

Enterprise Content Delivery Network

User Guide

Product Documentation





Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

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

Trademark Notice

🔗 Tencent Cloud

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

Service Statement

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



Contents

User Guide **Domain Name Management Domain Name Operations Configuration Management Configuration Overview Basic Configuration Cache Configuration** Access Control **IP Access Limit Configuration** IP Blocklist/Allowlist Configuration Advanced Configuration **Configure HTTP Header HTTPS Setting** Alarm Monitoring Configuration **Origin-Pull Management** Advanced Origin-Pull Policies Permission Management **Console Permission Description Creating Policies** Statistical Analysis Statistics Overview **Access Statistics** Status Code Statistics Cache Purge Certificate Management Log Management

User Guide Domain Name Management Domain Name Operations

Last updated : 2021-08-05 11:29:39

In the ECDN Console, you can enable, disable, and delete the acceleration service or modify the projects for acceleration domain names.

Note:

If your application has been migrated to the CDN console, you can go to the console for operation by referring to Content Delivery Network.

Enabling Acceleration Service

You can **activate** a **deactivated** domain name in the following steps. It takes about 5 minutes to enable the acceleration service.

Log in to the ECDN Console and click **Domain Management** on the left sidebar to enter the **Domain Management** page. In the "Operation" column of the target domain name, click **Activate**.

Domain Name Management							
i If you add or disable a domain na	ime, the system will de	ploy relevant configuration for the dom	ain name on the backend. The co	nfiguration takes about 5 minutes to tak	xe effect.		
Create Distribution Purge	Enable ECDN Servi	ce More Operations			Please enter the prefix to query Q		
Domain Name	Status T	CNAME	Project T	Acceleration Region T	Operation		
	(i) Disabled	$\mathcal{A}_{i}^{i}(\mathbf{x})$, where \mathbf{x} is the $i=1,\ldots,n$	Default Project	Mainland China	Manage Enable More -		

If you want to activate multiple acceleration domain names in batches, you can check them and click **Activate ECDN** above.

🕗 Tencent Cloud

Domain Name Management

() If you add or disable a domain name, the system will deploy relevant configuration for the domain name on the backend. The configuration takes about 5 minutes to take effect.								
Create Distribution Purge	Enable ECDN Ser	/ice More Operations ▼			Please enter the prefix to query	Q		
Domain Name	Status ⊤	CNAME	Project T	Acceleration Region T	Operation			
 The second state of the second second	(i) Disabled	$d = \log^2 k^2$ with $k \ge 0$, where $k \ge 0$	Default Project	Mainland China	Manage Enable More 🔻			
 Contracting out 	(j) Disabled	and a second of the second	Default Project	Mainland China	Manage Enable More 🔻			

Disabling Acceleration Service

You can **deactivate** an **activated** domain name in the following steps. After the domain name is deactivated, it will no longer be accelerated, but its configuration will be retained. It takes about 5 minutes for domain name deactivation to take effect.

Log in to the ECDN Console and click **Domain Management** on the left sidebar to enter the **Domain Management** page. In the "Operation" column of the target domain name, click **Deactivate**.

Domain Name Management							
i If you add or disable a domain name, the system will deploy relevant configuration for the domain name on the backend. The configuration takes about 5 minutes to take effect.							
Create Distribution Purge	Enable ECDN Servi	ce More Operations 💌			Please enter the prefix to query Q		
Domain Name	Status T	CNAME	Project T	Acceleration Region T	Operation		
🗌 ne statutet	Enabled	- and short around a sec-	Default Project	Mainland China	Manage Close More 🔻		
🗌 ta El festivi cara	Enabled	σ is the decise of the σ .	Default Project	Mainland China	Manage Close More 🔻		

If you want to deactivate multiple acceleration domain names in batches, you can check them and select **Deactivate ECDN** in the **More Actions** drop-down list above.

Note :

Before disabling the acceleration service, make sure that your domain names have been resolved to the origin server, as ECDN nodes will no longer provide acceleration service for them and will directly return the status

code 404 for received user requests after acceleration is disabled. To avoid affecting your user access experience, you are recommended to perform the following steps when disabling the acceleration service:

1. Change the acceleration domain name resolution

Resolve the acceleration domain name to the origin server and make sure that it will not be resolved to the ECDN domain name through the CNAME record. Change of the domain name resolution generally takes 10–30 minutes to take effect in most regions.

2. Check the traffic change

After the domain name resolution is switched to the origin server, user requests will no longer be forwarded to the ECDN acceleration platform. In the ECDN Console, you can see that the access traffic of the corresponding domain name will drop significantly. Before disabling the service, please confirm that the ECDN access traffic of the corresponding domain name has decreased to 0; otherwise, directly disabling the service will affect user access.

3. Disable the acceleration service

Domain Name Management

() If you add or disable a domain n	ame, the system will de	eploy rel	levant configuration for the dom	ain name on the backend. The o	configuration takes about 5 minutes to ta	ke effect.	
Create Distribution Purge	Enable ECDN Serv	vice	More Operations			Please enter the prefix to query	Q
Domain Name	Status T	CNA	Disable ECDN Service	Project T	Acceleration Region T	Operation	
🗹 in Colorad	C Enabled	test1	Delete	Default Project	Mainland China	Manage Close More -	
 In the first set of the set 	C Enabled	- 1	Pland shin, e. a. Jan	Default Project	Mainland China	Manage Close More -	

After confirming that all or most users no longer use ECDN for access, you can deactivate the domain name in the following steps:

Note :

- Domain name deactivation will affect user access. Please do so with caution.
- After the domain name resolution is switched to the origin server, user requests may still be forwarded to ECDN cache nodes, as local DNS servers of a minority of users do not follow the domain name TTL rule. In this case, those users need to change their local DNS server addresses or set hosts resolution.
- Generally, you are recommended to switch the domain name resolution to the origin server first and then disable the domain name acceleration service after 24 hours.

Deleting Acceleration Domain Name

You can delete a deactivated domain name. Its configuration will not be retained upon deletion.

Log in to the ECDN Console and click **Domain Management** on the left sidebar to enter the **Domain Management** page. In the "Operation" column of the target domain name, select **Delete** in the **More** drop-down list.

Domain Name Management								
(i) If you add or disable a domain name, the system will deploy relevant configuration for the domain name on the backend. The configuration takes about 5 minutes to take effect.								
Create Distribution Purge	Enable ECDN Servio	ce More Operations -			Please enter the prefix to query			
Domain Name	Status T	CNAME	Project T	Acceleration Region T	Operation			
	(i) Disabled	$\sim 10^{-10}$ of the large standard 1	Default Project	Mainland China	Manage Enable More -			
	(i) Disabled	nany na analy and analogue .	Default Project	Mainland China	Manage Et Modify Project			

If you want to delete multiple acceleration domain names in batches, you can check the target domain names and select **Delete** in the **More Actions** drop-down list above.

Domain Name Management								
() If you add or disable a domain name, the system will deploy relevant configuration for the domain name on the backend. The configuration takes about 5 minutes to take effect.								
Create Distribution Purge	Enable ECDN Servic	e	More Operations 🔻			Please enter the prefix to query	Q	
Domain Name	Status T	CNA	Disable ECDN Service	Project T	Acceleration Region T	Operation		
🗹 langun anangan	(i) Disabled	wit	Delete .	. Default Project	Mainland China	Manage Enable More -		
🗹 makanta man	(i) Disabled		nini ana ina a	. Default Project	Mainland China	Manage Enable More 🔻		

Modifying Project of Domain Name

To facilitate management, you can modify the project of your domain name in the following steps.

 Log in to the ECDN Console and click Domain Management on the left sidebar to enter the Domain Management page. In the "Operation" column of the target domain name, select Modify Project in the More



drop-down list.

Domain Name Management								
If you add or disable a domain name, the system will deploy relevant configuration for the domain name on the backend. The configuration takes about 5 minutes to take effect.								
Create Distribution Purge	Enable ECDN Ser	vice More Operations 🔻			Please enter the prefix to query Q			
Domain Name	Status ⊤	CNAME	Project T	Acceleration Region \mathbf{T}	Operation			
Land of the grant	C Enabled	$(m^{2})^{2}$ with $(m^{2}_{\rm B})^{2}$ and $(m^{2}_{\rm B})^{2}$ and	Default Project	Mainland China	Manage Close More 🔻			
 conversion services care 	C Enabled	и такин алаандаган алаан	Default Project	Mainland China	Manage C Modify Project			

2. The **Project** drop-down list will be displayed in the pop-up dialog box. You need to select a project for the domain name. Click **OK** to modify the domain name's project.



If you want to modify the project of multiple acceleration domain names in batches, you can check the target domain names and select **Modify Project** in the **More Actions** drop-down list above.

Domain Name Management								
If you add or disable a domain name, the system will deploy relevant configuration for the domain name on the backend. The configuration takes about 5 minutes to take effect.								
Create Distribution Purge	Enable ECDN Servi	ce More Operations	·		Please enter the prefix to query	Q		
Domain Name	Status ⊤	CNA Disable ECDN Service	Project ⊤	Acceleration Region T	Operation			
 International system 	C Enabled	test1 Delete	Default Project	Mainland China	Manage Close More -			
 Antipatrical state 	C Enabled	an and that signal we are	Default Project	Mainland China	Manage Close More 🔻			

Note:

- You can use the project feature to manage Tencent Cloud resources by project. Tencent Cloud Project Management can be applied to multiple products at the same time.
- You can create and modify projects on the Account Center Project Management page in the Tencent Cloud Console.

Configuration Management Configuration Overview

Last updated : 2020-04-28 14:50:49

This document describes how to configure ECDN. You can set ECDN as needed to optimize the acceleration performance.

Basic Configuration

Configuration Name	Document Description
Getting Started	It describes how to activate the service and quickly connect domain names to the service.
Domain Name Connection Configuration	It describes how to connect a domain name to ECDN for acceleration.
CNAME Record Configuration	It describes how to configure a CNAME record.
Domain Name Status Switch	It describes how to enable, disable, and delete domain name acceleration service.
Project Configuration	It describes how to modify a domain name's project and acceleration region.
Origin Server Configuration	It describes how to change the origin server type to origin IP or origin domain.

Advanced Configuration

Configuration Name	Document Description
HTTPS Settings	ECDN supports HTTPS configuration to implement secure acceleration.
HTTP Header Configuration	HTTP header configuration can be added, which will affect the browser's response behaviors.
Cache Rule Configuration	Static cache policies can be configured for domain names with both dynamic and static content.
Alarm Monitoring Configuration	The acceleration service can be monitored and configured with alarms.

Configuration Name	Document Description
Advanced Origin-Pull Configuration	Advanced origin-pull policies based on weight and master/slave architecture are supported.

Basic Configuration

Last updated : 2021-12-13 17:38:45

You can view basic information and origin server information of a domain name in the ECDN Console. You can modify **Project**, **Origin Server Type**, and **Origin Server Address** of the domain name as needed.

- Basic information includes the acceleration domain name, CNAME record, project, and creation time of the acceleration service.
- Origin server information includes origin server type and origin server address.

Note:

If your application has been migrated to the CDN console, you can go to the console for operation by referring to Content Delivery Network.

Domain Name Configuration Page

- 1. Log in to the ECDN Console and click **Domain Management** on the left sidebar to enter the management page.
- 2. Select Manage on the right of the target configuration domain name to enter the domain name configuration page.

