Content Delivery Network

Getting Started

Product Documentation

Contents

Getting Started

Configuring CDN from Scratch

Last updated：2023-06-29 17:57:26

Preparation

1. Register on Tencent Cloud
2. Activate the CDN service

   Tencent Cloud CDN supports two service areas, namely, **Chinese mainland** and **Outside Chinese mainland**. By default, the service is billed in **bill-by-hourly-traffic** mode. For more information on billing rules, see Billing Overview.

   Read and agree to the Terms of Service, click **Activate CDN**.
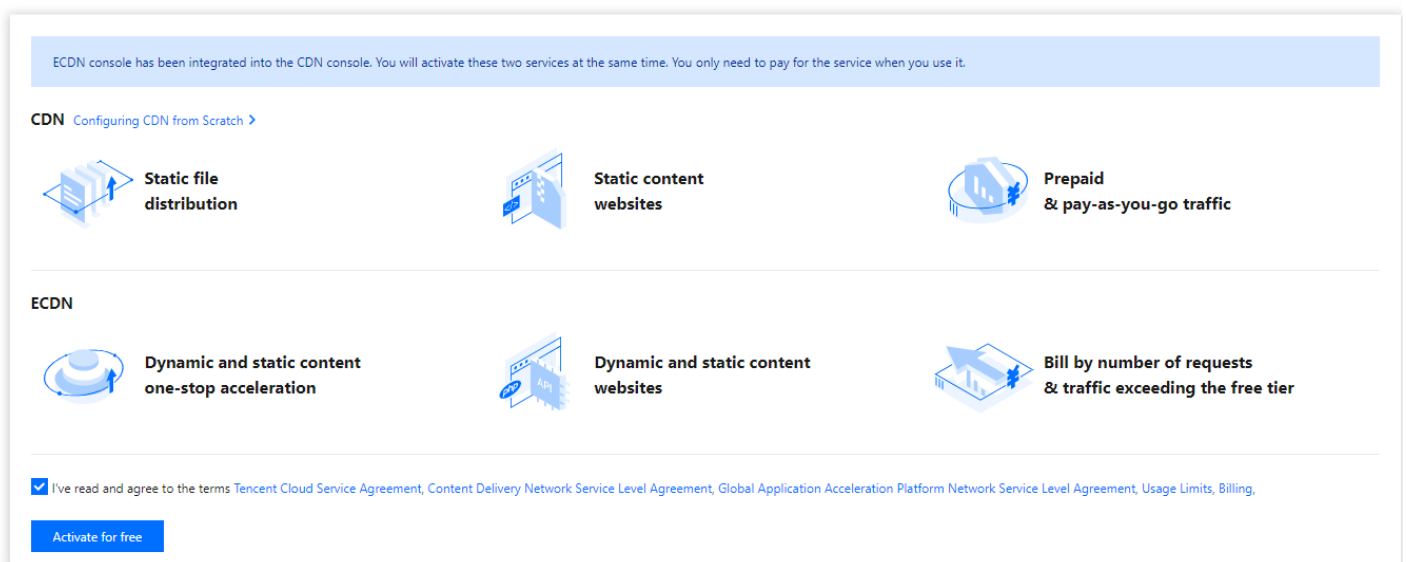
3. Prepare a domain name and an accessible site.

Configuring CDN/ECDN from Scratch

Step 1. Add a domain name

1. Log in to the CDN console.
2. Click **Domain Management** on the left sidebar to enter the domain name management list.

3. Click **Add Domain Name**.

4. Configure the basic information.

Configuration Item	Description

Configuration Item	Description
Accelerator region	You can select an acceleration area as needed. Valid values: **Chinese mainland**: All requests are scheduled to the nearest cache nodes in the Chinese mainland. If you select this option, an **ICP filing** is required for the specified domain name. **Outside Chinese mainland**: All requests are scheduled to the nearest cache nodes in regions outside the Chinese mainland, such as Hong Kong (China), Macao (China), and Taiwan (China). If you select this option, **an ICP filing is not required** for the specified domain name. **Global**: All requests are scheduled to the nearest cache nodes in global regions. If you select this option, an **ICP filing** is required for the specified domain name. **Note:** 1. We recommend that you set the origin server region and acceleration region to the same region. For example, if you select **Chinese mainland** for **Accelerator region**, we recommend that you also select an origin server within the Chinese mainland. If you select an origin server in Hong Kong, the origin-pull may fail or be slow due to cross-border access. However, if you select **Global** for **Accelerator region**, you can add a domain name, and set two origin server configurations, one for the Chinese mainland, and the other for outside the Chinese mainland. 2. The billing rules vary with regions. For more information, see Billing Overview of CDN and Billing Overview of ECDN. 3. A regional traffic package is not applicable to the deduction of cross-region traffic fees. For example, if you purchase a traffic package of 500 GB for North America (Toronto), it offsets only the traffic generated by users who access nodes in the North America (Toronto) region.
Acceleration domain name	**Length:** The domain name can contain up to 81 characters. **Regulatory compliance:** 1. If you select **Chinese mainland** or **Global** for **Accelerator region**, an **ICP filing** is required for the domain name. 2. The synchronization of an ICP filing may take a while. You can add the domain name one or two hours after the registration. 3. The content connected to CDN must comply with applicable national laws and regulations. If you have connected `*.example.com` , `*.a.example.com` , and `b.a.example.com` to CDN, and `b.a.example.com` is banned for illegal content, `*.example.com` and `*.a.example.com` are also banned. **Format:** 1. Supported domain name formats include `example.com` and `a.b.example.com` . CDN acceleration configuration takes effect only on the added domain names. For example, if you connect `example.com` to CDN, access to `example.com` is accelerated, whereas access to `www.example.com` or `m.example.com` is not accelerated. 2. To add a domain name containing a underscore (_) or in Chinese, you need to convert it to punycode. A domain name in Chinese must have obtained an ICP filing.

Configuration Item	Description
	Wildcards: 1. CDN allows you to add a wildcard domain name such as `*.example.com` and `*.a.example.com`. After you connect a wildcard domain name to CDN, you cannot connect its sub-domain names or second-level wildcard domain names to CDN under another account. For example, if you have added `*.example.com`, access to `a.example.com` is accelerated, but access to `example.com` is not accelerated. 2. CDN supports domain name nesting under the same account. For example, you can connect `*.example.com`, `*.path.example.com`, and `a.path.example.com` to CDN under the same account. In this case, the usage of domain name configurations and traffic statistics are based on the matching priority. The more the domain name matches a rule, the higher the priority. For example, the configuration for `a.path.example.com` applies to access to `a.path.example.com`, the configuration for `*.path.example.com` applies to access to `b.path.example.com`, and the configuration for `*.example.com` applies to access to `c.example.com`. Traffic statistics also adopt this rule. 3. Before you add a wildcard domain name, if a matching sub-domain name is already added to another account, you must first delete the sub-domain name from that account. For example, if you want to add `*.example.com` under Account B, but `a.example.com` is already added to Account A, you must first delete `a.example.com` from Account A. **Ownership verification:** You must verify your ownership of a domain name in the following circumstances. For more information about the verification methods, see Domain Name Ownership Verification: 1. When a domain name, for example, `a.example.com` is connected to CDN for the first time. After the domain name is added, its same-level and sub-level alterations, such as `b.example.com`, can be connected without ownership verification. However, ownership verification is still required to add its superior alterations, such as `example.com`. 2. When a sub-domain name of the domain name you want to add is already added to another account. If the verification succeeds, you can add the domain name under the current account. 3. When you add a same-level wildcard domain name. For example, if `a.example.com` is already added, ownership verification is required to add `*.example.com`, but not required to add `*.a.example.com`, which is a sub-level wildcard domain name.

