Alibaba Cloud
Alibaba Cloud CDN

User Guide

Issue: 20190418

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Introduction

Quick start

Alibaba Cloud Content Delivery Network(CDN) is a distributed network that overlays on the bearer network and is composed of edge node server clusters distributed across different regions. The CDN network replaces the traditional data transmission modes centered on web servers. The CDN console can help you add a CDN domain, refresh cache, and perform other configuration tasks. It also provides resource monitoring services including real-time data analysis. This document presents basic information about the CDN console.

Overview of CDN operation

After you log on to the *CDN console*, the CDN operation information for the current account is displayed on the home page as follows:

1. Billing method display and change:
2. Key data: the number of domains in normal status and the total traffic for all domains this month
3. This month's data:
   a. Domain peak bandwidth
   b. Top 4 domain names according to the accumulated downstream traffic
   c. Region distribution of users who access the acceleration resources
   d. Real-time cache hit rate of users who access acceleration resources

 Note:
This month indicates the current calendar month.

You can complete relevant function settings and view data in the left-side navigation pane:

Functions	Brief introduction
Domain name management	Add a CDN domain name, manage, or delete a CDN domain name, and change the basic and configuration information of the CDN domain name.

Functions	Brief introduction
Monitoring	Include Resource Monitoring and Real-time Monitoring.
Refresh	URL refresh and directory refresh are available.
Log	Log downloads, log storage (upcoming), Cloud reports
Tools	Link diagnostic tools, IP queries

2 Function overview

HTTPS secure acceleration

Function	Description	Default
HTTPS secure acceleration	Provides a full link HTTPS secure acceleration scheme, just upload the CDN domain name certificate/private key after you activate secure acceleration mode, and supports viewing , disabling, enabling, editing of certificates.	Disabled
Force redirect	When the "HTTPS secure acceleration" is enabled , the CDN domain name supports custom settings , and redirect the user' s original request in a forcible way.	Disabled
HTTP/2	HTTP/2 can be seen as an advanced edition of HTTP/1.1. It has many advantages, including binary protocol, content security, multiplexing, header compression, and so on.	Disabled
TLS	TLS is a cryptographic protocol designed to ensure communication security and data integrity of a computer network.	TLS Version 1.0, TLS Version 1.1, and TLS Version 1.2 are enabled by default.
HSTS	HSTS is specified in RFC 6797. HSTS instructs clients, such as a browser, that a domain can only be accessed by using HTTPS.	Disabled

Back-to-source settings

https://www.alibabacloud.com/help/doc-detail/57653.htm

Function	Description	Default
Back-to-source host	Specifies the host domain name that a CDN node accesses in the back-to-source process. Three options are available: CDN domain name, original site domain name, and custom domain name.	CDN domain name
Back-to-source with the same protocol	Back-to-source requests for resources use exactly the same protocol as used by the client to request the resources.	Disabled
Private bucket back-to-origin authentication	After authentication is successful and authentication configuration is enabled, domain names enabled with private bucket authentication have the permission to access the private bucket.	Disabled

Cache settings

Function	Description	Default
Cache expiration time	Customizes cache expiration rules for specified resources.	Disabled
Setting the HTTP Request Header	Sets an HTTP request header. Nine parameters are currently available for HTTP request header customization.	Disabled
Custom 404 page	Available in three options: default 404, public welfare 404, custom 404	Default 404 page

Access control

Function	Description	Default
Anti-leech	Configures a referer blacklist or whitelist to identify and filter visitors.	Disabled
URL authentication	Uses URL authentication methods to protect resources on an origin site.	Disabled
IP blacklist	Configures the access IP blacklist to identify and filter visitors.	Disabled

Performance optimization

Function	Description	Default
Page optimization	Compresses and removes useless blank lines and carriage return characters to effectively reduce the page size.	Disabled
Smart compression	Supports smart compression for content in multiple formats to effectively reduce the size of user transmitted content.	Disabled
Filter parameter	Removes parameters after ? in a URL request during the back-to-source process .	Disabled

Video-related settings

Function	Description	Default
Back-to-source of range	Allows a user to notify an origin site server to return partial content within a specified range. This function helps with accelerated delivery of large files.	Disabled
Drag/drop playback	Enables random drag or drop playback in a video or audio on-demand scenario.	Disabled
Notify_URL	【Applicable to Live】Real-time information callback of stream status, promptly notifies users about the operation results of streaming or stream disconnection.	Disabled

Advanced settings

Function	Description	Default
Peak Bandwidth	If the average bandwidth exceeds the maximum, the domain name automatically goes offline to protect your domain name security	Disabled

Refresh and preload

Function	Description	Default
URL refresh and preload	· Forces specified files on the CDN Cache node to expire in order to update back-to-source again. · Actively pushes content from the origin site to the L2 Cache node. Upon first access, you can directly hit cache to relieve pressure on the origin site.	Enabled

Data monitoring and statistical analysis

Function	Description	Default
Data monitoring	You can select Domain Name, Region, Operator, Time Granularity (1 minute, 5 minute or 1 hour) and Time Range(Today, Yesterday, 7 Days, 30 Days or Custom) to view the specific condition.	Enabled
Statistical analysis	In Statistical Analysis, you can check data of PV and UV, Area and ISP, Domain Name Rankings, Popular Referer, and Popular URLs.	Enabled

Usage query

Function	Description	Default
Usage query	You can use this function to obtain the actual usage of traffic, bandwidth, or requests during a certain period.	Enabled

Function	Description	Default
Billing export	You can export actual usage data by day or by month, so as to compare it with the report output from the billing center.	Enabled
Detail data export	You can export detail data for traffic/bps data or request times, so that you can calculate or review the usage you actually paid for .	Enabled

Log management

Function	Description	Default
Log Downloading	You can download the log files within 1 month.	Enabled

Other settings

Function	Description	Default
Set httpDNS	Provides a DNS service by using the HTTP protocol to directly access the server of Alibaba Cloud CDN.	Disabled

3 Business type

3.1 Type 1: Images And Small Files Acceleration

Use cases

Distribution of static website or application contents, such as various image files, HTML file, Flash animation, css and JavaScript files. Suitable for portal websites, e-commerce websites, news websites and applications, government and enterprise official websites, and entertainment and game websites and applications.

Procedure

1. Add a CDN domain

   See *Quick Start*. Make sure you select Acceleration of images and small files for the business type.

2. Configure domain

   After the domains are added, use the appropriate feature to configure the CDN domains based on your business needs. All domain configurations are optional. The following configurations are recommended for the acceleration of "images and small files".

   Recommended configurations:

   - *HTTPS Secure Acceleration*: You only need to enable the secure acceleration mode and then upload the certificate and the private key for the CDN domains.

You can also view, disable or edit the certificate. For more information, see *Certificates formats instructions*.

- *Cache configuration*: This feature can be used to set the actions of a cache server against resources in different directory paths or with different file name suffixes. You can customize cache expiration rules for specified resources.
- Access control settings: ensure the security of the distributed content, and prevent unnecessary traffic losses from leeching or malicious requests.
  - *Refer anti-leech protection*
  - *IP blacklist*
- Performance optimization settings: intelligently compress the distributed content and ignore URL parameters to improve cache hit rate.
  - *Page optimization*
  - *Smart compression*
  - *Filter parameters*
- For more features, see *CDN feature list*.

3.2 Type 2: Large File Downloads Acceleration

Use cases

Distribution of large static website or application files, such as game installation packages `. apk` , application update files `. rar` , patch files, and audio and video files. Suitable for download sites and audio and video applications.

Procedure

1. Add CDN domains

   See *Quick Start*. Make sure you select Acceleration of large file downloads for the business type.

2. Domain configuration

   After the domains are added, use the appropriate feature to configure the CDN domains based on your business needs. All domain configurations are optional.

The following configurations are recommended for the Acceleration of large file downloads.

Recommended configurations

- *HTTPS Secure Acceleration*, you You only need to enable the secure acceleration mode and then upload the certificate and the private key for the CDN domains. You can also view, disable and edit the certificate. For more information, see *Certificate format instructions*.
- *Cache configuration*: This feature can be used to set the actions of a cache server against resources in different directory paths and with different file name suffixes. You can customize cache expiration rules for specified resources.
- Access control settings: ensure the security of the distributed content, and prevent unnecessary traffic losses from leeching or malicious requests.
  - *Refer anti-leech protection*
  - *IP blacklist*
- *Range back-to-origin*: This feature can be used for reduced consumption of back-to-origin traffic and improved resource response time.
- *URL prefetch*: Proactively prefetches the content from the origin server to the L2 Cache node. You can directly hit the cache at the first visit to help relieve pressure on the origin server.
- For more features, see *Overview of domain configuration*.

3.3 Type 3: On-demand video/audio acceleration

Scenarios

All kinds of video/audio websites, such as video websites for films and TV dramas, video websites for online education, video websites for news, short video-featured social websites, and audio websites and applications.

Procedure

1. Add CDN domains.

   See *Quick Start*. Make sure you select Acceleration of on-demand video/audio for the business type.

2. Domain configuration

   After the domains are added, use the appropriate feature to configure the CDN domains based on your business needs. All domain configurations are optional. The following configurations are recommended for the Acceleration of on-demand video/audio.

   Recommended configurations

   - *HTTPS Secure Acceleration*: You only need to enable the secure acceleration mode and then upload the certificate and the private key for the CDN domains. You can also view, disable, enable and edit the certificate. For more information, see *Certificate format instructions*.
   - *Cache configuration*: This feature can be used to set the actions of a cache server against resources in different directory paths or with different file name suffixes. You can customize cache expiration rules for specified resources.
   - Access control settings: ensure the security of the distributed content, and prevent unnecessary traffic losses from leeching or malicious requests.
     - *Authentication configuration*: The URL authentication feature is implemented by collaboration between the Alibaba Cloud CDN nodes and client resource sites to provide a more secure and reliable way to protect origin server resources from theft.
     - *efer anti-leech protection*
     - *IP blacklist*
   - *Range back-to-origin*: This feature can be used for reduced consumption of back-to-origin traffic and improved resource response time.
   - *Drag/drop playback*: Enables random drag/drop playback in a video/audio on demand scenario.
   - *URL prefetch*: Proactively prefetches the content from the origin server to the L2 Cache node. You can directly hit the cache at the first visit to help relieve pressure on the origin server.
   - For more features, see *Overview of domain configuration*.

3.4 Type 4: Live Streaming Media Acceleration

Use cases

High-performance and stable live broadcast technical support is provided for video broadcast platforms, including interactive online educational websites, live broadcast gaming sites, personal live shows, and live broadcast platforms of event or vertical industry type. RTMP, HLS, and FLV live broadcasts. Currently, acceleration is applicable to `RTMP`, `HLS` and `FLV` live broadcasts.

Now, the live streaming service has been an independent service: *ApsaraVideo Live*.

3.5 Type 5: Dynamic Route for CDN

Now, this service has been an independent product:*Alibaba Cloud Dynamic Route for CDN*.

Introduction to application scenarios

The whole station accelerated the integration of dynamic acceleration and static acceleration, and broke through the previous individual acceleration, with simple configuration, it is intelligent to distinguish between dynamic and static requests, and achieve the whole station acceleration. All-station acceleration for dynamic and static content mixing across industries, with more dynamic resource requests (such as ASP, JSP), PHP and other format files) site:

- Scenario 1: rich and complex dynamic content reduces page loading speed and affects user experience.
- Scenario 2: single-line source stations, burst traffic, network congestion, and so on lead to page latency and content delivery failure.
- Scenario 3: Game-like customers, dynamic content, real-time communication, high concurrency, traditional communication protocols do not meet performance requirements.
- Scenario 4: The source station load distribution is uneven and the source station pressure caused by the burst visit.
- Scenario 5: Domestic operators have a complex environment, the website has been hijacked, and the content of the site has been altered, using only the HTTP protocol for transmission may be at risk of dynamic content disclosure, more secure and efficient network links and content distribution are needed.

Features

For each of the above scenarios, the Ali cloud CDN station-wide acceleration is provided:

- The dynamic and dynamic separation is accelerated, and the dynamic content uses intelligent routing, transmission protocol optimization, and link reuse technology , static content uses edge caching to improve the loading speed of the entire station resource.
- Real-Time Detection and smooth spanning technology stable and efficient handling of high-flow loads, providing all-day-to-day network availability.
- Back-to-Back load balancing, multi-source primary provisioning, connection reuse and ordered back-to-back technology reduces source pressure and Failure risk.
- All link HTTPS Security acceleration, anti-theft chain, IP flow limit, and so on, to ensure the security of the source station.
- Customize set up static rules, cache rules, and have panoramic information monitoring and warning capabilities.

 Note:
By default, all dynamic and static requests obtain resources through the optimal routed backsource, by configuring to specify a static file type or path, you can visually distinguish between dynamic and static resources, static resources cache on the edge node, dynamic resources use dynamic acceleration, to achieve the fastest acceleration effect.

4 Domain Names

4.1 Batch Configure

Introduction

You can copy specific configurations of a domain name then apply them to one or more other domain names.

Note:

You can only copy the configuration of a domain name when it is running normally.

Procedure

Make sure that you have configured the domain name that you want to copy.

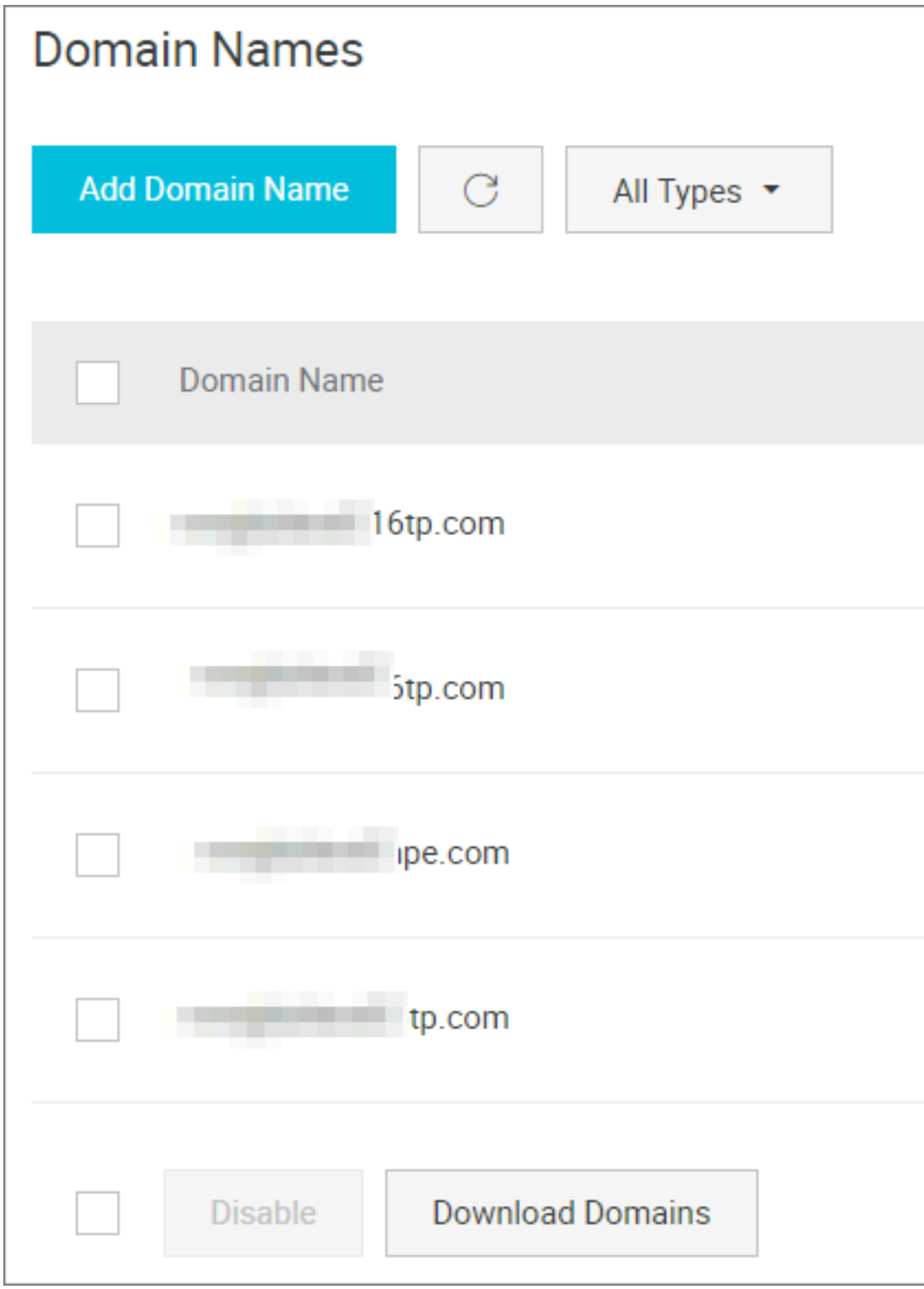
Note:

You cannot copy an HTTPS certificate to another domain name. Configure it independently.

Warning:

You cannot return to the configuration before copying. Make sure the source domain name is on service or has existing configuration, and its bandwidth is large. Copy with caution.

1. On the Domain Names page, select the domain name you want to copy, then click Copy Configuration.



2. Select the configuration items you want to copy, then click Next.

> **Note:**
> You cannot copy the origin site and other configurations at the same time.

3. Select the target domain name you want to apply configurations to, then click Next Step.

   You can also enter keywords to search for the domain name.

   > Note:
   > The copied configurations will overwrite any configurations you previously set for the target domain name. Take caution when copying configurations, or your service may become unavailable.

4. Click Confirm.

Note

- For Custom back-to-origin HTTP header, copying means adding configuration to your existing. For example, if Domain A has 2 Custom back-to-origin HTTP header configurations, and you copy 5 configurations from Domain B, you may have 7 configurations in total.
- For HTTP header, copying means covering existing configurations. For example, if Domain A's Cache_Control is set to Private, and you copy Domain B's configuration of Public, then your Cache Control is now set to Public.
- Copying configurations of switches, Referer or IP's blacklist or whitelists cover existing configurations.

4.2 Manage tags

This topic describes how to tag your domain names in the Content Delivery Network (CDN) console. You decide the usage of tags. Alibaba Cloud CDN only works to match and filter your tags and domain names by character string.

Feature introduction

You can use tags to mark the usage of domain names or to group them. Then, you can filter the data corresponding to specified domain names on the Domain Names page, Resource Monitoring page, and Usage page by using tags. This helps you query domain name data and manage domain name groups.

Limits

- Each tag consists of a key-value pair (key:value).
- Each domain name can be attached with up to 20 tags.

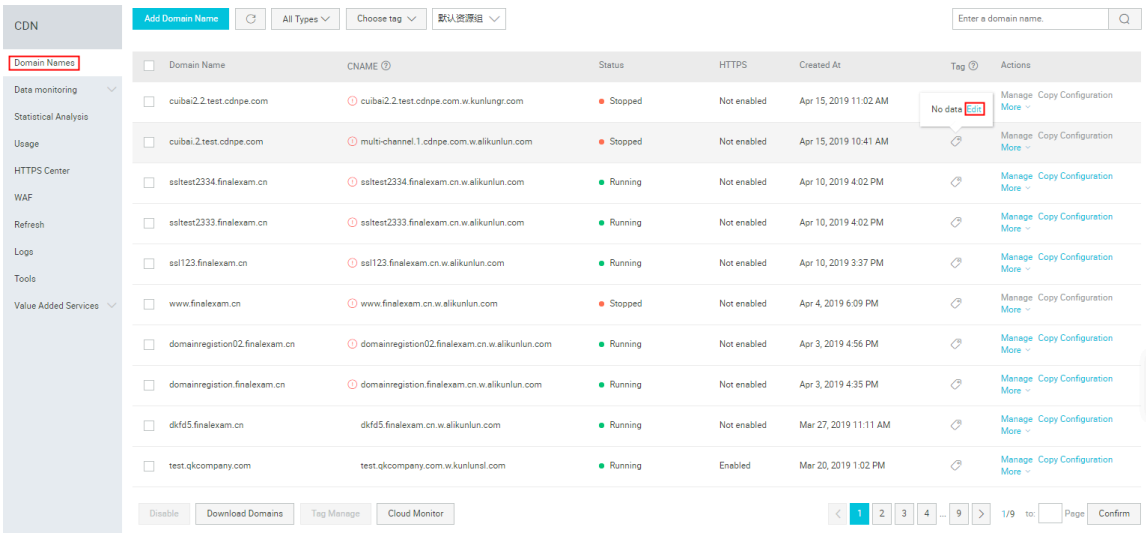
- The tag key of a domain name is unique. If you successively set two tags to have the same key but have two different values for a domain name, the new value overwrites the old one. For example, if you set the `Key1 : Value1` tag and `Key1 : Value2` tag for the domain name `test . example . com` , only the `Key1 : Value2` tag is attached to the domain name.
- A key cannot start with `aliyun :` or `acs :`. It cannot contain `http ://`, `https ://`, and it cannot contain empty strings.
- A value cannot contain `http ://`or `https ://`, but can contain empty strings.
- A key can contain up to 64 Unicode characters.
- A value can contain up to 128 Unicode characters.
- Letters in a key or a value are case-sensitive.

