阿里云
CDN

用户指南

文档版本：20180906

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止：** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告：** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明：** 您也可以通过按**Ctrl** + **A**选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 Value-added service

1.1 Yellow picture

Product introduction

- CDN photo yellow is a value-added service accelerated by CDN. After this feature is opened , during the user's use of the CDN service, the system automatically detects if the image accelerated by the CDN is yellow, the URL of the broken picture will be logged for export and deletion by the user.
- The CDN image is yellow and is charged by the scan counter, with the image of the return as the detection base, the same picture URL will only be detected once and will not be charged repeatedly, at the same time, the user can set a daily detection limit, and control the amount of consumption.
- Based on the cloud computing platform, CDN's images are capable of rapid detection of massive amounts of data, helps users save more than 90% of their labor costs.

Usage

The image yellow feature can be used in the value-added services of the CDN console:

1. Set the domain name and limit to be detected: for the first time, enter the unset detection domain name, the domain name in the CDN needs to be added to the detection list in the settings to start Detection:

   Click set now to enter the settings menu:

   - Detection domain name settings: select the domain name to be detected on the left, add to the domain name column in the right detection.
   - After you finally click OK to save, the cloud begins to detect new pictures accelerated via CDN.

     Note:

     The first-time provisioning service is the next day, 0: 00 to start testing.

     This function will not be detected on existing stock pictures. To detect stock images, You can manually refresh the cache, And then refresh the cache, the image will be detected

automatically the next time the user visits it via CDN, the entire test result is delayed by 3-4 hours.

2. View statistics and actions: After the configuration is complete, wait for the cloud to start detecting, there will be first batch of results in three to four hours.

   The image yellow menu opens to see the statistical information for the detection, including the total amount detected today, the number of pictures of suspected pornography and the amount of images determined to be porn:

   Click the picture List tab to view a list of pictures, and SELECT query criteria to filter pictures:

   You can turn the page below, you can view all detected images in the picture list (if they are deleted from the source station, they may cause control to fail to display this picture).

   Manual marking of porn pictures. Because the detection system can not achieve the accuracy of 100, A small number of images will be identified as suspected pornography or the result is wrong, at this point, the picture can be marked as porn or normal by hand. You can also select multiple images to batch mark simultaneously:

3. To export a list of yellow-colored pictures: the system will combine the results of the test and the results of manual marking to determine whether the picture is in violation, export all violation pictures with the export violation picture button:

   Users can delete from their own systems based on the exported list, then refresh the corresponding CDN cache.

Product pricing

- CDN picture yellow billing rules:
  - The billing cycle is 1 day and 1 time;
  - According to the same-day scanning volume charges, the larger the daily scanning volume, the lower the unit price;
  - The algorithm determines the part and the pending user confirmation part are charged according to the different unit price.
- The detailed billing criteria for the afterpayment model are as follows:

Ladder (sheet/day)	Determine part, unit price (RMB/kilobytes)	For user confirmation part, unit price (RMB/kilobytes)
> 0	£ 1. 80	0. 45
> 5000	£ 1. 62	0. 41
> 50000	£ 1. 53	0. 38
> 130000	£ 1. 44	0. 36
> 260000	£ 1. 35	0. 34
> 850000	1. 26	0. 32

- The price of the yellow package is as follows:

Yellow bag specifications	Price	Discount corresponding
0.5 million sheets	810 yuan	9-fold
3 million sheets	4590 yuan	15% off
5 million sheets	7200 yuan	20% off
10 million sheets	13500 yuan	25% off
0.1 billion sheets	126000 yuan	30% off
0.5 billion sheets	540000 yuan	40% off

- Yellow Resource Pack credit rule:

  The algorithm determines the part according to the 1-1 credit, pending the user confirmation part following the 1-0. 25 credit.

1.2 Dynamic Route for CDN

1.2.1 All Station Acceleration

Introduction to application scenarios

All-Stop acceleration is dynamic acceleration, for dynamic and static content mixing across industries, with more dynamic resource requests (such as ASP, JSP, PHP) files in equal format) the site of Ali cloud CDN is accelerated throughout the station to provide:

- 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:

The station-wide acceleration is the default pure dynamic acceleration, which means that 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.

Billing rules

The station is accelerated as a value-added service and the billing item is "base cost" + "request cost ". Where "base cost" is based on the "by peak bandwidth" or "by traffic" selected by the CDN service "base fee for the charge. "" The number of requests cost contains the number of dynamic HTTP requests, the number of dynamic HTTPS requests, and the number of static HTTPS requests, respectively according to the unit price on a daily basis. All Station acceleration details reference All Station accelerated introduction.

1.2.2 Dynamic Protocol follows back Source

Introduction

The Dynamic Resources return to the source using the protocol and the client access to the resource protocol is consistent. For example, the client requests dynamic resources using the HTTP protocol, the CDN node will also get the resources back from the HTTP protocol, similarly , if the client requests a dynamic resource with the HTTPS protocol, the CDN node will get the resource back to the source with the HTTPS protocol.

Configure boot

Domain name management, select domain name to enter the domain name configuration page, set up static acceleration rules.

Select in dynamic protocol follow back Source:

Note:
Dynamic Protocol follow-back source is configured for requests for dynamic resources, the protocol in the source settings follows back to the source is configured for requests for static resources, there is a difference between the two.

1.2.3 Special header settings

Introduction

Depending on the cache-control field in the header, select whether to accelerate dynamically. The cache-control content of the header is forced to start dynamic acceleration in accordance with any of the rules in the configuration, the remaining configurations are no longer checked.

Configure boot

Choose**Domain name management** > **Domain Name configuration page** > **Static acceleration rule settings**:

Select**Special header settings** > **Set the cache-control rule to force dynamic acceleration to be turned on:**

Note:
For example: set rules No-cache, dynamic acceleration is forced on all resources with no-cache in the cache-control in the Response Header, does not cache on edge nodes.

1.2.4 Static file type

Introduction

All-site acceleration defaults to pure dynamic acceleration, which means that all resource requests use dynamic acceleration, get resources through the best route back source. Therefore, static resources are not cached by edge nodes. You can visually distinguish between dynamic and static resources by configuring to specify the type of static file, optimal Scheme to achieve static Resource Use edge cache and dynamic acceleration of Dynamic resources;

Configure boot

Choose**Domain name management** > **Select domain name to enter the domain name configuration page** > **Dynamic static acceleration rule settings:**

Select a static file type to configure.

Check the file type for the static resource, and the selected resource type uses the edge cache, instead of going back to the source for resources each request.

1.2.5 Static path settings

Introduction

All-site acceleration defaults to pure dynamic acceleration, which means that all resource requests use dynamic acceleration, get resources through the best route back source. Therefore, static resources are not cached by edge nodes. You can distinguish between dynamic and static resources by configuring a path that specifies a static file, it can achieve the optimal scheme of static resources using edge cache and dynamic resources using dynamic acceleration.

Configure boot

Choose**Domain name management** > **Select domain name to enter the domain name configuration page** > **Dynamic static acceleration rule settings:**

Select static path settings to specify the path for the static resource:

The resource for the static PATH uses the edge node cache for the user's immediate acquisition, achieve better acceleration effects.

1.2.6 Set Static File URI

Function introduction

The function supports distinguishing static files by file URI. The set static files no longer use dynamic acceleration; instead, they use static acceleration and allocate the best edge nodes for caching and distribution.

Procedure

Click **Configure of the domain name you choose on the Domain Name Management page. > Click Modify on Dynamic and Static > Acceleration Rule Settings >**

Set Static File URL.

Type in the specified URL.