Domain Name Management						
() If you add or disable a domain n	ame, the system will d	eploy relevant configuration for the do	omain name on the backend. The	configuration takes about 5 minutes to	take effect.	
Create Distribution Purge	Enable ECDN Ser	vice More Operations •			Please enter the prefix to query	Q
Domain Name	Status T	CNAME	Project T	Acceleration Region T	Operation	
	C Enabled		Default Project	Mainland China	Manage Close More •	

3. The **Basic Info** page of the domain name displays its basic configuration information, including the CNAME record, project, acceleration region, origin server information, and origin domain.



	Cache Configuration	Access Configuration	Advanced Configuration
Basic Information			
Domain Name	j.c	com	
CNAME	t.	.com	
Project	Default Project Mo	odify 🎤	
Acceleration Region	Mainland China. M	lodify 🎤	
Time Created	2020-04-24 16:05:	52	
Origin Server Inform	natior Modify 🖍		
Origin Server Type	Domain Origin Ser	ver	
Origin Server Type Origin-pull Policy	Domain Origin Ser	ver	
Origin Server Type Origin-pull Policy Origin-pull Protocol	Domain Origin Ser - HTTP	ver	
Origin Server Type Origin-pull Policy Origin-pull Protocol Origin Server Address	Domain Origin Ser - HTTP	ver	
Origin Server Type Origin-pull Policy Origin-pull Protocol Origin Server Address Secondary Origin Server Address	Domain Origin Ser - HTTP -	ver .com	
Origin Server Type Origin-pull Policy Origin-pull Protocol Origin Server Address Secondary Origin Server Address	Domain Origin Ser - HTTP	ver .com	
Origin Server Type Origin-pull Policy Origin-pull Protocol Origin Server Address Secondary Origin Server Address	Domain Origin Ser - HTTP -	ver .com	

Basic Configuration Project

Modifying project of domain name

- 1. Click **Modify** on the right of the project.
- 2. In the pop-up window, select the target project name, and click $\ensuremath{\text{OK}}$.

Modifying domain name acceleration region

1. Click $\ensuremath{\textbf{Modify}}$ on the right of the acceleration region.

- 2. Select a domain name acceleration region. Currently, Mainland China, outside Mainland China, or global can be selected.
- 3. To avoid faulty operations, if you need to delete configuration of an acceleration region, please submit a ticket to apply for modification.

Note :

The acceleration service outside Mainland China is currently in beta test. If your account cannot modify the acceleration region, it indicates that you have not been granted the acceleration permission outside Mainland China. You can submit an application on the ECDN global acceleration eligibility application page, and we will review it in 5 business days and inform you of the result through SMS or internal message.

Modifying origin server configuration

- 1. Click "Modify" on the right of the origin server configuration to enter the origin server modification page.
- 2. In the pop-up window, modify your origin server type, origin-pull policy, and origin server address. For more information, please see Advanced Origin-Pull Policies.
- 3. After the modification is completed, click **OK** to submit the configuration. The system backend will distribute the new origin server modification to the domain name, which will take effect in 3–5 minutes.

Origin Server Type	Origin Server IP Origin Server Domain
Origin-pull Policy	Optimal Origin-pull Oweighted Origin-pull Primary/Secondary Origin-pull
Origin-pull Address	Please enter the IP list
	Multiple origin server IPs can be set (one IP per line); ports 1-65535 are supported
Origin-pull Protocol	Multiple origin server IPs can be set (one IP per line); ports 1-68

Modifying origin-pull configuration



Click Edit next to the origin domain and modify it in the dialog box:



Cache Configuration

Last updated : 2021-08-12 10:18:01

Features

ECDN can automatically identify static and dynamic content access requests based on the configured rules and intelligently apply an appropriate acceleration scheme, satisfying your needs for accelerating access to sites with static, dynamic or hybrid content at one stop.

- For static content requests, the edge servers are preferentially used to cache the content for response, improving access efficiency and reducing origin-pull traffic usage.
- For dynamic content requests, resources are directly pulled from the origin servers through high-quality origin-pull and intelligent routing, lowering the average response latency.

Note:

If your application has been migrated to the CDN console, you can go to the console for operation by referring to Content Delivery Network.

Directions

- 1. Log in to the ECDN Console and click **Domain Management** on the left sidebar to enter the management page.
- 2. In the list, find the domain name to configure and click **Manage** under the "Operation" column on the right to enter the domain management page.
- 3. On the "Cache Configuration" page, you can configure the content caching rules.
 - Ignore Query String cache configuration:

You can enable Ignore Query String cache to ignore parameters after "?" in a user request URL during caching. Suppose that content of the URL http://www.example.com/1.jpg?version=1.1 is cached on nodes. When a user request comes in the cache, the cache_key www.example.com/1.jpg will be looked up to



return a direct hit.

Basic Information	Cache Configuration	Access Configuration	Advanced Configuration
Ignore Query String	I		
If the query string is ignored when caching content, the string after "?" in the requested URL will be filtered. Enable Ignore Query String			

• Content cache configuration:

Click Edit Cache Rule to add a caching rule or modify an existing one and click Save for the rule to take effect.

Cache Configuration		
Edit Cache Rule Cache purge time>0: static content; edge caching is enabled for near Cache purge time=0: dynamic content; the ECDN acceleration route is	by access to content. s adopted for requests.	
Туре	Content	Cache Purge Time
All		0 Day(s)
File Type	gif,png,bmp,jpg,jpeg,mp3,wma,flv,mp4,wmv,avi,m3u8,ts	1 Day(s)
File Type	doc,docx,xls,xlsx,ppt,pptx,txt,pdf	1 Day(s)
File Type	exe,apk,ipa,rar,zip,7z,css,js,xml,ini,swf,ico	1 Day(s)

Caching rule types

Cache Type	Description	Example	Remarks
File type	Sets the caching time based on file extension	.jpg;.png;.jsp	 The content is case-sensitive and must be a file extension starting with . Different file extensions should be separated with ; .
Folder	Sets the caching time based on folder	/access;/pic	 The content is case-sensitive, and different paths should be separated with ; . It must be a folder starting with / . It cannot end with / .
Full-path file	Sets the caching time for a specified file	/a.jpg;/b.png	1. The content is case-sensitive, and files at different paths should be separated with ; .



			 2. * can be used to match a type of files by regex, such as /test/abc/*.jpg 3. It must be a folder starting with / .
Homepage	Sets the caching time for the homepage	/	The homepage content to cache is / by default and does not need to be modified.

Cache purge time

Description

- Cache purge time can be set by second, minute, hour, and day (up to 365 days).
- If the cache purge time is 0, requests from the dynamic content will be directly passed through to the origin server, and the response content will not be cached.
- If the cache purge time is greater than 0, requests come from the static content, and the edge caching feature will be enabled:
 - If the content accessed by the user has been cached on the edge server and the cache has not expired, the cached content can be directly accessed without making a request to the origin server.
 - If the content accessed by the user has not been cached on the edge server or the cache has expired, the content will be accessed after making a request to the origin server, and then will be cached on the edge server.

File Type	Scenario Example	Recommended Caching Time
Basically unchanged static content	Images and audio/video files	Set the cache purge time to 30 days.
Static content that needs updates	Files in formats such as .js and .css	Set the caching time of days or hours based on the update frequency.
Dynamic content that is frequently updated and shared by users	Weather queries and region-specific content	Set the caching time of minutes or seconds.
Content that is dynamically generated or cannot be accessed repeatedly by the same user	User registration and login APIs	Set the caching time to 0 to disable caching.

Suggested setting

Caching rule priority

You may get more than one hit result at the same time due to overlaps between caching rules you defined. Given this possibility, the setting of caching rule priority is included.

- Rules at the bottom of the configuration list take priority over those on the top. A new caching rule takes the highest priority.
- A user request will be matched with caching rules by rule priority from high to low. The first hit rule determines the cache purge time of the request.
- You can adjust the priority of rules as needed.

Click Edit Cache Rule. You can drag the icon to change the rule priority.

Cache Configuration

Cache purge time>0: static content; Cache purge time=0: dynamic content Use ";" to separate different contents and do not end it with "/". For example: ".gif;.png" (file type), "/text;/a/b/c" (folder), and "/index.html;/text/*.jpg" (full-path file).

Drag	Туре	Content	Cache Purge Time	Operation
* *	All	· 😔	0 Day(🔻 🧭	
	File Type 🛛 🔻	.gif;.png;.bmp;.jpg;.jpeg;.mp3;.wr	1 Day(🔻 🥥	Delete
	File Type 🔹	.doc;.docx;.xls;.xlsx;.ppt;.pptx;.tx	1 Day(🔻 🥑	Delete
	File Type 🔻	.exe;.apk;.ipa;.rar;.zip;.7z;.css;.js;	1 Day(🔻 🥑	Delete
Add Casha Du	drag up or down to a	adjust priority		

Rules are executed from bottom to top. Rules at the bottom of the list have higher priority. You can drag to adjust the order.

Cache Inheritance

If you configure edge caching for static content, the ECDN system will handle static requests with the caching rules configured. ECDN nodes will not inherit and process the Cache-Control field in the response header from the origin server by default, and will not cache the content if this field is private, no-store or no-cache.

Access Control IP Access Limit Configuration

Last updated : 2021-08-05 12:05:19

Configuration Scenario

To control the source of access to your business resources, you can use the IP access limit feature in ECDN. By limiting the number of access requests to a node per second from a client IP, you can defend against high-frequency CC attacks and prevent hotlinking by malicious users.

Note:

If your application has been migrated to the CDN console, you can go to the console for operation by referring to Content Delivery Network.

Configuration Guide

Viewing configuration

Log in to the ECDN Console, select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. You will find the IP access frequency limit configuration in **Access Configuration**. It is disabled by default:



Modifying configuration

1. Modify the configuration



Enter the frequency threshold and click OK to enable IP access limit.



Configuration description

- After the configuration is enabled, a 514 error will be returned for requests that exceed the QPS limit. A low access
 frequency limit may impact the normal use of your business by high-frequency users. Configure the proper
 threshold according to your actual business conditions and use cases.
- IP access limit is effective for attacks from a single IP to a single node. If a malicious user uses a high number of IPs to attack nodes on your entire network, this feature is no longer applicable.

2. Disable the configuration

You can switch to disable this feature. When the switch is off, this feature does not take effect in the production environment even if there is an existing configuration. When the switch is on, this configuration will take effect across the entire network:



Configuration Sample

Suppose the IP access limit for the acceleration domain name www.test.com is as follows:

IP Access Limits				
Set QPS limits for on	Set QPS limits for one IP to one node to defense CC attacks. What's IP access limit? 🗹			
IP Access Limit	Edit			
IP Access Limit	1QPS			

The actual access status will be as follows:

- 1. If a user with client IP 1.1.1.1 requests the resource http://www.test.com/1.jpg for 10 times in one second, and all access requests are made to one server on ECDN cache node A, then 10 access logs will be generated on this server, 9 of which exceed the QPS limit, and the status code "514" will be returned.
- 2. If a user with client IP 2.2.2.2 requests the resource http://www.test.com/1.jpg twice in one second, and the access requests may be distributed to two ECDN cache nodes for processing due to network conditions, then each node will return the content normally.

IP Blocklist/Allowlist Configuration

Last updated : 2021-09-22 14:37:54

Configuration Scenario

To control the source of access to your business resources, you can use the IP blocklist/allowlist feature in Tencent Cloud ECDN.

By configuring an access control policy on IPs of user requests, you can effectively control the source of access to prevent hotlinking by malicious IPs, attacks, etc.

Note:

If your application has been migrated to the CDN console, you can go to the console for operation by referring to Content Delivery Network.