Procedure

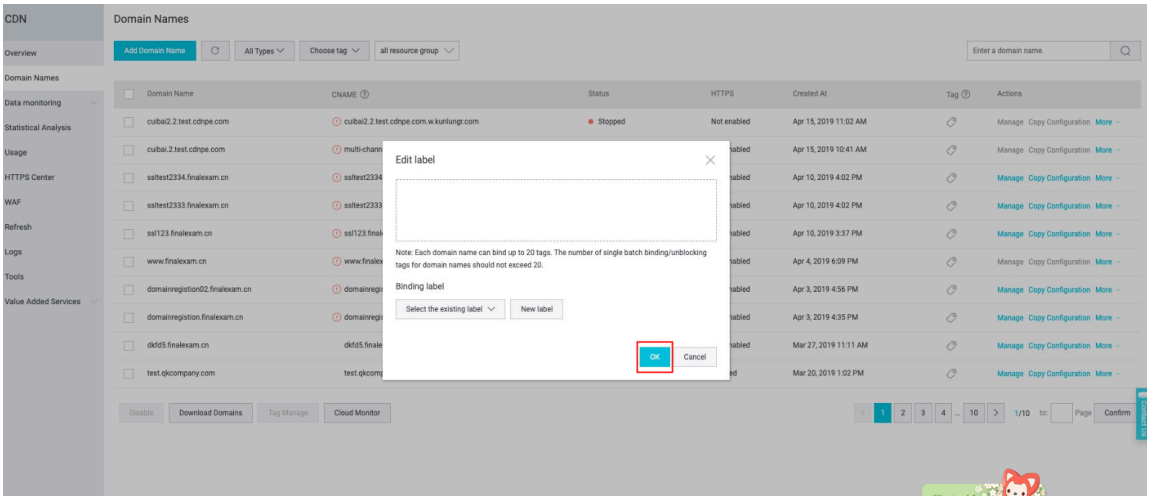
Tag editing

- To edit the tag of a single domain name, follow these steps:

  1. Log on to the *CDN console*.
  2. Click Domain Names.
  3. Select the target domain name, and then move the pointer over the corresponding tag.
  4. In the displayed shortcut menu, select Edit.



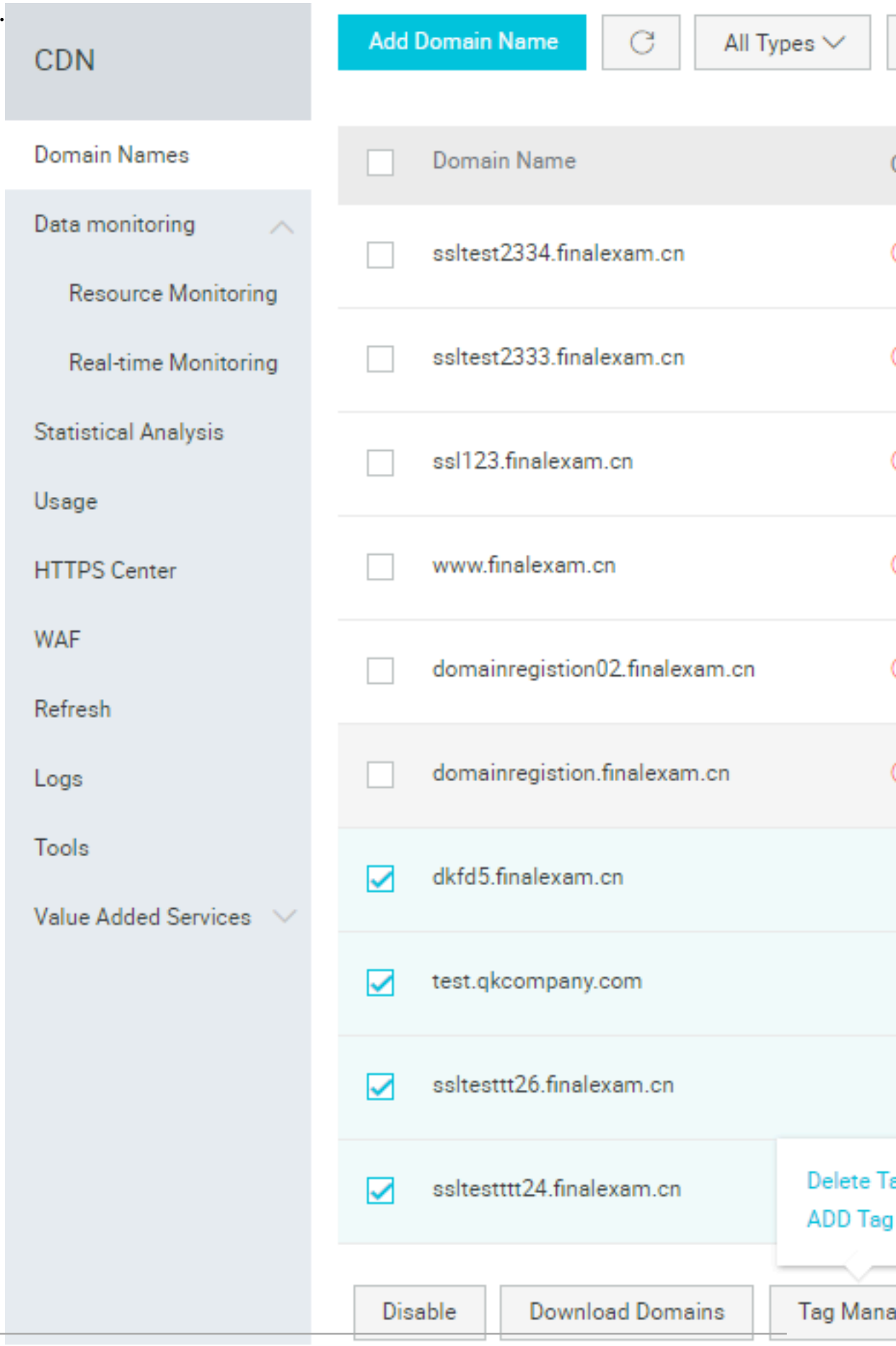
  5. In the Edit Tag dialog box, select Existing Tags or New Tags. After you finish editing the tag, click OK.



- To edit the tag of multiple domain names, follow these steps:

  1. Log on to the *CDN console*.
  2. Click Domain Names.

3. Select the target domain names, and then click Manage Tag.



4. Select Delete Tag or Add Tag.

Data filtering

To filter domain name data, follow these steps:

1. Log on to the *CDN console*.
2. On the Domain Names page, Resource Monitoring page, or Usage page, select the target tag (key:value), and then click Query.

Note:

If you select multiple tags, the query result is an intersection of the domain names corresponding to these tags.

Figure 4-1: Domain Names page

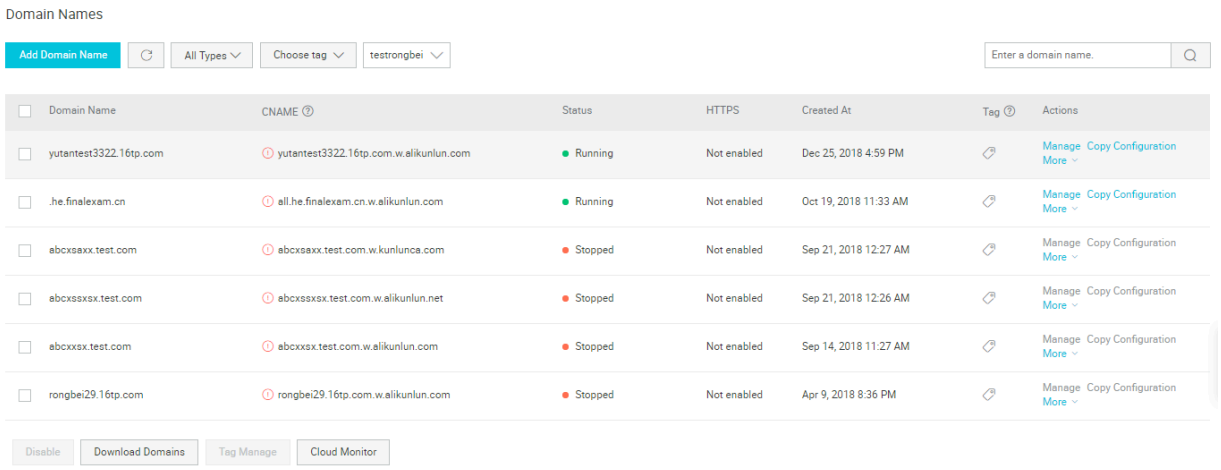


Figure 4-2: Resource Monitoring

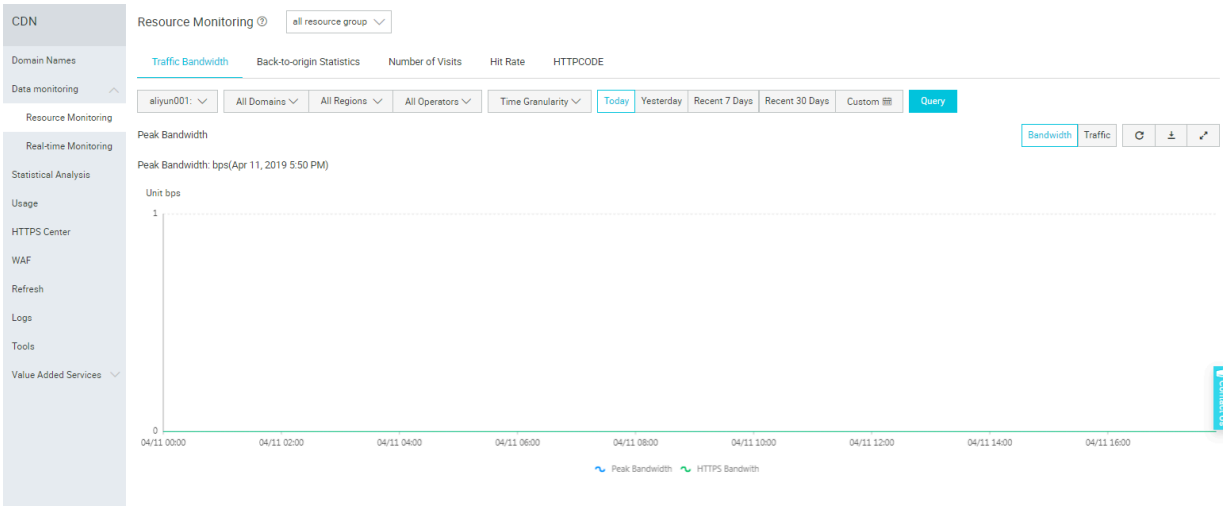
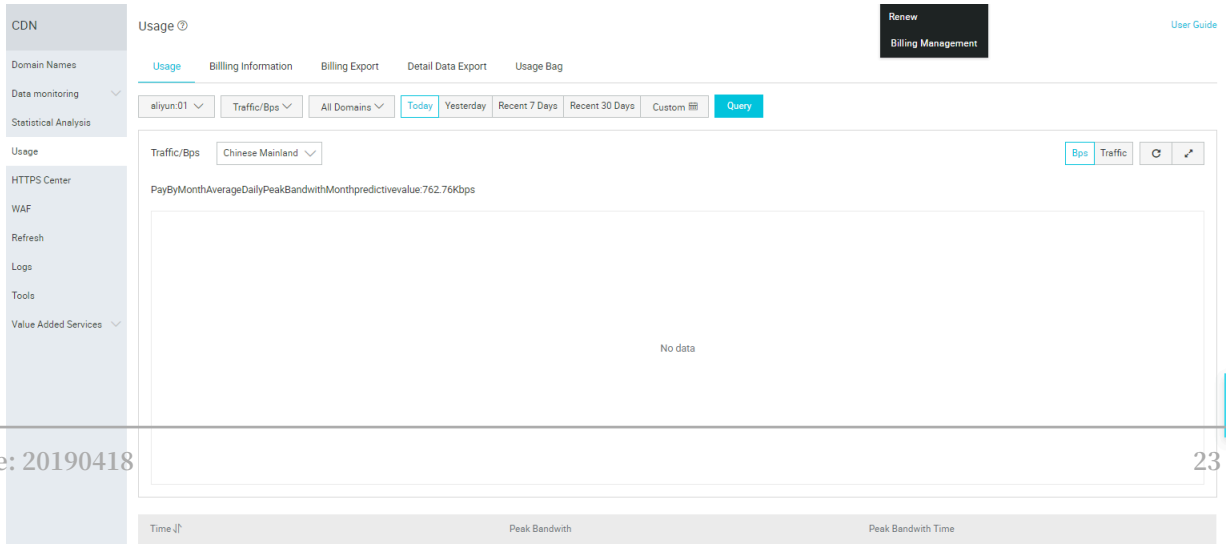


Figure 4-3: Usage



Example

Company C have 100 domain names in Alibaba Cloud CDN. These domain names are used by three departments (that is, the e-commerce, gaming, and entertainment departments) for marketing activities, Game G1, Game G2, and post-production. The company has three O&M leaders: Alice, Bob, and Chris.

Tag setting

Company C uses tags to manage its domain names and defines the following keys and values.

Key	Value
Department	E-commerce, gaming, and entertainment
Business	Marketing activities, Game G1, Game G2, and post-production
Leader	Alice, Bob, and Chris

Company C attaches these key and values to the domain names. The following table describes the relationships between the domain names and key-value pairs.

Domain name	Value for when the key is a department	Value for when the key is a business	Value for when the key is a leader
Domain 1	E-commerce	Marketing activities	Chris
Domain 2	E-commerce	Marketing activities	Chris
Domain 3	Gaming	Game G1	Alice
Domain 3	Gaming	Game G2	Alice
Domain 4	Gaming	Game G2	Alice
Domain 5	Gaming	Game G2	Bob
Domain 6	Gaming	Game G2	Bob
Domain 7	Gaming	Game G2	Bob
Domain 8	Entertainment	Post-production	Chris
Domain 9	Entertainment	Post-production	Chris
Domain 10	Entertainment	Post-production	Chris

Tag use

- If Company C wants to filter the domain names managed by Chris, the tag leader:Chris needs to be selected.
- If Company C wants to filter the domain names managed by Bob in the gaming department, the department:gaming tag and theleader:Bob tag need to be selected.

4.3 Configure origin site

In this document, you can get abreast of what is origin site and custom port, and how to configure them.

Introduction

Alibaba Cloud CDN supports three types of back-to-origin domain names: OSS back-to-origin domain name, IP address, and custom domain name. Multiple IP addresses and custom domain names are supported, and back-to-origin priority can be configured when multiple origin sites exist.

When the back-to-origin type is IP address or custom domain name, multiple origin sites are allowed and their priorities are configurable. When multiple origin sites are added, the site priority is "main" and "backup", and the priority is "main"> "backup".

All back-to-origin traffic is preferentially directed to higher-priority origin sites. If an origin site fails the health check for three consecutive times, all traffic is directed to lower-priority origin sites. If the origin site passes the health check, it is marked as available again and restored to its the original priority. When all origin sites have the same back-to-origin priority, CDN round-robin takes place.

Origin site health check: 4-layer health check is automatically performed on origin sites every 2.5 seconds.

Main supported scenario: Master/Slave origin site switch.

Procedure

1. Log on to the CDN console.
2. In the left-side pane, choose Domain Names. In the right-side pane, select a domain, and in the Actions column click Manage.
3. On the page that is displayed, choose Basic from the left-side pane, and click Modify in the Origin site info area.

4. In the Origin Site Configuration dialog box, set `Type`, `IP`, and `Port`. (You can `Port` to `Port 80`, `Port 443`, or `Custom Port`.)
   - If you set your `Origin site informatio n` to `IP` or `Origin Site`, pay as the internet-caused traffic.
   - If you set your `Origin site informatio n` to `OSS domain name`, pay as the intranet-caused traffic. For more information, see *OSS Pricing Details*.
   - If you have set an OSS domain name for your Origin Site, still pay as the intranet-caused traffic.
5. Click Confirm.

> Note:
> - Multi-source priority setting is only applicable to the IP address type and origin-site domain name type, but is not applicable to the OSS domain name type. You can select appropriate origin site types and set the reasonable priorities based on your needs.
> - Origin site setting is not applicable to acceleration of live video streaming.

Set Custom Port

You can set custom port after enabling the white list. The port number must be between 0 and 65535.

- You cannot set custom port when your static or dynamic protocol is set to Follow.
- Make sure that your back-to-origin protocol and custom port are properly in use if you want to set your back-to-origin protocol to Follow by using OpenAPI.
- Your back-to-origin method will always follow the protocol (HTTP or HTTPS) and custom port you have set by using port, no matter what you have set in console.

4.4 Content back-to-source settings

4.4.1 Back-to-origin HOST

Introduction

With this function, you can specify the domain name that the system need to access during CDN back-to-source. You can choose the domain type of acceleration domain, origin domain, or custom domain.

Note:
Specify the domain name if your origin site has been bound to multiple sites or domain names. Otherwise, your back-to-source will fail.

- By default, the Back-to-origin HOST is set as the following:
  - If the source site is of IP type, the return source host will by default accelerate the domain name.
  - If the source site is OSS source type, the source host is the source domain name by default.
- The options are: accelerating domain names, source site domain names, and custom domain names.

Note:
SNI back-to-origin is unavailable currently.

Configuration

Change configuration: Enter CDN domain name management page, select domain name access configuration page, return to source settings, you can modify the configuration of the returned host.

The difference between a source station and a return source host (one IP/host is capable of binding Multiple Domain Names/sites) ,, therefore, you need to specify which domain name/site to return to when the source is returned by setting the feed host):

- Source station: the source station determines which IP to request when the source is returned.
- Back to source host: The back to source host determines which site on the IP to access from Back To The Source request. (If you have an IP source station bound, you need to set up multiple domain names/sites The returned source host specifies which domain name the returned source is to, or the returned source fails).

Note:

- Example 1: The source station is the domain name source for www.a.com the return source host is set to www. B .com, So the actual return source is M. Www.a.com resolve to the IP corresponding to the specific site: www. B .com.
- Example 2: source station is IP source station 1. 1. 1. 1 The return source host is set to www. B .com, and the actual return source is the specific site that corresponds to 1. 1. 1. 1: www. B .com.

4.4.2 Back-to-origin with the Same Protocol

Introduction

When the back-to-source with the same protocol feature is enabled, back-to-source requests for resources uses the same protocol used by the client in order to request resources. If the client makes an HTTPS request for resources, but the resources are not cached on the node, the same back-to-source HTTPS request will be made for resources. This protocol is also applicable for HTTP requests.

Note:
The origin site must support both the port 80 and port 443; otherwise, the back-to-source may fail.

Procedure

1. Go to Domain Namespage, select the domain name, then click Manage.
2. Click Modify inCache Configuration > Back-to-origin with the Same Protocol.
3. Choose your Redirect Type: Follow HTTPS, or HTTP.

4.4.3 Private bucket back-to-origin authentication

Function overview

Private bucket back-to-origin authentication is performed when traffic of a CDN domain is diverted to the bucket marked as private under a user account. After authentication is successful and authentication configuration is enabled, domain names enabled with private bucket authentication have the permission to access the private bucket.

You can use functions such as the referer anti-leech protection and authorization provided by CDN to protect resource security.

Warning:

- After authentication is successful and the private bucket function of corresponding domains are enabled, the CDN domain can be used to access the resource content in your private bucket. Consider carefully when you decide whether to enable this function. If the content in the private bucket to be authorized is not suitable to function as the back-to-origin content of the CDN domain, do not perform authorization or enable the function.
- If your website faces attack risks, please buy Anti-DDoS service and do not perform authorization or enable the private bucket function.

Procedure

Enable private bucket back-to-origin authorization

1. Log on to the CDN console.
2. In the left-side pane, choose Domain Names. In the right-side pane, select a domain, and in the Actions column click Manage.
3. On the page that is displayed, choose Back-to-Origin from the left-side pane, and enable the function in the Private bucket back-to-origin area on the Back-to-origin configuration tab page.
4. After authorization is successful, enable private bucket back-to-origin configuration for the domain and click Confirm.

Disable private bucket back-to-origin authorization

 Note:
If your CDN domain is sending back-to-origin requests with the private bucket as the origin site, do not disable or delete private bucket authorization.