2 Usage Query

3 账单导出

功能介绍

您可以导出按日计费，或者是按月计费的实际用量数据，以便于与费用中心的出账用量进行比对。

- 您只能按账户维度导出。
- 您只能导出某一天，或者某个整月的数据。
- 导出数据格式：PDF。

操作步骤

1. 在CDN域名概览页，单击**用量查询**。

2. 在用量查询页签下，选择日期，然后单击查询账单。

3. 您可以单击下载

4 明细导出

功能介绍

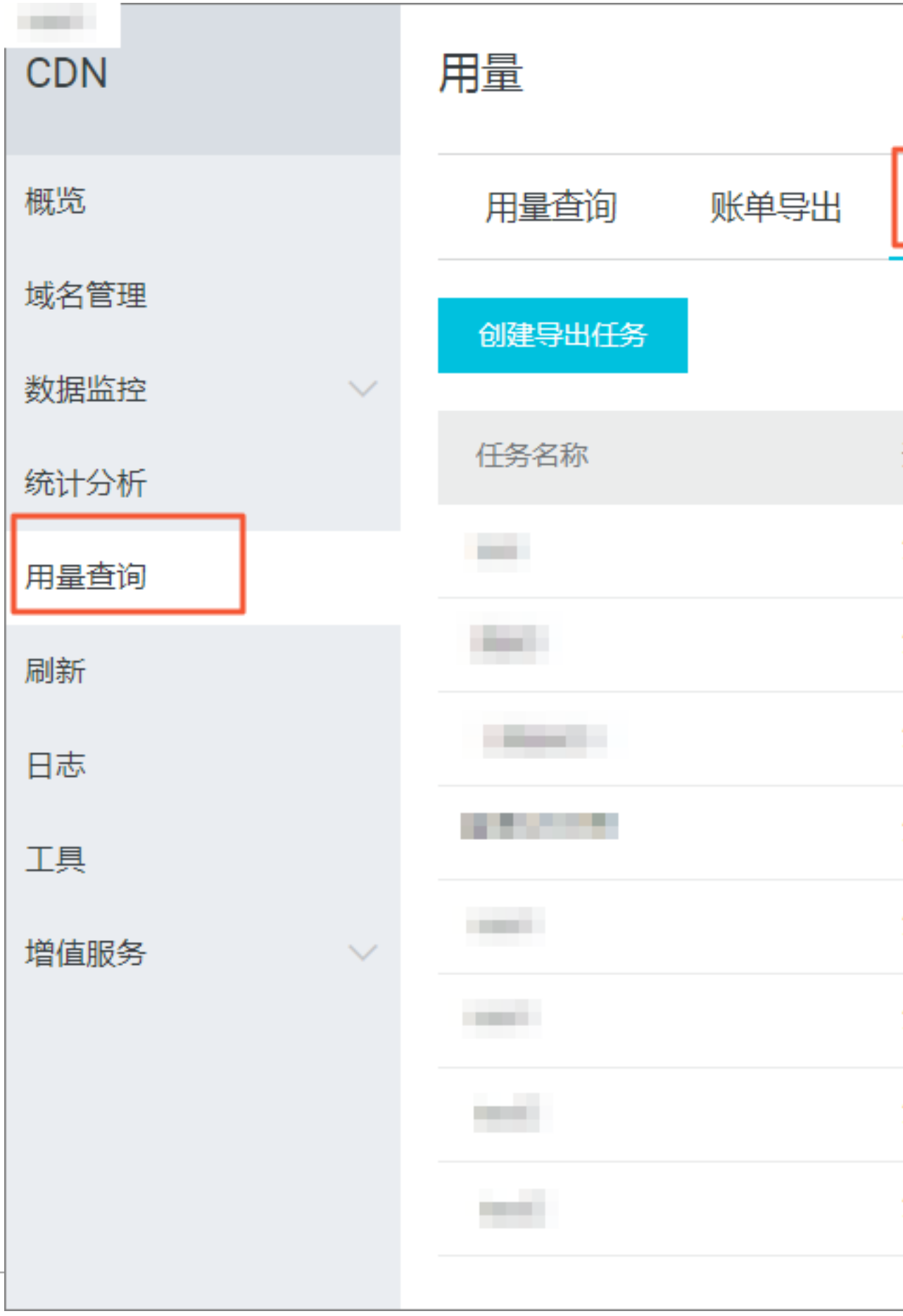
通过明细导出功能，您可以导出流量带宽及请求数的5分钟明细数据，便于您通过明细来核对或计算实际消费的计量数。

- 您可以按照账户、资源组、域名维度进行导出。
- 导出资源组时，会将资源组下所有域名也一并导出。
- 您一次性最多可以导出100个域名。超过100时，只保留资源组明细。
- 导出的所有数据，均为每五分钟一个点。
- 下载的数据格式：CSV。
- 导出的时间段不可以重复。

操作步骤

1. 登录CDN控制台，进入**域名管理**页面，选择需要设置的域名，单击**管理**。

2. 在用量查询 > 明细导出页面，单击创建导出任务。



3. 填写相应导出任务的任务名称（必填），并选择导出对账类型、查询时间（必选）和导出内容和导出频次。

4. 单击确定，创建导出任务成功。

5 Usage Query

Usage Query

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 domain name or by user.
- Choose traffic, bandwidth, or requests to query.
- When querying for traffic or bandwidth, you can obtain the usage data in each billing region. Currently, Alibaba Cloud CDN contains 8 billing regions: China, Asia Pacific 1, Asia Pacific 2, Asia Pacific 3, South America, North America, Middle East/Africa, and Europe.

Display rule of query charts and lists:

Time Span	Trend Chart	Data List
1-3 days	hours	By traffic: hours By bandwidth: days
More than 4 days	Days	Days

Note:

You cannot export data from the Usage Query page.

Billing Export

You can export daily or monthly usage data to check with the billing data issued in the Expense Center.

- You can only export data by account.
- You can only export data of a certain day or a whole month.
- Exported data format: PDF

Detail Data Export

You can export five-minute detailed data of traffic, bandwidth, or requests to check or calculate the actual usage.

- 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 at most 100 domain names at one time. When you export over 100 domain names, only the resource group details are retained.
- The time span for all exported data is five minute.
- Downloaded data format: CSV
- You cannot export repeated time span.

6 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

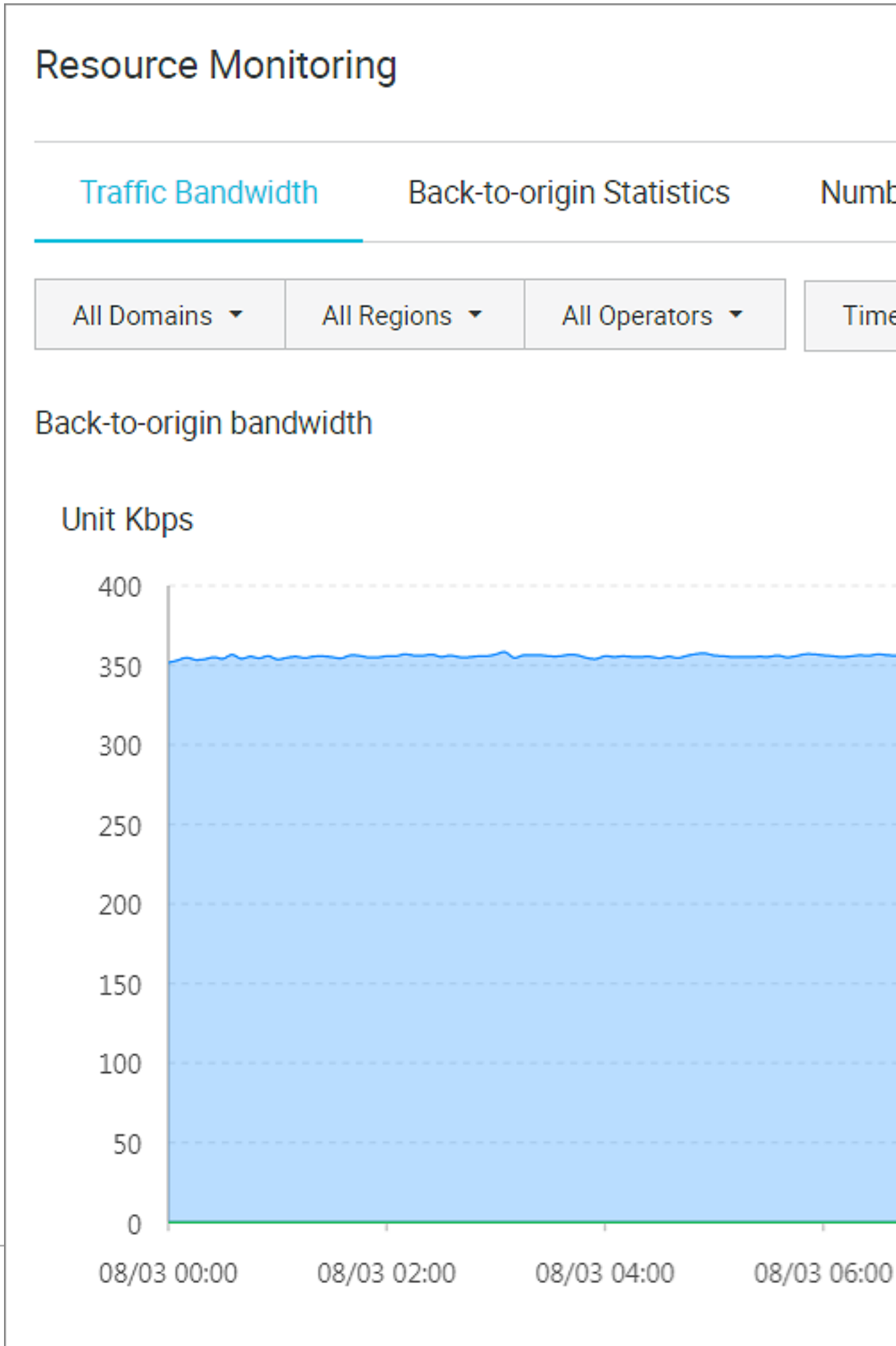
You can select the**Domain Name**, **Region**, **Operator** or the **Time Range** you want to view (**Past 1 Hour**, **Past 6 hours**, **Past 12 hours** or **Custom**) to view the specific condition in the following dimensions:

Items	Metrics
Basic Data	Bandwidth, Traffic, Number of requests, QPS
Back-to-origin Traffic	Back-to-origin Traffic, Back-to-origin Bandwidth
Quality monitoring	Request Hit Rate, Byte Hit Rate, 5xx status code, 4xx status code, 3xx status code, 2xx status code.