Configuration Guide

Viewing configuration

Log in to the ECDN Console, select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. You will find the IP blocklist/allowlist configuration in **Access Configuration**.



Modifying configuration

1. Modify the configuration



Click **Edit** to select "IP Blocklist" or "IP Allowlist", enter the list of IPs or IP ranges, and click **OK** to enable IP blocklist/allowlist configuration:



IP blocklist

If a client IP matches an IP or IP range in the blocklist, the accessed ECDN node will directly return a 403 status code.

IP allowlist

If a client IP does not match any IP or IP range in the allowlist, the accessed ECDN node will directly return a 403 status code.

Blocklist/Allowlist rules

- The IP blocklist and allowlist are mutually exclusive and cannot be configured at the same time.
- Only IP ranges /8 , /16 , \24 , and /32 are supported.
- The blocklist/allowlist does not support entries in IP:port format and can contain up to 50 entries.

Configuration Sample



Suppose the IP blocklist/allowlist of the acceleration domain name www.test.com is as follows:

IP Blacklist & Whitelist		
Set an IP blacklist and whitelist to filter requesting IPs. What't IP blacklist and whitelist? 🖬		
IP Blacklist & Whitelist Edit IPWhitelist		
2.2.2.2 1.0.0.0/8		

The actual access status will be as follows:

- 1. When a user with client IP 1.1.1.1 accesses the resource http://www.test.com/test.txt , as the IP matches an IP in the allowlist, the requested content will be returned.
- 2. When a user with client IP 2.1.1.1 accesses the resource http://www.test.com/test.txt, as the IP
 does not match any IP in the allowlist, a 403 status code will be returned.

Advanced Configuration Configure HTTP Header

Last updated : 2021-08-05 12:21:37

Note :

If your application has been migrated to the CDN console, you can go to the console for operation by referring to Content Delivery Network.

An HTTP message generally contains:

- Request message sent from client to server.
- Response message sent from server to client.

These messages all consist of a beginning line, one or multiple headers, a blank line indicating the end of headers, and an optional message body.



HTTP headers divide into common header, request header, response header, and entity header. Each header consists of a domain name, colon (":"), and domain value, such as Connection:keep-alive.

If you use the HTTP header configuration feature provided by ECDN, when an end user requests a business resource, you can add a custom header in the returned **response message** to implement cross-origin access.

Note:

- As the HTTP header configuration is for a specified domain name, once the configuration takes effect, the configured header will be added to the response messages of user requests for any resource under this domain name.
- HTTP header configuration affects only response of the client (such as browser) rather than ECDN node's caching behaviors.

Configuration Description

ECDN allows you to configure the following headers:

- Content-Disposition: it activates download in the browser and sets the default filename of the downloaded file.
- Content-Language: it specifies the language used in the client (such as browser) response for the resource.
- Access-Control-Allow-Origin: it specifies the sources of cross-origin requests allowed to access the resource.
- Access-Control-Allow-Methods: it specifies the allowed methods of cross-origin requests.
- Access-Control-Max-Age: it specifies the validity period for caching the returned result of preflight request for a particular resource when a cross-origin request is initiated.
- Access-Control-Expose-Headers: it specifies the headers visible to the client when a cross-origin request is initiated.

General configuration

Content-Disposition

Content-Disposition is used to activate download in the browser and set the default filename of the downloaded resource. When the server sends a file to the client browser, if it is in a type supported by the browser, such as .txt or .jpg, it will be directly opened in the browser by default. If you want to ask the user to save the file, you can configure the Content-Disposition field to override the browser's default behavior. The common configuration is Content-Disposition:attachment; filename=FileName.txt

Content-Language

Content-Language specifies the code of the language used by the webpage. Common configurations are as follows:

- Content-Language: zh-CN
- Content-Language: en-US

Cross-Origin access configuration

Cross-origin access refers to a scenario where a resource under a domain name, such as www.abc.com , initiates a request to another resource under another domain name, such as www.def.com . As the resource domain names are different, **cross-origin access** will occur. Using different protocols or ports can cause cross-origin access. You need to add configuration related to cross-origin access in the response header to make the first resource get the desired data.

Access-Control-Allow-Origin

Access-Control-Allow-Origin is used to solve the problem of cross-origin permissions of resources. Its value specifies the origins that can access the resource. You can also set the wildcard $\uparrow \star$ to allow all origins to access the resource. Common configurations are as follows:

- Access-Control-Allow-Origin: *
- Access-Control-Allow-Origin: http://www.test.com

Pay attention to the following limits when configuring Access-Control-Allow-Origin :

- Do not use wildcard domain names, e.g., *.qq.com .
- Only configure it as $\$ or specify a URI.
- When configuring a specified domain name, add the "http://" or "https://" prefix.

Access-Control-Allow-Methods

Access-Control-Allow-Methods is used to specify the HTTP request methods allowed for cross-origin access. Multiple methods can be set as follows:

Access-Control-Allow-Methods: POST, GET, OPTIONS

Access-Control-Max-Age

Access-Control-Max-Age specifies the validity period of a preflight request.

For a non-simple cross-origin request, before the formal communication, an HTTP query request called "preflight request" needs to be made to check whether the cross-origin request is secure and acceptable. The following requests are considered as non-simple cross-origin requests:

- The request is initiated in a method other than GET , HEAD , and POST or is initiated by using POST with a data type other than application/x-www-form-urlencoded , multipart/form-data , and text/plain , such as application/xml Or text/xml .
- A custom request header is used.

Access-Control-Max-Age is measured in seconds. Here, the configuration sample Access-Control-Max-Age: 1728000 indicates that no more preflight requests will be sent for the cross-domain access to this resource within 1,728,000 seconds (20 days).



Access-Control-Expose-Headers

Access-Control-Expose-Headers specifies which headers can be accessed when a cross-region request is initiated. By default, the following six types of headers can be exposed to the client:

- Cache-Control
- Content-Language
- Content-Type
- Expires
- Last-Modified
- Pragma

If you want the client to access other header information, you can set as follows (separate multiple headers with ;):

```
Access-Control-Expose-Headers: Content-Length, QCloud-DSA-MyCustom-HeaderY
```

 Then, the server will allow requests to contain the
 Content-Length
 and
 QCloud-DSA-MyCustom-HeaderY

 fields.

Custom header

ECDN allows you to add custom headers as needed. The following fields cannot be added currently:

```
Date
Expires
Content-Type
Content-Encoding
Content-Length
Transfer-Encoding
Cache-Control
If-Modified-Since
Last-Modified
Connection
Content-Range
ETag
Accept-Ranges
Aqe
Authentication-Info
Proxy-Authenticate
Retry-After
Set-Cookie
Vary
WWW-Authenticate
Content-Location
Content-MD5
```



Content-Range
Meter
Allow
Error

Configuration process

- 1. Log in to the ECDN Console and click **Domain Management** on the left sidebar. On the management page, click **Manage** on the right of the target domain name to enter the domain management page.
- 2. Click Advanced Configuration and click Add HTTP Header in the HTTP Header Configuration module.

Basic Information	Cache Configuration	Access Configuration	Advanced Configuration
HTTPS Configurati	on		
HTTPS provides identit You have not set HTTP: Go to Settings	y verification for network serve	r, in order to protect the privacy a	and integrity of data exchange.How to set HTTPS? 🛂
HTTP Header Conf	figuration		
The configuration of HT Add HTTP Header	TP Header may affect the resp	onses from client programs (bro	wser)How to set the HTTP Header? 🛛

In the pop-up window, select the HTTP header to be added and enter the corresponding value. You can click Add
 Parameter to add more header fields. Click OK to submit the settings.

arameter	Value	Operatio
Access-Control-Allow-Origin	▼ * or a domain name (e.g., http(s)://www.abc.com)	
l Parameter +		

4. The configuration will take effect in about 5 minutes. In the table at the bottom, you can view the added HTTP headers. You can click **Modify** or **Delete** on the right of a header to perform the corresponding operation as needed.

HTTP Header Configuration				
The configuration of HTTP Header may affect Add HTTP Header	the responses from client programs (browser)How to set the H	TTP Header? 🖸		
Header Parameter	Settings	Operation		
Access-Control-Allow-Origin		Modify Delete		

5. You can click Add HTTP Header to add more HTTP headers, each of which can be added only once.

HTTPS Setting

Last updated : 2021-08-05 12:26:43

Configuration Description

HTTPS refers to Hypertext Transfer Protocol Secure, which is a security protocol that encrypts and transfers data based on the HTTP protocol to ensure the security of data transfer. When configuring HTTPS, you need to provide a certificate for the domain name and deploy it on all ECDN nodes to implement encrypted data transfer across the network.

Note:

- Your domain name should have been connected to ECDN, and the status should be **deploying** or **activated**.
- If your application has been migrated to the CDN console, you can go to the console for operation by referring to Content Delivery Network.

Adding Configuration

Selecting domain name

- 1. Log in to the ECDN Console and click Domain Management on the left sidebar to enter the management page.
- 2. From the list, choose the domain name to configure, click **Manage** to enter your domain details, then select **Advanced Configuration**.
- 3. To use HTTPS, you need to deploy the domain name certificate first. Click **Go to Settings** to enter the certificate configuration page.



Basic Information	Cache Configuration	Access Configuration	Advanced Configuration
HTTPS Configurat	ion		
HTTPS provides identi You have not set HTTP Go to Settings	ty verification for network serve	r, in order to protect the privacy	and integrity of data exchange. How to set HTTPS?

Configuring certificate

On the certificate configuration page, your domain name can be configured with your certificate or a certificate hosted by Tencent Cloud. For more details, please refer to Certificate Management.



Select a Certi	ficate		
Certificate Source	O Self-owned Certificate	O Tencent Cloud-hosted Cer	tificate
Certificate Content	View Sample 🔀		
Private Key Content	View Sample 🗳		
Remark (optional)			

Modifying Configuration

• Enabling HTTP2.0:

To use HTTP2.0 for your configured domain name, enable it on the advanced configuration page.

• Enabling force HTTPS redirection:

To force any HTTP request to redirect to HTTPS, enable it for your configured domain name. You can also specify the status code to redirect, either 301 or 302 (default).

Modifying certificates and redirection:

To modify your certificate or redirection for your configured domain name, click **Go to Configuration** to enter the certificate management page.

HTTPS Configuration					
HTTPS provides identity verification for network server, in order to protect the privacy and integrity of data exchange. How to set HTTPS? 🛂					
HTTP 2.0 Enabled					
Forced Redirect to HTTPS 302I	Redirect Edit 🎤				
Certificate Source	Certificate Remark	Expiry Time	Origin-pull Method	Certificate Status	Operation
Self-owned Certificate	-	2020-10-22 20:00:00	HTTPOrigin-pull	Deployed successfully	Go to Configuration 🛂

Alarm Monitoring Configuration

Last updated : 2021-08-05 12:46:34

Note:

If your application has been migrated to the CDN console, you can go to the console for operation by referring to Content Delivery Network.