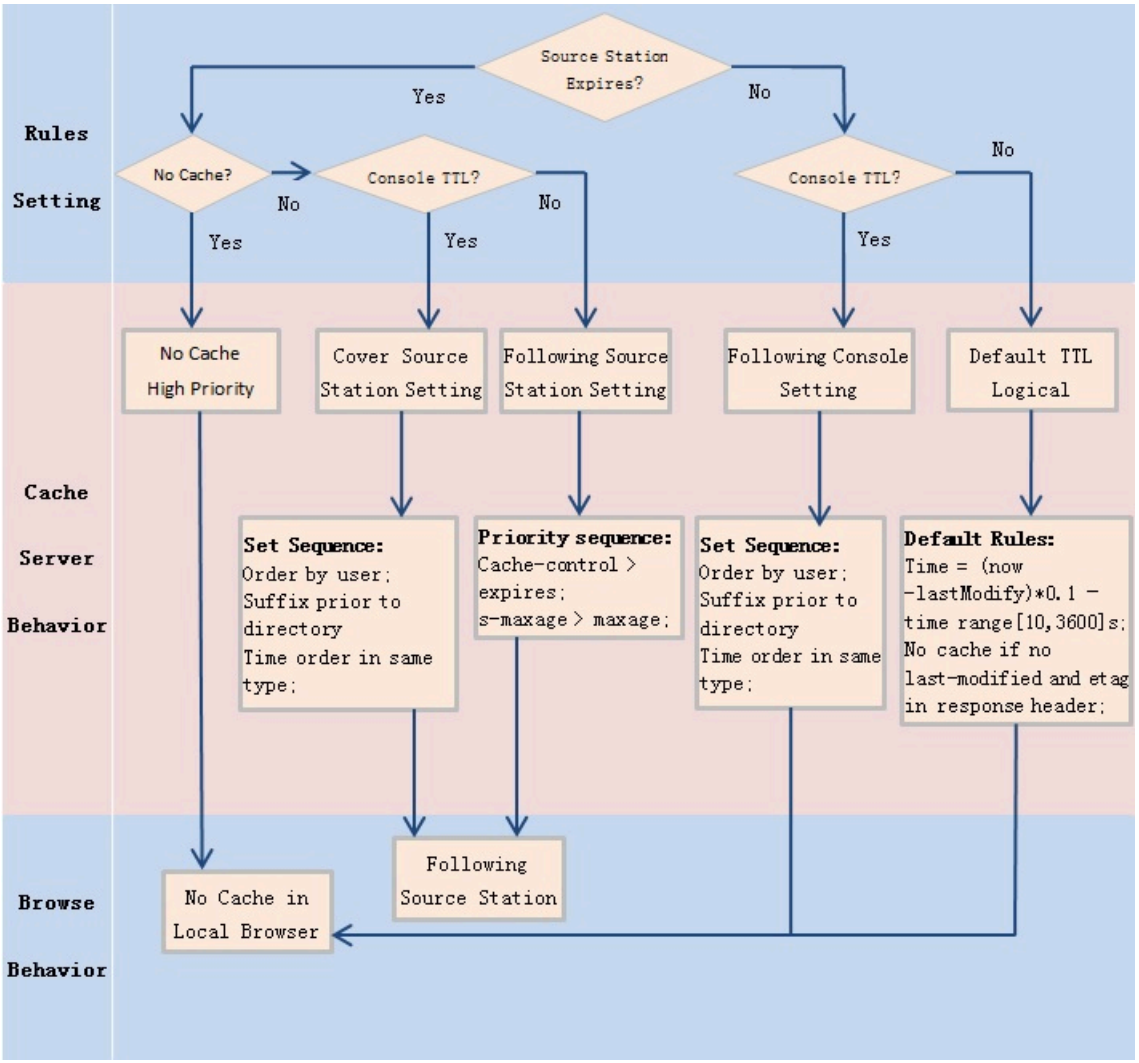
1. Choose Access Control > Role Management.
2. Delete AliyunCDNAccessingPrivateOSSRole authorization.
3. Private bucket authorization is successfully deleted.

4.5 Node Cache Settings

4.5.1 Cache Configuration

Introduction

- This function can be used to set the actions of a cache server against resources in different directory paths, or resources with different file name suffixes. You can customize cache expiration rules for specified resources.
- You can customize a cache policy priority.
- The following figure shows the default cache policies.



Note:

- This function is used to set file expiration time. The priority specified here is higher than that configured on the origin site. If no cache policy is configured on the origin site, you can set a cache policy by directory and file name suffix (the full path mode is supported).

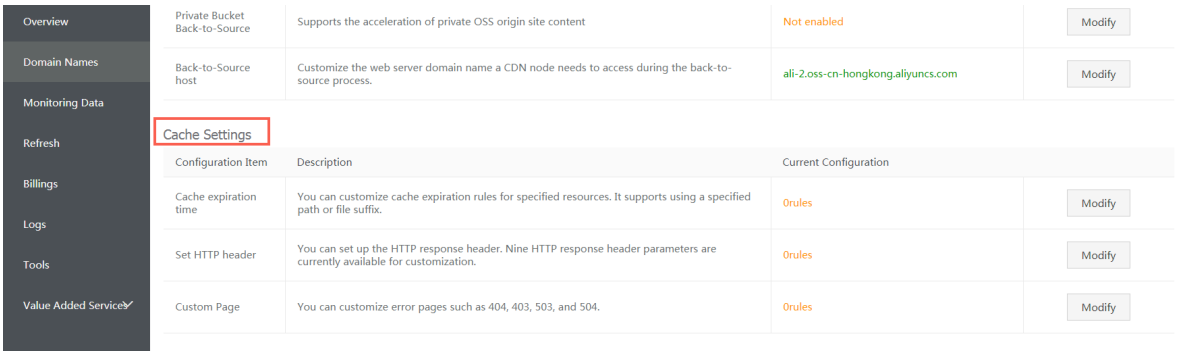
- CDN cached files can be removed from the CDN node if the cached files are not updated frequently.

Notes

- For infrequently updated static files (for example, image files or application download files), we suggest you set a cache time of 1 month or more;
- For static files that must be updated or are updated frequently (for example js and css files), you can set a shorter cache time based on the actual situation;
- For dynamic files (for example, PHP files, JSP files, and ASP files), we recommend that you set the cache duration as 0s, indicating that the files are not cached. If dynamic files such as PHP files are not updated frequently, we recommend that you set the cache duration to a small value.
- We recommend that the content on an origin site is updated with the same file name, but tagged with different version numbers; for example, img-v1.0.jpg and img-v2.1.jpg.

Configuration guide

1. Go to CDN Domain Names page, select a domain name to enter the Domain Names page and find Cache setting:



2. Click Modify, you can manage cache policies by perform adding, modifying, and deletion operations.
3. Click Add to add cache policies by directory paths or file name suffixes.

For example, set three cache policies for the CDN domain name `example . aliyun . com` :

- Cache policy 1: the cache duration for all files suffixed with .jpg and .png is one month, and the weight is 90.
- Cache policy 2: the cache duration for files in the /www/dir/aaa directory is one hour, and the weight is 70.

- Cache policy 3: the cache duration for the full path /www/dir/aaa/example.php is 0 s (No cache action will be performed), and the weight is 80.

The priority is Policy 1 > Policy 3 > Policy 2.

Note:

- The range of weight is from 1 to 99. The larger the number, the higher the priority.
- We recommended that you do not set the same weights for different cache policies. Cache policies with the same weight will be assigned a random weight value.

4.5.2 Set the HTTP Response Header

Introduction

HTTP headers (fields) are components of the header section of request and response messages in the Hypertext Transfer Protocol (HTTP). They define the operating parameters during the HTTP process. HTTP headers can be classified into general headers, request headers, response headers, and so on.

You can set an HTTP Response Header. The following HTTP response header parameters are available for customization:

Parameters	Description
Content - Type	Specifies the content type of the client program's response object.
Cache - control	Specifies the caching policy that the client program is following when requesting and responding.
Content - Dispositio n	Specifies the default file name provided by the client program when it is willing to save the contents accessed by request as a file.
Content - language	Specifies the language of the client program's response object.
Expires	Specifies the expiration time of the client program's response object.
Access - Control - Allow - Origin	Specifies the allowed origin domain of cross-origin requests.
Access - Control - Allow - Methods	Specifies the allowed method of cross-origin requests.

Parameters	Description
`Access-Control-Max-Age`	Specifies the length of time the response result is cached for a pre-fetch request initiated by a client program for a particular resource.
`Access-Control-Expose-Headers`	Specifies the custom header information that is allowed to be accessed.

Note

- The HTTP response header configurations will affect the response actions of all client programs of the resource under the CDN domain name, rather than the actions of the cache server.
- For now, you can only customize the HTTP header. *Submit a ticket* if you have other custom requirements for HTTP header.
- You can type in `*` (indicating all domain names) or a full domain name (such as `www.aliyun.com`) for the `Access-Control-Allow-Origin` parameter.
- For now, you cannot set HTTP headers for an extensive domain name.

Procedure

1. Log on to the CDN console, then go to the Domain Names page. Choose a domain name, then click Manage.
2. Go to Caching Configuration > HTTP Header, then click Modify or Delete for a parameter. You can also click Add, and then choose the parameter and enter value to add a custom HTTP header parameter

4.6 HTTPS Acceleration

4.6.1 HTTPS Secure Acceleration

Introduction

HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) is an HTTP channel designed to ensure security. It encapsulates HTTP with the SSL/TLS protocol, so the foundation of HTTPS security is SSL/TLS protocol.

HTTPS Acceleration Advantages:

- Encrypt important information during transmission, avoiding attack-caused information leaking, such as session ID or cookies.
- Perform the data integrity during transmission, preventing man-in-the-middle attack (MITM), such as DNS or contents being hijacked by third party.

Alibaba Cloud CDN provides HTTPS Secure acceleration. When you have uploaded certificate and secret keys after enabling HTTPS, so that you can check, disable, enable and edit the certificate.

How it works

The HTTPS Secure Acceleration encrypts your request to Alibaba Cloud CDN nodes. And the CDN nodes still follow your origin site's configuration to access resources in the origin site. We recommend you configure and enable HTTPS on your origin site, encrypting your full-link HTTPS acceleration.

Here is the HTTPS encryption process:

1. You start an HTTPS request.
2. The server generates a public key and a secret key (self-made or apply from professional organization).
3. The server sends the public certificate to your side.
4. You side verify the certificate.
   - If the certificate is correct, a random number (private key) is generated and encrypted with the public key, and transferred to the server.
   - If the certificate is incorrect, the SSL handshake fails.

    Note:
   The certificate verification includes: the certificate being within the period of validity, the reliability of certificate's CA, the certificate's public key being able to encrypt the number signature of the server's issuer, and the domain name on the server's certificate being matched with its real domain name.
5. The server uses the previous secret key to decrypt and get the random number (private key).
6. The server encrypt the transmitted data by using the private key.
7. You side decrypt the encrypted server date by using private key, and eventually get the data.

Notes

About configuration

- HTTPS secure acceleration is available in the following service types: Image and Small File, Download, Video, and Live Streaming Media.
- HTTPS acceleration for wildcard domain names is available.
- You can Enable or Disable HTTPS acceleration:
  - Enable: you can modify the certificate. The system is compatible with all your HTTP and HTTPS requests by default. You can also customize Forcible redirect for original request method.
  - Disable: the system will neither support HTTPS request nor save the certificate or secret key's information. You need to re-upload the certificate or secret key when you reopen the certificate.
- You can check the certificate, but cannot check the secret key due to its importance . Make sure that you have taken care of certificate information.
- Update your certificate with caution. The update will take effect in 1 minute.

About billing

HTTPS Secure Acceleration is a value-added service, so that you need to pay for the HTTPS requests. For more information, see HTTPS pricing.

 Note:
You need to pay for HTTTPS requests separately. Make sure that your account balance is sufficient , otherwise it may affect your CDN service.

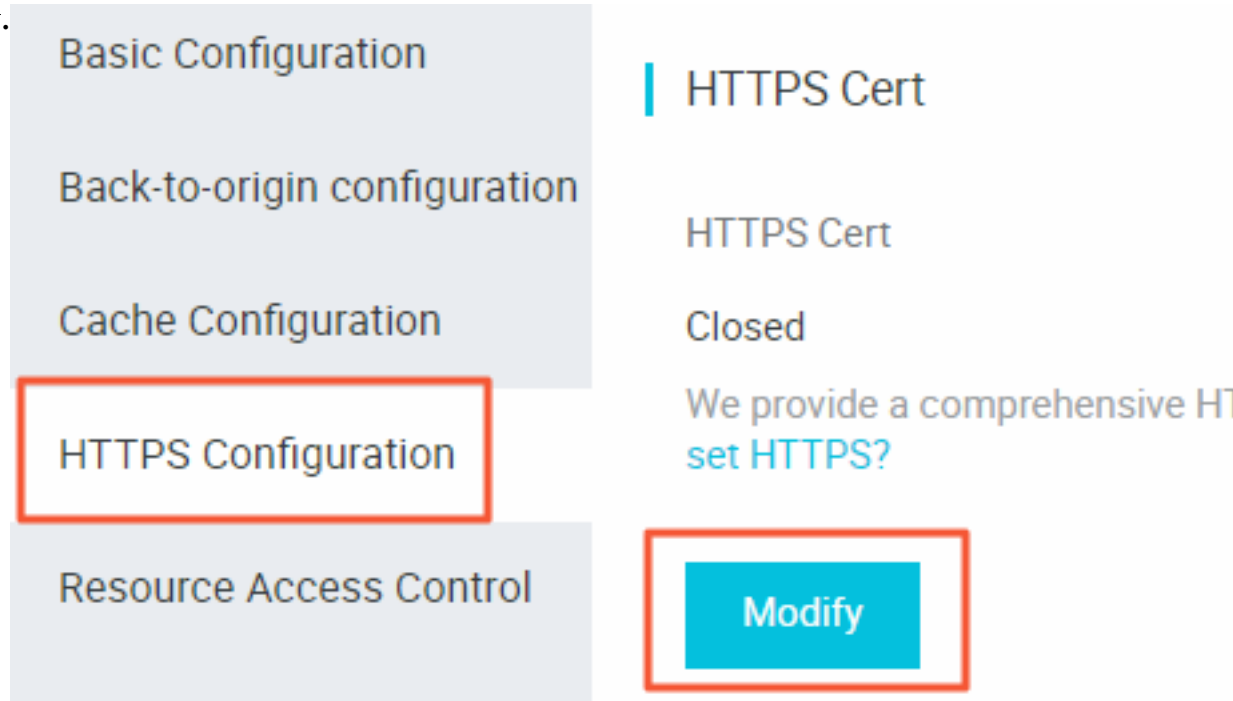
About certificate

- To enable acceleration domain name with the HTTPS Secure Acceleration feature, you need to upload the certificate and secret key in the `PEM` format.

   Note:
  As Alibaba Cloud CDN only adopts Nginx-based Tengine service, only the certificate in `PEM` format is available. For more information, see *Certificate Format*.
- Only SSL/TLS handshake with SNI information is available.
- The certificate you upload should be matched with your secret key, otherwise your verification may fail.
- Secret key with a password is unavailable.

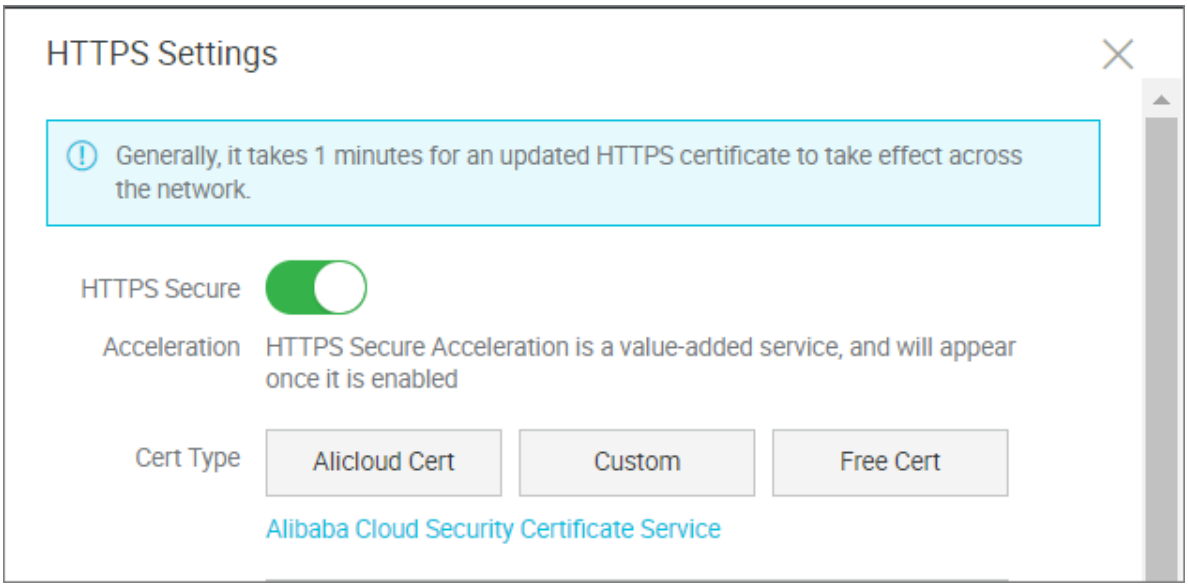
Procedure

1. Purchase a certificate. Only when you own the certificate that is matched with your domain name can you enable HTTPS Secure Acceleration. You can easily purchase Alibaba Cloud Certificate in the *SSL Certificate console*, or apply for free certificate.
2. Log on to the *CDN console*, and enter the Domain Names page. Select the domain name, and click Manage.
3. In HTTPS Configurations > HTTPS Cert, click Modify.

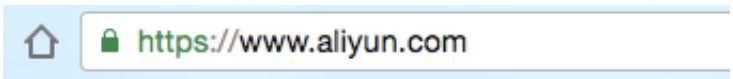


4. In the HTTPS Settings dialogue, enable HTTPS Secure.

5. Select your certificate type. You can choose Alibaba Cloud, Custom or Free Cert. Currently, only the `PEM` format is available.



   - You can choose the Alibaba Cloud Certificate. If you have no matched certificate in your list, choose custom certificate. You need to upload the certificate contents and secret key after setting the certificate name. This certificate will be saved in your Alibaba Cloud Security. You can check in *My Certificate*.
   - You can also choose free certificate, namely, Alibaba Cloud CDN Digicert DV version SSL Free certificate. This free certificate is only available for Alibaba Cloud CDN service, and it can't be managed in the SSL Certificates service of Alibaba Cloud Security. This certificate is only used to enable HTTPS Secure Acceleration in CDN, and you cannot obtain its public and private keys for other use. After you choose to use the Free Cert type, it takes about 10 minutes for the certificate to be effective.
6. Verify whether the certificate is effective. You can access resources by using HTTPS after the certificate becomes effective (about 1 hour). Green HTTPS mark indicates that you have established private connection with the website, and HTTPS secure acceleration has comes into effect.



Note:
About replacing your certificate:

- If you want to change your certificate to free certificate or Alibaba Cloud certificate, re-choose the target certificate (Free Cert or Alibaba Cloud Cert) in the HTTPS Settings page.
- If you want to change your certificate to custom certificate, choose Custom in the HTTPS Settings page. Enter the target certificate name and contents to the box of the window, then deliver it.

4.6.2 Certificate Format

Before *Enabling the HTTPS* service, you must configure certificates. You can directly select managed or purchased certificates in *SSL Certificates* , apply for free certificates, or manually upload custom certificates. Custom upload only supports certificates in `PEM` format. You must convert certificates and private keys from other formats to the PEM format.

Certificate format requirements

Certificate authorities (CAs) generally provide the following types of certificates. Among these, Alibaba Cloud CDN uses the Nginx format (certificates are .crt files and private keys are .key files):

- If certificates are issued by a root CA, you receive only one certificate.
- If you have obtained a certificate file consisting of multiple certificates from an intermediate CA, you must manually splice the server certificate and intermediate certificate before uploading them together.

 Note:
Splicing rules: The server certificate must be followed by the intermediate certificate without any blank line. Generally, the CA provides the relevant description when issuing a certificate. So pay attention to the rule description.

Example

Confirm the format is correct before uploading.

Certificates issued by a root CA

In Linux environments, certificates are in the `PEM` format:

```
-----BEGIN CERTIFICATE-----
MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzIwHhcNMTAxMDA4
MDAwMDAwWhcNMTMxMDA3MjM1OTU5WjBqMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
V2FzaGluZ3RvbjEQMA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv
bSBJbmMuMRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWn0uIVGdg76626ggOoJSaj48R2n0MnVcC
AwEAAaOCAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVlJTZWN1cmUtRzItY3JsLnZlcmlzaWduLmNvbS9TVlJT
ZWN1cmVHMi5jcmwwRAYDVR0gBD0wOzA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUF
BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBSl7wsRzsBBA6NKZZBIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWUlNlY3VyZUcyLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFow
WDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEF
GDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq3OP4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2LlDWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

Certificate rules:

- **Upload the `----- BEGIN CERTIFICAT E -----` and `----- END CERTIFICAT E -----` content together.**
- **Each line has 64 characters, but the last line can have less then 64 characters.**

Certificate links issued by intermediate CAs:

```
----- BEGIN CERTIFICAT E -----

----- END CERTIFICAT E -----

----- BEGIN Certificat e -----

----- END CERTIFICAT E -----

----- BEGIN CERTIFICAT E -----

----- END CERTIFICAT E -----
```

Certificate link rules:

- **Do not insert a blank line between certificates.**
- **Each certificate must comply with the certificate rules.**

RSA private key format requirements

RSA private key rules:

- Run the `openssl genrsa -out privateKey.pem 2048` command to generate a local private key, with `privateKey.pem` being the private key file.
- `-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----` indicate the beginning and end of the private key file, respectively. Upload the beginning and end content together.
- Each line has 64 characters, but the last line can have less than 64 characters.

If your private key is not generated in the format `-----BEGIN PRIVATE KEY-----`,

```
——- END PRIVATE
      KEY -----
```

based on the preceding rules, run the following command to convert the private key:

```
openssl rsa -in old_server_key.pem -out new_server
_key.pem
```

Then, upload `new_server_key.pem` content together with the certificate.

Certificate format conversion method

CDN HTTPS Secure Acceleration only supports certificates in the PEM format. Certificates in other formats must be converted to the PEM format. We recommend using the OpenSSL tool for conversion. The following shows the methods used to convert other common certificate 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 privatekey.der -out privatekey.pem
```

P7B to PEM

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

- Certificate conversion:

```
openssl pkcs7 -print_cert s -in incertificate.p7b -out outcertificate.cer
```

In `outcertificate.cer`, Retrieve the `-----BEGIN CERTIFICATE-----`, `-----END CERTIFICATE-----` content and upload the content as a certificate.

- Private key conversion: P7B certificates do not have private keys, so you only have to enter the certificate portion, not the private key portion, in the CDN console.