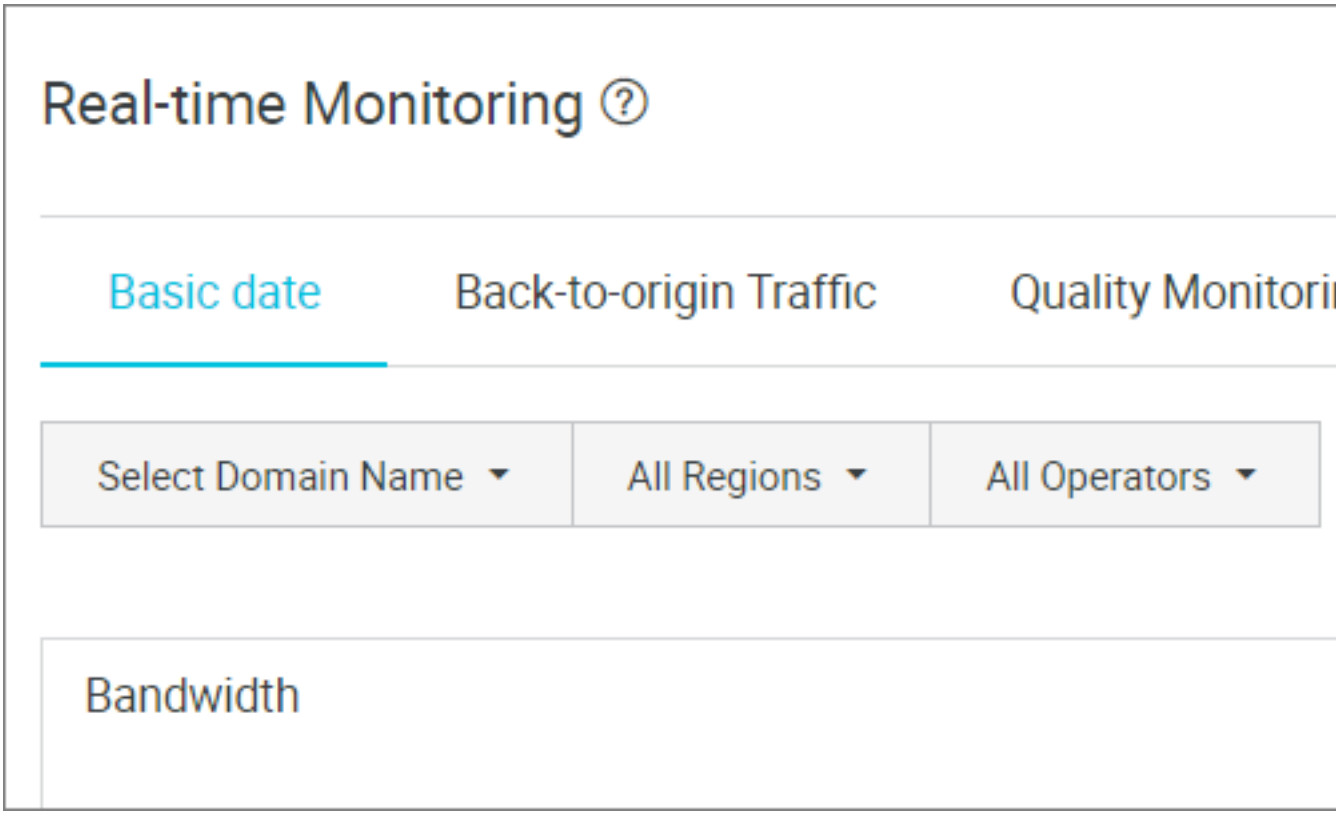
Procedure

1. Log on to the CDN console, then go to the **Domain Names** page. Choose a domain name, then click **Manage**.
2. Go to **Data Monitoring** > **Resource Monitoring** or **Real-time Monitoring**, and select the monitoring items and metrics. 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：



7 Cache refresh

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

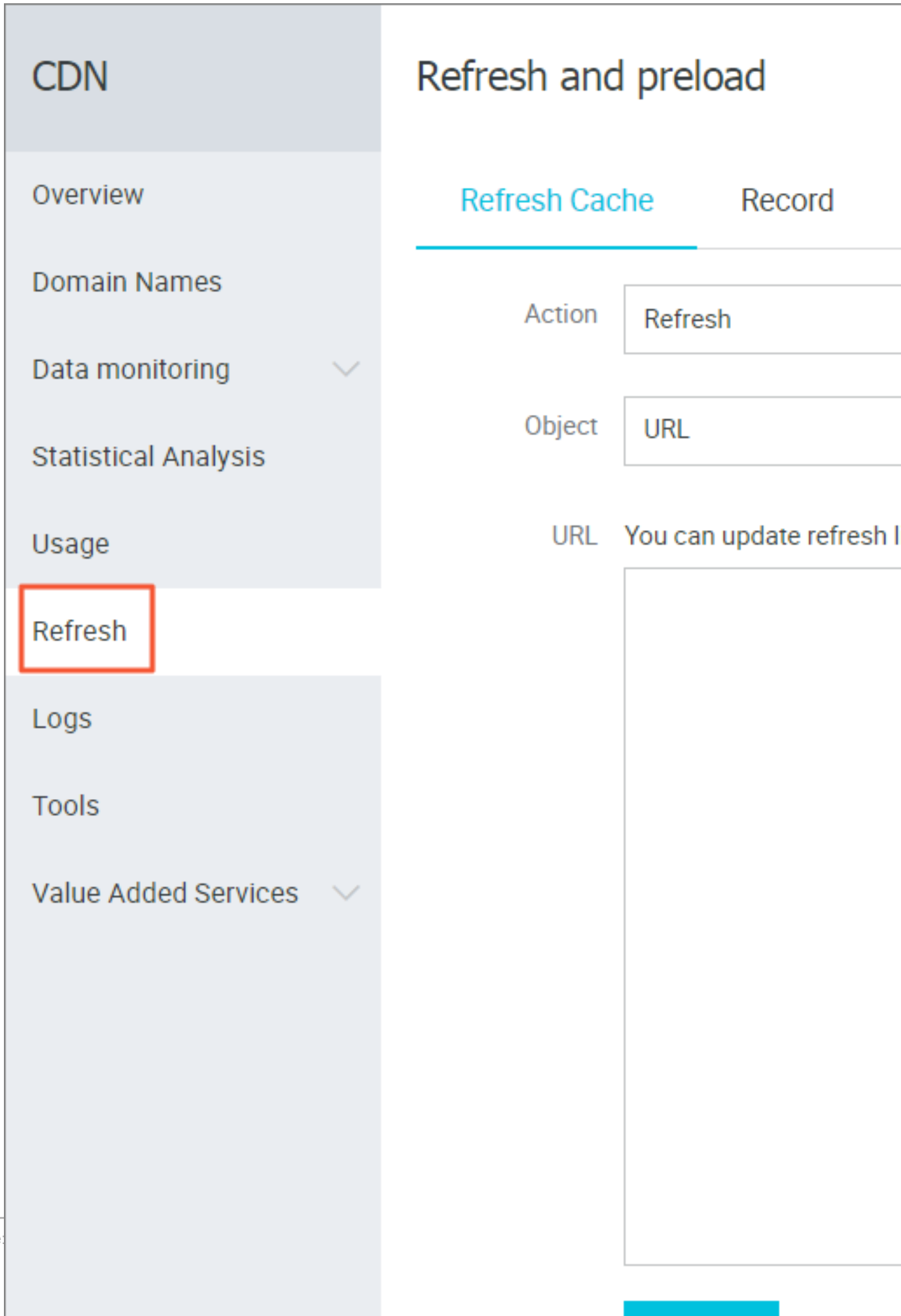
URL refresh

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

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 Records**to view the progress of the resource refresh or push.
- Alibaba Cloud CDN provides the API for querying progress: *DescribeRefreshTasks*.

8 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.

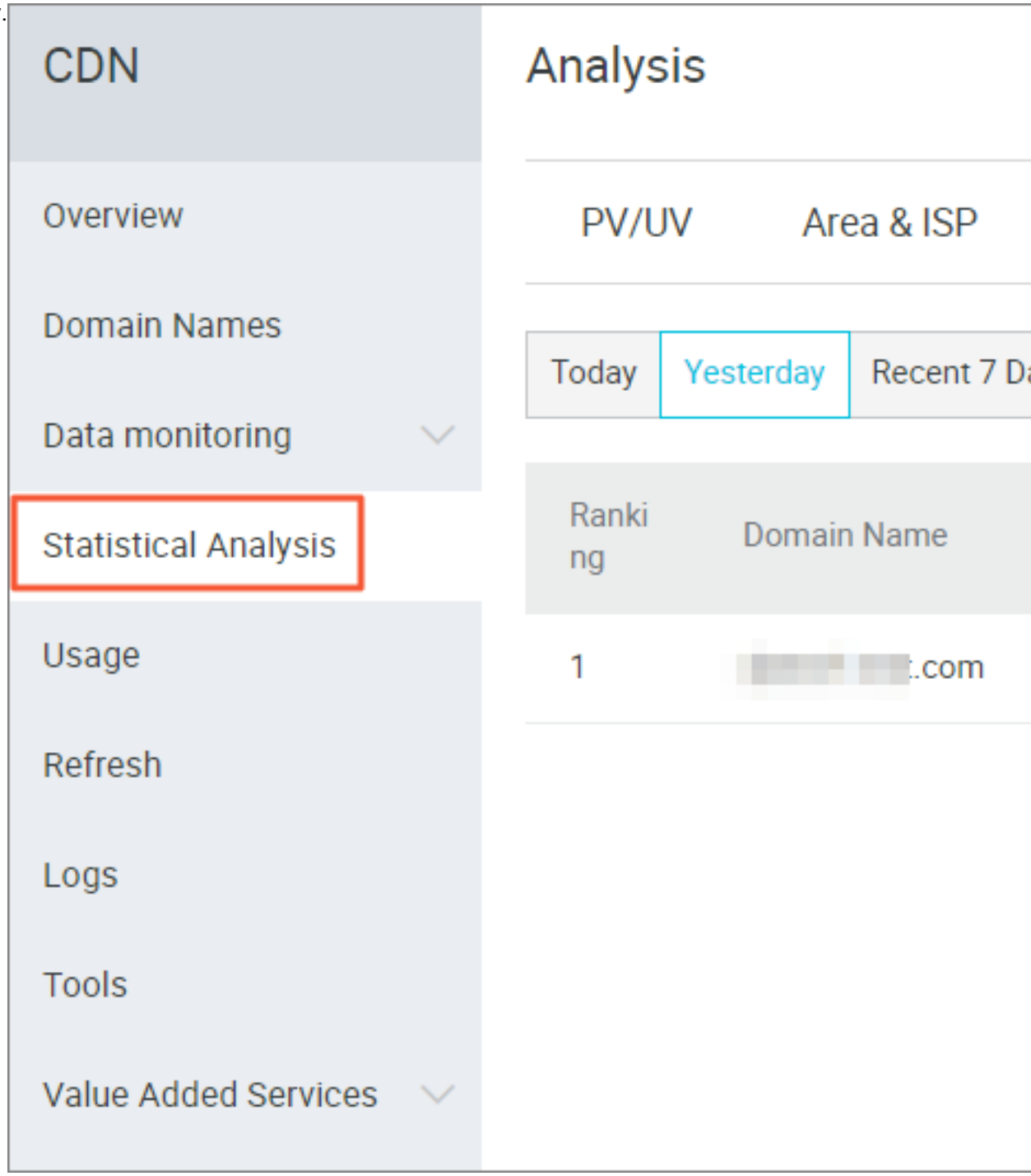
Note:
The precision of original data collection varies according to time spans, which are 300s, 3600s, and 14400s for daily export, weekly export, and monthly export, respectively.