Description of Connecting ECDN to Cloud Monitor

ECDN has been connected to Tencent Cloud Monitor. The following alarming metrics are supported in the current version:

Category	Metric	1-Minute Alarming Granularity Supported	5-Minute Alarming Granularity Supported
	Total number of requests	Yes	Yes
Access traffic metrics	Access bandwidth	Yes	Yes
	Access traffic (upstream)	Yes	Yes
	Access traffic (downstream)	Yes	Yes
Origin-pull traffic metrics	Total number of origin-pulls	Yes	Yes
	Number of failed origin-pull	Yes	Yes
	Origin-pull failure rate	Yes	Yes
	Origin-pull bandwidth	Yes	Yes
Access performance metrics	Average response time	Yes	Yes
Status code metrics	Number of 200, 206, 2XX, etc. status code occurrences and their ratio	Yes	Yes
	Number of 302, 304, 3XX, etc. status code occurrences and	Yes	Yes


their ratio		
Number of 401, 403, 404, 416, 4XX, etc. statu occurrences and their ratio	s code Yes	Yes
Number of 500, 502, 5XX, etc. status code occurr their ratio	ences and Yes	Yes

Note:

- You can activate and use Cloud Monitor free of charge.
- The system sends alarm messages through email, WeChat, and callback APIs free of charge, and you can enjoy a free tier of SMS alarm messages every month.
- If the monthly free tier of SMS alarm messages is exceeded, you need to purchase a higher tier for receiving more alarm messages through SMS.
- Alarm data is collected and reported in real time and may have certain deviation, as the data is delayed for about 5 minutes.
- Alarm data monitoring can be used only to assist in operation and cannot be used as the basis for billing or SLA.

Monitoring Configuration Entry



Log in to the Cloud Monitor Console and click **Alarm Policy** on the left sidebar to enter the management page.

Alarm Policy							Alarm Policy Use 0	Buide
Policy Name		Product/Policy Type	Product Type *	Please select	•			
Alarm Object	*	User Group	User group 👻	Please select	*	Query	Clear filter	
The alarm template function is available Alarms are started and stopped for alarm	now and supports the multiple use and un policies. Alarm policy can be masked in	unified modification of n policy dimensions a	f trigger conditions. I Ind instance dimensi	Please go to Trigger C ons. Click to view Alar	andition Template to co m On-Off Document	nfigure. Details		
Add Delete Modify	/ Alarm Channel						¢ ¢	Ŧ
Policy Name Trigger	Condition Project T Po	licy Type E	inabled/Instan	Last Modified \$	Alarm Channel	Alarm On-Off	Operation	
PrivateB GuestRe	landwidt DEFAULT PROJ Clo Ibcot, n	ud Virtual Ma 07	/0	100000824047 2020/04/13 11:3	Receiver group:1 Validity:00:00:00 - : Channel:Email, SP		Replication Delete	
en-policy-insGroup CPUUSIE DiskRear	ization > DEFAULT PROJ Clo donly, n	ud Virtual Ma 1 / Gr	/ 2 roup: copy-ttss1	100000624047 2020/04/10 18:3	Receiver group:1 Validity:00:00:00 - ; Channel:Email, SP		Replication Delete	
mingoccocccc CPUUtile GuestRe	ization > bbcot, n DEFAULT PROJ Clo	ud Virtual Me 07	/0	100000624047 2020/04/10 18:3	Receiver group:1 Validity:00:00:00 - ; Channel:Email, S#		Replication Delete	

Adding Alarm

The steps for adding an alarm policy are as follows:

1. Enter the policy name and remarks and select the ECDN alarm policy type.

Policy Name	1-20 Chinese, English chars or underlines
Remarks	1-100 Chinese and English characters or underlines
Delieu Tress	
Policy Type	
Project	DEFAULT PROJECT Existing: 38 item(s) and you can also create 262 polici

2. Select the alarm object.

Alarm Object	All Objects
	 Select some objects(0 selected)
	Select instance group Create instance group
	Region: Beijing Project: DEFAULT PROJECT Q
	ID/Name Network Type IP

3. Set the alarm trigger condition. Multiple conditions can be set at a time.

Trigger Condition	Trigger Condition Template Add Trigger Condition Template
	Configure trigger conditions
	if CPUUtilization Measurement Pe Vert > Vert 0 % Continuous1 then Alarm occurs every 1
	DiskReadonly Add



4. Set the alarm recipient, alarm time period, and alarm method.

Alarm Channel	Recipient Object	Recipient Group 🔻	Q Add Recipient Group	
		User Group Name	User Name	
		izzie	izzie	
		coswang	chen-test	
		[] II	Not set	
		88888	chen-test	
		99999	cym-inter-test、chen-test、toto、xiaowei、anitaxcli_wx、v_chengming	
	Valid Period	00:00:00 to 23:59:59		
	Receiving Channel	🗹 Email 🔽 SMS 🗌 Pho	one	

5. Set the alarm callback API.

Port Callback	http v such as console.cloud.tencent.com:8080/callback v
(optional)	Input the URL that can be accessed by the public network as the callback API address (domain name or IP[:port][/path]), and the cloud monitor will push the alarm information to this address in time.
	The callback domain name takes effect after verification. Please return the following code in the Response Body.
	en al frances de la companya de la c
Complete	

6. Click **Complete** to submit the settings.

Viewing Alarm



On the historical alarm page in Cloud Monitor, you can view the list of alarm details.



Other Alarm Policies

For more information on how to configure alarm policies, please see Creating Alarm Policies.

Origin-Pull Management Advanced Origin-Pull Policies

Last updated : 2021-08-05 12:51:05

ECDN supports the following advanced origin-pull policies:

Optimal origin-pull

The best-performing origin server is selected for origin-pull based on the detection result.

• Weighted origin-pull

Requests are assigned by weight for origin-pull based on the detection result.

Primary/secondary origin-pull

Your primary origin server is always a preferential option. The secondary works only if the primary is exceptional.

You can select one that is appropriate for your business needs.

Note:

- The default policy for ECDN is optimal origin-pull.
- The origin type can be set to origin IP or origin domain when you use any one of three origin-pull policies.
- The actual weight for weighted origin-pull may be slightly different from the set as your requests are being taken care of.
- In a primary/secondary origin-pull, the secondary will be automatically triggered by a status code of 400–599 (except for 416) from the primary.
- If your application has been migrated to the CDN console, you can go to the console for operation by referring to Content Delivery Network.

Adding Advanced Origin-Pull Policy

1. Optimal origin-pull



Optimal origin-pull is set as the default policy of the platform.

ECDN	Create Distribution	pution
Overview		
W. Domain Name Management	Domain Name Con	figuration
C Statistics	Add Acceleration Domain Name	Please enter the acceleration domain
✓ Cache Purge		Add
Certificate Management		Note: the origin servers of all added domain names should be exactly the same
Log Management	Project	Default Project
	Origin Server Type	Origin Server IP Origin Server Domain
	Origin-pull Policy	Optimal Origin-pull Oweighted Origin-pull Primary/Secondary Origin-pull
	Origin-pull Address	Please enter the IP list
		Multiple origin server IPs can be set (one IP per line); ports 1-65535 are supported
	Origin-pull Protocol	HTTP 🔻

Note :

You cannot use the same domain name for your origin and acceleration if you set the origin type to origin domain.

2. Weighted origin-pull



You can assign weights for different origin servers based on their loading capabilities.

N <	Create Distrib	pution
verview		
omain Name anagement	Domain Name Con	figuration
stics •	Add Acceleration Domain Name	Please enter the acceleration domain
ge		Add
t		Note: the origin servers of all added domain names should be exactly the same
ent	Project	Default Project
	Origin Server Type	Origin Server IP Origin Server Domain
	Origin-pull Policy	Optimal Origin-pull OWeighted Origin-pull Primary/Secondary Origin-pull
	Origin-pull Address	Please enter the origin-pull IP adc Weight
		Add
		Multiple origin server IPs can be set (one IP per line); ports 1-65535 are supported
	Origin-pull Protocol	HTTP 🔻

Note:

- A weight ranges from 0 to 100 (all zeros not allowed), and the system calculates the origin-pull ratio of different origin servers based on their weights.
- Up to 32 origin IP addresses or domain names can be configured. A mix of two types is not accepted.
- If you want to allow the list of ECDN intermediate node IPs, you can obtain the node information with this API ecdn.tencentcloudapi.com. To ensure origin-pull success, please access the latest node information and update your whitelist within 7 days after release.

3. Primary/secondary origin-pull

You can use this feature if you want to implement origin-pull based on a primary/secondary architecture.

ECDN	← Create Distrib	ution
Overview		
	Domain Name Cont	figuration(i)
Domain Name Management		
C Statistics	Add Acceleration Domain Name	Please enter the acceleration domain
🗇 Cache Purge		Add
Certificate Management		Note: the origin servers of all added domain names should be exactly the same
Log Management	Project	Default Project 💌
	Origin Server Type	Origin Server IP Origin Server Domain
	Origin-pull Policy	Optimal Origin-pull Veighted Origin-pull OPrimary/Secondary Origin-pull
	Primary Origin Server Address	Please enter the primary IP
	Secondary Origin Server Address	Please enter the secondary IP
		Multiple origin server IPs can be set (one IP per line); ports 1-65535 are supported

Modifying Advanced Origin-Pull Policy

After adding a domain name, you can modify advanced origin-pull policies on the domain management page in the following steps:

Step 1. Log in to the ECDN Console, click Domain Management on the sidebar, and click Manage.



ECDN	Domain Name Management						
Uverview	i If you add or disable a domain i	name, the system will c	leploy relevant configuration for t	ne domain name on the backer	nd. The configuration takes about 5 minutes to	o take effect.	
Domain Name Management	Create Distribution Purge	Enable ECDN Ser	vice More Operations	¥		Please enter the prefix to query	Q
C Statistics • C Cache Purge	Domain Name	Status ▼	CNAME	Fujint V	Acceleration Region T	Operation	
Certificate Management	.com	C Enabled		Ins Default Project	Mainland China	Manage Close More -	
🗈 Log Management	.com	Enabled		dn Default Project	Mainland China	Manage Close More -	

Step 2. On the **Basic Info** page, you can view the origin server configuration information. Click **Modify** to enter the editing page.

Basic Information	Cache Configuration	Access Configuration	Advanced Configuration
Basic Information			
Domain Name		i.com	
CNAME		l.com	
Project	Default Project M	odify 🧨	
Acceleration Region	Mainland China	Nodify 🧨	
Time Created	2020-04-23 21:26	:23	
Origin Server Inform	nation Modify 🖍		
Origin Server Type	IP Origin		
Origin-pull Policy	Optimal Origin-pu	II	
Origin-pull Protocol	HTTPS		
Origin Server Address			
Secondary Origin Server Address	-		
Origin-pull Configur	ation		
Origin Domain		Modify 🇨	

Step 3. In the pop-up window, you can adjust the origin server configuration as needed. For more information, please see Adding Advanced Origin-Pull Policy.

Modify Origin Server Configuration		×
Origin Server Type	Origin Server IP Origin Server Domain	
Origin-pull Policy	Optimal Origin-pull Oweighted Origin-pull Primary/Secondary Origin-pull	
Origin-pull Address		
Origin-pull Protocol	Multiple origin server IPs can be set (one IP per line); ports 1-65535 are supported HTTPS Yes Cancel 	

Note :

- The origin server configuration takes 5–30 minutes to be distributed and take effect.
- When adding an origin server address, please make sure that the origin server has been enabled for service; otherwise, some requests may fail after the switch.
- Before deleting an origin server address, delete the origin server configuration on the ECDN platform first and then disable the origin server service so as to reduce the risks of origin server switch.

Permission Management Console Permission Description

Last updated : 2020-04-28 14:50:48

Cloud Access Management (CAM) is a web-based service that helps you securely manage access permissions, resources, and usage permissions for your Tencent Cloud account. With CAM, you can create, manage, and terminate users (groups), and control the Tencent Cloud resources that can be used by the specified user through identity and policy management. For more information, please see User Guide.