PFX to PEM

The PFX format is generally used in 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
```

Free certificates

The free certificate here is Alibaba Cloud CDN Digicert DV version SSL Free certificate, only available for Alibaba Cloud CDN service. It cannot be managed in the SSL Certificates service of Alibaba Cloud Security. This certificate is only used to enable HTTPS Secure Acceleration in CDN, and you cannot obtain its public and private keys for other use.

- The application process for a free certificate takes 5-10 minutes. While waiting, you can also go back and choose to upload a custom certificate or select a managed certificate.
- You can always switch among custom, managed or free certificate no matter which one you enable at the beginning.
- Free certificates are valid for one year and automatically renewed upon expiration.
- When using this product, if you disable the HTTPS settings and then enable the free certificate option again, the system uses the free certificate you applied for previously, provided it has not expired. If your certificate has expired when you enable the free certificate option, the system reapplies for a free certificate.

Other certificate issues

- You can disable, enable, and modify certificates. After you disable a certificate, the system no longer retains the certificate information. When you re-enable the certificate, you must upload the certificate and private key again. See *HTTPS Secure Acceleration settings tutorial*.
- Only SSL/TLS "handshakes" with SNI information are supported.
- Ensure that the certificate and private key you upload match.
- Certificate updates take effect in 10 minutes.
- Private keys with passwords are not supported.

4.6.3 HTTP/2

Introduction

HTTP/2, the latest HTTP protocol published in 2015, is now available in many browsers, such as Chrome, IE11, Safari, and Firefox. With main features similar to SPDY, HTTP/2 can be seen as an advanced edition of HTTP/1.1.

HTTP/2 Benefits

- Binary protocol: Compared with HTTP 1. x, HTTP/2 segments transferring information into smaller frames and messages and encodes them by using binary, which makes the protocol more scalable. For example, data and command can be transferred by frame.
- Content security: Based on HTTPS, HTTP/2 gives considerations to both security and performance.
- Multiplexing: With HTTP/2, your browser can trigger multiple requests in one connection, and receive these requests in any order or at the same time. Moreover , stream dependencies is also available in multiplexing, allowing client servers to define which contents to be transferred in priority.
- Header compression: HTTP/2 compresses and transfers message headers in the HPACK format and creates an index table for the headers. Only the index are transferred, which improves the transferring efficiency and speed.
- Server push: Similar to SPDY, HTTP/2 allows servers to actively push contents to clients without a request, significantly improving web page loading speeds.

Procedure

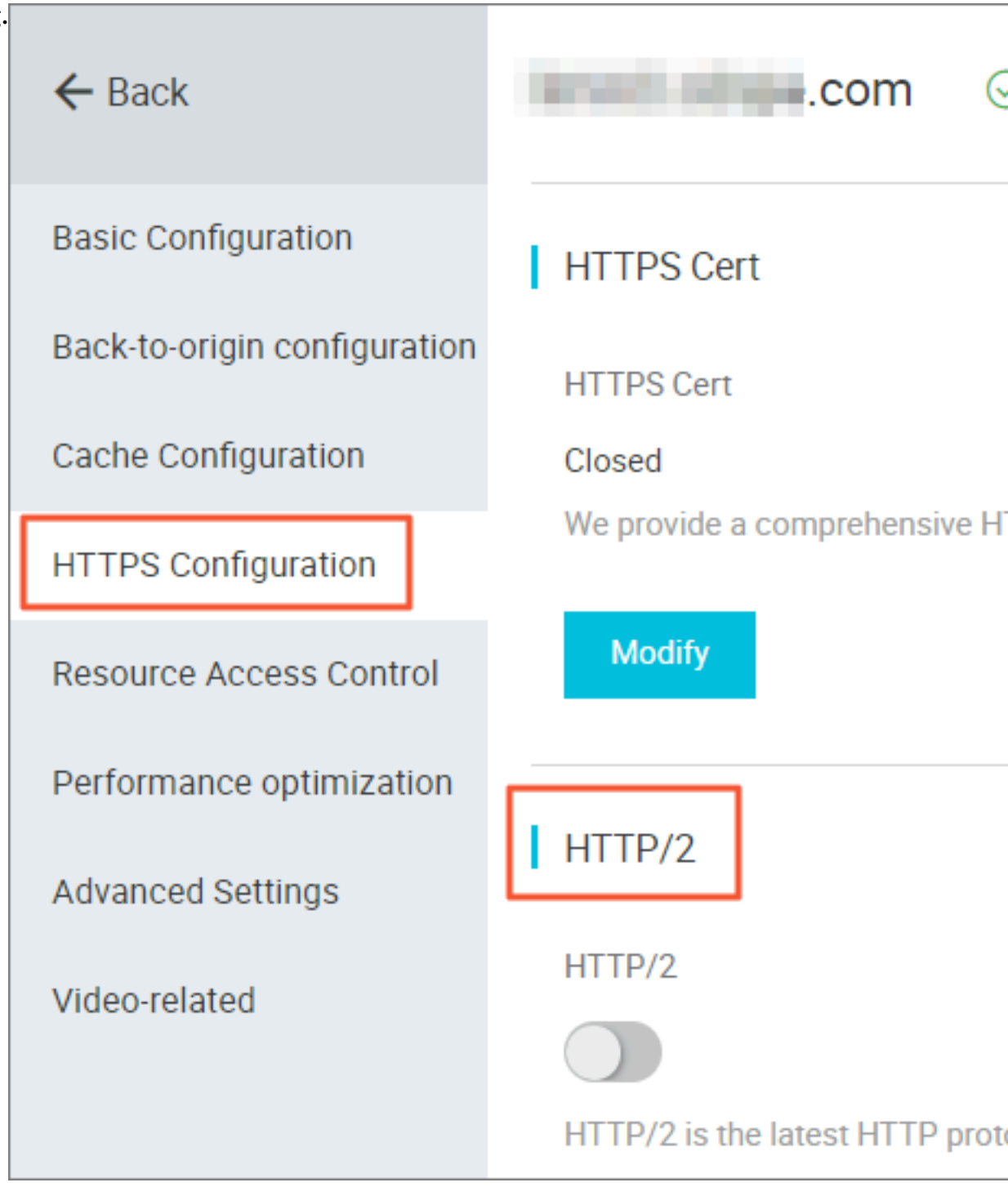
1. Log on to the *CDN console*.
2. On the Domain Names page, select a domain name and click Configure.

Note:

Make sure that you have configured HTTPS certificates before enabling HTTP/2.

- If it is your first time configuring HTTPS certificate, wait for a while until your configuration coming into effect.
- If you disable HTTPS certificates when your HTTP/2 service is running, your HTTP/2 service will be disabled automatically.

3. Enable the HTTP/2 in HTTPS Settings > HTTP/2 Setting.

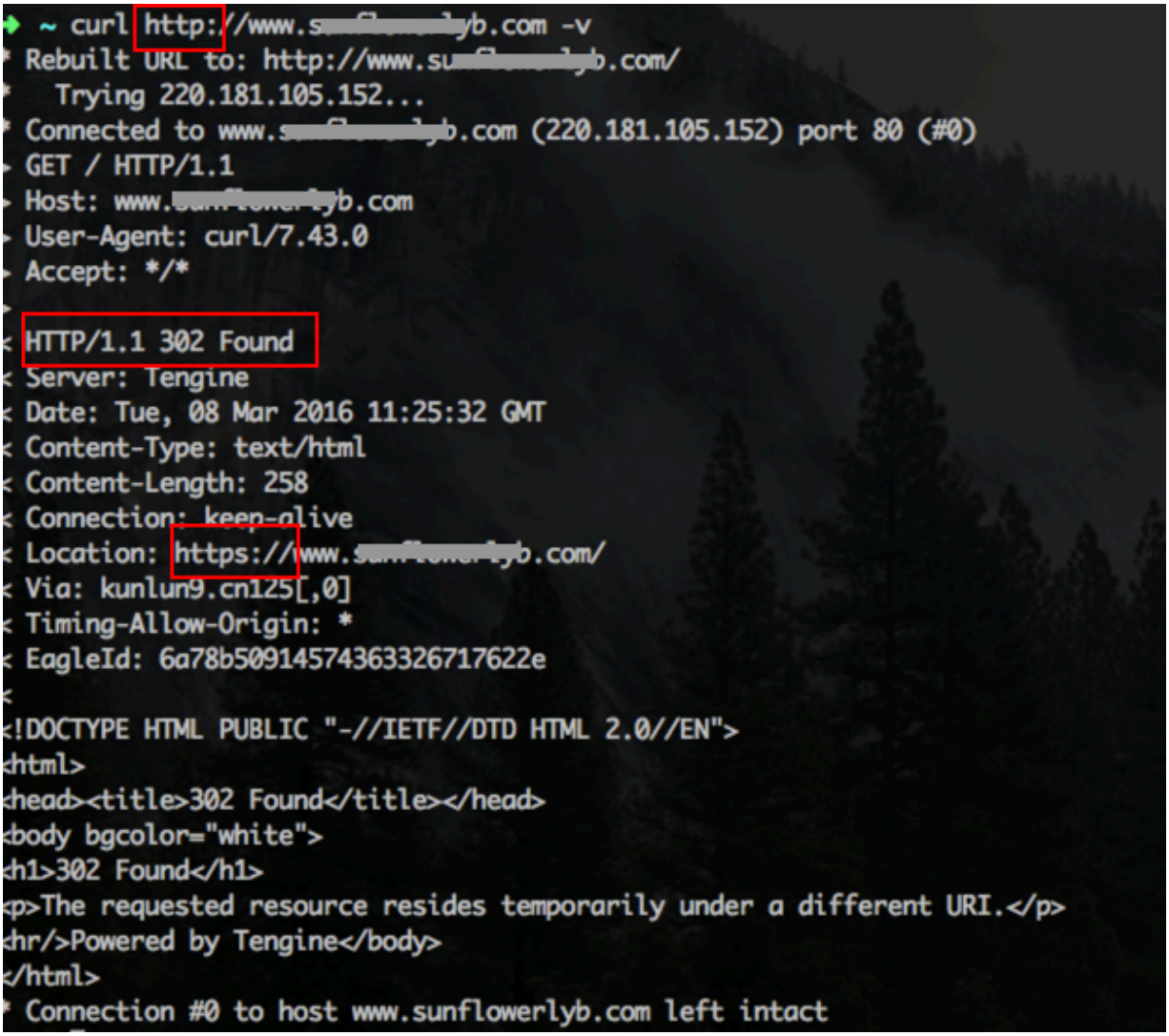


4.6.4 Force Redirect

Introduction

When HTTPS Secure Acceleration is enabled for a CDN domain, it supports custom settings to perform force redirects on users' original request methods.

For example, when force HTTPS redirect is enabled and a user initiates an HTTP request, the server returns a 302 redirect response and the original HTTP request is forcibly redirected to an HTTPS request, as shown in the following figure.



Force Redirect is disabled by default. When you enable the feature, both HTTP and HTTPS requests are enabled simultaneously by default.

Options: Default, Force HTTPS redirect, and Force HTTP Redirect.

- Force HTTPS redirect: User requests are forcibly redirected to HTTPS requests.
- Force HTTP redirect: User requests are forcibly redirected to HTTP requests.

Procedure

1. Go to Domain Namespage, select the domain name, then click Manage.
2. Enable the function in HTTPS Configuration > Forcible redirect .

4.6.5 TLS

This document describes the features of Transport Layer Security (TLS) and how to use TLS.

Features

TLS is a cryptographic protocol designed to ensure communication security and data integrity of a computer network. HTTP Strict Transport Security (HSTS) is a typical application of TLS. HTTPS, also known as HTTP over TLS, is a secure version of HTTP. HTTPS runs under the top application layer HTTP and above the transport layer TCP. HTTPS encrypts and decrypts user page requests.

TLS has four versions:

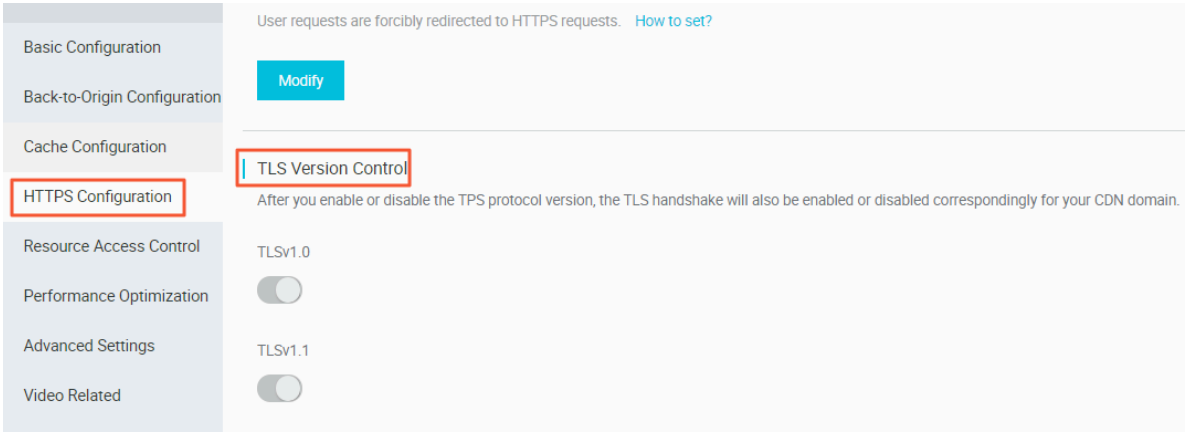
- TLS Version 1.0: TLS Version 1.0 was published as RFC 2246 in 1999 based on SSL Version 3.0. This version is vulnerable to various attacks, such as BEAST attacks and POODLE attacks. RFC 2246 provides weak encryption that is not strong enough to protect the current network connection. TLS Version 1.0 is not compliant with Payment Card Industry Data Security Standard (PCI DSS). Supported browsers include IE 6.0 or later, Chrome 1.0 or later, and Firefox 2.0 or later.
- TLS Version 1.1: TLS Version 1.1 was published as RFC 4346 in 2006. This version fixed some vulnerabilities of TLS Version 1.0. Supported browsers include IE 11.0 or later, Chrome 22.0 later, Firefox 24.0 or later, and Safari 7.0 or later.
- TLS Version 1.2: TLS Version 1.2 was published as RFC 5246 in 2008. This is currently the most widely used version. Supported browsers include IE 11.0 or later, Chrome 30.0 or later, Firefox 27.0 or later, and Safari 7.0 or later.
- TLS Version 1.3: TLS Version 1.3 was published as RFC 8446 in 2018. As the latest TLS version, RFC 8446 is faster because it supports the 0-RTT mode. Also, this version is more secure as it only supports perfect forward secrecy key exchange algorithms. Supported browsers include Chrome 70.0 or later and Firefox 63.0 or later.

 Note:
Currently, TLS Version 1.0, TLS Version 1.1, and TLS Version 1.2 are enabled by default.

Procedure

> **Note:**
> You must configure the HTTPS certificate and then enable TLS.

1. Log on to the *CDN console*.
2. In the left-side navigation pane, click Domain Names.
3. Select a domain name to be configured, and click Manage.
4. In the left-side navigation pane, click HTTPS Configuration.



5. In TLS Version Control, you can enable or disable a specific TLS version based on your needs.

4.6.6 HSTS

This document describes the technical details and scenarios of HTTP Strict Transport Security (HSTS), and how to operate HSTS in the Alibaba Cloud console.

Features

HSTS is specified in RFC 6797. HSTS instructs clients, such as a browser, that a domain can only be accessed by using HTTPS.

Scenarios

After you have enabled HTTPS on the entire website, redirect your users and search engines to the HTTPS page with 301 or 302 HTTP redirects. If you enter an HTTP URL in a Web browser or click an HTTP URL in another location, the server will redirect the HTTP request to HTTPS. When redirecting the requests to HTTPS, a man-in-the-middle (MITM) can still hijack the connection before the redirect. As a result, the requests cannot be sent to the specified server. To address this issue, you can set the HTTP HSTS header to standardize all client connections on HTTPS.

HSTS is a response header: Strict-Transport-Security: max-age=expireTime [; includeSubDomains] [; preload]. The parameters are described as follows:

- max-age is expressed in seconds.
- Strict-Transport-Security: HSTS is a Web security mechanism that restricts browsers to access Web servers over HTTPS for only a given amount of time. If a website accepts a connection through HTTP and the amount of time specified for the Strict-Transport-Security mechanism is not passed, the browser starts a 307 internal redirect from HTTP to HTTPS. This helps to avoid hijacks occurred in the 301 and 302 redirects.
- includeSubDomains is optional. If this parameter is specified, this rule applies to all subdomains of the site as well.
- preload is optional. The site owner can submit a website to the preload list.

 Note:

- Before HSTS takes effect, you still need to use the 301 or 302 redirect for the first redirect.
- The HSTS response header is valid in response to the HTTPS requests and invalid in response to HTTP requests.
- The HSTS response header is only valid to the 443 port.
- The HSTS response header is valid to domain names and invalid to IP addresses.
- After enabling HSTS, if the website certificate is incorrect, the certificate may need more time to process.

Procedure

 Note:
Configure the HTTPS certificate and then enable the TLS feature.

1. Log on to the *CDN console*.
2. In the left-side navigation pane, clickDomain Names.
3. Select a domain name, and click Mange.

4. In the left-side navigation pane, click HTTPS Configuration.

5. In HTST, click Modify. to complete the configuration.

4.7 Access Control Settings

4.7.1 Anti-leech

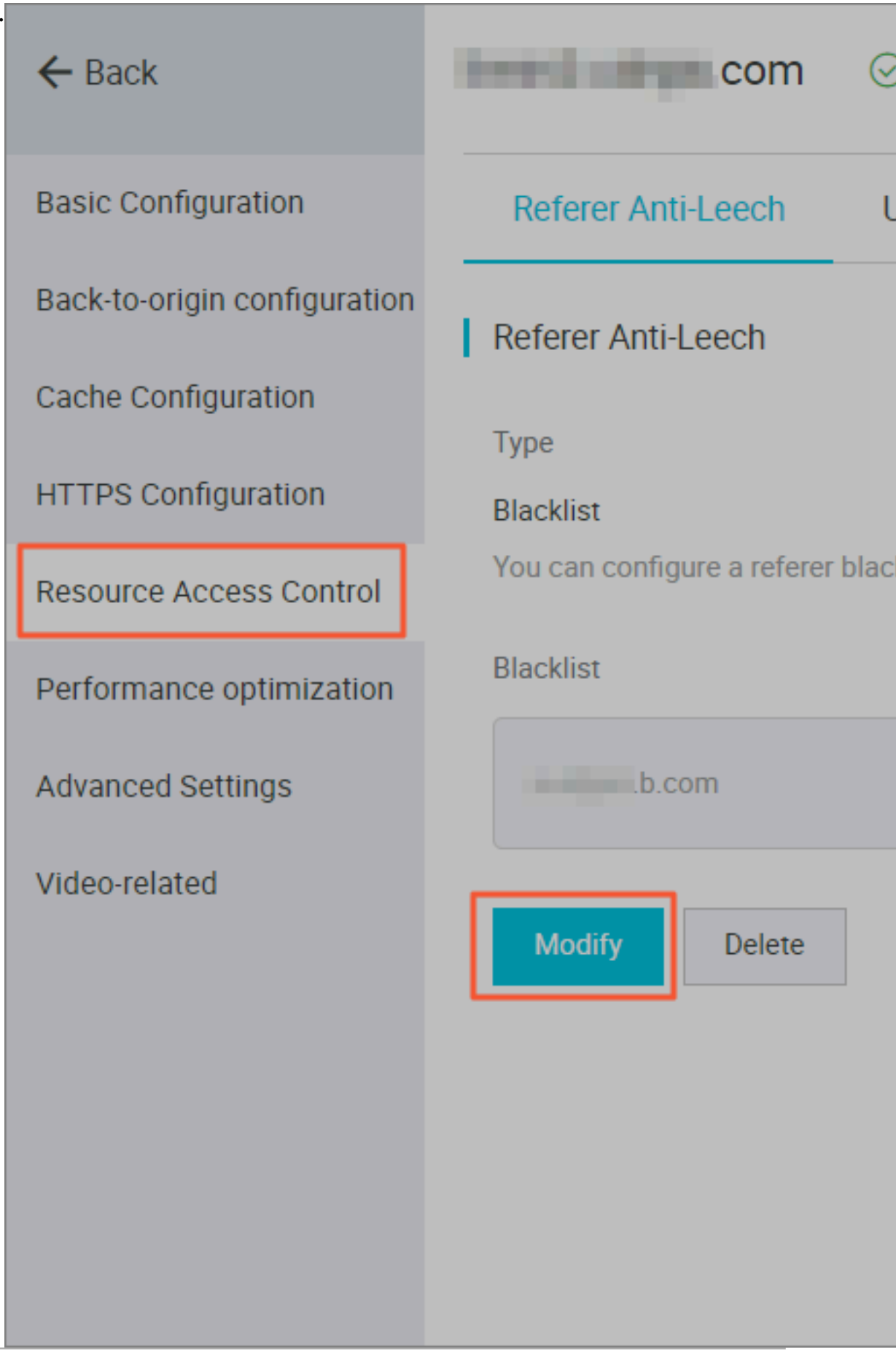
Introduction

- The anti-leech function is based on the HTTP referer mechanism where the referer , namely an HTTP header field, is used for source tracking, source recognition and processing. You can configure a referer black list or whitelist to identify and filter visitors in order to limit access to your CDN resources.
- Currently, the anti-leech function supports the black list or whitelist mechanism. After a visitor initiates a request for a resource, and the request arrives at a CDN node, the CDN node filters the identity of the visitor based on the preset configuration of the anti-leech black list or whitelist.
  - If the identity complies with the rules, the visitor can access the requested resource.
  - If the identity does not comply with the rules, the request is forbidden and a 403 response code is returned.

Procedure

1. Go to Domain Namespage, select the domain name, then click Manage.

2. On Resource Access Control > Anti-leech, click Modify.



3. ChooseBlacklist or Whitelist, and add the IP network segment in the box below.
4. Click Confirm.

Notes

- This function is optional and is disabled by default.
- You can only select one of Refer Blacklist or Refer Whitelist to edit at the same time .
- After configuration, wildcard domain name support is added automatically. For example, if you enter `a . com` , all sub-domain names under `*. a . com` take effect.
- You can set a null Referer field to access resources on a CDN node (that is, allowing to access the resource URL by typing the address in browser).

4.7.2 Authentication configuration

The URL authentication feature is designed to protect user's origin server resources from unauthorized downloading and misappropriation. Referer blacklist and whitelist with anti-leech can protect video content from some leeching attacks too some degree. However, it cannot completely protect site resources, as the referer contents can be forged. As a result, it is a more secure and effective way to protect your resources by using URL authentication.

How it works

URL authentication uses Alibaba Cloud CDN nodes together with client resource sites to provide more secure and reliable anti-leech protection for origin site resources.

1. The CDN client site provides an encrypted URL including verification information of permissions.
2. You use the encrypted URL to initiate a request to the CDN node.
3. The accelerated node authenticates the permission information in the encrypted URL to determine the legitimacy of the request. A normal response to a legitimate request will reject an illegal request.

Authentication method

Alibaba Cloud CDN supports 3 authentication methods: A, B, and C. You can choose the authentication method based on your business need, so that it will help protect your origin site.

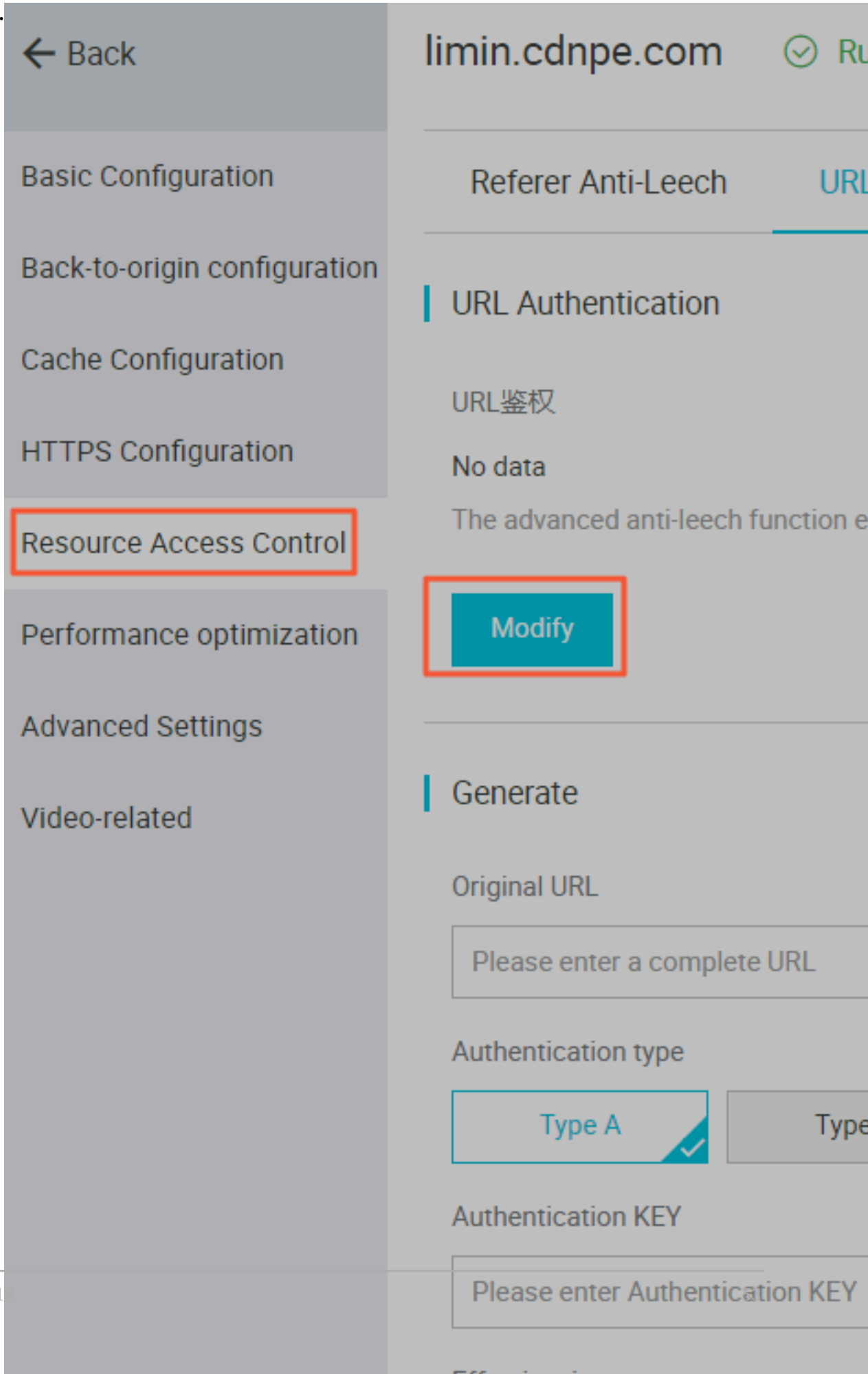
Sample authentication code

You can check *Sample authentication code*.

Procedure

1. Log on to the CDN console.
2. In the left-side pane, choose Domain Names. In the right-side pane, select a domain, and in the Actions column click Manage.
3. On the page that is displayed, choose Resource Access Control from the left-side pane, and then click Modify in

the URL Authentication area on the URL authentication tab page.



4. In the Authentication URL dialog box, switch on Authentication URL, select an Authentication type, and enter Master Key and Backup Key.
5. Click Confirm.

4.7.3 Authentication method A

How it works

Formats of the encrypted URL for user access