Configuration Item	Description
Acceleration type	You can select a CDN acceleration type to accelerate static resources or an ECDN acceleration type to accelerate dynamic resources based on the file types. **Note:** 1. The billing methods for CDN and ECDN acceleration are different. A CDN traffic package can be used for fee deduction of only CDN traffic. For more information about the comparison on features and billing methods, see User Tutorial. 2. Once confirmed, the acceleration type cannot be changed. To use another acceleration type, delete the domain name, add the domain name again, and then select a new acceleration type. **CDN acceleration:** You can select a CDN acceleration type to accelerate static resources such as HTML, CSS, and JS files, images, videos, software installation packages, APK files, and compressed files. When different users access a static resource, the origin server returns the same content. You can select one of the following CDN acceleration types to maximize the acceleration performance: **Webpage file download**: Applicable to e-commerce platforms, websites, UGC communities, and other business scenarios that mainly involve small static resources, such as webpage styles, images, and small files. **Large file download:** Applicable to business scenarios where large files, such as game installation packages, application update packages, and application program packages, are downloaded. **Audio and video on demand:** Applicable to audio and video on-demand scenarios that require acceleration, such as online on-demand audio and video streaming. **ECDN acceleration:** You can select an ECDN acceleration type to accelerate dynamic resources such as APIs and .jsp, .asp, .php, .perl, and .cgi files. When different users access a dynamic resource, the origin server returns different content. You can select one of the following ECDN acceleration types to maximize the acceleration performance: **Dynamic & static content:** Applicable to business scenarios where dynamic and static data is integrated, such as various website homepages. **Dynamic content:** Applicable to scenarios such as account login, order transaction, API call, and real-time query.

Configuration Item	Description
IPv6 Access	IPv6 access is disabled by default. After you add the domain name, you can manually enable IPv6 access, so that CDN nodes can be accessed over the IPv6 protocol. **Note** IPv6 access is available only in the Chinese mainland. For global acceleration domain names, if IPv6 access is enabled, it takes effect only in the Chinese mainland. For domain names with acceleration nodes outside the Chinese mainland, IPv6 access cannot be enabled.
Tag	Tags are used to manage resources by category from different dimensions. If the existing tags do not meet your requirements, go to the tag management page in the console to create more tags. 1. You can add up to 50 tags to a domain name. 2. You can select only existing tags when you set this parameter. 3. The tag key and value are required when you create a tag.

5. Set parameters for the origin server.

You can select the type of origin server as needed. Supported origin server types include private origin, Tencent Cloud COS, and third-party object storage. This section helps you configure each type of origin server.

If you use a private origin, such as a server or a CVM instance that you own, select **Customer Origin** for **Origin type** and est the parameters based on the following description.

Configuration Item	Description

Configuration Item	Description
Origin-pull Protocol	**HTTP**: Use HTTP for origin-pull requests. In this case, port 80 is used for origin-pull by default and you must ensure that port 80 is available. **HTTPS**: Use HTTPS for origin-pull requests. In this case, port 443 is used for origin-pull by default and you must ensure that port 443 is available. Some platforms do not support custom origin-pull ports over HTTPS. **Follow Protocol**: The origin-pull protocol depends on the access requests. For example, HTTP is used as the origin-pull protocol for HTTP requests. To prevent the failure of origin-pull requests, if you select **Follow Protocol** for **Origin-pull protocol**, you cannot specify a custom origin-pull port.
IPv6 Origin Server	You can enable this feature and add one IPv6 origin server to support IPv6 origin-pull only if you select **Dynamic & static content** or **Dynamic content** for **Acceleration type**. After you add the domain name, this parameter cannot be modified. **Note:** 1. You can add only one IPv6 origin server that is different from the origin server for the domain name. In addition, you cannot specify the port. 2. After you enable the IPv6 origin server, you cannot switch the service area of the acceleration domain name to **Outside Chinese mainland** or **Global**.
Origin address	You can specify the origin-pull address, port, and weight for the origin server address. **Origin-pull Address**: Enter a domain name or IP address. You can specify up to 50 domain names or IP addresses. **Port**: Enter a custom port number for origin-pull. If you do not specify a port number, CDN use the default port based on the origin-pull protocol. **Weight**: If you specify multiple origin server addresses, you can specify the weight for each one, and CDN will perform round-robin origin-pull based on the specified weights. **Note:** 1. You cannot use an acceleration domain name as an origin server address, or use two domain names as the origin server address for each other. Otherwise, the access fails due to a DNS loop. 2. If your Tencent Cloud COS bucket or third-party object storage allows public access, you can select **Customer Origin** for **Origin type**, and enter the address of your Tencent Cloud COS bucket or third-party object storage for origin-pull.

If you use a Tencent Cloud COS bucket, you can select **Tencent Cloud COS Origin** for **Origin type** and set the parameters based on the following description.

Configuration Item	Description
Origin-pull Protocol	**HTTP**: Use HTTP for origin-pull requests. **HTTPS**: Use HTTPS for origin-pull requests. A COS origin supports HTTPS access by default. Therefore, we recommend that you select **HTTPS**. **Follow Protocol**: The origin-pull protocol adopted depends on the access requests.
Origin address	If you select **Tencent Cloud COS Origin** for **Origin type**, you can select a Tencent Cloud COS bucket from the drop-down list. Fuzzy search is supported. 1. If you select a bucket for the first time, you must click **Add Authorization Service** to grant CDN the permissions to access to the bucket.

Configuration Item	Description
	Select **I agree to the above authorization** and click **OK**. 2. COS bucket addresses are divided into three types: default domain name, static website domain name, and global acceleration domain name. **Default domain name**: The default bucket access domain name, which can be used to access the current bucket directly. **Static website domain name**: If the static website configuration is enabled for the current bucket, use this domain name as the origin server address. Otherwise, the static website configuration may become invalid. **Global acceleration domain name**: If the current bucket has global acceleration enabled, use this domain name as the origin-pull address. Otherwise, the global acceleration configuration of the bucket may become invalid. **Note:** 1. If your bucket is configured with cross-origin rules, configure the same cross-origin rules in the HTTP response header of the CDN. Otherwise, cross-origin access problems may occur. 2. When the current origin server type is COS origin, only one origin server can be added.
Private bucket access	This feature is disabled by default. You can enable it if your COS bucket allows only private reads and writes. After you enable the feature, CDN automatically generates a valid access key for the origin-pull of files.

If you use a third-party object storage, you can select **Third-Party Object Storage Origin** for **Origin type** and set the parameters based on the following description.

Configuration Item	Description
Origin source	The following third-party object storage services are allowed: AWS S3, Alibaba Cloud OSS, Huawei Cloud OBS, and Qiniu Cloud kodo. The support for Huawei Cloud OBS and Qiniu Cloud kodo is still in canary testing. If you need to use one of the two options, contact Tencent Cloud engineers.
Origin-pull Protocol	You can select the origin-pull protocol based on the access protocol of the third-party object storage. **HTTP**: Use HTTP for origin-pull requests. In this case, port 80 is used for origin-pull by default. **HTTPS**: Use HTTPS for origin-pull requests. In this case, port 443 is used for origin-pull by default.
Origin address	Enter an available access address of the third-party object storage. CDN has no strict restrictions on the address format. Examples: **AWS S3**: `my-bucket.s3.ap-east-1.amazonaws.com` . **Alibaba Cloud OSS**: `my-bucket.oss-cn-beijing.aliyuncs.com` . **Huawei Cloud OBS**: `my-bucket.obs.cn-east-3.myhuaweicloud.com` . **Qiniu Cloud kodo**: Custom access domain name with no fixed format required.

Configuration Item	Description
Private bucket access	You can enable this feature if your third-party object storage allows only private reads and writes. After you enable the feature, click **Enter** under the switch to specify the access key. Private bucket access For origin-pull to a third-party private bucket, a key is required for origin-pull authentication. Enter

6. Click **Add domain name** to continue.

Step 2. Use recommended configurations

After you add the domain name, you can follow Recommended Configuration Guidelines and configure CDN acceleration as recommended based on the acceleration types to achieve the best acceleration results by improving the resource hit rate, access performance, and access security, and preventing fee overages.

The following 4 configurations are recommended for you, please click switch to view and set:

| 1. Improve resource hit rate | 2. Improve access performance | 3. Prevent fee overages | 4. Improve access security |

Node Cache Validity Configuration

	Type	Content	Validity	priority weight ⓘ	Operation
⠿	All Files	All Files	Cache for 30 days; Force Cache on	1	Modify │ Delete
⠿	File extension	html	Cache for 1 day	2	Modify │ Delete
⠿	File extension	php;jsp;asp;aspx	No Cache	3	Modify │ Delete
⠿	File Directory	/wp-admin	No Cache	4	Modify │ Delete

Define priority by the sequence of items in the list. The lower items are with higher priorities.