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, then go to the **Domain Names** page. Choose a domain name, then click **Manage**.

2. Go to **Statistical Analysis** , and select the monitoring items and metrics. Click **Query**.



9 Log Management

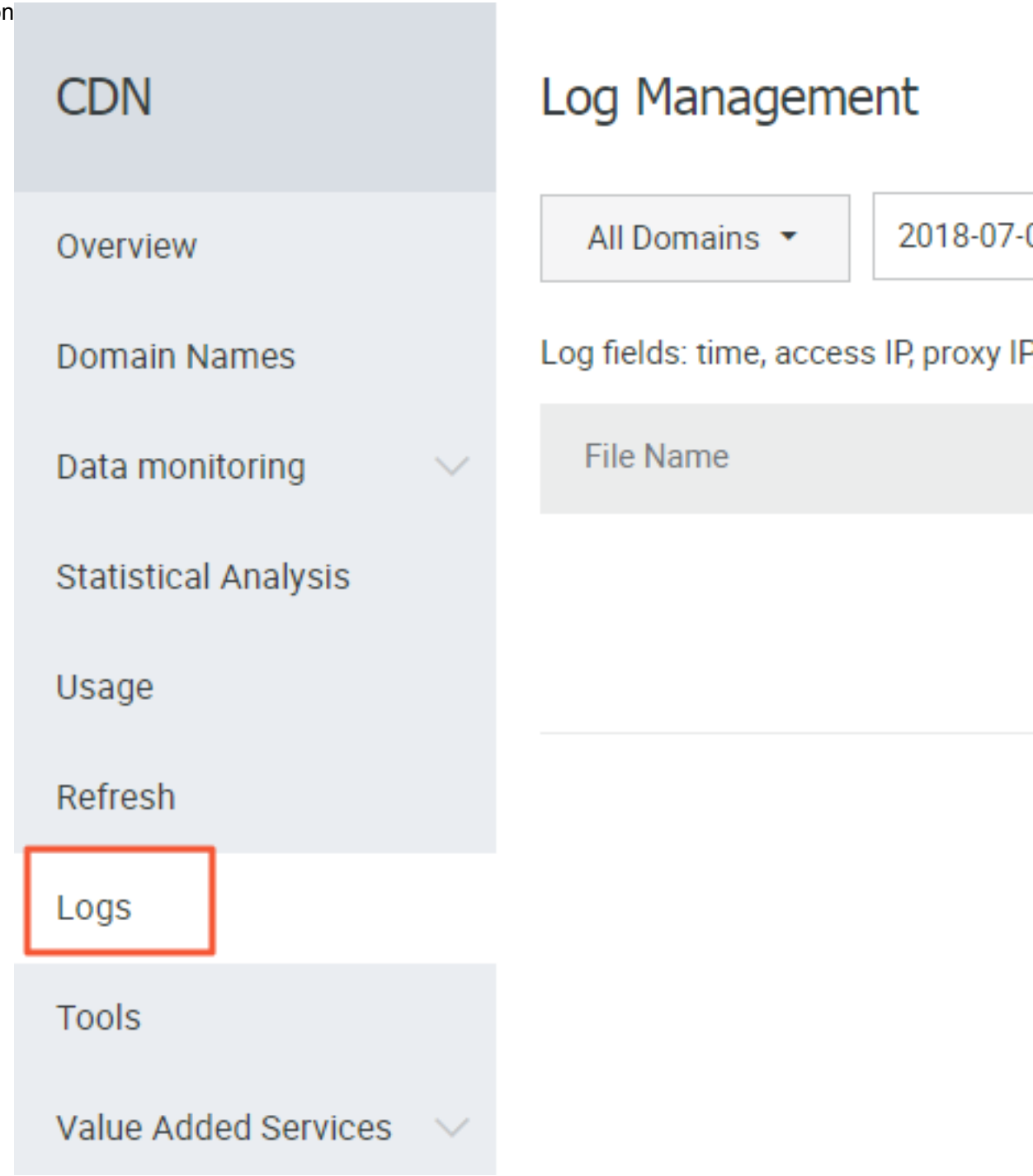
9.1 Log Downloading

- 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: `Acceleration domain name_year_month_date _start time_end time`.
- Log field format description.

Sample log content

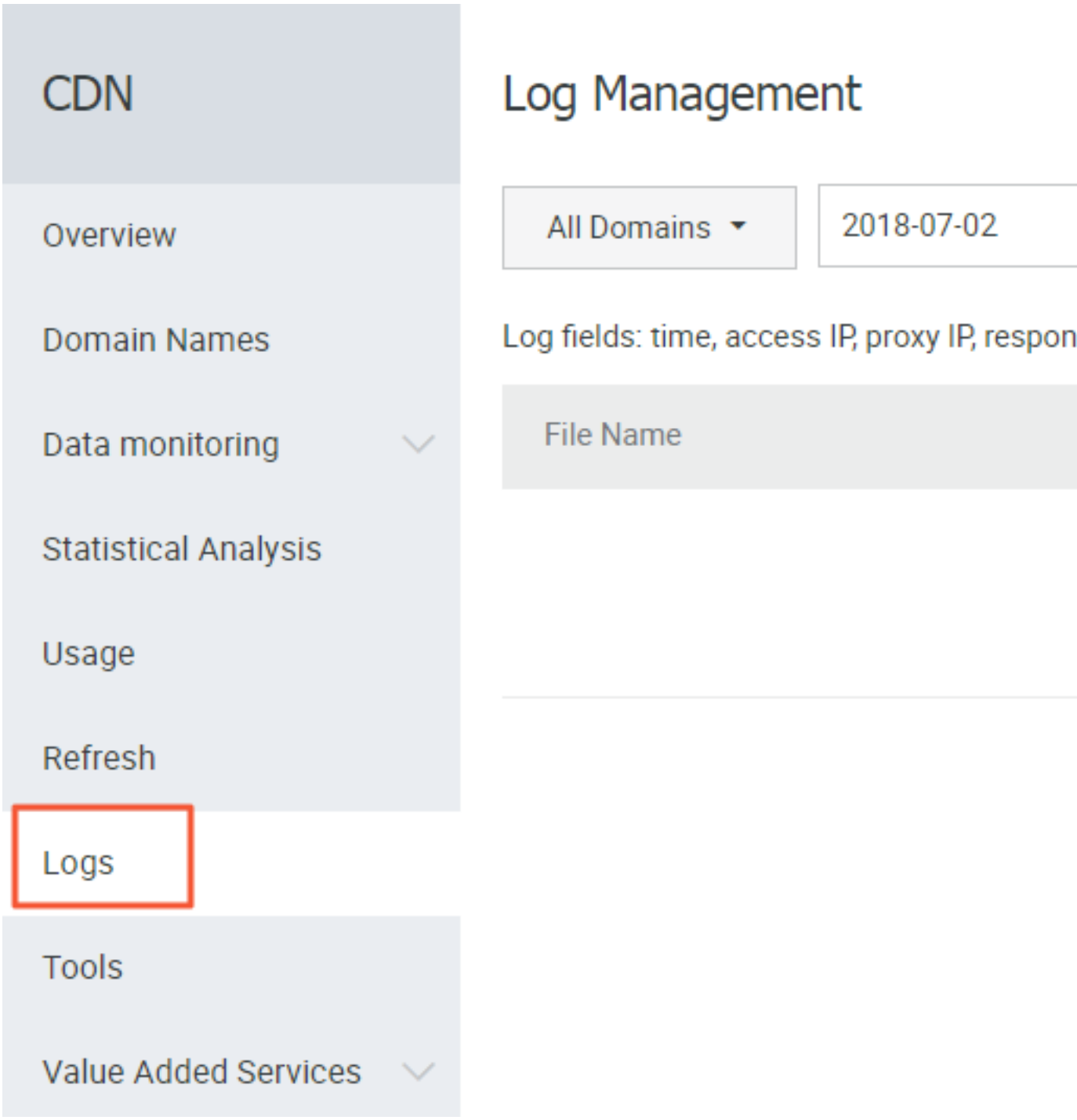
```
[9/Jun/2015:01:58:09 +0800] 188.165.15.75 - 1542 "-" "GET http://www
.aliyun.com/index.html" 200 191 2830 MISS "Mozilla/5.0 (compatible;
AhrefsBot/5.0; +http://ahrefs.com/robot/)" "text/html"
```

Log field description



Field	Parameter
time	[9/Jun/2015:01:58:09 +0800]

Field	Parameter
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
Log fields: time, access IP, proxy IP, respon
File Name

9.2 日志转存

日志转存，是阿里云CDN配合函数计算，共同推出的一项日志服务，可以帮助您将日志存储更长的时间，便于您基于长时间的日志做出自定义的数据分析。这将有助于您更好地了解您CDN的服务质量，以及您的终端客户的访问详情，提高您的业务决策能力。