```
http :// DomainName / Filename ? auth_key = timestamp - rand - uid -
md5hash
```

Authentication fields

- You can set the `PrivateKey` field.
- The validity period 1,800 seconds indicates that the authentication fails when the user fails to access the client source server 1,800 seconds after the preset access time. For example, if the user sets the access expiration time to 2020-08-15 15:00:00, the link actually fails at 2020-08-15 15:30:00.

Field	Description
timestamp	The expiration time. It is a positive integer with a fixed length of 10 and a time in seconds from January 1, 1970. This 10-digit integer is used to control the expiration time. Effective time is 1,800 seconds.
rand	random number, we recommend that you use UUID (not including hyphen “-” , for example, 477b3bbc253f467b8def6711128c7bec format)
uid	Not used yet (set to 0).

Field	Description
md5hash	Verification string calculated by the MD5 algorithm , which is a combination of numbers 0 to 9 and lowercase English letters a to z, with a fixed length of 32 characters

When the CDN server receives a request, it first determines whether the `timestamp` in the request is earlier than the current time.

- If the `Timestamp` is earlier than the current time, the URL is regarded as expired, and the CDN server returns an HTTP 403 error.
- If the `timestamp` is later than the current time, the CDN server constructs an equivalent string (see the construction of the sstring field described later). Use the MD5 algorithm to calculate `HashValue` , and compare it with `md5hash` . If they are consistent, the request passes the authentication and the requested file is returned. Otherwise, the request fails the authentication, and an HTTP 403 error is returned.

· The ` `HashValue` ` is calculated based on the following string:

```
sstring  = " URI - Timestamp - rand - uid - PrivateKey " ( URI   is
  the   relative   address   of   the   user ' s   request   object
.  It   does   not   contain   parameters   such   as  / Filename
.)
HashValue  =  md5sum ( sstring )
```

An instance of authorization

1. Request object by `req_auth` :

```
http ://  cdn . example . com / video / standard / 1K . html
```

2. Set key to: aliyuncdnexp1234 (you can configure yourself)
3. The expiration date of the authentication configuration file is October 10, 2015 00: 00:00. The calculated number of seconds is 1,444,435,200.

4. The CDN server constructs a signature string for the calculation of HashValue:

```
/ video / standard / 1K . html - 1444435200 - 0 - 0 - aliyuncdne
 xp1234 "
```

5. Depending on the signature string, the CDN server evaluates hashvalue:

```
HashValue  =  md5sum ("/ video / standard / 1K . html - 1444435200
- 0 - 0 - aliyuncdne  xp1234 ") =  80cd3862d6  99b7118eed
99103f2a3a  4f
```

6. When requested, the URL is:

```
http :// cdn . example . com / video / standard / 1K . html ?
auth_key = 1444435200 - 0 - 0 - 80cd3862d6  99b7118eed  99103f2a3a
4f
```

If the calculated HashValue matches the value of md5hash = 80cd3862d6 99b7118eed99103f2a3a4f that is carried in the user request, authentication succeeds.

4.7.4 Authentication method B

Principles

Formats of the encrypted URL for user access

*** The user access URL is as follows:**

```
http :// DomainName / timestamp / md5hash / FileName
```

Encrypted URL structure: domain name/URL generation time (accurate to minutes) (timestamp)/md5 value (md5hash)/real path of the source server (FileName). The URL validity period is 1,800 s.

When the request passes the authentication, the back-to-source URL is as follows.

```
http :// DomainName / FileName
```

Authentication fields

- **Note:** `PrivateKey` **is set by CDN clients.**
- *** Validity period of 1,800 seconds: The user fails the authentication if attempting to access the client source server 1,800 seconds (specified in the Timestamp field) later than the preset access time. For example, if the preset access time is 15:00:00 on August 15, 2020, the link expires at 15:30:00 on the same day.**

Field	Description
DomainName	CDN client domain name.
timestamp	Resource failure time, as part of the URL and as a factor in the calculation of `md5hash` , is formatted: `YYYYMMDDHHMM` , effective time 1800 s
md5hash	//md5hash: The "timestamp", "FileName", and preset "PrivateKey" are used in the MD5 algorithm to get this string, i.e., (`PrivateKey` + `timestamp` + `FileName`)"
FileName	The actual URL of the origin access. Note that FileName must start with a slash (/) in authentication.

Example

1. Back-to-source request object.

```
http :// cdn . example . com / 4 / 44 / 44c0909bcf  c20a01afaf
256ca99a8b  8b . mp3
```

2. The key is set to aliyuncdnexp1234 (user-defined).
3. The time for the user to access the client source server is 201508150800 (format: YYYYMMDDHHMM).
4. The CDN server constructs a signature string used to calculate the "md5hash":

```
aliyuncdne  xp12342015  08150800 / 4 / 44 / 44c0909bcf  c20a01afaf
256ca99a8b  8b . mp3
```

5. The CDN server calculates the "md5hash" according to the signature string:

```
md5hash  =  md5sum (" aliyuncdne  xp12342015  08150800 / 4 / 44
/ 44c0909bcf  c20a01afaf  256ca99a8b  8b . mp3 ") =  9044548ef1
527deadafa  49a890a377  f0
```

6. The URL to request CDN:

```
http :// cdn . example . com / 2015081508  00 / 9044548ef1
527deadafa  49a890a377  f0 / 4 / 44 / 44c0909bcf  c20a01afaf
256ca99a8b  8b . mp3
```

The calculated "md5hash" is the same as the "md5hash = 9044548ef1527deadafa 49a890a377f0" value in the user request, so the request passes authentication

4.7.5 Authentication method C

Principles

Formats of the encrypted URL for user access

Format 1

```
http :// DomainName /{< md5hash >/< timestamp >}/ FileName
```

Format 2

```
http :// DomainName / FileName {& KEY1 =< md5hash >& KEY2 =<
timestamp >}
```

- The content in braces represents the encrypted information that is added based on the standard URL.
- `< md5hash >` is the MD5 encrypted string of authentication information.
- `< timestamp >` is a non-encrypted string expressed in plaintext.. The fixed length is 10 bits. It is the number of seconds since January 1, 1970, Coordinated Universal Time (UTC), expressed in hexadecimal format.
- Use format 1 to encrypt a URL, for example:

```
http :// cdn . example . com / a37fa50a5f  b8f71214b1  e7c95ec7a1
bd / 55CE8100 / test . flv
```

`< md5hash >` a37fa50a5fb8f71214b1e7c95ec7a1bd`< timestamp >` is 55CE8100.

Authentication fields

- Field description for `< md5hash >`:

Field	Description
PrivateKey	Interference string. Different clients use different interference strings.
FileName	The actual URL of the origin fetch access. Note that the path must start with a slash (/) in authentication.
time	The UNIX time of the user’s access to the origin server, expressed in hexadecimal format.

- PrivateKey value: `aliyuncdne  xp1234`
- FileName value: `/ test . flv`

- time value: `55CE8100`
- So the "md5hash" value is:

```
md5hash  =  md5sum ( aliyuncdne  xp1234 / test . flv55CE810  0 ) =
a37fa50a5f  b8f71214b1  e7c95ec7a1  bd
```

- Plaintext: `timestamp  =  55CE8100`

  The encrypted URL is then generated as follows:

  Format 1:

```
http :// cdn . example . com / a37fa50a5f  b8f71214b1  e7c95ec7a1
bd / 55CE8100 / test . flv
```

  Format 2:

```
http :// cdn . example . com / test . flv ? KEY1 = a37fa50a5f
b8f71214b1  e7c95ec7a1  bd & KEY2 = 55CE8100
```

Example

The user accesses the acceleration node using the encrypted URL. The CDN server first extracts the encrypted string 1, obtains

`< FILENAME >`

After this process, the CDN server authenticates the URL.

1. Use `< FileName >`of the original URL, request time, and PrivateKey to do MD5
2. Compare whether the encrypted string 2 and the encrypted string 1 are the same. The access request is rejected if the two strings are inconsistent.
3. Use the current time on the CDN server to subtract the plaintext time in the access URL to determine whether the preset time limit t expires (the time limit t is set to 1 ,800 s by default).
4. The validity period 1,800s means that authentication fails when the user fails to access the client source server 1,800s after the preset access time. For example, if the preset access time is 2020-08-15 15:00:00, the actual link expiry time is 2020-08-15 15:30:00
5. If the time difference is less than the preset time limit, the request is valid, and the CDN acceleration node responds normally. Otherwise, the request is rejected and an HTTP 403 error is returned.

4.7.6 Sample authentication code

For URL authentication rules, see URL Authentication Document. Using this demo, you can perform URL authentication based on your business needs. The demo provides three authentication methods and describes the composition of requested URLs and hash strings for each method.

Python version

```
import re
import time
import hashlib
import datetime
def md5sum ( src ):
    m = hashlib . md5 ()
    m . update ( src )
    return m . hexdigest ()
def a_auth ( uri , key , exp ):
    p = re . compile ("^( http ://| https ://)?([ ^/?] +)(/[^?] *)?
( \\?. *)?$")
    if not p :
        return None
    m = p . match ( uri )
    scheme , host , path , args = m . groups ()
    if not scheme : scheme = " http ://"
    if not path : path = "/"
    if not args : args = ""
    rand = " 0 " # " 0 " by default , other value is
ok
    uid = " 0 " # " 0 " by default , other value is
ok
    sstring = "% s -% s -% s -% s -% s " %( path , exp , rand ,
uid , key )
    hashvalue = md5sum ( sstring )
    auth_key = "% s -% s -% s -% s " %( exp , rand , uid ,
hashvalue )
    if args :
        return "% s % s % s % s & auth_key =% s " %( scheme , host
, path , args , auth_key )
    else :
        return "% s % s % s % s ? auth_key =% s " %( scheme , host
, path , args , auth_key )
def b_auth ( uri , key , exp ):
    p = re . compile ("^( http ://| https ://)?([ ^/?] +) (/[^?]
*)? ( \\?. *)? $ ")
    if not p :
        return None
    m = p . match ( uri )
    scheme , host , path , args = m . groups ()
    if not scheme : scheme = " http ://"
    if not path : path = "/"
    if not args : args = ""
   # convert unix timestamp to " YYmmDDHHMM " format
    nexp = datetime . datetime . fromtimest amp ( exp ). strftime
('% Y % m % d % H % M ')
    sstring = key + nexp + path
    hashvalue = md5sum ( sstring )
    return "% s % s /% s /% s % s % s " %( scheme , host , nexp ,
hashvalue , path , args )
def c_auth ( uri , key , exp ):
```