+ Create Rule

Cache Key Rule Configuration

	Type	Content	Ignore Query String	Ignore case	Operation
⠿	All Files	All Files	Not Ignore	No	Modify

Define priority by the sequence of items in the list. The lower items are with higher priorities.

+ Create Rule

Browser Cache Validity Configuration

Type	Content	Validity	Operation
		No data yet	

Define priority by the sequence of items in the list. The lower items are with higher priorities.

+ Create Rule

If you do not want to use the recommended configurations at the moment, you can click **Back** to return to the domain name management list, or click **skip, next step** to continue.

You can also modify the recommended configurations as needed and click **Submit configuration** to continue.

2.1 Improving the resource hit rate

Configuration Item	Acceleration Type	Recommended Configuration

Configuration Item	Acceleration Type	Recommended Configuration
Node cache validity configuration	Webpage file download, large file download, audio and video on demand, and dynamic & static content	We recommend that you do not cache dynamic files, but set a long cache validity period for rarely updated content such as images and JS files to improve the resource hit rate. **Note:** If you need to update the CDN node cache immediately after your source resources are updated, you can use the cache refresh feature to proactively update the CDN node's unexpired files. For more information, see Purge Cache **Recommended configuration (the priority of rules increases from top to bottom):** 1. Cache all files for 30 days. 2. Do not cache .php, .jsp, .asp, and .aspx files.
Cache key rule configuration	Webpage file download, large file download, audio and video on demand, and dynamic & static content	CDN nodes identify resource versions by using the parameter after the question mark (?) in the user request URL. If the resource version is not indicated, CDN nodes can ignore the parameter to increase the resource hit rate. **Recommended configuration:** 1. If the resource version is indicated by using the parameter after the question mark (?), we recommend that you keep the parameter. 2. If the resource version is not indicated by using the parameter after the question mark (?), we recommend that you ignore the parameter.
Browser cache validity configuration	Webpage file download and dynamic & static content	You can specify browser caching rules so that the browner caches rarely updated files to improve the resource response speed. **Recommended configuration:** We recommend that you specify the extensions or directories of rarely updated files and the browser cache validity period. For example, you can cache images with extensions such as .jpg, .png, .gif, .bmp, .svg, and .webp, and set the browser cache validity period to 1 hour.

2.2 Improving the access performance

Configuration Item	Acceleration Type	Recommended Configuration
Node cache validity configuration	Dynamic content	If you select **Dynamic content** for **Acceleration type**, we recommend that you do not cache dynamic files. Otherwise, the access or login may fail. **Recommended configuration:** All files are not cached.

Configuration Item	Acceleration Type	Recommended Configuration
Smart compression configuration	Webpage file download and dynamic & static content	You can specify a smart compression rule, so that CDN performs Gzip or Brotli compression on the resources as specified before it returns content. This effectively reduces the volume of the transmitted content and saves overhead. **Recommended configuration:** By default, CDN performs Gzip compression on .js, .html, .css, .xml, .json, .shtml, and .htm files whose sizes range from 256 bytes to 2 MB. You can add more file types as needed.
Range GETs configuration	Large file download, and audio and video on demand	If most of your files are large static files, enabling Range GETs can help increase the file response speed during origin-pull and improve the large file delivery efficiency. **Recommended configuration:** If your origin server supports Range requests, and your files are larger than 4 MB in size, we recommend you enable Range GETs for such files.
Follow 301/302 configuration	Webpage file download, and dynamic & static content	If the follow 301/302 redirect configuration is enabled, a CDN node will actively redirect when receiving a 301/302 redirect request during origin-pull until the node obtains the requested resource. The node will then return the actual resource to the client, which does not need to be redirected. This reduces returning links and improves the response speed. **Recommended configuration:** If a client obtains the requested resources from your site after multiple redirections, we recommend that you enable the follow 301/302 redirect configuration
Video dragging configuration	Audio and video on demand	Video dragging generally happens in VOD scenarios. If the video dragging configuration is enabled, when a user drags the video progress bar, a CDN node directly responds to the request. After you enable the video dragging configuration, you must also configure **Ignore Query String** of all rules in **Cache Key Rule Configuration** as **Ignore all**. **Recommended configuration:** We recommend that you enable the video dragging configuration in VOD scenarios.

2.3 Preventing high bills

Configuration Item	Acceleration Type	Recommended Configuration

Configuration Item	Acceleration Type	Recommended Configuration
Usage limit configuration	All acceleration types	The usage limit configuration allows you to configure traffic usage alarming and the corresponding control measure based on your budget and business estimation. **Recommended configuration:** We recommend that you specify a usage limit and configure the traffic control rules as needed.

2.4 Improving access security

Configuration Item	Acceleration Type	Recommended Configuration
HTTPS configuration	All acceleration types	The HTTPS protocol is an encrypted and reliable transmission protocol, which effectively protects the security of your transmitted data. We recommended that you complete the HTTPS certificate configuration.
IP access limit configuration	All acceleration types	The IP access frequency limit configuration prevents malicious access to resources and APIs by a single client. You can adjust the access frequency limit as needed. Note that this configuration cannot prevent DDoS attacks. **Recommended configuration:** We recommend that you specify the access frequency limit based on the actual traffic of your website.

Step 3. Configure a CNAME record

Configure a CNAME record

After adding the domain name, you have to configure a CNAME record to enable CDN acceleration. Tencent Cloud CDN supports two CNAME configuration methods. For more information, see CNAME Configuration.

Verifying the effect of the CNAME record

1. After you configure the CNAME record, you can click **Verify CNAME status** to verify the status the CNAME record for the domain name. If the value in the **Status** column is **Activated**, the CNAME record has taken effect, and CDN acceleration is already enabled for the domain name. If the status is **Not activated**, you need to check whether you have correctly configured the CNAME record. If yes, the issue may be caused by the CNAME resolution latency.
2. You can also view the domain name list in the CDN console to verify the effect. **If at least one CNAME record is activated for the domain name, the CDN acceleration is already enabled for your domain name**.
3. You can also run the `nslookup` or `dig` command. Assume that you have added `www.test.com` . If you use Windows, open the command prompt and run the `nslookup -qt=cname www.test.com` command. Check the CNAME resolution record in the output. If the CNAME resolution record is the same as the CNAME

address that is provided by CDN, the CDN acceleration service has taken effect for the domain name.

```
[[root@VM-0-6-centos ~]# nslookup -qt-cname            .com
*** Invalid option: qt-cname
Server:
Address:

Non-authoritative answer:
             com    canonical name =                cdn.dnsv1.com.
```

If you use macOS or Linux, open the command prompt and run the `dig www.test.com` command. Check the CNAME resolution record in the output. If the CNAME resolution record is the same as the CNAME address that is provided by CDN, the CDN acceleration service has taken effect for the domain name.

```
t                               dig
; <<>> DiG 9.10.6 <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51159
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;.              .com.            IN      A

;; ANSWER SECTION:
               600     IN      CNAME                dn.dnsv1.com.cn.
                        . 600 IN CNAME               tdnsv5.com.
        .         tdnsv5.com. 60 IN     A       119.188.85.108
               tdnsv5.com. 60 IN     A       119.188.85.90
               tdnsv5.com. 60 IN     A       119.188.85.79
```

Understanding Cache, Cache Purging, and Cache Prefetch

1. After connecting a domain name to CDN, you can configure CDN cache based on file types. CDN caches static files on edge nodes, so that client requests for files are responded faster with lower origin-pull traffic. For more information, see Node Cache Validity Configuration.
2. Cache purging is manually triggered by users to delete the files that are already cached on a node when new files are published or the files violate certain rules. For more information, see Purge Cache.
3. Cache prefetch is performed by users to cache their large or hot files on Tencent Cloud CDN nodes in advance, so as to avoid origin-pull upon client requests. Cache prefetch effectively reduces origin-pull traffic and improves the access experience. For more information, see Prefetch Cache.