功能介绍

目前CDN的离线日志服务，只能默认提供1个月的存储时间。如果您有更长时间的存储需求，可以将日志转存至OSS，方便您根据实际情况对日志进行保存和分析。

CDN的日志转存服务搭载函数计算来实现转存。使用日志转存服务时，您需要开通函数计算服务。授权CDN后，CDN会帮您一键创建函数计算服务来实现日志转存。此外，您也可以登录函数计算控制台，通过已有的函数计算服务来完成日志转存的服务。

计费： CDN不收取任何日志转存费用。当您通过函数计算完成日志转存时，会消耗函数计算的计算资源，因此函数计算会收取非常低廉合理的费用，函数计算每月也提供一定免费使用额度。具体价格，请参考函数计算计费方式。

CDN与函数计算

CDN和函数计算无缝集成，使您可以为CDN的各种事件设置处理函数，并通过事件中的域名等参数进行过滤，只接收自己感兴趣的域名的数据。当CDN系统捕获到指定类型的、满足过滤条件的事件后，会自动调用函数处理。

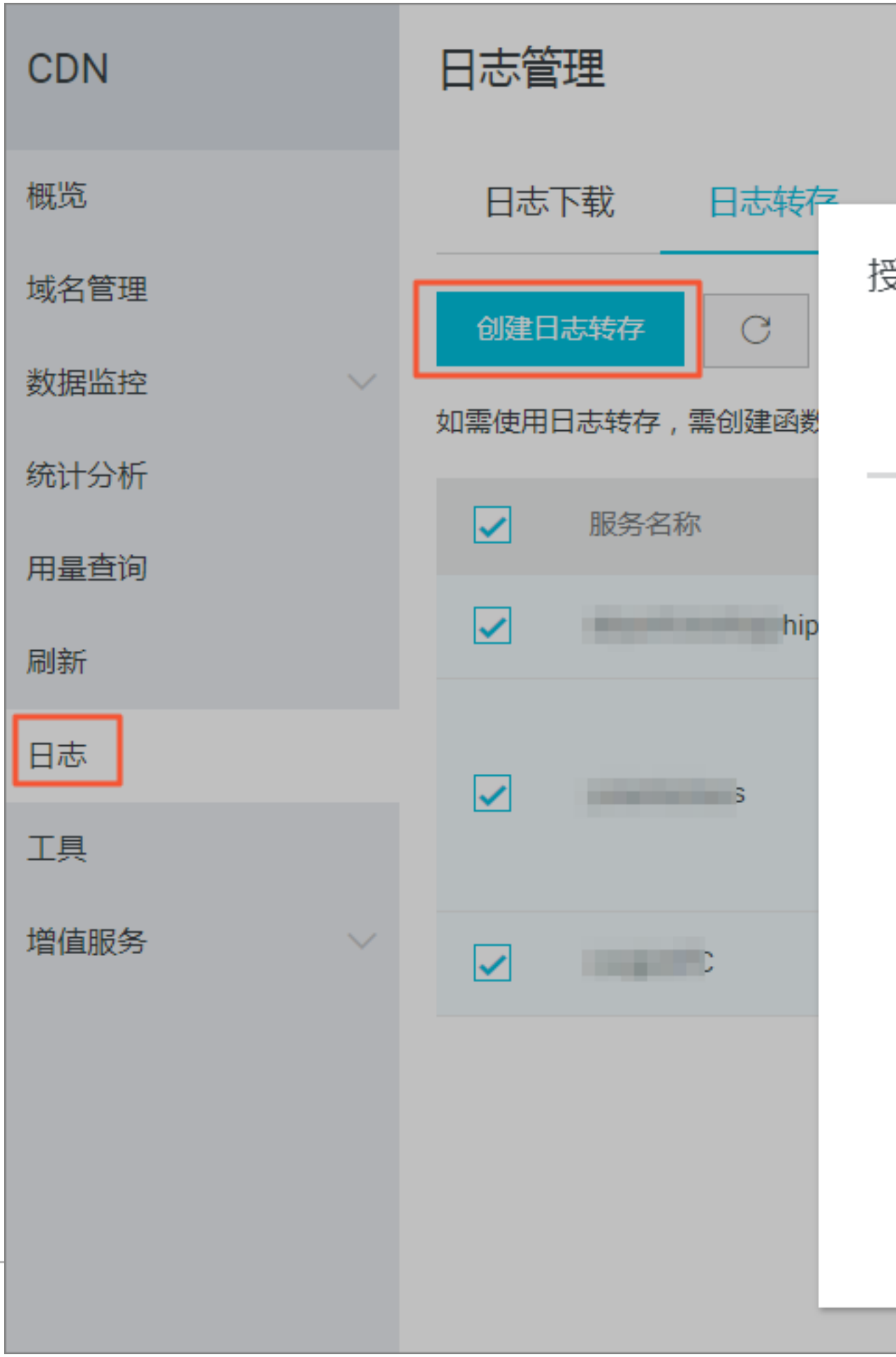
目前函数计算已经支持了多种CDN的场景，包括：日志转存、刷新、预热、资源封禁、域名添加和删除，域名启用和停用。触发这些场景的具体方式，请参考*CDN*事件触发器。