ECDN supports resource-level authorization. By specifying the Action and Resource to create a custom policy, you can directly call APIs to perform operations on resources such as acceleration domain names. This document describes the mappings between console features and Action .

Overview

Feature Module	Authorized Action	Remarks
My service - Connected domain names	DescribeDomains	The total number of authorized domain names will be displayed
My service • Total number of requests in the current month • Total traffic in the current month • Average bandwidth in the current month	DescribeEcdnStatistics	The access data of authorized domain names in the current month will be displayed



Feature Module	Authorized Action	Remarks
Today's data	DescribeEcdnStatistics	Today's access data of authorized domain names will be displayed
Request trend in the current month	DescribeEcdnStatistics	The trend curve of requests in the current month will be displayed

Domain Management

Feature Module	Authorized Action	Remarks
Domain name list and query	DescribeDomains	Basic configuration items of a domain name can be queried or displayed To get all detailed configuration items, DescribeDomainsConfig should be authorized
Adding domain name	AddEcdnDomain	-
Deactivating ECDN	StopEcdnDomain	-
Activating ECDN	StartEcdnDomain	-
Deleting domain name	DeleteEcdnDomain	-



Feature Module	Authorized Action	Remarks
Modifying domain name project	UpdateDomainConfig	The domain name project is in the domain name configuration All configuration items of a domain name can be modified after authorization
Domain name configuration management	UpdateDomainConfig DescribeDomainsConfig	All configuration items of a domain name can be viewed/modified after authorization

Statistical Analysis

Feature Module	Authorized Action	Remarks
Usage statistics	DescribeEcdnDomainStatistics DescribeEcdnStatistics	All access data metrics under a domain name can be queried after authorization
Status code statistics	DescribeEcdnStatistics	All status code metrics under a domain name can be queried after authorization

Cache Purge

Feature Module	Authorized Action
Submitting URLs for purge	PurgeUrlsCache
Submitting directories for purge	PurgePathCache



Feature Module	Authorized Action
Querying purge records	DescribePurgeTasks

Certificate Management

Feature Module	Authorized Action	Remarks
Querying certificate list	DescribeDomainsConfig	All configuration items of a domain name can be viewed after authorization
Configuring certificate	UpdateDomainConfig	All configuration items of a domain name can be modified after authorization
Batch configuring certificates	UpdateDomainsHttps	It is used to configure certificates in batches

Log Service

Feature Module	Authorized Action
Querying log download link	DescribeEcdnDomainLogs

Creating Policies

Last updated : 2021-08-12 10:25:13

Note:

If your application has been migrated to the CDN console, you can go to the console for operation by referring to Content Delivery Network.

To make it easier for you to configure domain name queries and manage permissions in a more refined manner, the ECDN permission policies have been completely upgraded, so that you can grant permissions at the domain name level through custom policy statements.

1. Log in to the CAM Console and click Policies to enter the policy management page. Click Create Custom Policy:

Policies All Policies T				
i Bind users or user groups with the policy to a	assign them related permissions.			
Create Custom Policy Delete			Support search by policy name/description	Q
Policy Name	Description	Service Type T	Operation	
AdministratorAccess	This policy allows you to manage all users under your account and t	-	Bind User/Group	
ReadOnlyAccess	This policy authorizes you with the read-only access to all cloud ass	-	Bind User/Group	



2. Select Create by Policy Generator:

Select a	method to create policy	×
S	Create by policy generator Select services and operations from the list to automatically generate policy syntax	>
	Create by Policy Syntax Compile policy syntax to create related policy	>
Ţ	Authorize by tag Resources that have certain type of tag attribute are quickly authorized to users and user groups	>

3. Select **ECDN** in the product drop-down list and select features to be authorized. If you want to grant full read/write permission, check **All** to select all services. For mappings between features and console elements, please see

Console Permission Description.

Cloud Access Management	← Crea	te by policy generator				
Dashboard						
Users -	1 Sel	ect service and operation > (2)	Edit Policy			
User Groups	Effect •					
Policies	Soprico					
Roles	Service	Enterprise Content Delivery Ne 🔻				
Identity Providers	Action	Select Action (22 in total)			Selected (0)	
Access Key 🔻		Search Action name/description (multiple keyw	vords separated by spaces)	2	Action Name	Description
		Action Name	Description			
		AddEcdnDomain	Add domain			
		CheckDomainCertificate	Check if the certificate has expired			
		CheckEcdnDomain	Check whether the domain name is filed	\leftrightarrow		
		DeleteEcdnDomain	Delete domain			
		DescribeDomains	Describe domains' basic information			
		DescribeDomainsConfig	Describe domains' specific config			
		Support multi-selection by holding down shift ke	ıу			

4. Enter the domain name that needs to be authorized as the "resource" in the format of

qcs::ecdn::uin/xxxxxxx:domain/xxx.com, where you should replacexxxxxxxxxwith youraccount ID, andxxx.comwith the domain name you will authorize. You can directly enter*to represent alldomain names. After the configuration is complete, click Add Statement and Next to create a policy. Thenassociate the created policy with existing users/user groups for further authorization:

Resource	*	Note 🖸			
Condition	0 conditions				
	Add Statement				
Effect		Service	Operation	Resource Description	Operation
Allow		Enterprise Content Delivery Network	*	*	Delete
Next	l				



Note :

Due to product upgrade and rename, the DSA custom policy you configured needs to be modified. Click **Edit** on the policy details page, change "dsa" to "ecdn" in the policy statement, and map the original DSA permission policy to the ECDN permission policy.

policygen-20200313121328	• •	
policygen-20200313121328	-	
policygen-20200313121328 -	-	
policygen-20200313121328 -	-	
Market and a second second		
<pre>1 k 2 "version": "2.0", 3 "statement": [4 { 5 "effect": "allow", 6 "action": [7 "name/dsa:*" 8].</pre>		
9 "resource": [10 "*" 11] 12 } 13] 14]		

Statistical Analysis Statistics Overview

Last updated : 2020-04-28 14:50:53

ECDN provides the following data analysis and query tools to give you a comprehensive view of user access to your business resources:

Statistics Type	Description
Access statistics	You can view statistics of access to domain names and projects, including the number of requests, access traffic, and response time
Status code statistics	You can view the statistics of status codes of the acceleration service

Access Statistics

Last updated : 2021-06-25 11:15:36

ECDN usage statistics allow you to query historical statistics and monitoring data. You can view metrics such as the number of requests, access traffic, and response time.

You can log in to the ECDN Console, then click **Statistics** on the left sidebar to enter the Usage Statistics page and try out this feature.

Query Filters

- Period: queries data in the last 12 calendar months with a maximum time span of 31 days.
- Project: queries usage by project.
- Domain Name: queries usage of the specified domain name.
- Granularity: indicates an interval in which you query data and is subject to the selected period.
 - i. For a 1-day period, you can query data at a granularity of 5 minutes, 15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, or 24 hours.
 - ii. For a period of 2–3 days, you can query data at a granularity of 15 minutes, 30 minutes, 1 hour, 2 hours, or 4 hours.
 - iii. For a period of 4–7 days, you can query data at a granularity of 30 minutes, 1 hour, 2 hours, or 4 hours.
 - iv. For a period of 8–30 days, you can query data at a granularity of 1 hour, 2 hours, 4 hours or 24 hours.
- Region: queries usage by geographic area (regions within Mainland China or outside, or global regions).

Query	Filter		
Period	2021-06-22 ~ 2021-06-22	Region All	
Project	Select All 🔹	Domain Name Select All	

Usage Data Display

The usage data is displayed in three statistics modules:

- Data overview: displays the total usage.
- Monitoring details: displays detailed historical usage in curves.
- Domain name statistics: displays usage of each domain name in a list.



Query profile

As shown below, the query profile page displays statistics by account. You can quickly view the total usage in the specified query period.

Result Overview		
Total Requests	Peak Bandwidth O Bps	Average Response Time O ms

Access statistics

The access statistics section displays curves of historical monitoring data. You can view data of metrics in different categories.

- All domain names that were connected in the last 30 days, including deleted ones, will be included in the All Domain Names drop-down list.
- The real-time monitoring data you query will have a near 5-minute lag. If you run a query at 14:26:00, you will get the 00:00:00-14:21:00 data.
- Monitoring data is tracked over a time interval. For a 5-minute interval, a query start at 10:00:00–10:04:59 will start at the 10:00:00 sample point.
- If the time you query is longer than that of domain name connection, you will only get the connection statistics rather than those unconnected or deleted.
- To query monitoring data of multiple domain names or metrics, you can use the DescribeEcdnStatistics API.



Access Statistics		
Number of Requests Access Traffic Resp	ponse Time monitor index	
125		
100		
75		
50		
25		
0	4-03 04-05 04-07 04-09 04-11 04-13 04-15 04-17 04-19 04-21 04-23	
	- Total Requests - Dynamic Requests - Static Requests Curve label	

Domain name statistics

As shown below, the list of domain name statistics displays the usage details. You can sort different metrics to view the data.

Domain Name Statistics					
Domain Name 🗘	Total Requests \$	Dynamic Requests \$	Static Requests \$	Bandwidth \$	Average Response \$
.com	142	23	116	6.33Kbps	1155ms

Status Code Statistics

Last updated : 2021-06-25 11:17:49

ECDN status code statistics allow you to query monitoring data of status codes. You can log in to the ECDN Console, then click **Statistics** on the left sidebar to enter the <u>Status Code Statistics</u> page and try out this feature.

Query Filters

- Period: queries data in the last 12 calendar months with a maximum time span of 31 days.
- Project: queries usage by project.
- Domain Name: queries usage of the specified domain name.
- Granularity: indicates an interval in which you query data and is subject to the selected period.
 - i. For a 1-day period, you can query data at a granularity of 5 minutes, 15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, or 24 hours.
 - ii. For a period of 2–3 days, you can query data at a granularity of 15 minutes, 30 minutes, 1 hour, 2 hours, or 4 hours.
 - iii. For a period of 4–7 days, you can query data at a granularity of 30 minutes, 1 hour, 2 hours, or 4 hours.
 - iv. For a period of 8–30 days, you can query data at a granularity of 1 hour, 2 hours, 4 hours or 24 hours.
- Region: queries usage by geographic area (regions within Mainland China or outside, or global regions).

Query Filter		
Period 2021-06-22 ~ 2021-06-22	Region All +	
Project Select All *	Domain Name Select All Time Interval 5 minute(s) •	

Status Code Data Display

Status code data is displayed in a pie chart and a trend curve. All data can be exported.

- All domain names that were connected in the last 30 days, including deleted ones, will be included in the All Domain Names drop-down list.
- The real-time monitoring data you query will have a near 5-minute lag. If you run a query at 14:26:00, you will get the 00:00-00-14:21:00 data.

🔗 Tencent Cloud

- Monitoring data is tracked over a time interval. For a 5-minute interval, a query start at 10:00:00–10:04:59 will start at the 10:00:00 sample point.
- If the time you query is longer than that of domain name connection, you will only get the connection statistics rather than those unconnected or deleted.
- To query monitoring data of multiple domain names or metrics, you can use the DescribeEcdnStatistics API.



Status Code Description

```
533533ECDN edge or relay transfer fails, read times out, or connection establishmen t fails.t fails.Please<a href="https://console.tencentcloud.com/workorder/category"> submit a ticket </a>for assistance.
```

Category	Status Code	Description	Solution
277	200	The access succeeds.	A 2XX status code generally
2^^	206	The access succeeds.	indicates a normal access state.