Common Problems

1. After I connect `example.com` to CDN, does CDN accelerate access to `www.example.com` ?
   No. `example.com` and `www.example.com` are two separate domain names. To accelerate access to `www.example.com` , you must connect it to CDN as well.

2. After I connect `*.example.com` to CDN, does CDN accelerate access to `example.com` ?

No. After you connect `*.example.com` to CDN, CDN accelerates access to domain names such as `a.example.com` and `a.b.example.com` . To accelerate access to `example.com` , you must connect it to CDN as well.

Adding Domain Names

Last updated：2022-04-27 10:54:09
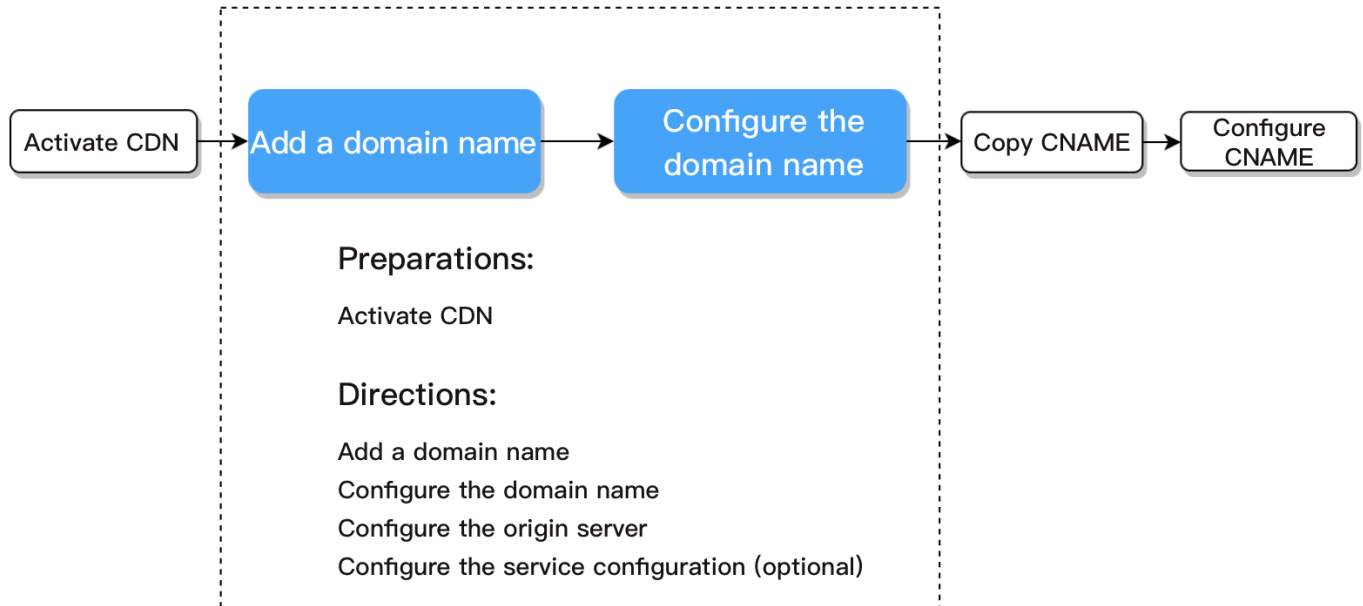
Preparations

Activating CDN

Before configuring CDN, you need to activate it first. If you have already activated it, proceed directly.

## Confusing concepts

Configuration Item	Description	Use Position
Acceleration domain name	Domain name to be connected to CDN, which is the actual domain name accessed by end users	Create a Domain Name > Domain Configuration

Configuration Item	Description	Use Position
Origin address (IP/domain name)	IP address (domain name) of the origin server. If the requested content is not on the CDN node, this address (domain name) will be accessed to get the requested content. **Origin server**: server that provides a service, which can process and respond to user requests. End users access your business at the origin address. An origin address can be a domain name or IP address.	Create a Domain Name > Origin Configuration
Origin domain	Server content actually requested during origin-pull of the CDN node. This is generally consistent with the acceleration domain name. You can enter the actually requested content in the origin-pull request based on your business needs.	Create a Domain Name > Origin Configuration
CNAME domain name	After your acceleration domain name is connected, the system will automatically assign a CNAME domain name suffixed with `.cdn.dnsv1.com` or `.dsa.dnsv1.com`. After your acceleration domain names are mapped to the CNAME domain name, Tencent Cloud will dynamically change the IP address pointed to by the CNAME record and update all your acceleration domain names, eliminating your need to manually change the IP addresses pointed to them.	Configure CNAME

- **Acceleration domain name:** if end users access your business through `cdntest.com`, then `cdntest.com` is the acceleration domain name.
- **CNAME domain name:** after an acceleration domain name is connected, the system will automatically assign a CNAME domain name suffixed with `.cdn.dnsv1.com` or `.dsa.dnsv1.com`, such as `cdntest.com.cdn.dnsv1.com` and `cdntest.com.dsa.dnsv1.com`.
- **Origin address:** if the CDN node does not cache the content requested by the user, the node will request such content at `1.1.1.1`, which is the origin address.
- **Origin domain:** when the CDN node is requesting `1.1.1.1`, if you expect that the actually requested address is `originhost.com`, which is different from `cdntest.com` in the end user's request, then set the origin domain to `originhost.com`, and the end user will access the content at `originhost.com` after origin-pull through `cdntest.com`. Generally, the acceleration domain name and the origin domain should be the same, which can be adjusted based on your business needs.

Directions

Go to the CDN console, select **Domain Management** on the left sidebar, and click **Create a Domain Name**.
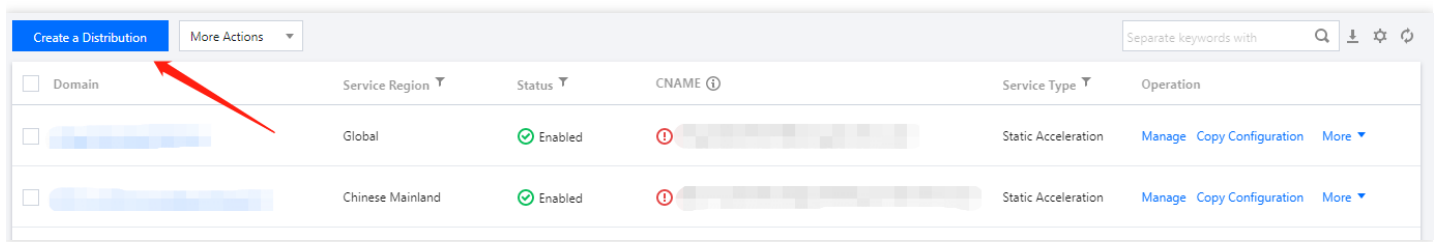
You need to configure the following three parts to connect a domain name:

- Domain name configuration
- Origin server configuration
- Service configuration (optional)

Configuring the domain name

1. Select an acceleration region.
2. Enter an acceleration domain name.

   If your connected domain name meets one of the following conditions, you need to verify your ownership as instructed in Domain Name Ownership Verification.

   - The domain name is being connected for the first time.
   - The domain name has been connected by another user.
   - The domain name is a wildcard domain name.
3. Select an acceleration type.
4. Set other optional items (which can be modified in **Domain Management** subsequently).

Configuration item description

Configuration	Description

Configuration	Description
Region	**Chinese mainland**: all requests are scheduled to cache nodes in the Chinese mainland. **Outside the Chinese mainland (including Hong Kong/Macao/Taiwan (China))**: all requests are scheduled to cache nodes outside the Chinese mainland. **Global**: requests are scheduled to the nearest optimal node. **Notes:** acceleration services in and outside the Chinese mainland are billed separately. For more information, see Billing Overview.
Acceleration Domain Name	1. The domain name can contain up to 81 characters. 2. ICP filing is required for domain names running in the Chinese mainland. 3. Sub-domains (`a.test.com` or `a.b.test.com`) and wildcard domain names (`*.test.com` or `*.a.test.com`) are supported. 4. You need to verify the domain name ownership when connecting a domain name for the first time, a wildcard domain name, or a connected domain name. **Notes:** 1. If a wildcard domain name is connected here, its sub-domains and second-level wildcard domain names cannot be connected by any other accounts. 2. Domain names in the format of `*.test.com` and `*.a.test.com` cannot be configured at the same time. 3. Malicious or high-risk domain names cannot be connected to. For more information, see Use Limits.