此外，函数计算已经和阿里云多个云产品联合使用，包括*OSS*、*VPC*、日志服务、*API*网关等，帮助您快速构建应用。

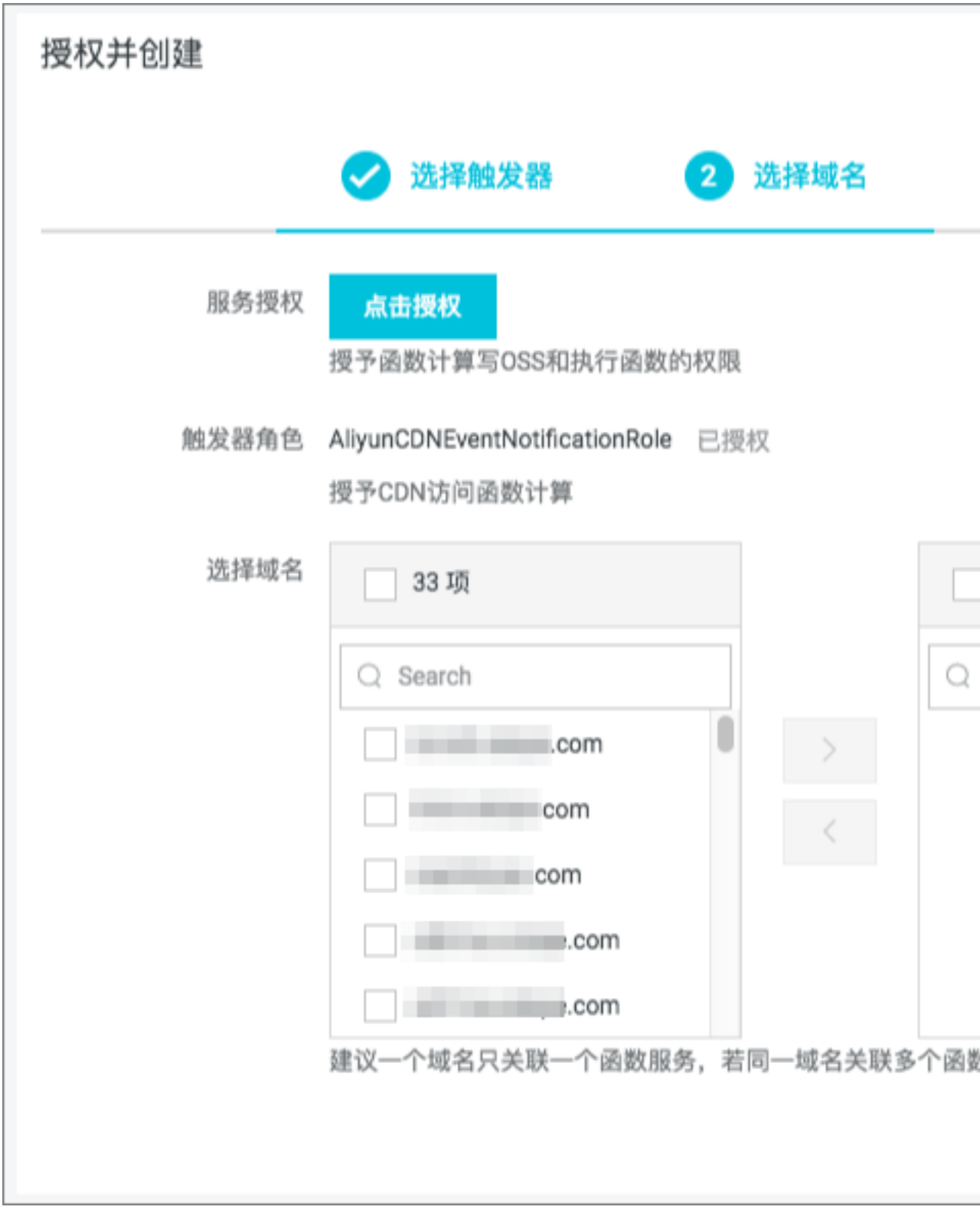
操作步骤

1. 登录CDN控制台，进入域名管理页面，选择需要设置的域名，单击管理。
2. 在日志管理 > 日志转存页面，单击创建日志转存。

3. 输入服务名称，选择OSS Bucket。然后单击下一步。



4. 单击点击授权，并选择域名关联函数服务。然后单击创建。

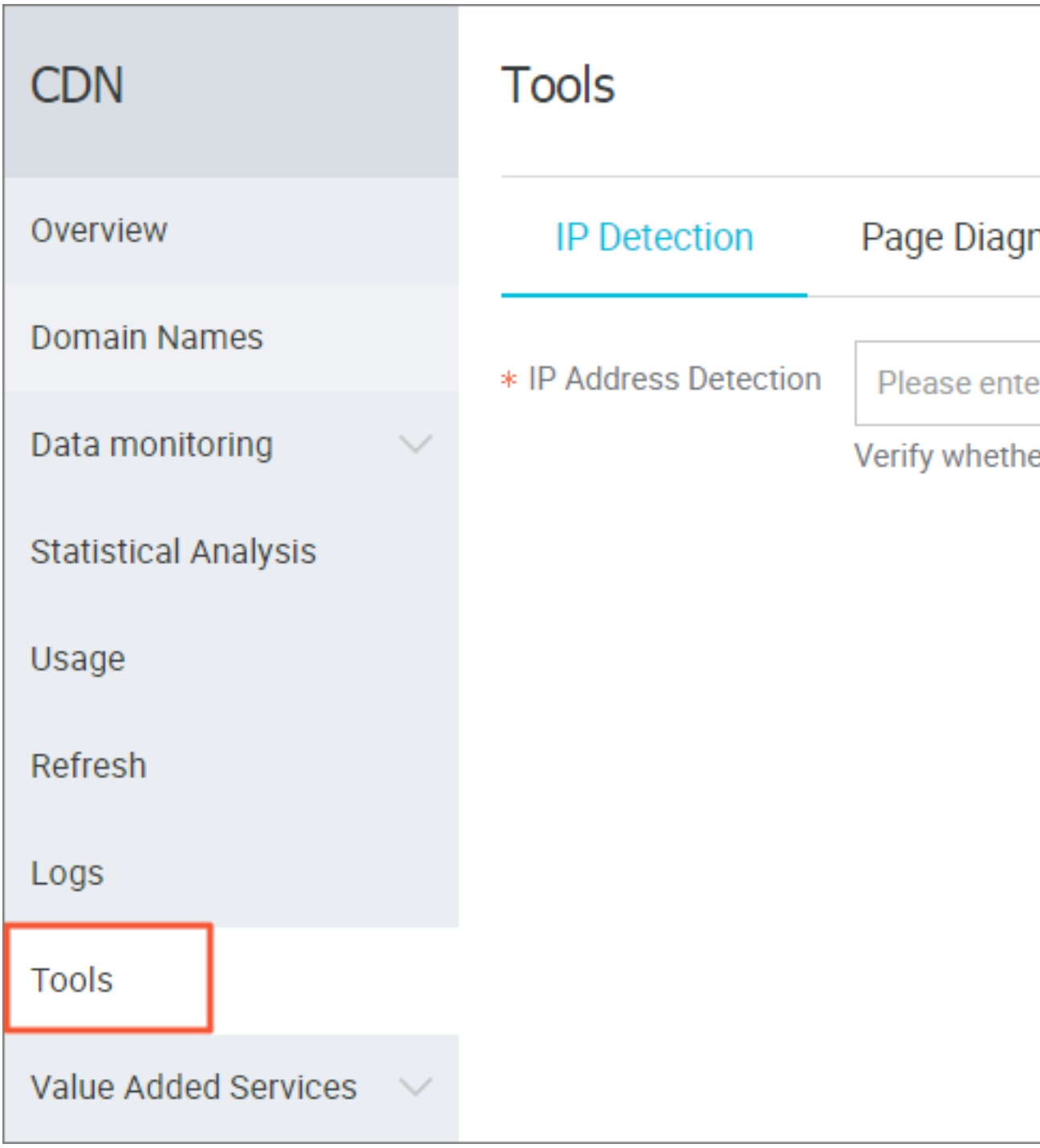


5. 单击完成。


授权并创建
选择触发器
选择域名
日志转存设置成功
当域名产生新的日志后，会根据您的触发器规则推送日志，
管理触发器规则，或在OSS查看已转存的日志

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 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}
```

12 CDN Sub-Account User's Guide

This document is available to customers of CDN domain name resource group management requirements, the sub-account + Resource Group is used to authorize the isolation of resources between different departments, and the access process is as follows.

Access Process

1. Log on to the Enterprise Console.

   Note:
   Resource Group setup and sub-account management need to be done in the Enterprise Console, after you have set up the appropriate resource groups and permissions, A child account is logged into the CDN console and limited resource viewing and operation is performed in accordance with the rules that have been set, ensure that operations and resource displays are completely isolated between sub-accounts.

   Use the master account to log on to the *Enterprise Console* (attached: *Enterprise Console User 's Manual*).

2. Create a sub-account.

   - Entering the personnel management module for the first time requires the creation of a directory, A user must and only belong to a directory.**personnel management**
   - After creating the directory, you can**Personnel Management** > **User management**Create a sub-account in.

   Note:
   Groups can also be created and managed in a unified manner, depending on your business needs.

3. Create a Resource Group + authorization.

   Enter the **Resource management**resource management module, create a resource group, and create the following **1 BU**。No. 1 bu Resource Group.

   Complete**resource**、**personel**and**set**。

EnterResources management > Resource To achieve accelerated domain name grouping settings, select the product CDN in the filter area, check the accelerated domain name to which you want to join the resource group, and click **go to** complete the accelerated domain name settings within the resource group.

EnterResource management > MembersComplete the authorization for the sub-account, click **Add-on**, you can select a sub-account that needs to manage this resource group and complete the policy authorization: authorization template description.

4. Log in to the CDN console using a sub-account.

   Login address: *http://signin.aliyun.com/<custom domain>.onaliyun.com/login.htm*

   After the sub-account is logged in, you can select a resource group that shows that the current sub-account has permissions, accelerate domain names according to resource group column.

   Self-account support Domain name management, monitoring, refresh and log download, and other operations are in full agreement with the master account, please refer to *Quick Start*.

Appendix

Current Ram template Policy

1. CDN management authorization: supports additional Delete check changes.

```
Version: "1 ",
"Statement ":[

    Action: CDN :*",
    "Resource ":"*",
    "Effect": "allow"
```

2. CDN read-only permission.

