with your business needs.

- If it does, perform Step 5.
- If it does not, consult Node Caching Rule Configuration and set the rules as needed.

404 Status Code

Last updated：2021-11-24 14:41:49

Error Description

What should I do if a 404 status code is returned by a CDN domain name?

Cause

1. The origin server is exceptional.
2. The configuration of the origin server information and host header in the console are changed.

Solution

1. Check whether your origin server works properly.
2. Check whether configuration of the origin server information and host header in the console are correct.

Troubleshooting Procedure

1. Check whether your origin server is exceptional.
    - If it is so, fix the origin server.
    - If it is not, go to Step 2.

2. Check the configuration of the origin server information and host header in the console.
   Log in to the CDN console, select **Domain Management**, find the corresponding domain name, select **Basic Configuration** > **Origin Server Information**, and check whether the settings of **Origin address** and **Host header** are correct.
    - Origin type:

Customer origin server	If you select customer origin server, you should provide an IP address or domain name of the business server that can be normally accessed.

Customer origin server	If you select customer origin server, you should provide an IP address or domain name of the business server that can be normally accessed.
COS origin server	If you select a bucket in COS as the origin server, select **Default Domain** or **Static Website** based on your bucket configuration. If your bucket is private, authorize CDN and enable origin-pull authentication to turn on private bucket access.
Third-Party object storage	If you select a third-party object storage service, enter the valid bucket access address as the origin server. Currently, AWS S3 and Alibaba Cloud OSS are supported. If the bucket is private, enter a valid key and enable origin-pull authentication to turn on private bucket access.

- Host header:
  It refers to the domain name accessed on the origin server by a CDN node during origin-pull. It defaults to the acceleration domain name. If a wildcard domain name is connected, it will be the actual access subdomain name by default and can be customized. (**Note:** it cannot be modified if the origin server type is COS or a third-party object storage service).

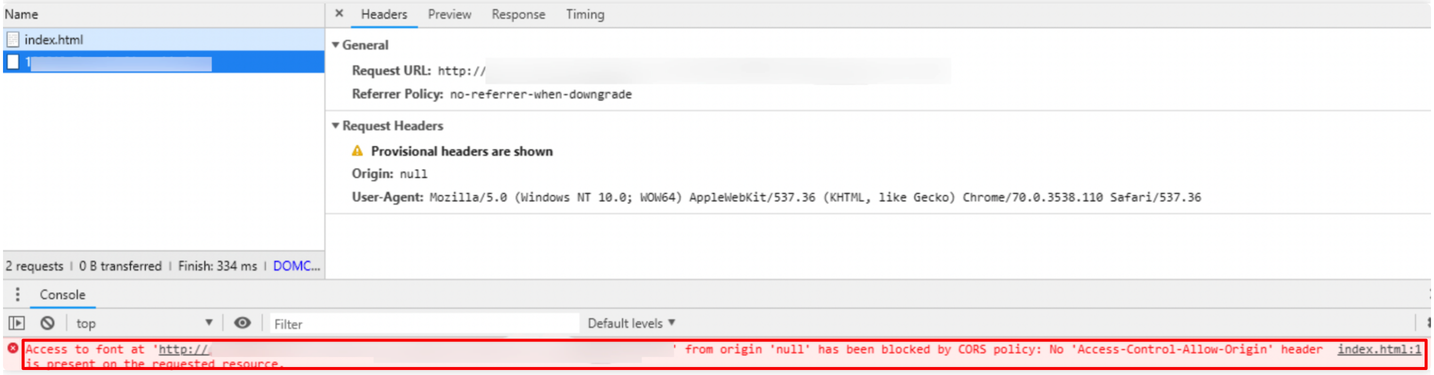
For more information on origin server configuration, see Origin Server Configuration.