Configuration	Description
Acceleration type	CDN optimizes acceleration performance based on service type. For better acceleration effect, we recommend selecting the acceleration type similar to that of your actual business. **CDN** Static acceleration: applicable to small-scale resource acceleration scenarios such as e-commerce, website, and game photos. Download acceleration: applicable to downloading scenarios such as game installation packages, audio and video source file downloads, and mobile phone firmware distribution. On-demand video streaming acceleration: applicable to online education and on-demand video streaming. **ECDN** Dynamic/Static acceleration: applicable to business scenarios where static and dynamic data is integrated, such as various website homepages. Dynamic acceleration: applicable to scenarios such as account login, order transaction, API call, and real-time query. **Note:** The billing standards vary by acceleration type. For more information, see Billing Overview of CDN and Billing Overview of ECDN respectively.
IPv6 Access	IPv6 access is disabled by default. If it is enabled, CDN nodes can be accessed over the IPv6 protocol. **Notes:** • IPv6 access is currently not supported due to platform upgrade. Please stay tuned for the official launch. • IPv6 access is only available in the Chinese mainland. •For global acceleration domain names, if IPv6 access is enabled, it will take effect only in the Chinese mainland.
Project	Project is a set of resources shared by all Tencent Cloud products. You can manage it on the Project Management page.
Tag	The tag key and value are required. If you have not created a tag, create one in Tag Management.

Origin server configuration

1. Select the origin server type.

2. Select the origin-pull protocol.

3. Enter the origin address.

4. Configure the origin domain.

Origin Configuration

Origin Type   ● External   ○ COS Origin

Origin-pull Protocol   ● HTTP   ○ HTTPS   ○ Follow Protocol

Origin Address

Enter multiple origin IPs (one entry per line) or one origin domain name
Port (0-65535) and weight (1-100) settings can be added to configurations. Supported format: Origin Server:Port:Weight and Origin Server::Weight
If HTTPS origin-pull is selected, the port must be 443, or you can leave it empty.
Enter up to 511 characters

Origin Domain

Configuration item description

Configuration Item	Description
Origin Type	**Customer Origin**: Select this if you already have your own business server (i.e., origin server). Tencent Cloud COS: If COS is used, you can directly select the corresponding bucket. Third-Party Object Storage: a third-party object storage platform other than Tencent Cloud. Currently, AWS S3 and Alibaba Cloud OSS are supported. **Note:** This option is unavailable for some platforms at the moment. Please stay tuned for the official launch.

Configuration Item	Description
Origin Server Address	**Customer Origin**: 1. Multiple IPs can be configured as the origin server, which will be polled during origin-pull. 2. You can configure port (0 - 65535) and weight (1 - 100) **in the format of** `origin server:port:weight`. The port can be omitted and the format becomes `origin server::weight`. **Note:** HTTPS protocol currently only supports port 443. 3. You can configure a domain name as the origin server, which **should be** different from the CDN acceleration domain name. **Note:** using a connected CDN acceleration domain name as the origin server will cause resolution loop and origin-pull failure. **Tencent Cloud COS:** 1. You can select a bucket of Tencent COS as the origin server. 2. Set the origin server type to default domain name or static website according to the bucket configuration and your actual use case. 3. For a private bucket, grant CDN access to the bucket. **Third-party Object Storage**: 1. If the resource is stored in a third-party object storage platform, please enter a valid bucket access address as the origin server. For now, AWS S3 and Alibaba Cloud OSS are supported. **Note**: `http://` and `http://` cannot be included. `my-bucket.oss-cn-beijing.aliyuncs.com` and `my-bucket.s3.ap-east-1.amazonaws.com` are supported. 2. For a third-party private bucket, enter the valid key and enable forwarding authentication to access the bucket.
Origin-Pull Protocol	This can be selected based on the protocols supported by the origin server: HTTP: HTTP/HTTPS access requests use HTTP origin-pull. HTTPS: HTTP/HTTPS access requests use HTTPS origin-pull (the origin server must support HTTPS access). Follow protocol: HTTP access requests use HTTP origin-pull, while HTTPS access requests use HTTPS origin-pull (the origin server must support HTTPS access).

Configuration Item	Description
Origin Domain	This refers to the domain name accessed on the origin server by a CDN node during origin-pull. **Customer Origin**: 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. **Tencent Cloud COS**: it defaults to the bucket access address, which is the same as the origin address and cannot be modified. **Third-party Object Storage**: it defaults to the bucket access address, which is the same as the origin address and cannot be modified.

Service configuration (optional)

CDN provides common service configuration items for you to configure as needed. If you don't want to configure the service right now, you can do so after connecting the domain name.

Configuration item description

Configuration	Description
Ignore Query String	A node caches resources by following the `Key-Value` mapping, where `Key` is the resource URL. If `Ignore Query String` is enabled, parameters after "?" in the URL will be ignored. Otherwise, `Key` will be a complete resource URL. By default, this feature is **enabled** for download and streaming VOD acceleration, but **not** for static acceleration.

Configuration	Description
Enable Range GETs	This specifies whether to process partial requests during origin-pull. It can be enabled only if the origin server supports Range GETs. **By default**, this feature is **enabled** for COS origin server or download and streaming VOD acceleration.
Cache Configuration	Validity of node cache. For static acceleration, the general dynamic files (such as PHP, JSP, ASP, and ASPX files) will not be cached, and other files will be cached for 30 days by default. For download and streaming VOD acceleration, the cache validity of all files is 30 days. The configured cache validity is the longest possible time, the actual cache validity is related to the resources on nodes.

Completing the Configuration

After adding the domain name, wait for the domain name configuration to be distributed to the entire network, which usually takes 5 to 10 minutes.

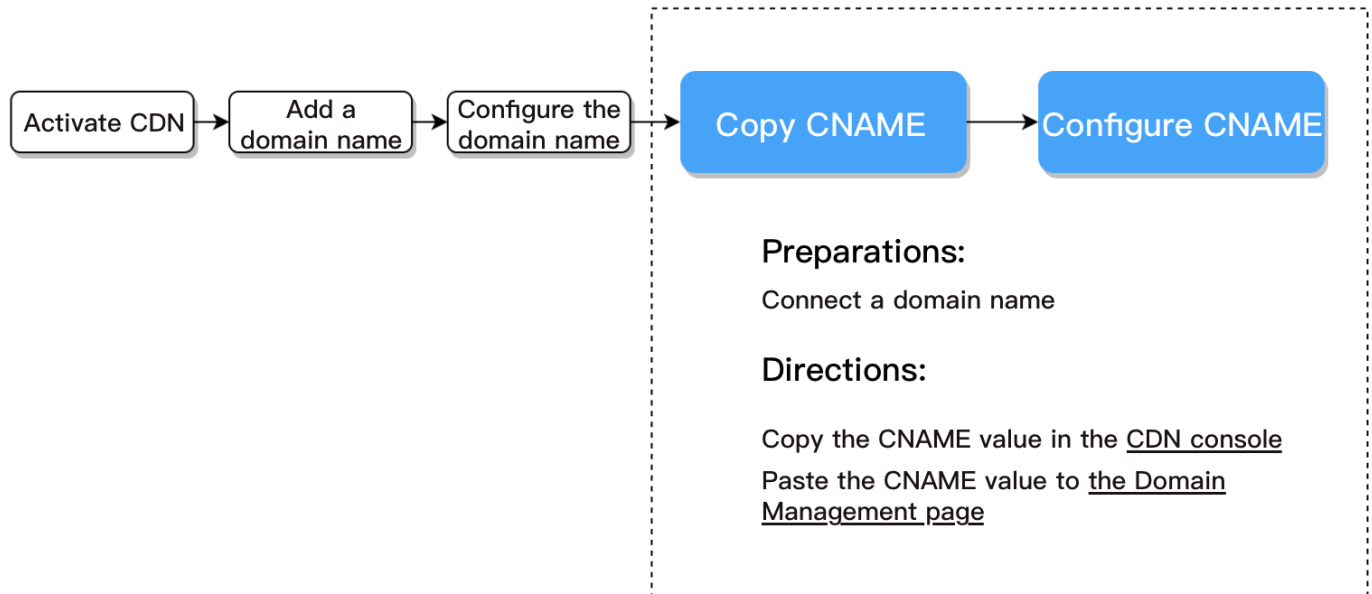## Subsequent Steps

When the distribution is completed, CDN will allocate a corresponding CNAME address to you. You need to configure the CNAME to use the CDN service. For detailed directions, see CNAME Configuration.