3XX	301	The accessed content has been permanently migrated.	A 3XX status code generally indicates a normal access state.	
	302	The access is redirected.		
	304	The content to be accessed has not changed.		
	400	A request parameter is incorrect.		
	401	The access request verification fails.	A 4XX status code generally	
	403	Access to the content is denied.	indicates that the client request is incorrect or	
477	404	The requested content cannot be found.	the acceleration service of the domain name has been	
	405	The request method is not supported.	disabled.	
	416	The range is invalid.		
5XX	500	An internal server error occurs.	Please check whether the origin server	
	502	The server cannot	 service is exceptional; if not, please 	



	provide service currently.	submit a ticket for assistance.
501	The request method is not supported by the server and cannot be processed.	Please check the request method.
513	The ECDN edge server is overloaded, which is generally caused by user request surge or CC attacks.	Please check that the business request surge of the domain name is normal.
522	Internal HTTP ECDN connection establishment fails, or HTTP ECDN origin- pull connection establishment fails.	Please check that the origin server port 80 has been opened.
529	The domain name is newly added, and the route configuration has not taken effect.	It takes 5–10 minutes for the platform to deploy the configuration. Please confirm that the configuration has taken effect before switching to



	The ping command is blocked by the origin server, and the origin-pull route information cannot be obtained.	the CNAME resolution. You need to grant the ping permission on your ECDN intermediate nodes. You can submit a ticket to get the list of IPs of ECDN intermediate nodes.	
538	HTTPS SSL handshake fails, internal ECDN transfer fails, or ECDN origin-pull SSL handshake fails.	Please check that the origin server port 443 has been opened and SSL handshake is normal.	
564	ECDN origin- pull times out.	Please check whether there are jitters on the origin server egress network.	
Other	0	The client actively closes the connection during response.	Generally, it is caused by a client network problem or active stop of



		access by
		the user.

Cache Purge

Last updated : 2021-08-05 14:43:55

Feature Overview

ECDN is capable of configuring basic cache. Cache expiration time can be configured according to rules such as specified business types, directories, and specific URLs to regularly purge resources cached on nodes, pull latest resources from the origin server and cache them again.

Note:

If your application has been migrated to the CDN console, you can go to the console for operation by referring to Content Delivery Network.

In addition, ECDN can purge cache for specified URLs or directories in batches:

- Purge URL: Delete the cache of corresponding resources on all ECDN nodes.
- Purge directory: if you select the "Purge Changed Resources" mode, when an end user accesses a resource under the corresponding directory, the Last-Modify information of the resource will be obtained from the origin-pull.
 If it is the same as that of the currently cached resource, the cached resource will be directly returned; otherwise, the changed resource will be pulled from the origin server and cached again. If you select the "Purge All Resources" mode, when the user accesses a resource under the corresponding directory, the latest version of the resource will be directly pulled from the origin server and cached again.

After a purge is successfully executed, the corresponding resource on the node does not have a valid cache. When the user initiates an access request again, the node will pull the required resource from the origin server and cache it on the node again. If you submit a large number of purge tasks, many caches will be cleared, resulting in a surge in origin-pull requests and high pressure on the origin server.

Use Cases

New resource release

After a resource is overwritten by a new one with the same name on the origin server, to prevent users on the entire network from accessing the legacy version of the resource cached on the node, you can submit a request to purge the URL/directory for the resource and clear all caches so users can directly access the latest version of the resource.

Illegal resource cleanup

When illegal resources (such as resources related to pornography, drug, or gambling) are found on your origin server, they may still be accessible even after you delete them on the origin server because of node cache. To protect your network environment security, you can delete the cached resources through URL purge for timely cleanup.

Operation Guide

Wildcards are not supported now. Available purge URLs for today: 9999 (Mainland)

Submit and purge The operation may take about 5 minutes

How to use

Log in to the ECDN Console, click **Purge and Prefetch** on the left sidebar, and submit a **Purge URL** or **Purge Directory** task:

Purge URL Purge Directory Prefetch URL History URL https://examplebucket1-1259222427.file.myqcloud.com/test.png

©2013-2022 Tencent Cloud. All rights reserved.

Purge URLs API 🛂

1/1000

Purge and Prefetch

🕗 Tencent Cloud

Purge URL Purg	ge Directory Prefetch URL History	
		Purge Directories API 🖍
URL	https://avamplehucket1-1259222427 file mvorloud.com/testPath/	
		1/20
	Available purge directories for today: 100 (Mainland)	
Choose how to refresh	Refresh changed resources Refresh all resources	
Submit and purge	The operation may take about 5 minutes.	

In the **History** section, you can query tasks by specified time period, keyword, and purge task type. With regard to keyword, you can only query tasks by specifying a domain name or a complete purged URL/directory:

Purge and Pre	efetch					
Purge URL	Purge Directory	Prefetch URL	History			
Select a date	2019-12-11 00:00:00 ~	2019-12-11 23:59:59	i			
Search term	Enter a domain name,	or a complete URL (inc	ludes Scheme)			
Query type	O Purge URL O Pu	rge Directory OPre	efetch URL			
Check						
						Ŧ
Purge Record	is			Purge Time	Status T	
https://examp	lebucket1-1259222427.fil	e.myqcloud.com/test.p	ng	2019-12-11 17:03:58	Purging	
Total items: 1					Records per page 10 💌	₩ 4 1 /1page > M

Precautions

URL purge:

• Up to 10,000 URLs can be purged per day for each account, and up to 1,000 URLs can be submitted for purge at a time.

- S Tencent Cloud
- You need to add the http:// or https:// protocol identifier when submitting a purge task.
- URLs in the format of http://*.test.com/ cannot be purged. Even if you connect a wildcard domain name to CDN, you need to submit the corresponding sub-domain names for purge.
- When submitting URLs for purge, domain names should have already been connected to CDN; otherwise, the submission will fail.
- URLs containing Chinese characters cannot be purged.
- By default, URLs will be purged by acceleration regions of domain names in the URLs.

Directory Purge:

- Up to 100 directories can be purged per day per account, and up to 20 directories can be submitted for purge at a time.
- You need to add the http:// or https:// protocol identifier when submitting a purge task.
- Directories in the format of http://*.test.com/ cannot be purged. Therefore, even if you connect a wildcard domain name to CDN, you need to submit the corresponding sub-domain names for purge.
- When submitting URLs for purge, domain names should have already been connected to CDN; otherwise, the submission will fail.
- URL directories containing Chinese characters cannot be purged.

Sub-user permissions configuration:

- The operations of directory purge, URL purge, and purge history query must have already been connected to the latest permission system and support permission configuration at the resource (domain name) level.
- For permission assignment method, please see Permission Configuration.

Use Cases

Directory purge - purge changed resources

The acceleration domain name is purge-test-1251991073.file.myqcloud.com, the origin server is Tencent Cloud Object Storage (COS), and resources on the origin server are as follows:

examplebucket1-1259222427 / fileTest			Task completed (succeeded: 2,	failed: 0, paused: 0)	Documentation Guide 🗹
Upload Files Create Folder More Actions 💌				Please enter a prefix	Q Refresh
Object Name	Size	Storage Class	Last Updated	Actions	
1.txt	258B	Standard Storage	2019-12-11 17:12:12	Download Delete	Details Extract
2.txt	135B	Standard Storage	2019-12-11 17:12:18	Download Delete	Details Extract

1. Initiate requests to access resources 1.txt and 2.txt respectively. Nodes to be hit can be determined based on X-Cache-Lookup: Hit From Disktank3 and Server: NWS_SPMid, resources will be directly returned by the nodes:



[root@VM_0_14_centos ~]# curl https://examplebucket1-1259222427.file.myqcloud.com/fileTest/1.txt -sv
* About to connect() to examplebucket1-1259222427.file.myqcloud.com port 443 (#0)
* Trying 101.69.121.120... * Connected to examplebucket1-1259222427.file.myqcloud.com (101.69.121.120) port 443 (#0) * Initializing NSS with certpath: sql:/etc/pki/nssdb * CAfile: /etc/pki/tls/certs/ca-bundle.crt CApath: none * SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 * Server certificate: subject: CN=*.weixin.qq.com,O=Shenzhen Tencent Computer Systems Company Limited,L=shenzhen,ST=guangdong,C=CN * start date: May 13 08:45:29 2019 GMT * expire date: May 13 08:45:29 2020 GMT common name: *.weixin.qq.com * * issuer: CN=GlobalSign Organization Validation CA - SHA256 - G2,O=GlobalSign nv-sa,C=BE > GET /fileTest/1.txt HTTP/1.1 > User-Agent: curl/7.29.0 > Host: examplebucket1-1259222427.file.myqcloud.com > Accept: */* < HTTP/1.1 200 OK < Date: Wed, 11 Dec 2019 09:28:53 GMT < Content-Type: text/plain < Content-Length: 258 < Connection: keep-alive < Server: nws_ocmid_hy < Cache-Control: max-age=600 < Expires: Wed, 11 Dec 2019 09:38:53 GMT < Last-Modified: Wed, 11 Dec 2019 09:12:12 GMT
< X-NWS-UUID-VERIFY: b45f12ce9711b2c57b1a7b35904ac403</pre> < X-NWS-LOG-UUID: d4f507fc-38a5-4a35-bf59-2cbf2f392855</pre> X-Cache-Lookup: Hit From Disktank3 < Accept-Ranges: bytes < X-Daa-Tunnel: hop_count=3 < X-Cache-Lookup: Hit From Inner Cluster < X-Cache-Lookup: Hit From Upstream < X-Cache-Lookup: Hit From Inner Cluster * Connection #0 to host examplebucket1-1259222427.file.myqcloud.com left intact



[root@VM_0_14_centos ~]# curl https://examplebucket1-1259222427.file.myqcloud.com/fileTest/2.txt -sv About to connect() to examplebucket1-1259222427.file.myqcloud.com port 443 (#0) Trying 101.71.72.212... * Connected to examplebucket1-1259222427.file.myqcloud.com (101.71.72.212) port 443 (#0) * Initializing NSS with certpath: sql:/etc/pki/nssdb CAfile: /etc/pki/tls/certs/ca-bundle.crt CApath: none SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 * Server certificate: * subject: CN=*.weixin.qq.com,O=Shenzhen Tencent Computer Systems Company Limited,L=shenzhen,ST=guangdong,C=CN * start date: May 13 08:45:29 2019 GMT * expire date: May 13 08:45:29 2020 GMT common name: *.weixin.qq.com * * issuer: CN=GlobalSign Organization Validation CA - SHA256 - G2,O=GlobalSign nv-sa,C=BE > GET /fileTest/2.txt HTTP/1.1 > User-Agent: curl/7.29.0 > Host: examplebucket1-1259222427.file.myqcloud.com > Accept: */* > < HTTP/1.1 200 OK < Date: Wed, 11 Dec 2019 09:24:54 GMT < Content-Type: text/plain < Content-Length: 135 < Connection: keep-alive < Server: nws_ocmid_hy < Cache-Control: max-age=600 < Expires: Wed, 11 Dec 2019 09:34:54 GMT < Last-Modified: Wed, 11 Dec 2019 09:12:18 GMT < X-NWS-UUID-VERIFY: 236746c2d95b242ef56fdf904c1c9e50</pre> X-NWS-LOG-UUID: 6858ac8e-58d1-4959-a25a-45521dbebf5d < X-Cache-Lookup: Hit From Disktank3</pre> < Accept-Ranges: bytes
< X-Daa-Tunnel: hop_count=2</pre> < X-Cache-Lookup: Hit From Inner Cluster < X-Cache-Lookup: Hit From Upstream 1 * Connection #0 to host examplebucket1-1259222427.file.myqcloud.com left intact

2. On the origin server, replace 1.txt with a file that has the same name, and the file's last modified time changes,

while 2.txt stays the same:
🔗 Tencent Cloud	
-----------------	--

Basic Information	
Object Name	1.bt
Object Size	2588
Last Modified	2019-12-11 17:12:12
ETag	"3f4989383498b548700c122d56a708ed"
Specified Domain(i)	Default CDN Accelerati 💌
Object Address	https://examplebucket1-1259222427.file.myqcloud.com/fileTest/1.txt 🔓
Temporary Link	To Copy Temporary Link 🛓 Download Objects 🧳 Refresh
	The temporary link carries the signature parameter, and the temporary link can be used to access the object during the validity period of the signature, and the signature is valid for 1 hour (2019-12-11 18:12:56).
	Be sure to avoid leaking the temporary link, otherwise your objects may be accessed by other users.