```
    p  =  re . compile ("^( http ://| https ://)?([ ^/?] +) (/[^?]
*)? ( \\?. *)?$")
    if   not   p :
        return   None
    m  =  p . match ( uri )
    scheme ,  host ,  path ,  args  =  m . groups ()
    if   not   scheme :  scheme  = " http ://"
    if   not   path :  path  = "/"
    if   not   args :  args  = ""
    hexexp  = "% x " % exp
    sstring  =  key  +  path  +  hexexp
    hashvalue  =  md5sum ( sstring )
    return  "% s % s /% s /% s % s % s " %( scheme ,  host ,
hashvalue ,  hexexp ,  path ,  args )
def   main ():
    uri  = " http :// xc . cdnpe . com / ping ? foo = bar " #
original   uri
    key  = "< input   private   key >"                          #
private   key   of   authorizat  ion
    exp  =  int ( time . time ()) +  1  *  3600                    #
expiration   time :  1   hour   after   current   itme
    authuri  =  a_auth ( uri ,  key ,  exp )                      #
auth   type :  a_auth  /  b_auth  /  c_auth
    print (" URL  : % s \ nAUTH : % s " %( uri ,  authuri ))
if   __name__  == " __main__ ":
    main ()
```

4.7.7 IP Blacklist and Whitelist

Introduction

CDN supports the blacklist and whitelist rules. You can add IP addresses on the IP blacklist. An IP address on the blacklist cannot access the target domain. Likewise, only IP addresses on the whitelist can access the target domain.

Note:
If you add one IP address to the blacklist, it can still access to CDN node. But it will be refused with 403. As a result, these request logs will still exist in your CDN logs.

Example

You can use an IP network segment to add IP addresses to the blacklist or whitelist. For example, 127.0.0.1/24.

127.0.0.1/24. 24 indicates that the first 24 bits in the subnet mask are used as effective bits, for example, 32-24=8 bits are used to express host numbers. In this way, the subnet can accommodate 2 ^ 8-2 = 254 hosts. And 127.0.0.1/24 indicates the IP network segment scope of 127.0.0.1~127.0.0.255.

Procedure

1. Go to Domain Namespage, select the domain name, then click Manage.

2. On Access Control > IP Blacklist/Whitelist, click Modify.
3. ChooseBlacklist or Whitelist, and add the IP network segment in the box below.
4. Click Confirm.

4.8 Performance Optimization settings

4.8.1 Page Optimization

Introduction

The page optimization function can be used to delete comments and repeated whitespaces embedded in HTML in order to remove redundant page content, reduce file size, and improve the efficiency of delivery.

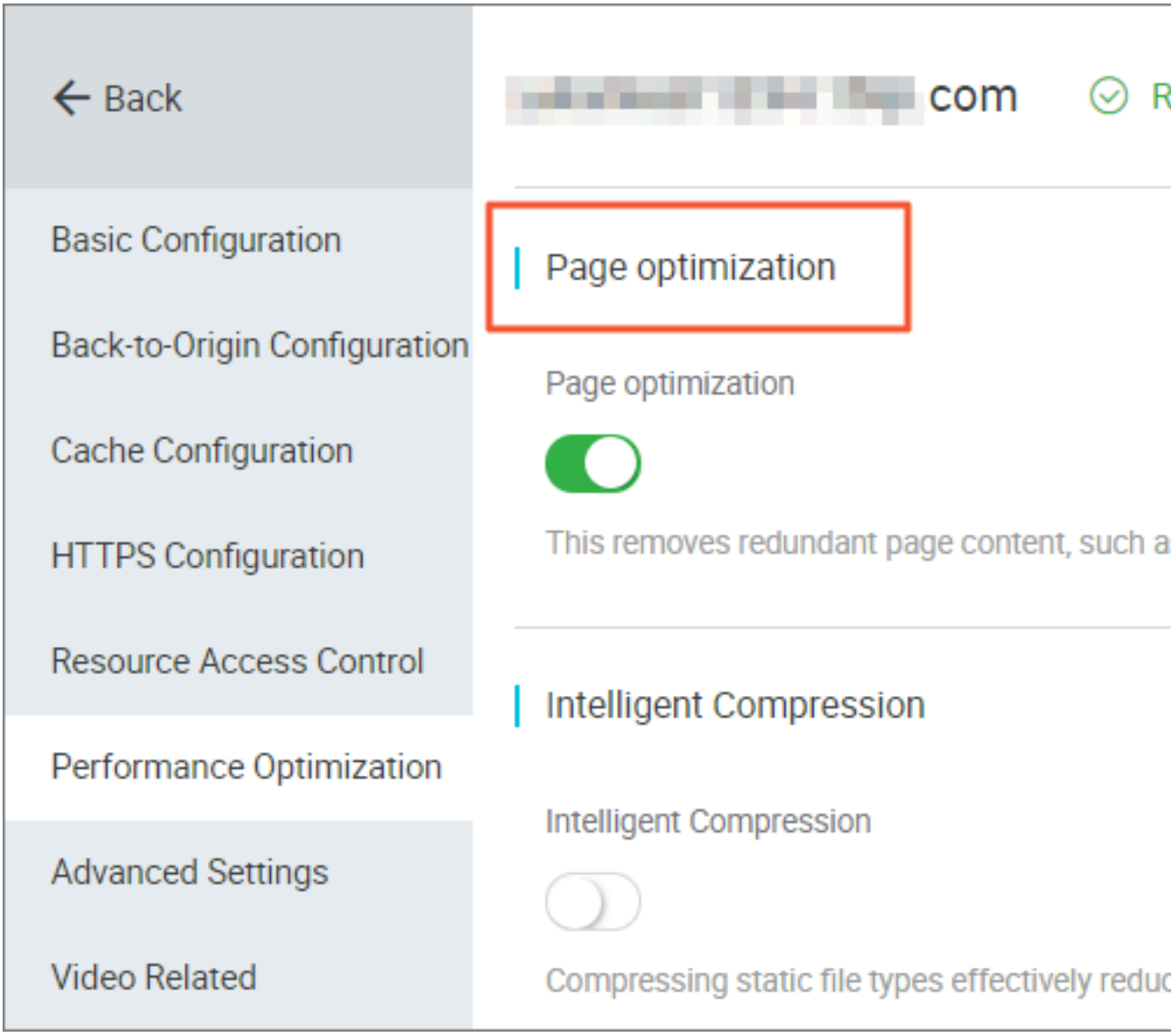
Procedure

Notice:

When we are optimizing your page, the file's md5 value will be changed. It will be different from that of the file I your origin site. Do not enable this feature if your origin site has some verification.

1. Go to Domain Namespage, select the domain name, then click Manage.

2.



3. Enable the function in Performance Optimization > Page Optimization.

4.8.2 Smart Compression

Introduction

After enabling Smart Compression function, you can compress most types of static files, so as to reduce the size of content transmitted by users and accelerates the content delivery.

Contents in the following formats can be compressed: text/html, text/xml, text/plain、text/css, application/javascript, application/x-javascript application/rss+xml, text/javascript, image/tiff image/svg+xml, application/json, application/xmltext.

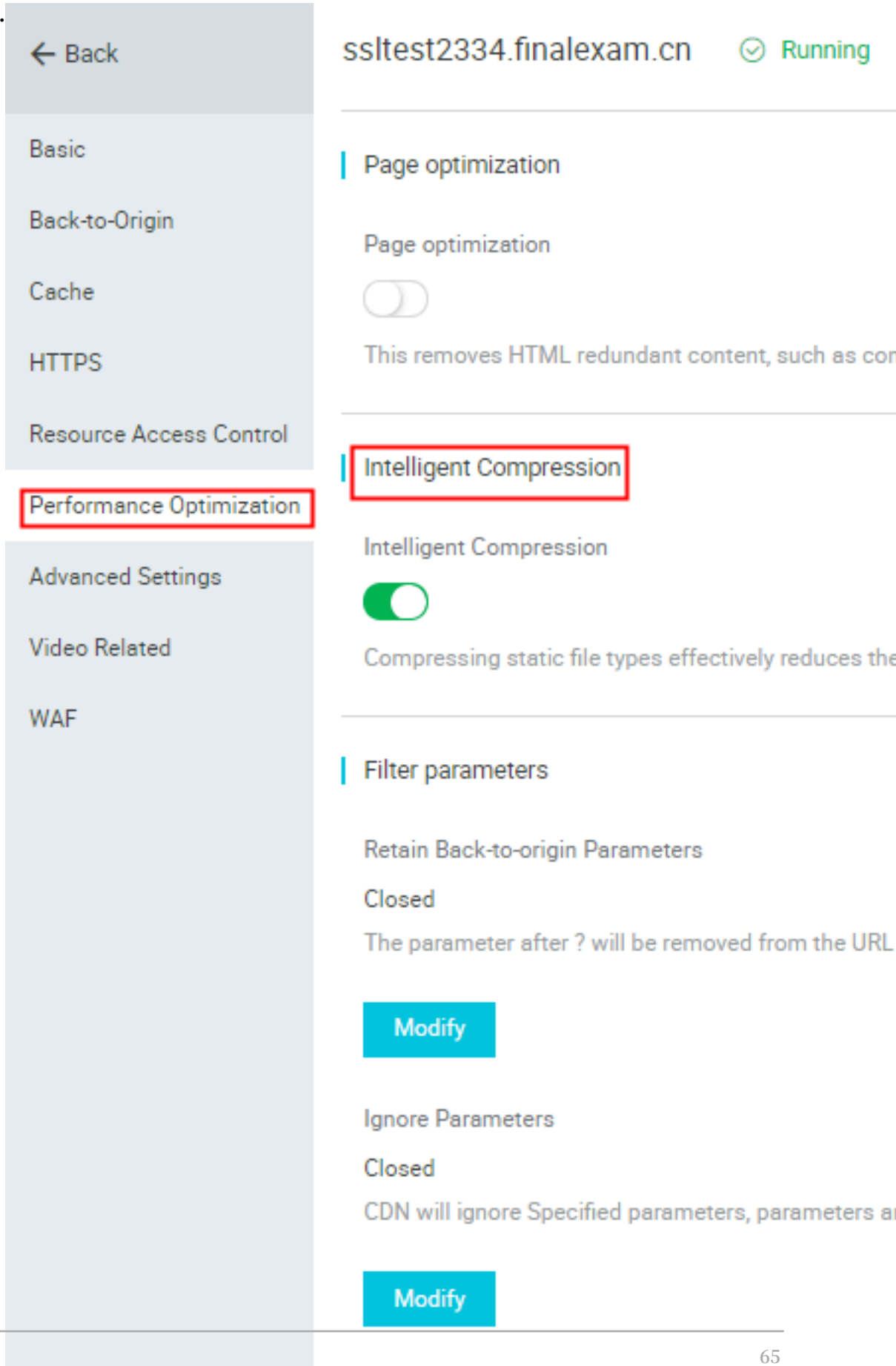
Applicable business type: All.

Procedure

 **Notice:**
When we are optimizing your page, the file's md5 value will be changed. It will be different from that of the file I your origin site. Do not enable this feature if your origin site has some verification.

1. Log on to the CDN console.
2. In the left-side pane, choose Domain Names. In the right-side pane, select a domain, and in the Actions column click Manage.

3. On the page that is displayed, choose Performance Optimization from the left-side pane, and in the Intelligent Compression area enable the function.



4.8.3 Filter Parameter

Introduction

When a URL request carrying? and request parameters are sent to a CDN node, the CDN node determines whether to send the request to the origin site.

- If you enable Filter Parameter function: after the request arrives at the CDN node, the URL without parameters is intercepted and requested against the origin site. Additionally, the CDN node retains only one copy.
  - An HTTP request typically contains the requisite parameters. If the content of a parameter has a low priority and the parameter overview file can be ignored, it recommended to enable the Filter Parameter function. This improves the file cache hit rate and the delivery efficiency.
  - If a parameter has important indicators (for example, if it contains file version information), we recommend that you disable this function.
- If you disable Filter Parameter function, different copies are cached on the CDN node for different URLs.

Applicable business type: All.

Example

The `http :// www . abc . com / a . jpg ? x = 1` URL request is sent to a CDN node.

- If the Filter Parameter function is enabled, the CDN node initiates to the origin site the `http :// www . abc . com / a . jpg` request (ignore parameter x = 1). After the origin site returns a response, the CDN node retains a copy. Then, the origin site continues to respond to the terminal `http :// www . abc . com / a . jpg` . For all requests similar to `http :// www . abc . com / a . jpg ? parameters` , the origin site responds to the CDN copy `http :// www . abc . com / a . jpg` .
- If the Filter Parameter function is disabled, `http :// www . abc . com / a . jpg ? x = 1` and `http :// www . abc . com / a . jpg ? x = 2` respond to the response content of different parameter origin site.

 Note:

URL authentication has a higher priority than the Filter Parameter function. Because type A authentication information is contained in the parameter section of an HTTP request, the system first performs the authentication and then caches a copy on the CDN node after the authentication succeeds.

Procedure

1. Go to Domain Namespage, select the domain name, then click Manage.
2. Enable the function in Performance Optimization > Filter Parameter.

4.9 Advanced settings

4.9.1 Peak Bandwidth

Introduction

The bandwidth cap function sets the maximum bandwidth value for average bandwidth measured during each statistical cycle (five minutes). If the average bandwidth exceeds the maximum, the domain name automatically goes offline to protect your domain name security. In this situation, all requests are sent back to the origin site. When the bandwidth cap is reached, CDN stops acceleration services to avoid excessive fees produced by abnormal traffic volumes. After your domain name goes offline, you can restart it in the console.

Note:
The bandwidth cap function is not currently available for wildcard domain names, so the function has no effect even it is enabled.

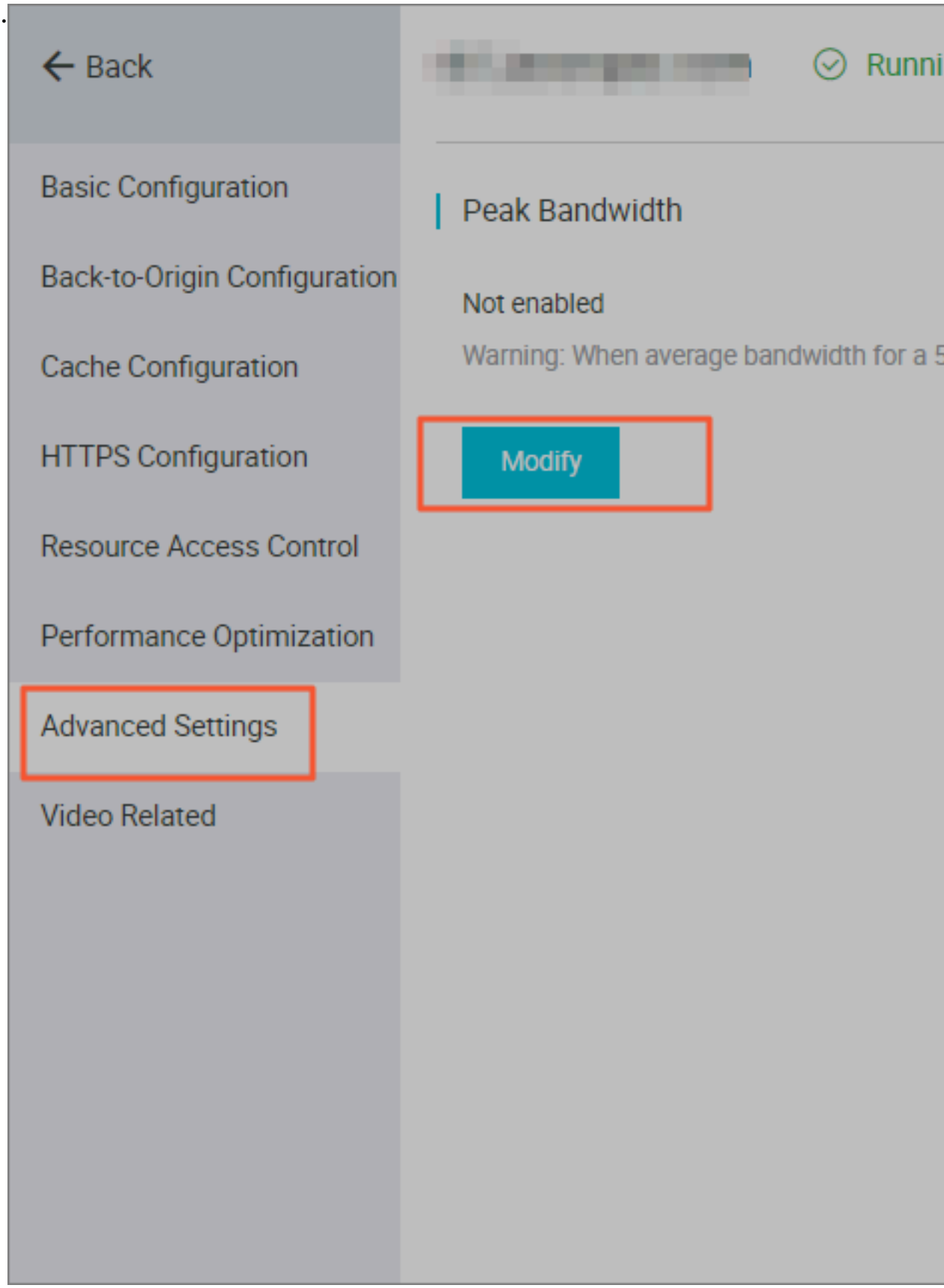
RAM subaccounts require CloudMonitor authorization to use this function. To grant authorization, use the AliyunCloudMonitorFullAccess policy group.

Procedure

Note:
After you have enabled the peak bandwidth function, your services are limited by the bandwidth cap and go offline if it is exceeded. To guarantee your services running continuously on your domain name, we recommend you set the cap value with discretion based on reasonable estimation.

1. Log on to the CDN console.

2. On the Domain Names page, choose the domain name, then click Manage.
3. Choose Advanced Settings, then click Modify under the Peak Bandwidth label.



4. Enable the bandwidth cap function. Choose the unit from Mbps, Gbps, or Tbps.

   Note:
   Bandwidth value can be set in powers of thousand.

5. Click Confirm. Then the peak bandwidth is successfully enabled.

You can choose to enable or disable the peak bandwidth function based on the actual usage of your domain name.

4.10 Video Service Configuration

4.10.1 Notify_URl setting

Introduction

Call back stream-status real-time information and promptly notify users about the video streaming results.

Attentions

- Principle: By sending GET requests to the user server through the HTTP interface , the real-time stream status feedback is sent to the users. The user server returns 200 to the return interface.
- You do not have to identify the URL if normal access is ensured. See the following rules for URL response.
- In case of access time-out, the URL can be retried. The current time-out duration is 5 seconds, the number of retries is 5, and the interval is 1 second.

Procedure

Configuration can be performed on the console, and it is optional.

Example:

```
http :// 1 . 1 . 1 . 1 / pub ? action = publish & app = xc . cdnpe .
com & appname = hello & id = world & ip = 42 . 120 . 74 . 183 & node
= cdnvideoce  nter010207  116011 . cm3
```

Parameter	Value description
time	unix timestamp
usrargs	User streaming parameters

Parameter	Value description
action	publish indicates push streaming, and publish_done indicates completion of push streaming
app	Default value is the custom streaming domain name. If no streaming domain name is bound, it is the playback domain name
appname	Application name
id	Stream name
node	The name of the node or machine in the CDN that receives the stream
ip	Streaming client's IP

4.10.2 Drag/Drop Playback

Introduction

In a video-on-demand scenario, when the playback progress bar is dragged, the end user will send a URL request, such as `http :// www . aliyun . com / test . flv ? start = 10`, to the server. The server returns the data from the key frame prior to the10th second to the client (If start=10 is not the key frame).

After receiving such a request from an end user and the Drag/Drop Playback function is enabled, a CDN node can directly return the data from the key frame prior to the10th second (If start=10 is not the key frame) (FLV format) or from the 10th second to the end user.

Note

- To use the Drag/Drop Playback function, an origin site must support Range requests. The origin site must be able to return correct 206 Partial Content for an HTTP request header containing a Range field.
- Two available file format: MP4 and FLV.
- Currently, FLV format only supports the coding formats with the audio format of aac and video format of avc.

File Format	Meta Information	start Parameter	Example
MP4	Meta information of an origin site video must be contained in the file header. A video with its meta information contained in the file tail is not supported.	The start parameter specifies the time in seconds. Decimals are supported to indicate milliseconds. For example, start=1.01 indicates that the start time is 1.01s. If the current start is not a key frame, the CDN locates the key frame prior to the time specified by the start parameter.	The request http://domain/video.mp4?start=10 playing a video from the 10th second.
FLV	An origin site video must contain meta information.	The start parameter specifies a byte. If the current start is not a key frame, the CDN automatically locates the key frame prior to the frame specified by the start parameter.	For http://domain/video.flv, the request http://domain/video.flv?start=10 playing a video from the key frame prior to the10th byte(If start=10 is not the position of the key frame) .

Procedure

1. Go to Domain Namespage, select the domain name, then click Manage.
2. Enable the function in Video-related > Drag/Drop Playback.

4.10.3 Back-to-origin of range

Introduction

The Back-to-origin of Range function allows a client to notify an origin site server to return partial content within a specified range. It accelerates delivery of large files by reducing the consumption of back-to-origin traffic and improving the resource response speed.

The origin site must support the range request, that is, the range field is included in the HTTP request header, and the origin site can respond to the correct 206 file slice.

When the Back-to-origin of Range is	Description	Instances
Enable	A parameter request can be returned to an origin site. In this case, based on the Range parameter, the origin site returns the file byte range, while the CDN node returns the content in the byte range to the client.	If a request sent from a client to a CDN node contains range:0-100, the range:0-100 parameter will also be contained in the request received on the origin site. When the origin site returns the parameter content to the CDN node, the node returns the content in 101 bytes ranging from 0 to 100 to the client.
Disable	A CDN higher-level node requests an origin site for all files. However, the requested files will not be cached on the CDN node because a client will automatically disconnect HTTP links after receiving bytes specified by Range . This causes a low cache hit rate and large back-to-origin traffic.	If a request sent from a client to a CDN node contains range:0-100, the range:0-100 parameter will not be contained in the request received on the server. The origin site will return a complete file to the CDN node and the CDN node will return only 101 bytes to the client. However, the file cannot be cached on the CDN node because the link is disconnected.

 Note:

To use the Back-to-origin of Range function, an origin site must support Range requests, meaning that the origin site must be able to return correct 206 Partial Content for an HTTP request header containing a Range field.

Procedure

Back-to-origin of Range feature is optional and is disabled by default. You can change the configuration to enable it.

1. Go toDomain Namepage,selete your domain name, and click Manage.
2. Click Modify Configuration in Video-related > Back-to-origin of Range.
3. Select Enable, Disable or Force.

Go to the CDN domain name management page, click Configure, select Enable/Disable/Force Back-to-origin of Range function.

 **Note:**
You can enable Force if your origin site is capable of using this feature. After enabling it, all requests will be forced to perform Back-to-origin of range.

See *Back-to-origin of Range* for more API information.

5 Data monitoring

Data Monitoring includes Resource Monitoring and Real-time Monitoring.

Resource Monitoring

You can select Domain Name, Region, Operator, Time Granularity (1 minute, 5 minute or 1 hour) and Time Range (Today, Yesterday, 7 Days, 30 Days or Custom) to view the specific condition in the following dimensions:

Items	Metrics
Traffic Bandwidth	Bandwidth, Traffic
Back-to-origin Statistics	Back-to-origin Bandwidth, Back-to-origin Traffic
Number of Visits	Number of requests, QPS.
HTTPS Hit Rate	N/A
HTTPCODE	5xx, 4xx, 3xx, 2xx

A difference exists between the graph data and the billing data in Resource Monitoring. For example, a 30-day statistical curve takes a granularity of 14400s, while the billing statistical curve takes a granularity of 300s. As a result, the graph, ignoring some metering points, is mainly used to show the trends of bandwidth. The billing data, with more precise granularity, always serves as the basis to calculate your bandwidth usage.

 Note:
HTTP Hit Rate is not available for selecting Region or Operator.

Real-time Monitoring

You can select theDomain Name, Region, Operator or the Time Range you want to view (Past 1 Hour, Past 6 hours, Past 12 hours or Custom) to view the specific condition in the following dimensions:

Items	Metrics
Basic Data	Bandwidth, Traffic, Number of requests, QPS
Back-to-origin Traffic	Back-to-origin Traffic, Back-to-origin Bandwidth

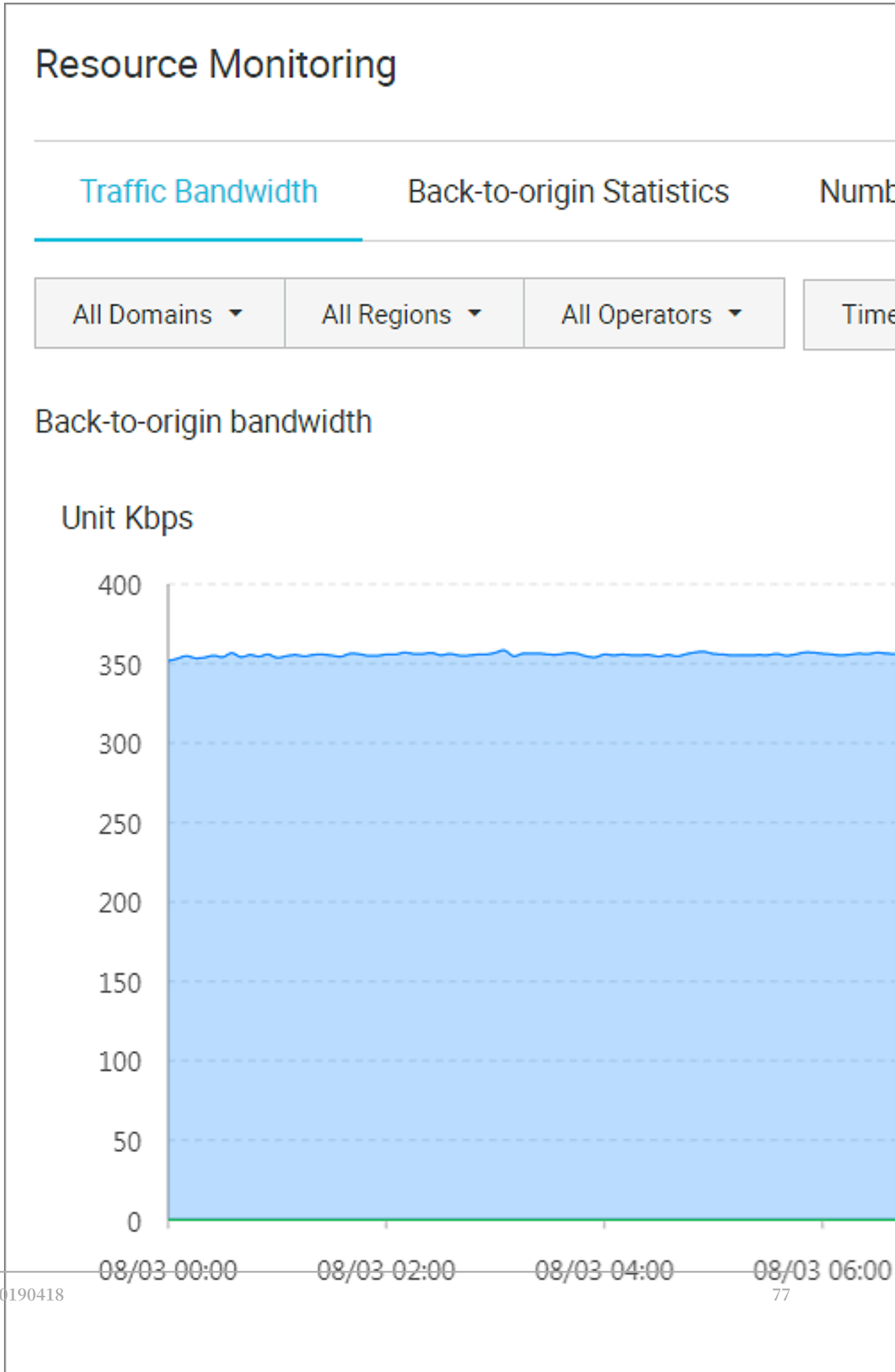
Items	Metrics
Quality monitoring	Request Hit Rate, Byte Hit Rate, 5xx status code, 4xx status code, 3xx status code, 2xx status code.

Procedure

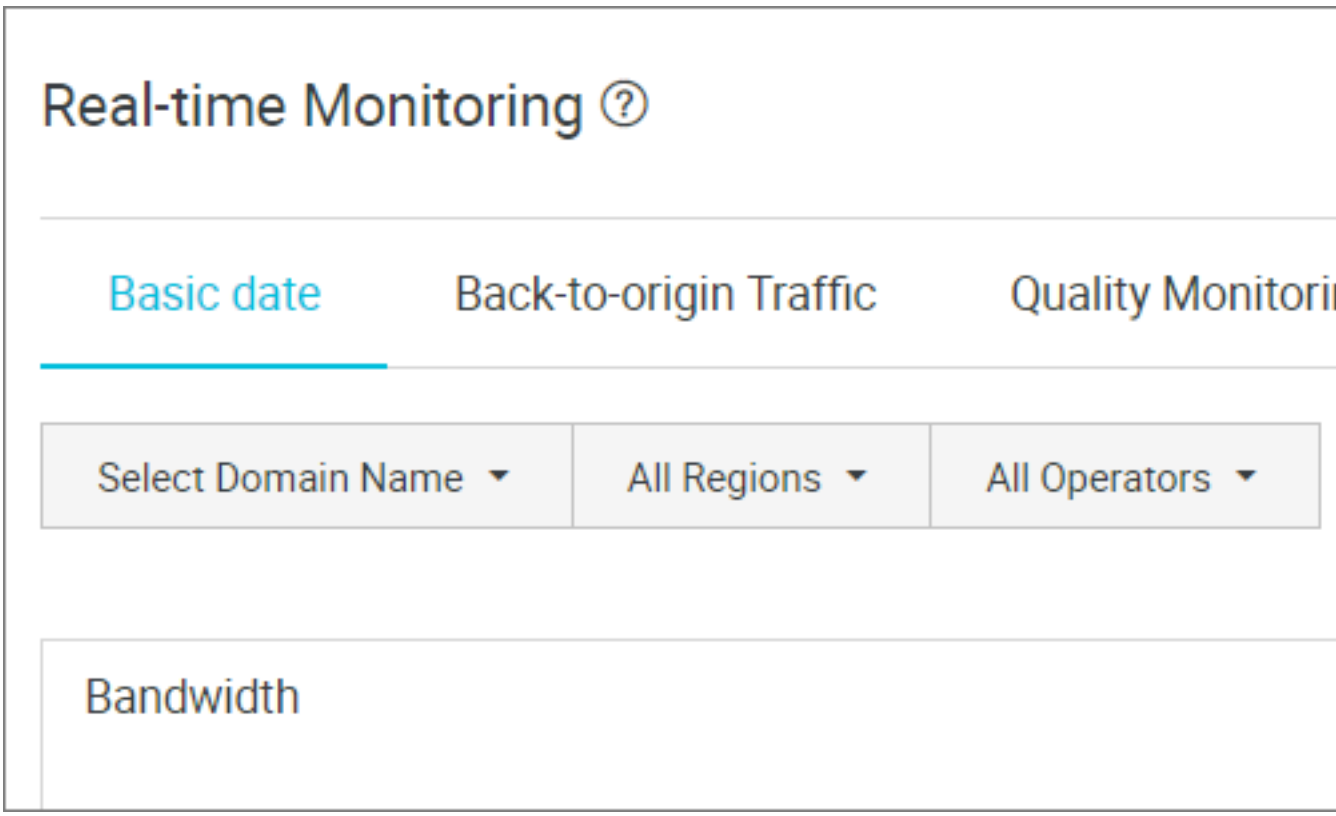
1. Log on to the CDN console.

2. **In the left-side pane, choose Data Monitoring > Resource Monitoring or Data Monitoring > Real-time Monitoring. In the right-side pane, select monitoring items and metrics, and click Query.**

   Resource Monitoring:


Resource Monitoring
Traffic Bandwidth
Back-to-origin Statistics
Numb
All Domains
All Regions
All Operators
Time
Back-to-origin bandwidth
Unit Kbps
400
350
300
250
200
150
100
50
0
08/03 00:00
08/03 02:00
08/03 04:00
08/03 06:00

Real-time Monitoring:



6 Statistical Analysis

In Statistical Analysis, you can check data of PV and UV, Area and ISP, Domain Name Rankings, Popular Referer, and Popular URLs. You can also export detailed raw data, such as network bandwidth, traffic, the traffic-based ranking of domain names, visitor area, operator distribution, and so on.

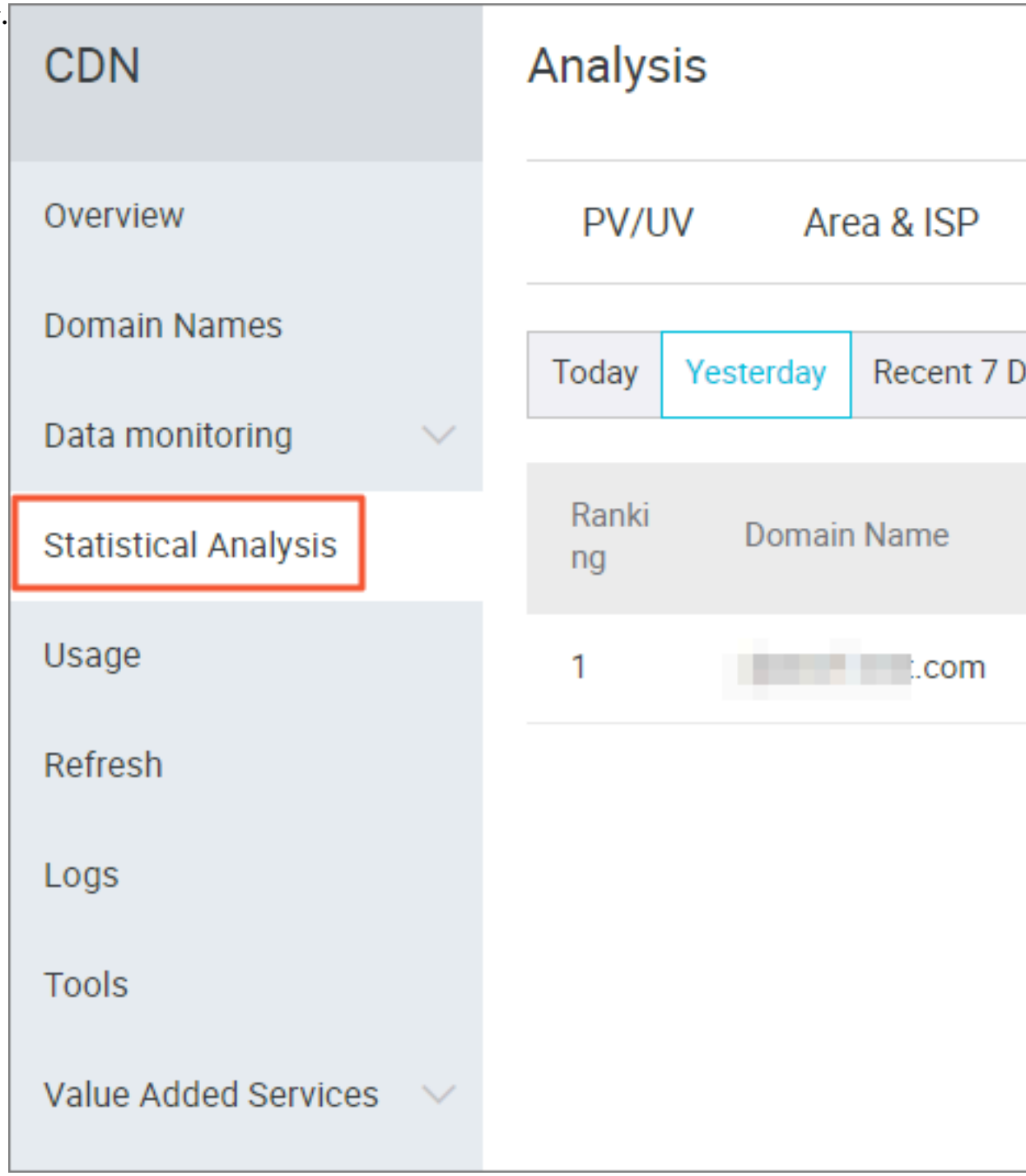
Note:
The precision of original data collection varies according to time spans, which are 300s, 3600s, and 14400s for daily export, weekly export, and monthly export, respectively.

Item	Index	Time Span
PV and UV	PV, UV, regional user distribution, and operator proportions	Today, yesterday, past 7 days, past 30 days, and custom (within 90 days).
Area and ISP	Ranking, region, total traffic, traffic proportion, number of visits, by QPS, response time.	Today, yesterday, past 7 days, past 30 days, and custom (within 90 days).
Domain Name Rankings	Access rankings for each CDN domain name	Today, yesterday, past 7 days, past 30 days, and custom (within 90 days).
Popular Referer	Traffic, traffic proportion, number of visits, and visits proportion	You can view the daily data within your customized days (at most 90 days).
Popular URLs	Traffic, traffic proportion, number of visits, and visits proportion	You can view the daily data within your customized days (at most 90 days).

Procedure

1. Log on to the CDN console.

2. In the left-side pane, choose Statistical Analysis. In the right-side pane, select monitoring items and metrics, and click Query.



7 Usage Query

7.1 Usage Query

Introduction

You can use this function to obtain the actual usage of traffic, bandwidth, or requests during a certain period. You can customize the time span (3 months at most) to query .

You can query the data by the following dimensions:

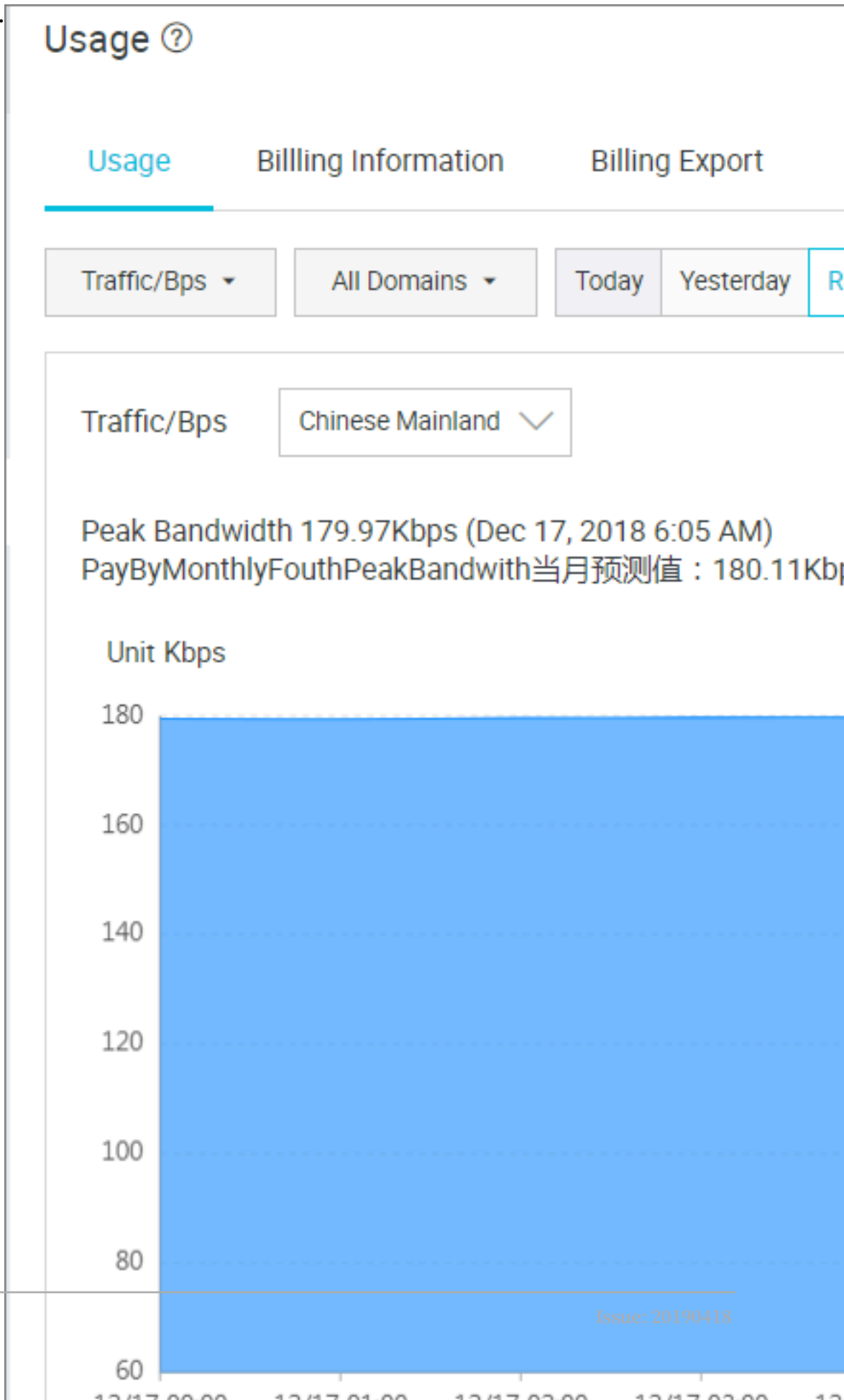
- Domain name or user
- Traffic, bandwidth, or requests.
- Billing regions. For more information, see *Billing regions*.

 **Note:**
You cannot export data from the Usage page. To export the data you require, go to Billing export or Detail export.

Procedure

1. Log on to the *CDN Console*.
2. On CDN Overview page, click Usage on the left.

3. On the Usage page, configure all conditions, including traffic/bandwidth/requests, time range, and billing regions. Then clickQuery.



Other Checklist

- You can click Billing Informationto query your billing list by day.
- You can click ***Billing Export*** to export your billing list.
- You can click ***Detailed Data Export*** to export detailed data.
- You can also click Usage Bag to check the Usage Bag Name, Total, Remaining, Effective Date, Expiry Date, and Status of each usage bag.

7.2 Billing export

Introduction

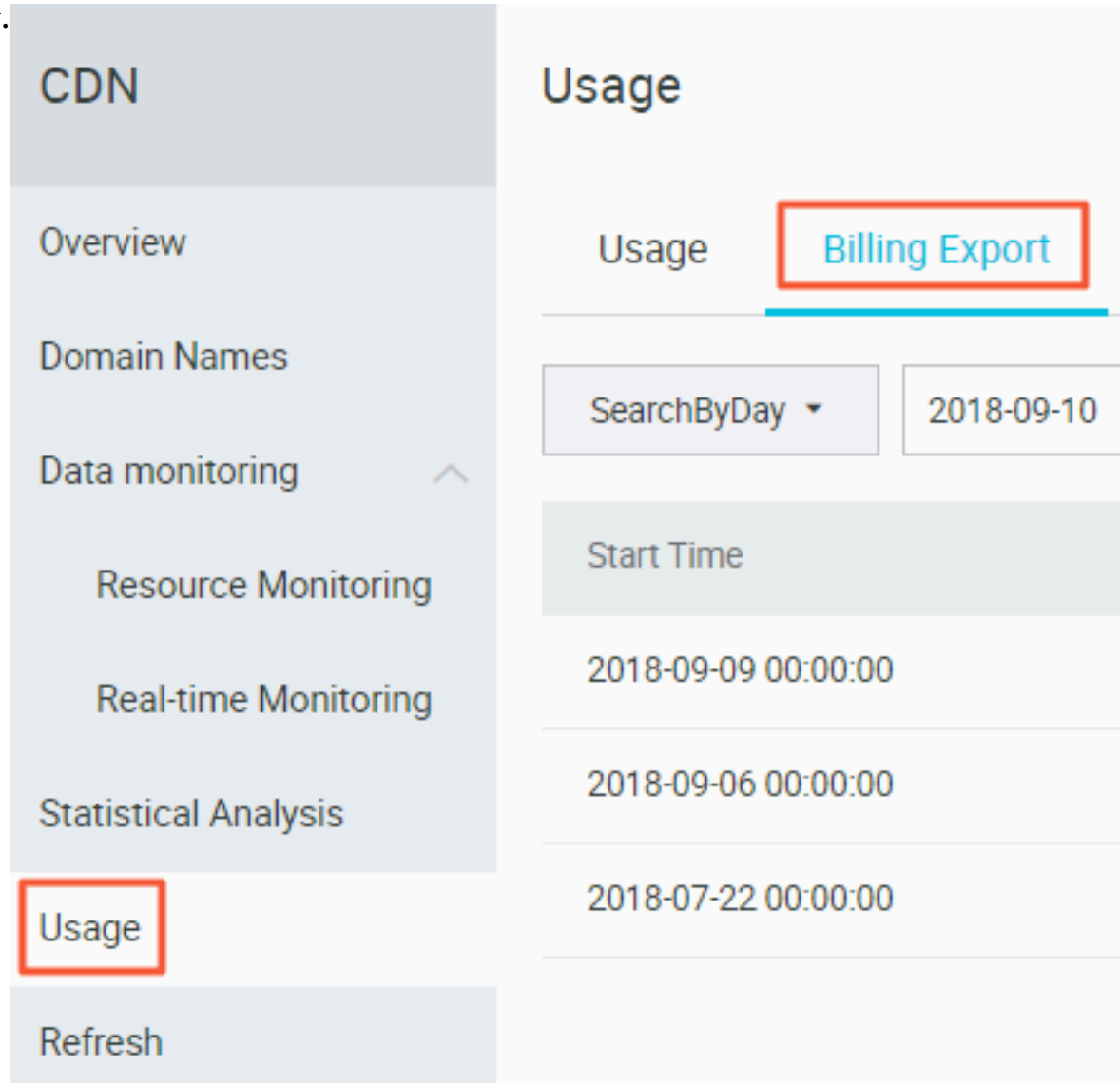
You can export actual usage data by day or by month, so as to compare it with the report output from the billing center.

- You can only export data by account.
- You can only export data for one day, or for a whole month.
- Export format: PDF.

Procedure

1. Log on to the *CDN Console*.
2. On CDN Overview page, click Usage.

3. On the Usage page, select the date, then clickQuery.



4. Click Download at the end of the line you choose.

7.3 Detail Data Export

Introduction

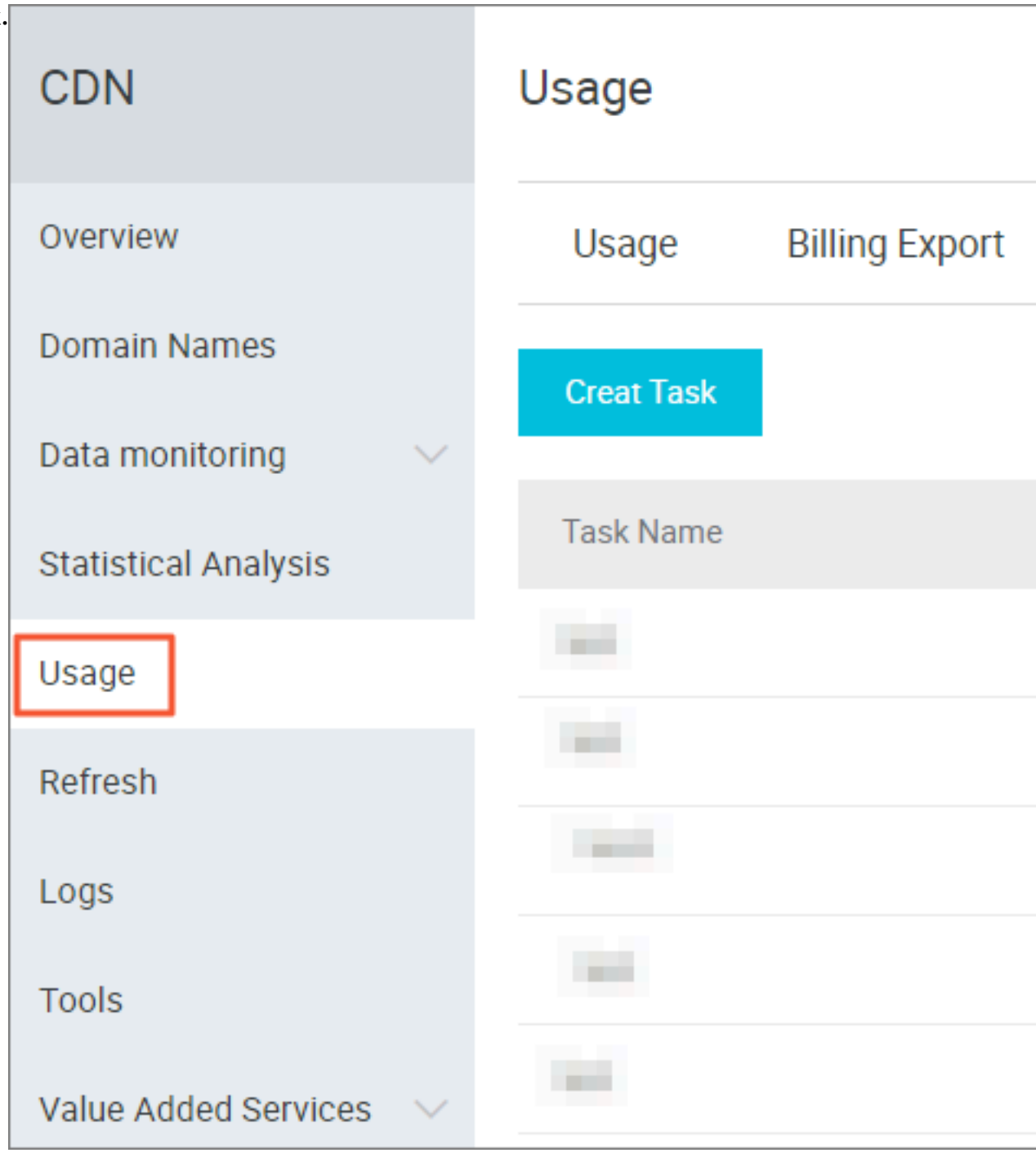
With this feature, you can export detail data for traffic/bps data or request times, so that you can calculate or review the usage you actually paid for,

- You can export data by account, resource group, or domain name.
- At the same time, all domain names of the resource group are also exported.
- You can export up to 100 domain names at a time. Only the resource group details are exported if you export over 100 domain names.
- The time span for all exported data is five minute.

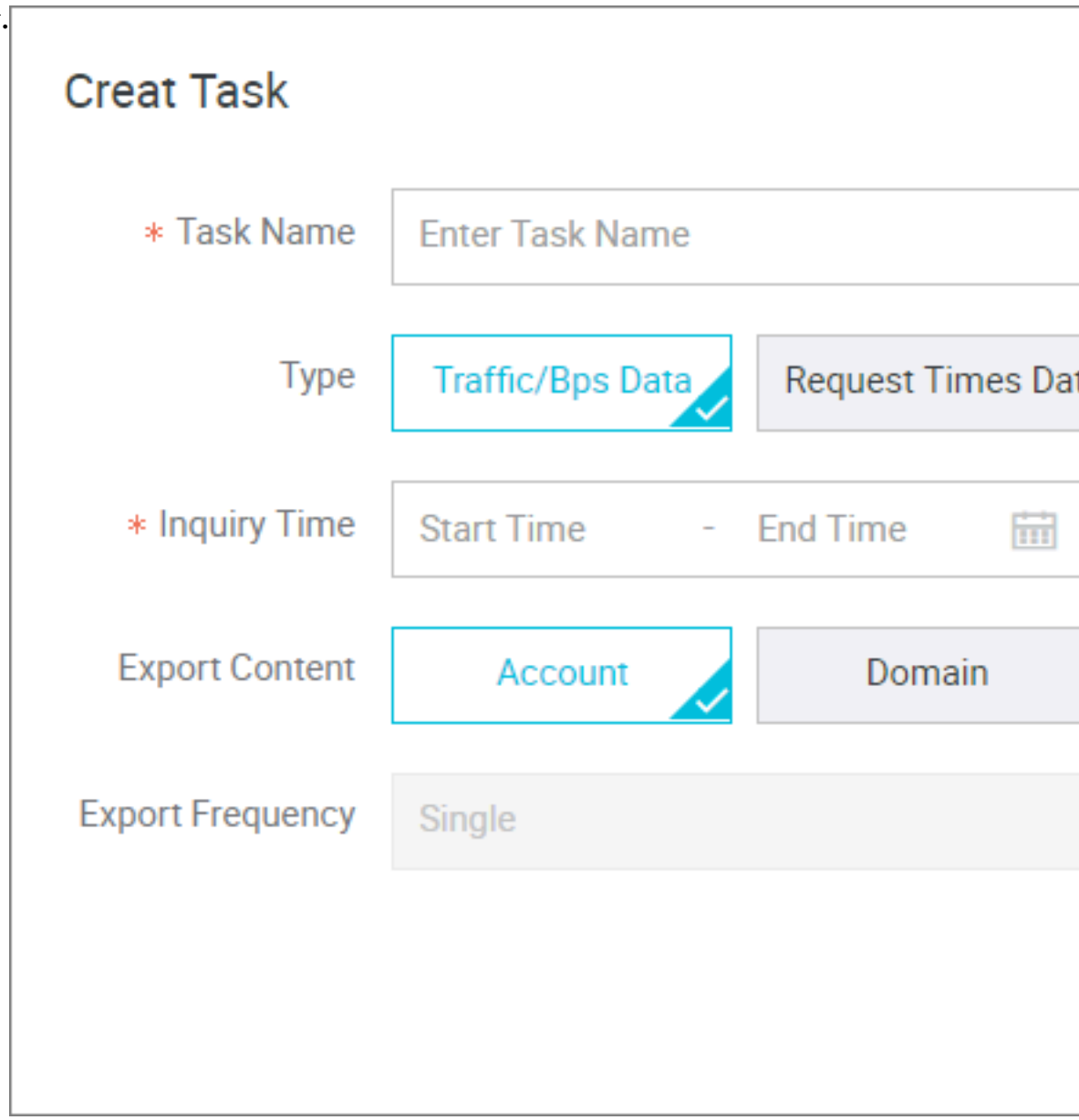
- Download data format: CSV.
- You cannot export repeated time span.

Procedure

1. Log on to the CDN console, enter the Domain Names page, select the domain name, then click Manage.
2. On the Usage > Detail Data Export page, click Create Task.



3. Enter Task Name (required), the choose Type、Inquiry Time(required), Export Content, and Export Frequency.



4. Click Confirm.

8 Refresh and Preload

Log on to the CDN console, click Refresh to perform refresh operation.

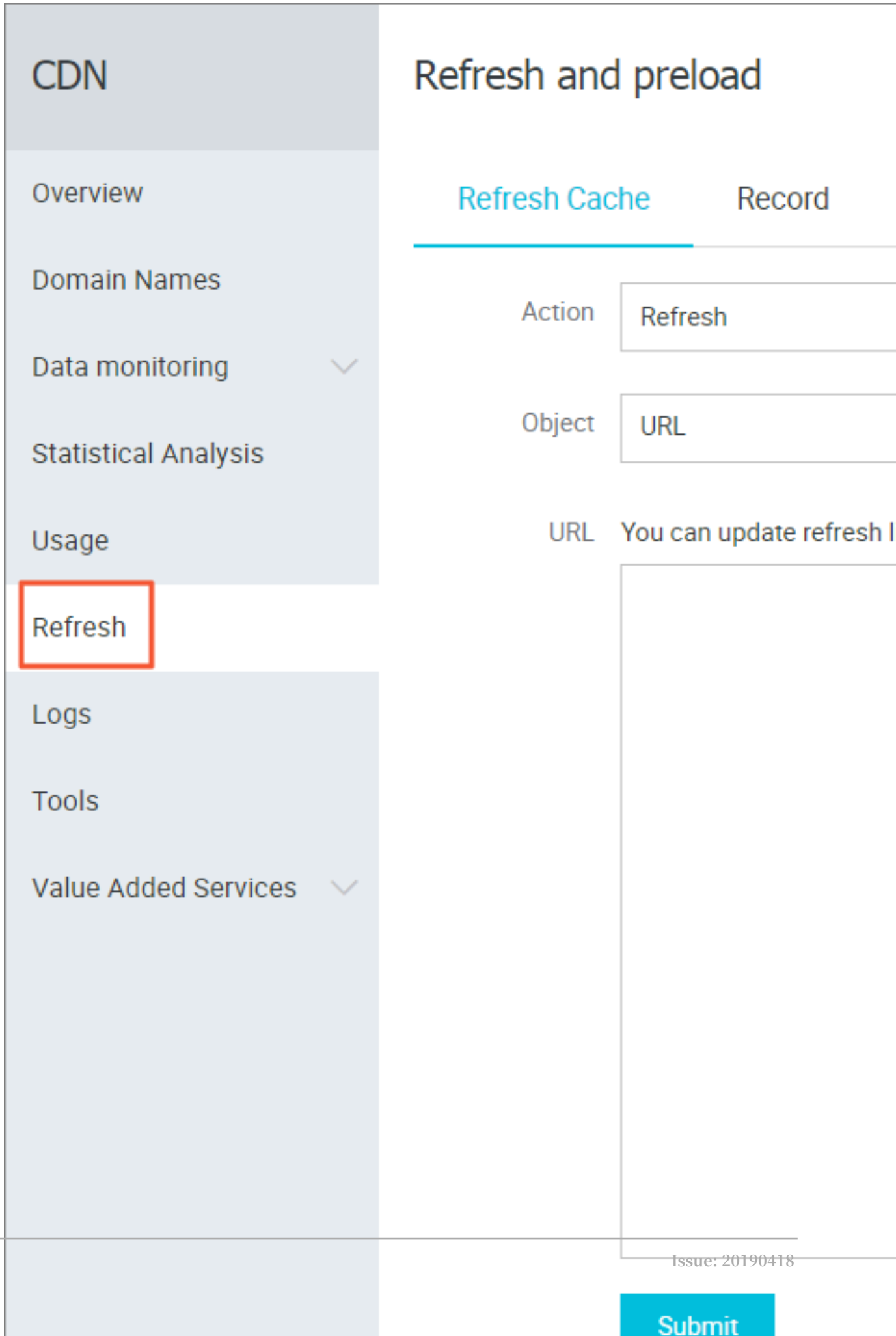
URL refresh

Concept: Forces specified files on the CDN Cache node to expire in order to update back-to-source again.

Time to Take Effect: 5 to 10 minutes

Attentions:

- Entered URL must contain `http://` or `https://`
- Up to 2,000 URLs with the same ID can be refreshed and warmed up each day.
- Provides an interface to refresh the cache in batches. For more information, see *RefreshObjectCaches*.


CDN
Overview
Domain Names
Data monitoring
Statistical Analysis
Usage
Refresh
Logs
Tools
Value Added Services
Refresh and preload
Refresh Cache
Record
Action
Refresh
Object
URL
URL
You can update refresh l
Submit

Directory refresh

Concept: Forces files in the specified directory on the CDN Cache node to expire in order to update back-to-source again. Can be used in scenarios with large amounts of content.

Time to Take Effect: 5 to 10 minutes

Attentions:

- Up to 100 refresh requests can be submitted each day.
- Entered content must begin with `http://` or `https://`, and end with `/`.
- Provides an interface to refresh the cache in batches. For more information, see *RefreshObjectCaches*.

URL push

Concept: Actively pushes content from the origin site to the L2 Cache node. Upon first access, you can directly hit cache to relieve pressure on the origin site.

Time to Take Effect: 5 to 10 minutes

Attentions:

- Entered URL must contain `http://` or `https://`
- Up to 500 URLs with the same ID can be pushed each day.
- Time to complete pushing resources depends on the number of pushed files submitted by the user, file size, origin site bandwidth, network condition and other factors.
- Provides the interface to push resources in batches. For more information, see *PushObjectCache*.

Progress view

- You can log on to the CDN console Refresh > Operation Recordsto view the progress of the resource refresh or push.
- Alibaba Cloud CDN provides the API for querying progress: *DescribeRefreshTasks*.

9 Log Management

9.1 Log Downloading

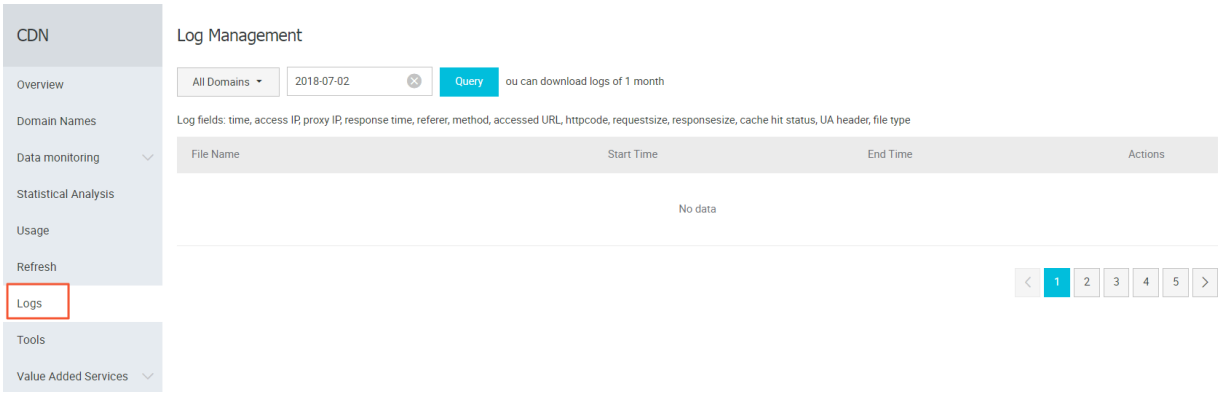
- You can query the log files in the Log Management within 4 hours.
- Log files are segmented on an hour basis.
- You can download the log files within 1 month.
- Name a log file based on the rule: `Accelerati on domain name_year_ month_date _start time_end time`.
- Log field format description.

Sample log content