CNAME Configuration

Last updated：2021-11-24 14:51:40

Preparations

Adding domain name

Before configuring a CNAME record, you need to add a domain name first. If you have already added one, proceed directly.

Directions

Configuration steps

You need to complete the configuration at the DNS service provider of your domain name. This document describes the configuration steps in Tencent Cloud and Alibaba Cloud:

- Settings for Tencent Cloud
- Settings for Alibaba Cloud

Tencent Cloud

Quick configuration

If your domain service provider is Tencent Cloud, we recommend you use the quick CNAME record configuration feature. For more information, see Configuring CNAME via DNSPod.

Manual configuration

1. Log in to the CDN console and copy the CNAME address.

   Before your domain name is successfully resolved, a prompt icon is displayed next to the CNAME record. Copy the CNAME record value.

2. Log in to the DNSPod console and click **Record**.

3. Add a CNAME record and click **OK**.

4. Wait for the configuration to take effect.

Configuration description:

Configuration	Description
Host	It is the domain name prefix. **Example:** to add a record for `dnspod.com` , select @ for **Host**. To add a record for `www.dnspod.com` , select **www** for **Host**.
Record Type	Select **CNAME**.
Split Zone	Select **Default**. DNSPod offers various split zone options for you to specify records for specific users. For more information, see Split Zone Description.
Value	Enter the domain name pointed to by the CNAME, e.g., `xxx.xxx.com.cdn.dnsv1.com` . After the record is generated, a `.` will be automatically added after the domain name.
Weight	Different record values in the same split zone of a host record can be set with different weights, so that resolution will be returned according to their weight ratios. Value range: 1–100.
MX	It refers to the priority. The lower the value, the higher the priority. We recommend you leave it empty.
TTL	It refers to the time to live. The smaller the value is, the less the time cost for record changes to take effect globally. The default value is 600 seconds.

Alibaba Cloud

If your DNS service provider is Alibaba Cloud, you can add a CNAME record as follows.

1. Log in to the CDN console and copy the CNAME address.
   Before your domain name is successfully resolved, a prompt icon is displayed next to the CNAME record. Copy the CNAME record value.

2. Log in to the Alibaba Cloud DNS console.

3. Click the domain name to be resolved to enter the resolution record page.

4. Click **Add Record**.

5. Select ***CNAME** as the record type. Enter the host record as needed (such as `www`), which is the domain name prefix. Enter the CNAME record copied in step 1 as the record value. Retain the default settings of the split zone and TTL.

6. Finally, click **Confirm**.

Subsequent Operations

CNAME verification

The time it takes for a CNAME record to take effect varies by DNS service provider. It is generally within half an hour. You can also check whether the CNAME record is in effect by running `nslookup` or `dig` . If the CNAME record response is the CNAME configured, it indicates that the configuration is successful and the acceleration is enabled.
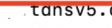
```
[[root@VM-0-6-centos ~]# nslookup -qt-cname ██ █ █████ █ █l.com
*** Invalid option: qt-cname
Server:
Address:        █ █ █ █ █

Non-authoritative answer:
███ █ █ ████l.com     canonical name = ███ █ █████ ███ █ █m.cdn.dnsv1.com.
```

- nslookup -qt=cname

- dig

```
[[root@VM-0-6-centos ~]# dig ███ ████ ██ l.com

; <<>> DiG 9.11.26-RedHat-9.11.26-4.el8_4 <<>> ████ ██ ███████ █
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38864
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;████████ █ ██ .com.            IN      A

;; ANSWER SECTION:
██ ██████ █ █.com.    600     IN      CNAME   s████ █ ███ com.cdn.dnsv1.com.
██████ ██.com.cdn.dnsv1.com. 600 IN CNAME ████ ███      ██.tdnsv5.com.
dqc18e8j.sched.vp.tdnsv5.com. 60 IN      A       182.254.53.75
dqc18e8j.sched.vp.tdnsv5.com. 60 IN      A       182.254.53.33
dqc18e8j.sched.vp.tdnsv5.com. 60 IN      A       182.254.49.84
dqc18e8j.sched.vp.tdnsv5.com. 60 IN      A       182.254.53.94

;; Query time: 57 msec
;; SERVER: 183.60.83.19#53(183.60.83.19)
;; WHEN: 六 9月 18 16:42:46 CST 2021
;; MSG SIZE  rcvd: 197
```

Directions

You have completed the basic configuration of the CDN service. For more CDN configurations, see the corresponding document in Configuration Guide.

Domain Name Ownership Verification

Last updated：2023-03-10 16:32:56

When do I need to verify my domain name?

1. When you connect a domain name, such as `a.example.com`, for the first time, the same-level domain names, such as `b.example.com`, and subdomain names can be directly connected without verification. However, if you want to connect second-level domain names, such as `example.com`, ownership verification is required.
2. The subdomain names that are connected under another account must be verified. If the subdomain names pass the verification, you can connect the subdomain names under the current account.
3. The same-level wildcard domain names that you want to connect must be verified. If you connected a domain name, such as a.example.com, any same-level wildcard domain name must be verified before it is connected, whereas a second-level wildcard domain name, such as `*.a.example.com`, can be directly connected.

Method 1: DNS Verification (Recommended)

1. When a domain name that you add requires ownership verification, a message appears below the domain name field to inform you of the requirement details. To view the requirements for verification methods, click **Verification Method**.

2. Use the default verification method, which is DNS verification.
   To start DNS verification, add the "_cdnauth" host record of the TXT type for the domain name at your DNS provider.

   Note：

In scenarios where multi-level domain names are used, host records must be added only for the domain name regardless of the level of the added domain name, such as `c.b.a.example.com`, `*.example.com`, and `test.example.com`. For example, if you add the `c.b.a.example.com` subdomain name, you must add the `_cdnauth.example.com` resolution record.

To add a resolution record of Tencent Cloud DNS, perform the following operations:

If your DNS provider is Tencent Cloud, log in to the DNSPod console, find the target domain name, click **DNS**, and add a TXT record. Set the **Host** parameter to `_cdnauth`, the **Record Type** parameter to `TXT`, and the **Record Value** parameter to the record value provided by Tencent Cloud CDN. Use the default settings for other parameters.

To add a resolution record of Alibaba Cloud DNS, perform the following operations:

If your DNS provider is Alibaba Cloud, log in to the DNS console of Alibaba Cloud, find the target domain name, and click **DNS Settings** in the **Actions** column. Set the **Record Type** parameter to `TXT`, configure the **Hostname** and **Record Value** parameters, and use the default settings for other parameters.

3. Wait for the TXT record to take effect before you click the verification button to start verification. If the domain name fails to be verified, make sure that the TXT record is valid and has taken effect at the DNS provider. For information on how to check whether the TXT record has taken effect, see the related documentation.

4. After the domain name is verified, check whether the domain name is connected under another account. If yes, click **Retrieve** to retrieve the domain name. After the domain name is retrieved, the settings that are configured for the domain name under another account are cleared.

Method 2: File Verification

1. When a domain name that you add requires ownership verification, a message appears below the domain name field to inform you of the requirement details. To view the requirements for verification methods, click **Verification Method**.

2. Click the **File verification** tab.

3. Click **verification.html** to download the file for verification.

4. Upload the file to the root directory on the server of your domain name, such as a Tencent Cloud Cloud Virtual Machine (CVM) instance, a Tencent Cloud Object Storage (COS) bucket, an Alibaba Cloud Elastic Compute Service (ECS) instance, or an Alibaba Cloud Object Storage Service (OSS) bucket. For example, if your domain name is `test.example.com`, you must upload the file to the `example.com/` or `test.example.com/` root directory.