Basic Information	1
Object Name	1.bxt
Object Size	240B
Last Modified	2019-12-11 17:30:21
ETag	"282ba0ab22810e2eb79aa52fcdcacccb"
Specified Domain	Default CDN Accelerati *
Object Address	https://examplebucket1-1259222427.file.myqcloud.com/fileTest/1.bxt
Temporary Link	🗈 Copy Temporary Link 👎 Download Objects 🗘 Refresh
	The temporary link carries the signature parameter, and the temporary link can be used to access the object during the validity period of the signature, and the signature is valid for 1 hour (2019-12-11 18:30:25).
	Be sure to avoid leaking the temporary link, otherwise your objects may be accessed by other users.

3. Initiate requests again. As the cache has not expired, the legacy content of the 1.txt resource will be accessed:





4. Submit a directory purge task, select **Purge Changed Resources**, and wait for the purge to complete:

rge URL Purge Directory Prefetch URL	History			
elect a date 2019-12-11 00:00:00 ~ 2019-12-11 23:59:	59 İ (i)			
earch term Enter a domain name, or a complete URL	(includes Scheme)			
	Prefetch URL			
uery type O Purge URL O Purge Directory				
Obeck				
ueny type Purge URL O Purge Directory O				
Uvery type O Purge URL O Purge Directory O				
Uuery type Purge URL Purge Directory		Purge Time	Status T	
Check Purge Records https://examplebucket1-1259222427.file.myqcloud.com/file	=Test/	Purge Time 2019-12-11 17:35:55	Status T Purging	

5. After the purge is completed, because Last-Modified of 1.txt has been changed, the request will be forwarded to the origin server. As 2.txt has not been changed, even after a directory purge task is submitted, it will still be hit by nodes and returned:



[root@VM_0_14_centos ~]# curl https://examplebucket1-1259222427.file.myqcloud.com/fileTest/1.txt -sv * About to connect() to examplebucket1-1259222427.file.myqcloud.com port 443 (#0) * Trying 101.71.72.212.. * Connected to examplebucket1-1259222427.file.myqcloud.com (101.71.72.212) port 443 (#0) * Initializing NSS with certpath: sql:/etc/pki/nssdb CAfile: /etc/pki/tls/certs/ca-bundle.crt * CApath: none * SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 * Server certificate: * subject: CN=*.weixin.qq.com,O=Shenzhen Tencent Computer Systems Company Limited,L=shenzhen,ST=guangdong,C=CN start date: May 13 08:45:29 2019 GMT * expire date: May 13 08:45:29 2020 GMT common name: *.weixin.qq.com * * issuer: CN=GlobalSign Organization Validation CA - SHA256 - G2,0=GlobalSign nv-sa,C=BE > GET /fileTest/1.txt HTTP/1.1 > User-Agent: curl/7.29.0 > Host: examplebucket1-1259222427.file.myqcloud.com > Accept: */* > < HTTP/1.1 200 OK < Date: Wed, 11 Dec 2019 09:43:10 GMT < Content-Type: text/plain < Content-Length: 254 < Connection: keep-alive < Server: tencent-cos < Last-Modified: Wed, 11 Dec 2019 09:40:37 GMT
< X-NWS-UUID-VERIFY: 965fe357269927d4fde83e5011335643</pre> < Accept-Ranges: bytes < ETag: "ba792676560655b3bbaf4e09f642c547" < x-cos-request-id: NWRmMGJhMmVfNWJiMjU4NjRfM2I1NF85NmQ1ZDA=</pre> < X-Daa-Tunnel: hop_count=4 < X-NWS-LOG-UUID: e1318191-923d-4544-b759-b298b1ef8897</pre> < X-Cache-Lookup: Hit From Upstream < X-Cache-Lookup: Hit From Inner Cluster < X-Cache-Lookup: Hit From Upstream < X-Cache-Lookup: Hit From Inner Cluster Connection #0 to host examplebucket1-1259222427.file.myqcloud.com left intact



[root@VM_0_14_centos ~]# curl https://examplebucket1-1259222427.file.myqcloud.com/fileTest/2.txt -sv
* About to connect() to examplebucket1-1259222427.file.myqcloud.com port 443 (#0) * Trying 101.69.121.120... * Connected to examplebucket1-1259222427.file.myqcloud.com (101.69.121.120) port 443 (#0) * Initializing NSS with certpath: sql:/etc/pki/nssdb * CAfile: /etc/pki/tls/certs/ca-bundle.crt CApath: none * SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 * Server certificate: subject: CN=*.weixin.qq.com,O=Shenzhen Tencent Computer Systems Company Limited,L=shenzhen,ST=guangdong,C=CN start date: May 13 08:45:29 2019 GMT * * expire date: May 13 08:45:29 2020 GMT common name: *.weixin.qq.com * * issuer: CN=GlobalSign Organization Validation CA - SHA256 - G2,O=GlobalSign nv-sa,C=BE > GET /fileTest/2.txt HTTP/1.1 > User-Agent: curl/7.29.0 > Host: examplebucket1-1259222427.file.myqcloud.com > Accept: */* < HTTP/1.1 200 OK < Date: Wed, 11 Dec 2019 09:44:24 GMT < Content-Type: text/plain < Content-Length: 135 < Connection: keep-alive < Server: nws_ocmid_hy < Cache-Control: max-age=600 < Expires: Wed, 11 Dec 2019 09:54:24 GMT
< Last-Modified: Wed, 11 Dec 2019 09:12:18 GMT</pre> < X-NWS-UUID-VERIFY: 77063706e00075a84cdf6d5f5c4ff03f < X-NWS-LOG-UUID: b639cf12-0f1c-4908-9978-c8f9fe70e494</pre> < X-Cache-Lookup: Hit From Disktank3 < Accept-Ranges: bytes < X-Daa-Tunnel: hop_count=3 < X-Cache-Lookup: Hit From Inner Cluster < X-Cache-Lookup: Hit From Upstream < X-Cache-Lookup: Hit From Inner Cluster Connection #0 to host examplebucket1-1259222427.file.myqcloud.com left intact

Certificate Management

Last updated : 2021-08-05 14:52:52

You can configure HTTPS certificates for domain names connected to ECDN. ECDN supports configuration of existing certificates or certificates hosted or issued in the SSL Certificates Service Console.

Note :

If your application has been migrated to the CDN console, you can go to the console for operation by referring to Content Delivery Network.

Certificate Management List

Log in to the ECDN Console and click **Certificate Management** on the left sidebar to enter the list page where you can:

- View basic HTTPS configuration information of domain names, such as certificate source, expiration time, originpull method, and deployment status.
- Deploy certificates by domain name. For detailed directions, please see Configuring Certificate below.
- Deploy domain name certificates in batches. For detailed directions, please see Batch Deployment below.
- Edit or delete HTTPS configuration.

Certificate Management							
 All certificates deployee If you have not obtaine 	d on ECDN nodes are managed ir Id any certificate yet, you can appi	a centralized manner. For s	security concerns, your cer d SSL Certificates 🗹 . Free	tificates are not stored in Tencent C certificates for the trial are from Tru	Cloud but directly deployed IstAsia®.	to all ECDN nodes.	
Configure Certificate	Batch Deploy Purge	Delete				Please enter the pre	Q
Domain Name	Certificate Remark	Certificate Source	Expiry Time	Origin-pull Method	Certificate Status	Operation	

Configuring Certificate

On the domain management page, click **Configure Certificate** to enter the management page and deploy a certificate in the following steps:

1. Select a domain name

- 2. Associate the domain name with the certificate
- 3. Submit for deployment

Selecting domain name

In the **Domain Name** drop-down list, select the domain name for which to configure a certificate.

Note:

The domain name should already have been connected to ECDN, and the domain name status should be **activated**. Certificates cannot be configured for **deactivated** or **deploying** domain names.

÷	Certificate Configuration
	Please make sure that the deployed certificate has been connected to Tencent Cloud ECDN, and its status is "Activated".
P	lease select the domain name for certificate configuration
D	omain ame:

Associating domain name with certificate

After selecting a domain name, you need to configure it with a certificate. ECDN supports configuration of private and Tencent Cloud-hosted certificates. You can choose an appropriate certificate based on your selected domain name. Directions for configuring these two types of certificates are detailed as below:

Certificate Source Type	Configuration Steps	Remarks
Private certificate	You need to paste certificate content and private key content into the text box and add remarks for certificate identification.	The certificate content must be in PEM format. For more information, please see Private Certificate Configuration Guide.



Certificate Source Type	Configuration Steps	Remarks
Tencent Cloud-hosted certificate	You can select an appropriate Tencent Cloud-hosted certificate in the certificate drop-down list.	You can log in to the SSL Certificates Service Console to apply for a certificate free of charge or host a private certificate in Tencent Cloud.



Select a Certificate				
Certificate Source	Self-owned Certificate	Tencent Cloud-hosted Certificate		
Certificate Content	View Sample ⊠			
Private Key Content	View Sample 🛂			
Remark (optional)				

Submitting for deployment

Click **Deploy** to submit the task. You can view the certificate deployment status on the **Certificate Management** page.

- When a domain name certificate is added or deleted, the certificate status will be displayed as **deploying**, and the deployment usually takes 5 minutes to take effect. You can click **Refresh** to view the certificate deployment status.
- The domain name certificate deployment features seamless overwriting; therefore, modification of domain name certificate configuration will not cause any disruption to your business.

Batch Deployment

If your submitted certificate is associated with multiple acceleration domain names, you can manage their certificate configurations in a unified manner through batch deployment in the following steps:

- 1. Select a certificate
- 2. Associate domain names
- 3. Submit for deployment

Selecting certificate

You can select a multi-domain name certificate or wildcard certificate when using batch deployment. For detailed directions, please see Certificate Configuration Steps.



Select a Certificate				
Certificate Source	Self-owned Certificate	O Tencent Cloud-hosted Certificate		
Certificate Content	View Sample			
Private Key Content	View Sample			
Remark (optional)				

Associating domain names

After a certificate is selected, the system will automatically associate the certificate domain name with an ECDN acceleration domain name. You can also filter domain name certificates by their deployment status to quickly select domain names that need to be configured with the certificate.

Certificate Do	omain Name				
Certificate Domain Name	 A maintaine martine 				
Bomain Name	" of adalasis and				
Select domai	n names to associate				
Associated	All Domain Names	•			
Domain Name Type					
Domain N	lame	Certificate Status	Expiry Time		
	Australia -	Normal	2020-10-22 20:00:00		
in an internal	aria are				
		Normal			

Submitting for deployment

Tencent Cloud

After the configuration is completed, click **submit** to submit it. You can go to the certificate management list to view the certificate configuration status.