```
[ 9 / Jun / 2015 : 01 : 58 : 09 + 0800 ] 188 . 165 . 15 . 75 -
 1542 "-" " GET http :// www . aliyun . com / index . html " 200
 191 2830 MISS " Mozilla / 5 . 0 ( compatible ; AhrefsBot / 5 .
 0 ; + http :// ahrefs . com / robot /)" " text / html "
```

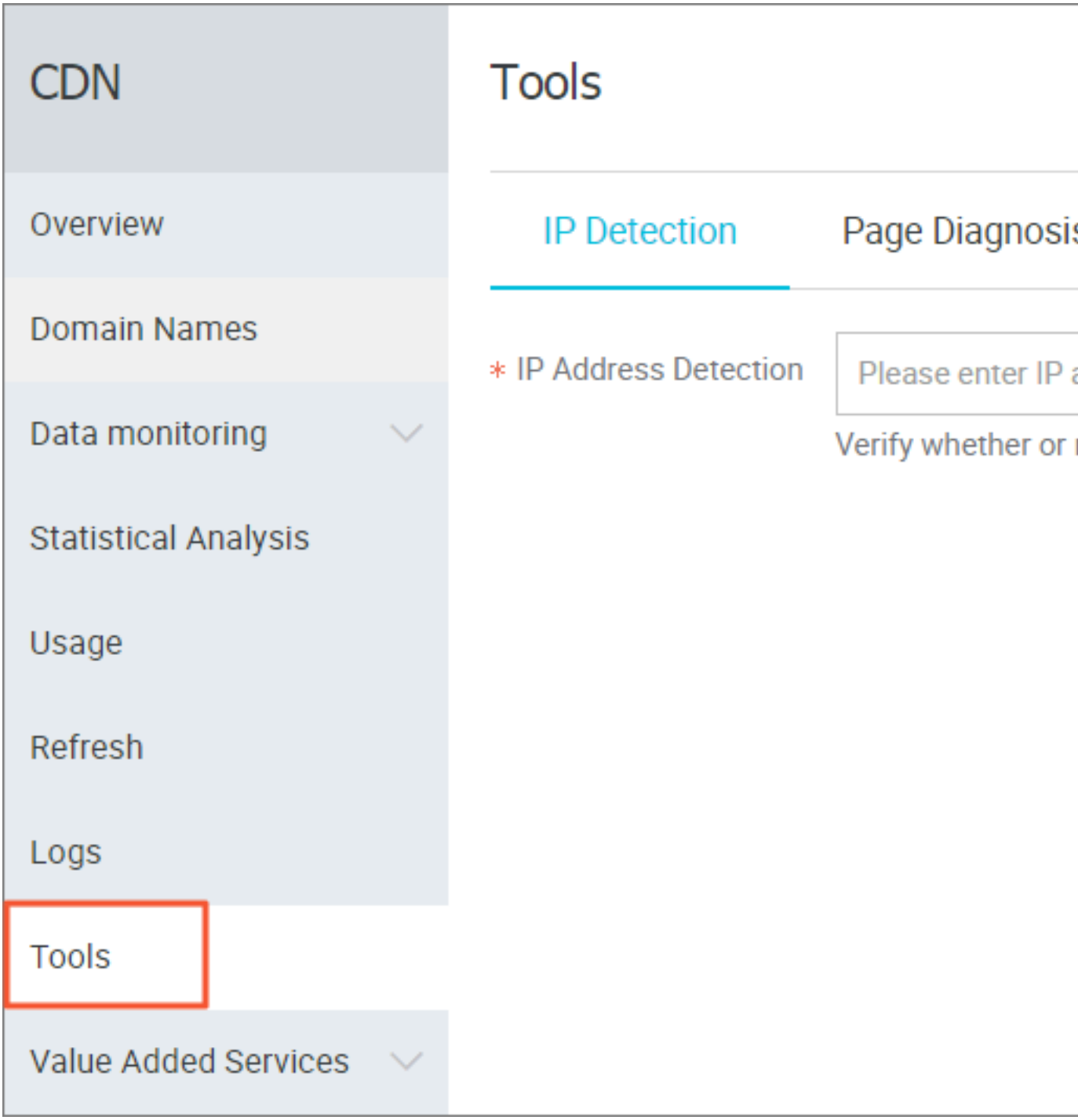
Log field description

Field	Parameter
time	[9/Jun/2015:01:58:09 +0800]
access ip	188.165.15.75
proxy IP	-
Responsetime (Unit: ms)	1542
referer	-
method	GET
access url	*http://www.aliyun.com/index.html*
httpcode	200
requestsize (Unit: byte)	191
responsesize (Unit: byte)	2830
cache hit status	MISS
UA header	Mozilla/5.0 (compatible; AhrefsBot/5.0; + *http://ahrefs.com/robot/*)
File type	text/html


CDN
Overview
Domain Names
Data monitoring
Statistical Analysis
Usage
Refresh
Logs
Tools
Value Added Services
Log Management
All Domains
2018-07-02
Query
ou can download logs of 1 month
Log fields: time, access IP, proxy IP, response time, referer, method, accessed URL, httpcode, requestsize, responsesize, cache hit status, UA header, file type
File Name
Start Time
End Time
Actions
No data
1
2
3
4
5

10 Diagnostic Tools

An IP address detection tool is provided in order to verify whether a specified IP address is an Alibaba Cloud CDN node IP address or an IP address from a third-party node.



11 Value-added service

12 Set httpDNS

Introduction

- A traditional DNS resolution is implemented by accessing the local DNS of a carrier in order to obtain the resolution result. However, this action can easily allow for DNS hijacking, DNS errors, and inter-network traffics, and lead to slowed, or failed , website access.
- httpDNS is a DNS service that uses HTTP protocol to directly access the Alibaba Cloud CDN server. Because it bypasses the carrier's local DNS, it can avoid DNS hijacking and obtain real-time accurate DNS resolution results.
- Principle: Initiate a request to access a designated Alibaba Cloud CDN httpDNS server through HTTP protocol. The httpDNS server performs domain resolution based on second-level DNS nodes distributed everywhere, obtains the domain name resolution result, and returns the result.

httpDNS interface

Direct access through an HTTP interface is supported. The access method is as follows.

1. Service URL

```
http :// umc . danuoyi . alicdn . com / multi_dns_ resolve
```

2. Request method: `POST`
3. Supported parameter: `client_ip = x . x . x . x` . This parameter can be ignored if the IP address of the client initiating the httpDNS request is used.
4. Request example: Multiple domains to be resolved are placed in the body of a POST request and are separated by whitespaces (blank spaces, TABs, newline characters).

```
# curl ' http :// umc . danuoyi . alicdn . com / multi_dns_
 resolve ? client_ip = 182 . 92 . 253 . 16
```

```
' - d  ' d . tv . taobao . com '
```

5. **Returned format: json data is returned. After resolution, domain IP addresses are extracted and polling can be performed among them. TTL cache and expiration rules must be followed.**

```
{" dns ":[{" host ":" d . tv . taobao . com ," ips ":[{" ip ":" 115
 . 238 . 23 . 240 ," spdy ": 0 },{" ip ":" 115 . 238 . 23 . 250 ,"
 spdy ": 0 }]," ttl ": 300 ," port ": 80 }]," port ": 80 }
```

6. **Request example with multiple domains**

   - **Request example**

```
# curl  ' http :// umc . danuoyi . alicdn . com / multi_dns_
 resolve ? client_ip = 182 . 92 . 253 . 16
' - d  ' d . tv . taobao . com   vmtstvcdn . alicdn . com '
```

   - **Return example**

```
{" dns ":[{" host ":" vmtstvcdn . alicdn . com ," ips ":[{" ip
 ":" 115 . 238 . 23 . 250 ," spdy ": 0 },{" ip ":" 115 . 238 . 23
 . 240 ," spdy ": 0 }]," ttl ": 300 ," port ": 80 },{" host ":" d
 . tv . taobao . com ," ips ":[{" ip ":" 115 . 238 . 23 . 240 ,"
 spdy ": 0 },{" ip ":" 115 . 238 . 23 . 250 ," spdy ": 0 }]," ttl
 ": 300 ," port ": 80 }]," port ": 80 }
```