> Note：
>
> You can perform verification by uploading the file to a subdomain name only if you use the file verification method.

5. Make sure that the file is accessible via `http://example.com/verification.html` or `http://test.example.com/verification.html` before you click **Verify**. Your domain name will be successfully verified if the record you added is consistent with the content of the file. If the domain name cannot be verified, check whether the record and the content of the file are consistent.

> Note：
>
> File verification does not support domain name retrieval. You can retrieve your domain name only if you use the DNS verification method.

Example:

In this example, the acceleration domain name is `a.test.com` and the origin server is a COS biucket.

1. Upload the verification.html file to the root directory of COS.
2. Add a CNAME record for the acceleration domain name at your DNS provider. Set the **Record value** parameter to the COS domain name.
3. Check whether the verification.html file is accessible via http(https)://Acceleration domain name/verification.html. Click **Verify**.

Method 3: API Operation Verification

1. Call the CreateVerifyRecord operation to generate a TXT resolution record for an acceleration domain name.

```
{
"Response": {
"Record": "202009071516044acd018wf498457628cn75ba018ec9cv",
```

```
    "RecordType": "TXT"
    "RequestId": "8518c99c-a8eb-4930-a7d0-eff586d9cc37",
    "SubDomain": "_cdnauth",
    }
    }
```

2. Add the TXT resolution record at your DNS provider, such as DNSPod.

3. Call the VerifyDomainRecord operation to check whether the resolution record takes effect.

```
{
"Response": {
"RequestId": "b6926bb2-d0b5-42bc-b17f-e4402bdb9e9b",
"Result": "true"
}
}
```

4. If the resolution record takes effect, call the AddCdnDomain operation to add the domain name.

FAQs

How do I know whether a TXT record takes effect?

Windows:

If the domain name that you connected is `test.example.com` , open the command prompt and run the `nslookup -qt=txt _cdnauth.example.com` command. Check whether the TXT record takes effect or is valid based on the output.

Linux or macOS:

If the domain name that you connected is `test.example.com` , open the command prompt and run the `dig _cdnauth.example.com txt` command. Check whether the TXT record takes effect or is valid based on the

output.

```
[ti         ]@     udeMacBook-Pro ~ % dig _cdnauth.     cn txt              ]

; <<>> DiG 9.10.6 <<>> _           txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26083
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;_cdnauth.                         IN       TXT

;; ANSWER SECTION:
cdnauth.            .   600       IN       TXT       "20220606163634a806e0a3c6f73b7db
98f007b60a67fb3"

;; Query time: 55 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Jun 06 16:58:45 CST 2022
;; MSG SIZE  rcvd: 119
```

Why do I get an error that the VOD domain name cannot be accessed?

It's because your domain name has already been added to the VOD console. If you want to manage the domain name in the CDN console, it must be deleted from the VOD console and wait about 1 minute before adding it to the CDN console, or access other subdomain names.

FAQs about Domain Name Connection

Last updated：2023-03-10 14:51:23

How do I connect a domain name?

You can connect a domain name in the Content Delivery Network (CDN) console. For more information, see Adding Domain Names.

Are there any requirements for connecting a domain name to CDN?

1. The domain name cannot exceed 81 characters in length.

2. If the domain name requires acceleration in the Chinese mainland or global acceleration, you must obtain an ICP filing for the domain name from the Ministry of Industry and Information Technology (MIIT). If the domain name requires acceleration outside the Chinese mainland, you do not need to obtain an ICP filing for the domain name.

3. It takes 1 to 2 hours to synchronize ICP filing information. Re-add the domain name 1 or 2 hours after the ICP filing is complete.

4. The domain name can contain underscores (_) and Punycode-converted Chinese characters. You must obtain ICP filings for Chinese domain names before you convert the Chinese characters in the domain names to Punycode.

5. You can connect wildcard domain names in various formats, such as `*.example.com` and `*.a.example.com`. After you connect a wildcard domain name, its subdomain names or second-level wildcard domain names cannot be connected under another account. For example, if you connect the `*.example.com` wildcard domain name, the access traffic to the `a.example.com` domain name is accelerated based on the settings that are configured for the `*.example.com` wildcard domain name, whereas the access traffic to the `example.com` domain name is not accelerated.

6. You can connect multiple levels of nested domain names, such as `*.example.com`, `*.path.example.com`, and `a.path.example.com`, at the same time under an account. In this case, the domain name settings are applied and traffic statistics are calculated based on the priorities of the domain names. A more accurate match between the accessed domain name and a connected domain name indicates a higher priority for the connected domain name. For example, the access traffic to `a.path.example.com` is accelerated based on the settings of `a.path.example.com`, the access traffic to `b.path.example.com` is accelerated based on the settings of `*.path.example.com`, and the access traffic to `c.example.com` is accelerated based on the settings of `*.example.com`. The same analogy applies to traffic statistics.

7. If the subdomain names of a wildcard domain name are connected under other accounts, the wildcard domain name can be connected only after the subdomain names are disconnected under the accounts. For example, if the `a.example.com` subdomain name of the `*.example.com` wildcard domain name is connected under Account A, you must delete the subdomain name under Account A before you can connect the `*.example.com` wildcard domain name under Account B.

Does CDN support connecting wildcard domain names?

Yes, CDN supports connecting wildcard domain names, for which domain name ownership verification is required. Once verified, domain names can be connected or retrieved.
In addition:

1. If a wildcard domain name such as `*.test.com` is already connected to Tencent Cloud, then none of its sub-domain names can be connected to another account.
2. If the `*.test.com` wildcard domain name is connected under the current account, wildcard domain names in a format such as `*.path.test.com` can be connected only under the current account.
3. If multiple levels of nested domain names are connected at the same time under an account, the domain name settings are applied and traffic statistics are calculated based on the priorities of the domain names. A more accurate match between the accessed domain name and a connected domain name indicates a higher priority for the connected domain name. For example, the access traffic to `a.path.test.com` is accelerated based on the settings of `a.path.test.com`, and the access traffic to `b.path.test.com` is accelerated based on the settings of `*.path.test.com`.

Why do I get an error that the VOD domain name cannot be accessed?

It's because your domain name has already been added to the VOD console. If you want to manage the domain name in the CDN console, it must be deleted from the VOD console and wait about 1 minute before adding it to the CDN console, or access other subdomain names.

How long does it take to configure CDN?

Most CDN configurations take effect within 5 minutes. Some CDN configurations take effect within 5 to 15 minutes because a large number of tasks need to be run to complete the configurations. Please wait.

Can I configure multiple origin server IPs?

Yes. After you configure multiple IPs, CDN will randomly access one of the IPs when forwarding a request to the origin server. If the number of origin-pull failures with this IP exceeds the threshold, the IP will be isolated for 300 seconds by default, during which no origin-pull requests will be forwarded to the IP.

How do I bind CNAME to a domain name after the domain name is connected to CDN?

See CNAME Configuration for how to bind CNAME with your DNS service provider.

What business types does CDN support?

The selected service type determines which resource platform is used by the domain name. Acceleration configurations vary by resource platforms. Please choose the service type that matches your business:

- Acceleration of small webpage file downloads: applicable to e-commerce, websites, UGC communities, and other business scenarios that mainly involve small static resources, such as webpage styles, images, and small files.
- Acceleration of large file downloads: applicable to business scenarios where large files, such as game installation packages, application updates, and application program packages, are downloaded.
- Audio and video on demand acceleration: applicable to audio and video on-demand scenarios that require acceleration, such as online on-demand audio and video streaming.
- Dynamic and static content acceleration: applicable to business scenarios where dynamic and static data is integrated, such as various website homepages.
- Dynamic content acceleration: applicable to scenarios such as account login, order transactions, API calls, and real-time queries.

Why do exceptions such as old resources, old content, and incorrect content occur after the acceleration?

CDN nodes cache resources based on the cache validity configuration. If the resources that are cached on a CDN node are not expired, the CDN node does not synchronize the latest resources from the origin server.
After a resource on the origin server is updated, its cache on the CDN node must be updated immediately. You can use the cache purge feature to update unexpired caches on the CDN node, so as to ensure that resources cached on the CDN node and stored on the origin server are consistent.