- When a domain name certificate is added or deleted, the certificate status will be displayed as deploying, and the deployment usually takes 5 minutes to take effect. You can click Refresh to refresh the certificate deployment status.
- The domain name certificate deployment features seamless overwriting; therefore, modification of domain name certificate configuration will not cause any disruption to your business.

Private Certificate Management Description

Certificate and private key

1. If you need to configure your domain name with an existing certificate, please read this section. If you need to configure a certificate hosted or issued in the SSL Certificates Service Console, you can skip this step and directly view the certificate configuration process below.



The certificates provided by CAs include the following types, of which Nginx is used by ECDN.

퉬 Apache	2017/8/9 10:46
🐌 IIS	2017/8/9 10:46
퉬 Nginx	2017/8/9 10:46
퉬 Tomcat	2017/8/9 10:46

2. Go to the Nginx folder and open ".crt" (certificate) and ".key" (private key) files with a text editor to view the content of the certificate and private key in PEM format.



- 3. Certificate description
 - Common certificate extensions include ".pem", ".crt", and ".cer". Open the certificate file in a text editor and you can see content similar to the one shown below.

A .pem certificate begins with "-----BEGIN CERTIFICATE-----" and ends with "-----END CERTIFICATE-----".

Every line in between contains 64 characters, while the last line may have less than 64 characters.



• If your certificate is issued by an intermediate CA, your certificate file will consist of multiple certificates. In this case, you need to splice the server certificates and intermediate certificates manually for upload by putting the

server certificate content before the intermediate certificate content without any blank lines in between. Please refer to the rules or instructions that came with the certificate.

Note :

- There should be no blank lines between the certificates.
- All certificates are in PEM format.
- A certificate chain from an intermediate CA comes in this format:

-----BEGIN CERTIFICATE----------END CERTIFICATE----------BEGIN CERTIFICATE----------BEGIN CERTIFICATE----------BEGIN CERTIFICATE-----

- 4. Private key description
 - Common private key extensions include ".pem" and ".key". Open a private key file in a text editor and you will see a certificate similar to the content as shown below.
 - A .pem private key begins with "-----BEGIN RSA PRIVATE KEY-----" and ends with "-----END RSA PRIVATE KEY-----". Every line in between contains 64 characters, while the last line may have less than 64 characters.

BEGIN RSA PRIVATE KEY
MIIEpAIBAAKCAQEAvZiSSSChH67bmT8mFykAxQ1tKCYukwBiWZwkOStFEbTWHy8K
tTHSfD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A
Xw95grqFJMJcLva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ
/fD0XXyuWoqaIePZtK9Qnjn957ZEPhjtUpVZuhS3409DDM/tJ3Tl8aaNYWhrPBcO
jNcz0Z6XQGf1rZG/Ve520GX6rb5dUYpdcfXzN5WM6xYg8alL7UHDHHPI4AYsatdG
z5TMPnmEf8yZPUYudT1xgMVAovJr09Dq+5Dm3QIDAQABAoIBAG168Z/nnFyRHrFi
laF6+Wen8ZvNqkm0hAMQwIJh1Vplfl74//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35
cgQ93Tx424WGpCwUshSfxewfbAYGf3ur8W0xq0uU07BAxaKHNcmNG7dGyolUowRu
S+yXLrpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2
06W/zHZ4YAxwkTY1KGHjoieYs111ah1AJvICVgTc3+LzG2pIpM7I+KOnHC5eswvM
i5x9h/0T/ujZsyX9P0PaAyE2bqy0t080tGexM076Ssv0KVhKFvWjLUnhf6WcqFCD
xqhhxkECgYEA+PftNb6eyX1+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhqgHuOedU
ZXIHrJ9u6BlXE1arpijVs/WHmFhYSTm6DbdD7SltLy0BY4cPTRhziFTKt8AkIXMK
605u0UiWsq0Z8hn1Xl4lox2cW9ZQa/HC9udeyQotP4NsMJWgpBV7tC0CgYEAwvNf
0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzfEG8/AR3Md2rhmZi
GnJ5fdfe7uY+JsQfX2Q5JjwTadlBW4ledOSa/uKRaO4UzVgnYp2aJKxtuWffvVbU
+kf728ZJRA6azSLvGmA8hu/GL6bgfU3fkSkw03ECgYBpYK7TT7JvvnAErMtJf2yS
ICRKbQaB3gPSe/lCgzy1nhtaF0UbNxGeuowLAZR0wrz7X3TZqHEDcYoJ7mK346of
QhGLITyoehkbYkAUtqO38YO4EKh6S/IzMzBOfrXiPKg9s8UKQzkU+GSE7ootli+a
R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUhKIKcP/+xn
R3kVl06MZCfAdqirAjiQWaPkh9Bxbp2eHCrb81MFAWLRQSlok79b/jVmTZMC3upd
EJ/iSWjZKPbw7hCFAeRtPhxyNTJ5idEIu9U8EQid81l1giPgn0p3sE0HpDI89qZX
aaiMEQKBgQDK2bsnZE9y0ZWhGTeu94vziKmFrSkJMGH8pLaTiliw1iRhRYWJysZ9
BOIDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcv0Bh5Hx0yy23m9hFRzfDeQ7z
NTKh193HHF1joNM81LHFyGRfEWWrroW5gfBudR6USRnR/6iQ11xZXw
END RSA PRIVATE KEY

• If your private key begins with "-----BEGIN PRIVATE KEY-----" and ends with "-----END PRIVATE KEY-----", you are recommended to convert the format by using OpenSSL with the following command:

openssl rsa -in old_server_key.pem -out new_server_key.pem

Completing certificate chain

When configuring a private certificate, you may encounter a problem where the **certificate chain cannot be completed**. In this case, you can paste the CA-issued certificate (in PEM format) after the domain name certificate (in PEM format) to complete the certificate chain. You can also submit a ticket for assistance.

🔄 1_root_bundle.crt	\mathbb{N}^{-1}	2016/11/8 15:07
🔄 2 <u>.</u>	.crt	2016/11/8 15:07
3	om.key	2016/11/8 15:07

Converting certificate format

Currently, ECDN only supports certificates in PEM format. Certificates in other formats need to be converted to PEM format first. You are recommended to use OpenSSL to perform the conversion. The following shows how to convert several common formats to PEM.

DER to PEM

The DER format is generally used on Java platforms.

Certificate conversion

openssl x509 -inform der -in certificate.cer -out certificate.pem

• Private key conversion

openssl rsa -inform DER -outform PEM -in **private**key.der -out **private**key.pem

P7B to PEM

The P7B format is generally used on Windows Server and Tomcat.

Certificate conversion

openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer

Open outcertificat.cer with a text editor to view the content of the PEM certificate.

Private key conversion

Private keys can generally be exported on IIS servers.

PFX to PEM

The PFX format is generally used on Windows Server.

Certificate conversion

openssl pkcs12 -in certname.pfx -nokeys -out cert.pem

Private key conversion

openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes

Log Management

Last updated : 2021-08-05 14:57:12

You can download the detailed logs of user access to your connected domain names for the last 40 days for analysis, which are recorded hourly.

Note :

If your application has been migrated to the CDN console, you can go to the console for operation by referring to Content Delivery Network.

Downloading Logs

Log in to the ECDN Console and select Log Management on the left sidebar. Select the domain for which you want to check logs and the time period. Then, click OK to get the log download link.

ECDN	Log Management
Overview Domain Name Management Statistics	 Contents in the log files are request time, client IP, access domain name, file path, number of bytes, district code, ISP code, HTTP status code, Referer, Request-Time, UA, Range, HTTP Method, protocol identification, and cache HIT/MISS. For detailed field information, please see Log Description C*. The log data of the current day have a delay and are not recommended for reference. A log records the number of bytes of the returned data packet at the application layer (HTTP protocol). The bandwidth or traffic counted through the HTTP layer is smaller than that counted through the TCP layer counted.
✓ Cache Purge	Districts and ISPs are represented by codes. For details, please see <u>District and ISP Code Mapping Table</u>
Certificate Management	Query Filter
Log management	Period 2020-04-01 ~ 2020-04-25 Domain
	Data List
	Start Time End Time File Address Operation
	2020-04-25 13:00:00 2020-04-25 13:59:59

No access logs will be generated for the queried time period in which there is no request received, and you will see **No Data** on the page.

Note:

• By default, the ECDN logs requests on an hourly basis, that is, there can be 24 log files generated per day. No logs will be generated for the hour in which there is no request received.



• ECDN logs can be delayed by approximately 30 minutes.

Log Field Description

Decompress the downloaded log data packages and view the log files in text format. The fields are separated by space. Below is an example:

20170719174306	10.10.10.10	www.test.com	/test.png	77487	320) NU	LL 140)8 "Mo	zilla/
20170719174407	10.10.10.10	www.test.com	/test2.png	72488	52	200	NULL	13569	"Mozi
20170719174520	10.10.10.10	www.test.com	/test3.png	74864	42	200	NULL	9474	"Mozil
20170719174544	10.10.10.10	www.test.com	/test4.png	81453	22	200	NULL	9218	"Mozil
20170719174532	10.10.10.10	www.test.com	/test5.png	54678	72	200	NULL	9041	"Mozil

The corresponding fields (from left to right) and their descriptions in a log are as shown below:

Order	Log Content
1	Request time
2	IP of the client accessing the domain name
3	Accessed domain name
4	File request path
5	Number of bytes of this access request
6	District (for the district codes, please see District mappings below)
7	ISP (for the district codes, please see ISP mappings below)
8	HTTP status code
9	Referer information
10	Response time in milliseconds
11	User-Agent information
12	Range parameter
13	HTTP Method
14	HTTP protocol identifier



Order	Log Content
15	Cache hit/miss (all resources are not cached in dynamic acceleration by default)

Region mappings

1: North China; 2: Northwest China; 3: Northeast China; 4: East China; 5: Central China; 6: Southwest China; 7: South China; 8: outside Mainland China.

District mappings

22: Beijing; 86: Inner Mongolia; 146: Shanxi; 1069: Hebei; 1177: Tianjin; 119: Ningxia; 152: Shaanxi; 1208: Gansu; 1467: Qinghai; 1468: Xinjiang; 145: Heilongjiang; 1445: Jilin; 1464: Liaoning; 2: Fujian; 120: Jiangsu; 121: Anhui; 122: Shandong; 1050: Shanghai; 1442: Zhejiang; 182: Henan; 1135: Hubei; 1465: Jiangxi; 1466: Hunan; 118: Guizhou; 153: Yunnan; 1051: Chongqing; 1068: Sichuan; 1155: Tibet; 4: Guangdong; 173: Guangxi; 1441: Hainan; 0: Other; 1: Hong Kong, Macao, and Taiwan; -1: outside Mainland China.

ISP mappings

2: China Telecom; 26: China Unicom; 38: CERNET; 43: Great Wall Broadband Network; 1046: China Mobile; 3947: China Mobile Tietong; -1: ISP outside Mainland China; 0: Other ISPs.

Precautions

The bandwidth or traffic data recorded in logs is the returned data at the application layer (HTTP protocol), which is smaller than that calculated at the TCP layer due to such factors as TCP protocol packet loss, three-way handshake, and retransmission.

Downloading ECDN Logs Outside China

At present, ECDN outside Mainland China is in beta test. If you have enabled it, you can submit a ticket to apply for the log service.