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:



▾ General

Request URL: http://[redacted]

Referrer Policy: no-referrer-when-downgrade

▾ Request Headers

⚠ Provisional headers are shown

Origin: null

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36

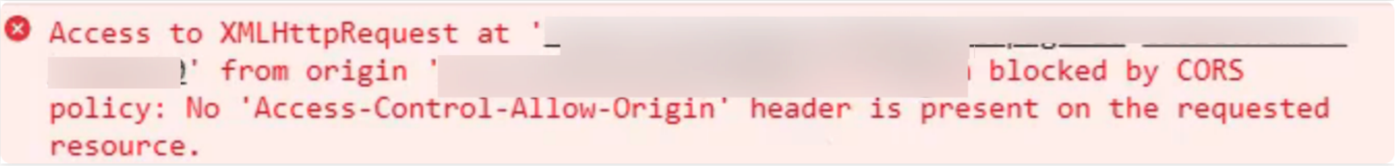
```
Access to font at 'http://[redacted]' from origin 'null' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header    index.html:1
is present on the requested resource.
```

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:



```
Access to XMLHttpRequest at '[redacted]' from origin '[redacted] blocked by CORS
policy: No 'Access-Control-Allow-Origin' header is present on the requested
resource.
```

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 `*` 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: `POST, GET, OPTIONS` .
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).

Header Parameter	Description
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.
Specified port	`https://cloud.tencent.com:8080`	When a request is initiated from `https://cloud.tencent.com:8080` , which hits the rule, the header `Access-Control-Allow-Origin:https://cloud.tencent.com:8080` is added to the response. However when there is a request from `https://cloud.tencent.com` , 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.

Resource Cache Failure

Last updated：2021-11-24 14:41:49

Error Description

After the node cache expiration time is set and prefetch is completed, the request still cannot hit the node cache.

Cause

1. There are multiple cache rules, but their priorities are unclear.
2. "Follow origin server" is configured, but the `Cache-Control` field on the origin server is set to `no-cache/no-store/private`.

Solution

1. Set the cache rule priority correctly.
   You can set multiple CDN cache rules. The lower the rule position, the higher the rule priority. You need to ensure that the rule priority meets your expectation for the rules to take effect as expected.
2. Set the cache validity correctly.
   Check whether the cache validity set in the console is too short.

   > Note：
   > URLs with infrequent file access have the risk of being removed from the node cache even they meet all cache rules.

3. Check whether the cache rules meet your expectation.
   - Check whether the "Ignore Query String" setting in a CDN cache key rule causes a failure to cache the resources on the node.
   - Check whether "No cache" is set in a CDN node cache validity rule.
   - Check whether the header of the request from the origin server returns `no-cache/no-store/private` during origin-pull when the set CDN node cache expiration time is the same as that on the origin server.

Troubleshooting Procedure

1. Check the cache rule priority (the one at the bottom has the highest priority).
   Log in to the CDN console, select **Domain Management** on the left sidebar, locate the desired domain name, click **Manage** in the **Operation** column to enter the **Domain Configuration** page, switch to the **Cache Configuration** tab, and you can find the **Cache Key Rule Configuration**. As shown below, the priority of the rule where .jpg files are excluded for "Ignore Query String" is higher than that of the rule where "Ignore Query String" is configured for all files. You need to ensure that the business cache policies meet the priority settings.

2. Check the cache validity.
   Log in to the CDN console, select **Domain Management** on the left sidebar, locate the desired domain name, and click **Manage** > **Cache Configuration** > **Node Cache Validity Configuration**. As shown below, if the set cache validity is too short, the cache configuration may be mistaken as ineffective. Ensure that the cache configuration meets your business cache policies.

3. Check the cache policies.
   Check whether the policies in the cache key rule configuration and node cache validity configuration meet the expectation.
   If "Follow origin server" is configured, ensure that the `Cache-Control` field on the origin server is not set to `no-cache/no-store/private` .

4. Prefetch the resource to be cached again. After prefetch is completed, request the resource again.