How do I modify the project of a domain name in CDN?

Log in to the CDN console, select **Domain Management** on the left sidebar, click **Manage** on the right of a domain name, open the **Basic Configuration** tab, and then modify the domain name project. To modify the projects of multiple domain names in batches, please tick target domain names on the **Domain Management** page, click **More Actions** drop-down list, and select **Edit Project**. Up to 50 domain names can be operated at a time.

> Note：
> Users on the CDN permission system should proceed with caution, since this operation may cause changes to the permissions of sub-users.

My domain name has already obtained an ICP filing from the MIIT. Why does the system prompt that it does not have an ICP filing when I try to connect it to CDN?

After you obtain your ICP filing, it takes some time to sync the information from the MIIT to Tencent Cloud CDN. Please wait 24 hours and try again.

Can I configure ports for acceleration domain names or origin servers?

- CDN acceleration domain name port: currently, CDN acceleration ports can only be 80, 443, and 8080.

- Origin server port: the ports 1 to 65535 can be configured after the origin server address.

What is CDN origin domain configuration?

The origin domain is the website domain name that is accessed on the origin server during origin-pull on a CDN node. The IP or domain name that is configured on the origin server allows a CDN node to find the corresponding origin server during origin-pull. If multiple websites run on the origin server, the origin domain configuration specifies the domain name of the website to which requests are forwarded. If only one website runs on the origin server, you do not need to modify the origin domain, and the acceleration domain name is used as the origin domain by default.
If you use a Tencent Cloud Object Storage (COS) bucket or a bucket of a third-party object storage service as the origin server, you cannot modify the origin domain, and the origin-pull address is used as the origin domain by default.

How do I tell whether CDN has taken effect?

1. View the domain name list in the CDN console. The CDN acceleration service has taken effect for your domain name if at least one CNAME resolution record is valid for the domain name. This means that the CNAME resolution of the domain name is complete.

2. Alternatively, run the `nslookup` or `dig` command. In this example, the domain name is `www.test.com`.
   - If you use Windows, open the command prompt and run the `nslookup -qt=cname www.test.com` command. Check the CNAME resolution record in the output. If the CNAME resolution record is the same as the CNAME address that is provided by CDN, the CDN acceleration service has taken effect for the domain name.

   - If you use macOS or Linux, open the command prompt and run the `dig www.test.com` command. Check the CNAME resolution record in the output. If the CNAME resolution record is the same as the CNAME address

that is provided by CDN, the CDN acceleration service has taken effect for the domain name.

```
t ▓   ▓   ▓   ▓        ▓   dig ▓▓▓ ▓  ▓  ▓
; <<>> DiG 9.10.6 <<>>   ▓▓  ▓  ▓
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51159
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;.          ▓........com.         IN      A

;; ANSWER SECTION:
▓    ▓    ▓      ▓         600      IN      CNAME  ▓  ▓    ▓  ▓    dn.dnsv1.com.cn.
▓     ▓    ▓    ▓       ▓  .  600 IN CNAME  ▓  ▓    ▓   tdnsv5.com.
    .   ▓   ▓  tdnsv5.com. 60 IN     A      119.188.85.108
 ▓      ▓   ▓ tdnsv5.com. 60 IN     A      119.188.85.90
             tdnsv5.com. 60 IN     A      119.188.85.79
```

What do I do if files fail to be downloaded from CDN?

If files cannot be downloaded from CDN, we recommend troubleshooting by the following methods:

1. Check whether files can be downloaded normally from the origin server.
2. Check whether the domain name is correctly configured in the CDN console (see the origin domain in the **Basic Configuration** tab). Make sure that the configured origin domain name can be connected properly. Otherwise, origin-pull may fail, which will affect your business.
3. Check the security policy of the origin server. Check whether the origin-pull failure is caused by the security policy that is configured on the origin server. If so, obtain the intermediate IP range and add the origin server to the allowlist.

What should I do if I cannot log in to the WordPress backend after CDN acceleration is configured?

When you configure CDN acceleration for WordPress, you must properly configure cache rules for resources that are related to dynamic requests, such as interface-related resources and login-related resources (resources in the /wp-admin backend login address). Otherwise, you may encounter a login failure. We recommend that you do not cache dynamic files.

What do I do if the origin-pull protocol or port is invalid when I configure the origin server?

Tencent Cloud CDN supports port customization when you configure the origin server. If you set the origin-pull protocol to HTTP, port 80 is used for origin-pull by default. If you set the origin-pull protocol to HTTPS, port 443 is used for origin-pull by default. If you configure a custom port, the custom port is used for origin-pull. Make sure that you properly configure the origin-pull protocol and port when you configure the origin server. Otherwise, origin-pull may fail. The following examples list the common configuration errors:

1. The origin-pull protocol is set to HTTP, but the origin server supports only HTTPS-based origin-pulls.
2. The origin-pull protocol is set to HTTP, and the custom port 443 is used. However, the origin server supports only HTTPS-based origin-pulls.
3. The origin-pull protocol is set to HTTP, and the custom port 8080 is used. However, the origin server does not support access requests from port 8080.

If the origin-pull protocol is valid and the default port is invalid, use a custom port. After you enter the information about the origin server, the system automatically checks whether the origin server supports access from the custom port and returns the check result. If the check fails, troubleshoot issues based on the returned check result.

Does CDN support .top domain names?

Yes. CDN already supports domain names suffixed with .pw or .top.

Does CDN support Chinese domain names?

CDN supports domain names that contain underscores (_) and Punycode-converted Chinese characters.

- You must obtain ICP filings for Chinese domain names before you convert the Chinese characters in the domain names to Punycode.
- After you add a Chinese domain name to the allowlist, you can convert the domain name to `xn--fiq228c.xn--eqrt2g` by using a thrid-party tool, and then connect `xn--fiq228c.xn--eqrt2g` to CDN.
- You can directly add domain names that contain underscores (_), such as `test_qq.tencent.cloud` .

What will happen to the files on CDN nodes if I disable the connected domain name in the CDN console?

If you disable the CDN service of a connected domain name, CDN nodes will retain the connection configurations of the domain name, CDN traffic will no longer be generated, and the domain name will be inaccessible.

Why does the "The CAM policy is not configured for the sub-account" error message appear?

The error message appears when you use a sub-account to perform operations, such as adding domain names and querying data, and you have not used the root account to attach policies to the sub-account. To resolve the problem, use the root account to go to the Policies page in the CAM console, create CDN-related policies, and attach the policies to the sub-account. After the authorization is complete, you can go to the user list to view the policies that are attached to the sub-account.

How do I disable or delete an acceleration domain name? Will the configuration be retained after the acceleration domain name is disabled or deleted?

To stop acceleration, log in to the CDN console, disable the domain name, and then delete the domain name. For more information, see Domain Name Operations. If you cannot delete the domain name after you disable it, check whether the domain name is in the Disabling state. If not, check whether you are logged in to the CDN console with a sub-account. If yes, use the root account to grant the required permissions to the sub-account.

After a domain name is disabled, resources that have been configured are retained, but the acceleration stops and the 404 error code is returned for incoming user requests. After the domain name is deleted, resources that have been configured are immediately deleted and cannot be recovered.

How do I enable CDN acceleration for the `example.com`, `www.example.com`, and `m.example.com` domain names at the same time?

1. To enable CDN acceleration for the three different domain names, connect them one by one to CDN. If you want to apply the same settings to the three domain names, add the domain name in batches or replicate the settings when you add the domain names.

2. To access the same resource from multiple domain names, such as `example.com` and `www.example.com`, add an implicit or explicit URL at your DNS provider to point the domain names to a website by using the 301 redirect technology. For more information, see Implicit and Explicit URL Records.

Does CDN support a WebSocket connection?

We recommend that you enable dynamic and static content acceleration or dynamic content acceleration by using Enterprise Content Delivery Network (ECDN). You can configure the timeout period for the WebSocket connection. The timeout period can be up to 300 seconds. The WebSocket connection may be unstable or even fail when you use the following acceleration types: small webpage file downloads, large file downloads, and audio and video on demand.