```
Version: "1 ",
"Statement ":[

    Action: CDN: Describe *",
    "Resource ":"*",
    "Effect": "allow"
```

13 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 diaplay 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:

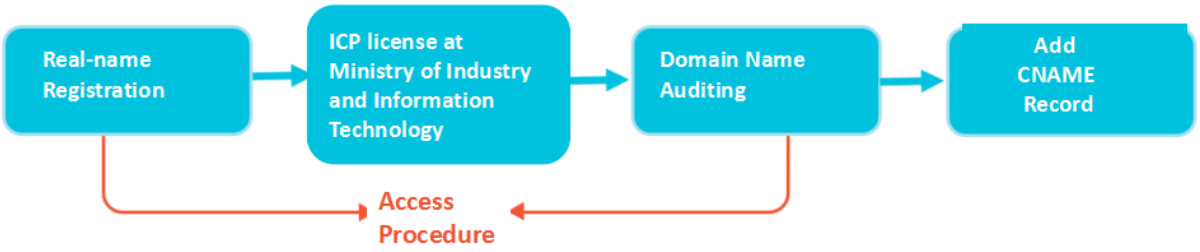
Functions	Brief introduction
Domain name management	Add a CDN domain name, manage, or delete a CDN domain name, and change the basic and configuration information of the CDN domain name.
Monitoring	Include four parts, Traffic Monitoring, User Access Monitoring, Data Analysis, and Security Protection

Functions	Brief introduction
Refresh	URL refresh and directory refresh are available.
Expenditure	View expenditure of all types of services.
Log	Log downloads, log storage (upcoming), Cloud reports
Tools	Link diagnostic tools, IP queries

14 Limits

Restrictions on the use of CDN

Procedure



1. Real-name registration must be performed for accounts on the Alibaba Cloud official website.
2. A CDN domain must have an *ICP license*and be connected to Alibaba Cloud.
3. A CDN domain must have an ICP license and be connected to Alibaba Cloud.
4. The origin site content of a CDN domain must be stored on Elastic Compute Service (ECS) or Object Storage Service (OSS). If the origin site content is not stored on Alibaba Cloud, access must be reviewed.
5. Add CNAME record, and resolve your domain name to the CNAME domain name generated by CDN, that is, add CNAME record for your domain name at DNS service provider. For more information, see *Configure CNAME*.

Note:

- If your source station is deployed on ECS, focus on ECS bandwidth. We recommend that the ECS bandwidth is at least 20% of your overall bandwidth.
- In the origin site security software configuration, make sure that CDN cached node can access the origin site.
- Make sure that when the CDN acceleration service is disabled, all requests will be returned to the origin.
- After adding the CNAME, the cname domain name that you get cannot be accessed directly and can only be accessed using CNAME.
- Range 0 ~ Infinity is not recommended for large files.

Domain Name reviewing standards

All domains attempting to access CDN must be reviewed. CDN access is not allowed in any of the following scenarios:

- The CDN domain cannot be accessed normally or the content does not include any substantive information.
- The CDN domain is for a private game server.
- The CDN domain is used for role playing games or card games.
- The CDN domain name is for website that has no download rights such as pirate software
- The CDN domain is for a P2P website.
- The CDN domain is for a lottery website.
- The CDN domain is for an illegal hospital or pharmaceutical website.
- The CDN domain is for a site involving porn, gambling, drugs, etc.
- An automatic timeout rejection occurs, and outputs the following: Your domain name is rejected because it failed to comply with CDN access rules. Reference the feedback and submit a qualified domain name to be reviewed again.

The losses incurred by attacks or malicious download because the CDN domain name does not comply with the previous rules will be born on you, and Alibaba Cloud CDN carries no responsibilities.

- Domains that have accessed Alibaba Cloud CDN will be reviewed regularly. If any of these violations are detected, the system immediately terminates the CDN acceleration of the domain name, and stops the CDN service for all your domain names at the same time.
- If your CDN domain name cannot be accessed normally or is denied due to reason which does not contain any substantive information, and your business is a compliance business, you can submit a ticket, and send the screenshots of the web site business content(which contains the domain name) through the ticket. After the ticket is reviewed separately, you will be informed of the results of the second audit.

Restriction

Quantity	**Limit quantity**
Quantity	Limit quantity
Domain Name	The maximum number of CDN domains for each Alibaba Cloud account is **20** .

Quantity	Limit quantity
IP origin site	The maximum number of IP origin sites for each CDN domain is **10**.
Cache refresh and push operations	**refresh:**2000items/day/account. **Directory refresh:**100100 items/day/account.

If you have a large number of domain name acceleration needs, submit a ticket for special support .

CDN domain name reclaiming rules

If your CDN domain name...	The system will...	To continue using CDN acceleration, you must...
not access traffic for more than 90 days (including "normal operation")	Automatically deactivate the domain name to save the CDN domain name related records	Enable CDN domain names.
Is in the disabled state for more than 120 days (including auditing failed)	Automatically delete the domain name related records.	Re-add the domain name.

15 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

Back-to-source settings

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

Cache settings

Function	Description	Default
Cache expiration time	Customizes cache expiration rules for specified resources.	Disabled

Function	Description	Default
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

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

16 域名管理

16.1 Data monitoring

16.2 URL authentication

Introduction

The URL authentication function protects user's site resources from illegal download and misuse . Leeching issues are only partially solved by adding the referer blacklist or whitelist. Because the referer content may be forged, this method cannot protect site resources completely. Applying URL authentication is recommended to protect the security of origin site resources.

Concept

The URL authentication function uses Alibaba Cloud CDN nodes in combination with client resource sites to provide a more secure anti-theft protection for origin site resources. The CDN client site provides a user with an encrypted URL (including permission verification information), and the user uses it to initiate a request to the CDN node. The CDN node verifies the permission information in the encrypted URL to determine the legality of the request. Legal requests will receive a normal response and illegal requests will be rejected. This protects CDN client site resources.

URL authentication methods

Alibaba Cloud CDN supports authentication Method A, Method B and Method C. You can select an appropriate method to protect origin site resources based on your business requirements.

Concept

Structure of users' encrypted URLs

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

Authentication field descriptions

- `PrivateKey` field can be set by the user.
- The validity period 1,800 s indicates that the authentication fails when the user fails to access the client source server 1,800 s after the preset access time. For example, if the preset access time is 2020-08-15 15:00:00, the actual link expiration time is 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 1800s.
rand	Random number. We recommend that you use UUID (not including en dash "-", for example, 477b3bbc253f467b8def6711128c7bec format)
uid	Temporarily unused (set to 0).
md5hash	The verification string is calculated using the MD5 algorithm. It is comprised of digits and lowercase English letters (0-9, a-z) with a fixed length of 32.

After the CDN server receives the request, it first determines whether the request `timestamp` is less than the current time. If so, it determines that the request has expired and returns an HTTP 403 error. If the `timestamp` is greater than the current time, it constructs an equivalent string (see the following string construction method). Then, it uses the MD5 algorithm to calculate the `HashValue` and compares it with the `md5hash` contained in the request . If they are consistent, the request passes the authentication and the file is returned. Otherwise, the request authentication fails and an HTTP 403 error is returned.

- `HashValue` is calculated according to the following method:

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

Example

1. Request an object through `req_auth` .

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

2. Set the access key to aliyuncdnexp1234 (set by the user).
3. The expiration date of the authentication configuration file is 2015-10-10 00:00:00, and the calculated number of seconds is 1,444,435,200.

4. The CDN server constructs a signature string used to calculate the HashValue.

```
/video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234"
```

5. The CDN server calculates the HashValue according to the signature string.

```
HashValue = md5sum("/video/standard/1K.html-1444435200-0-0-
aliyuncdnexp1234") = 80cd3862d699b7118eed99103f2a3a4f
```

6. The request URL is as follows.

```
http://cdn.example.com/video/standard/1K.html?auth_key=1444435200-0-
0-80cd3862d699b7118eed99103f2a3a4f
```

   The calculated HashValue is the same as the md5hash = 80cd3862d699b7118eed99103f2a3a4f value in the user request, so the request passes the authentication.

Concept

Format of users' encrypted URLs

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 field descriptions

- Note: `PrivateKey` field can be set by the CDN user.
- The validity period 1,800 s indicates that the authentication fails when the user fails to access the client source server 1,800 s after the preset access time. For example, if the preset access time is 2020-08-15 15:00:00, the actual link expiration time is 2020-08-15 15:30:00.

Field	Description
DomainName	The domain name of the CDN client site.
timestamp	The time designated for when the user accesses the client source server. This is part of the URL as well as a factor used to calculate

Field	Description
	the `md5hash`. The format is `YYYYMMDDHHMM` and the validity period is 1,800 s.
md5hash	The timestamp, FileName, and preset PrivateKey are used in the MD5 algorithm to get this string, namely md5(`PrivateKey` + `timestamp` + `FileName`)
FileName	The actual back-to-source access URL (Note: during authentication, the FileName begins with /).

Example

1. Back-to-source request object.

```
http://cdn.example.com/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
```

2. Set the access key to aliyuncdnexp1234 (set by the user).
3. The time format for when the user accesses the client source server is 201508150800 (the format is YYYYMMDDHHMM).
4. The CDN server constructs a signature string used to calculate the md5hash .

```
aliyuncdnexp1234201508150800/4/44/44c0909bcfc20a01afaf256ca99a8b8b.
mp3
```

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

```
md5hash = md5sum("aliyuncdnexp1234201508150800/4/44/44c0909bcf
c20a01afaf256ca99a8b8b.mp3") = 9044548ef1527deadafa49a890a377f0
```

6. The request URL is as follows.

```
http://cdn.example.com/201508150800/9044548ef1527deadafa49a890a377f0
/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
```

The calculated md5hash is the same as the md5hash = 9044548ef1527deadafa49a890a377f0 value in the user request, so the request passes the authentication.

Concept

Format of users' encrypted URLs

Format 1

```
http://DomainName/{/}/FileName
```

Format 2

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

- Content in brackets indicates the encryption information added to the standard URL.
- `<md5hash>` is the authentication information string after MD5 encryption.
- `<timestamp>` is a non-encrypted string expressed in plaintext. It is a hexadecimal value with a fixed length of 10, indicating the time in seconds from January 1,1970.
- Format 1 is used to encrypt the URL. For example,

  ```
  http://cdn.example.com/a37fa50a5fb8f71214b1e7c95ec7a1bd/55CE8100/
  test.flv
  ```

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

Authentication field descriptions

- `<md5hash>` field descriptions:

Field	Description
PrivateKey	An interference string. Different users use different interference strings.
FileName	The back-to-source access URL (Note: during authentication, the path begins with /).
time	The time when the user accesses the source server. It is UNIX time expressed as a hexadecimal value.

- PrivateKey is set to `aliyuncdnexp1234`
- PrivateKey is set to aliyuncdnexp1234. FileName is set to `/test.flv`
- time is set to`55CE8100`
- So the md5hash value is as follows .

  ```
  md5hash = md5sum(aliyuncdnexp1234/test.flv55CE8100) = a37fa50a5f
  b8f71214b1e7c95ec7a1bd
  ```

- Plaintext: `timestamp = 55CE8100`

  The URL is generated as so :

Format 1:

```
http://cdn.example.com/a37fa50a5fb8f71214b1e7c95ec7a1bd/55CE8100/
test.flv
```

Format 2:

```
http://cdn.example.com/test.flv?KEY1=a37fa50a5fb8f71214b1e7c95ec7a1
bd&KEY2=55CE8100
```

Example

When the user uses an encrypted URL to access a CDN node, the CDN server extracts encrypted string 1 and obtains the `<FileName> of the original URL`

After this process, the CDN server authenticates the URL.

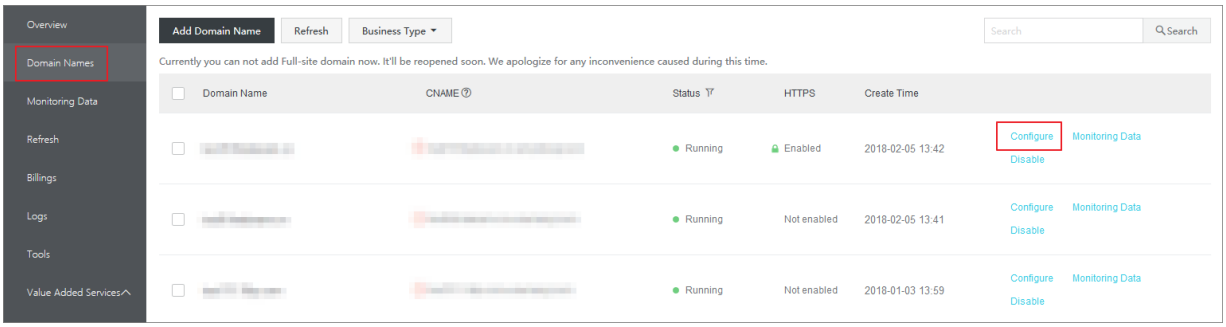
1. The CDN server uses the `<FileName>` of the original URL and the request time and PrivateKey to perform MD5 encryption and obtain encrypted string 2.
2. The CDN server compares encrypted string 2 with encrypted string 1. If the strings are not the same, the request is rejected.
3. The current time on the CDN server is used 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 1,800 s means that the authentication fails when the user fails to access the client source server 1,800 s after the preset access time. For example, if the preset access time is 2020-08-15 15:00:00, the actual link expiration time is 2020-08-15 15:30:00.
5. The request is valid if the time difference is less than the preset time limit. The CDN server will send a normal response. Any aberration from this means the request is rejected and an HTTP 403 error is returned.

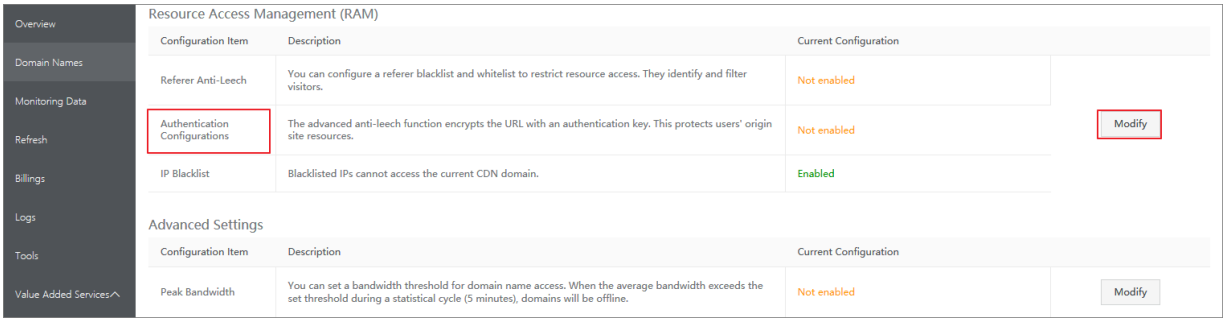
Sample authentication code

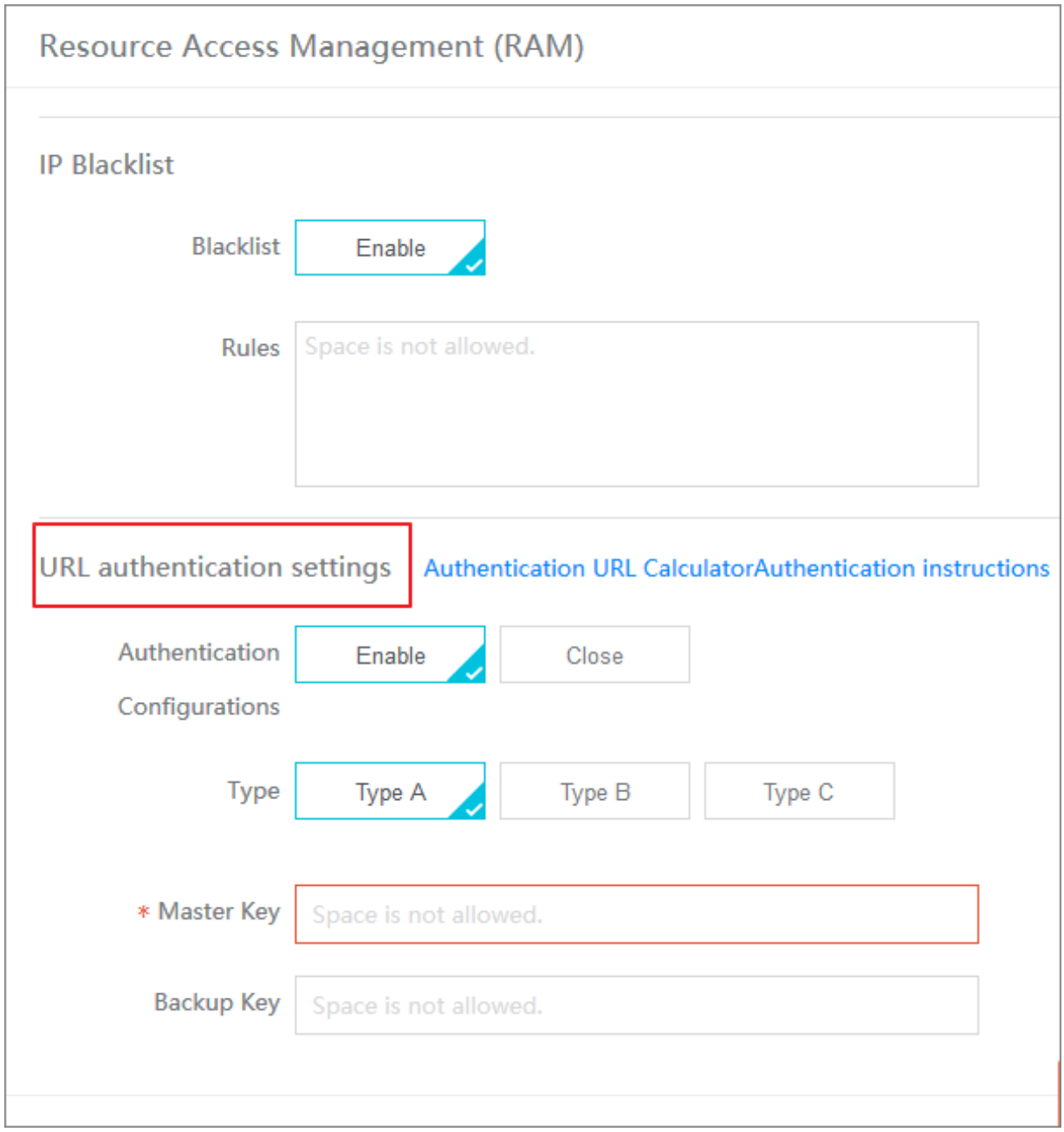
See *Sample Authentication Code* document in CDN Utilities.

Procedure

Go to the **Domain Names** page, select the desired domain name, and click **Configure**.


Overview
Domain Names
Monitoring Data
Refresh
Billings
Logs
Tools
Value Added Services
Add Domain Name
Refresh
Business Type
Search
Search
Currently you can not add Full-site domain now. It'll be reopened soon. We apologize for any inconvenience caused during this time.
Domain Name
CNAME
Status
HTTPS
Create Time
Running
Enabled
2018-02-05 13:42
Configure
Monitoring Data
Disable
Running
Not enabled
2018-02-05 13:41
Configure
Monitoring Data
Disable
Running
Not enabled
2018-01-03 13:59
Configure
Monitoring Data
Disable


Overview
Domain Names
Monitoring Data
Refresh
Billings
Logs
Tools
Value Added Services
Resource Access Management (RAM)
Configuration Item
Description
Current Configuration
Referer Anti-Leech
You can configure a referer blacklist and whitelist to restrict resource access. They identify and filter visitors.
Not enabled
Authentication Configurations
The advanced anti-leech function encrypts the URL with an authentication key. This protects users' origin site resources.
Not enabled
Modify
IP Blacklist
Blacklisted IPs cannot access the current CDN domain.
Enabled
Advanced Settings
Configuration Item
Description
Current Configuration
Peak Bandwidth
You can set a bandwidth threshold for domain name access. When the average bandwidth exceeds the set threshold during a statistical cycle (5 minutes), domains will be offline.
Not enabled
Modify


Resource Access Management (RAM)
IP Blacklist
Blacklist
Enable
Rules
Space is not allowed.
URL authentication settings
Authentication URL CalculatorAuthentication instructions
Authentication Configurations
Enable
Close
Type
Type A
Type B
Type C
* Master Key
Space is not allowed.
Backup Key
Space is not allowed.

16.3 鉴权配置

17 Business type

17.1 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*.

17.2 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*.

17.3 Type 3: On-Demand Video/Audio Acceleration

Use cases

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 settings*: 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.
     - *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.
- *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*.

17.4 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.

Procedure

1. See

   Please refer *Quick Start.*. Make sure you select**Acceleration of live streaming media**for the business type.

   Note:
   This business type does not support the custom live streaming server. The origin site address **live-origin.alivecdn.com** of the Alibaba Cloud CDN live broadcast center is used.

2. Stream push instructions

   Stream push address

   ```
   rtmp://video-center.alivecdn.com/app-name/video-name? vhost=test.
   example.com
   ```

   Operation on the console: Select the CDN domain for live broadcast in**Domain Name Management** to go to the configuration page:

Note:

- By default, the number of pushed streams is limited to 20.
- video-center.alivecdn.com is the domain name of the live streaming server. At present, it does not support customization.
- app-name indicates the application name. Customization is supported. The application name may include letters, numbers, and underscores. Special characters are not allowed. Modification is supported. The length must not exceed 255 characters.
- video-name indicates the stream name. Customization is supported. The stream name may include letters, numbers, and underscores. Special characters are not allowed. Modification is supported. The length cannot exceed 255 characters.
- vhost indicates the final domain name for broadcast on the edge node, that is, your CDN domain (For example: test.example.com).

3. Stream playback instructions

Based on the pushed streams, three reading modes are supported on edge nodes:

Mode	URL
RTMP	`rtmp://test.example.com/app-name/video-name`
FLV	`http://test.example.com/app-name/video-name.flv`
M3U8	`http://test.example.com/app-name/video-name.m3u8`

The following figure shows the location of a stream push address on the console.

4. Domain name 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 “live streaming media”.

- *Authentication settings*: 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.

> **Note:**
>
> - Currently, the same authentication scheme is adopted for stream push and stream playback.
> - The CDN domain performs stream push and playback only after authentication configuration is completed. Currently, the live broadcast business type supports the A-type authentication method only.
> - The streaming and playback addresses must receive authentication signature calculations respectively. Every signature is calculated based on the URL strictly, so you cannot apply the signature calculated from the streaming URL to the playback address. Similarly, different stream playback addresses correspond to different authentication calculation results.
> - During signature calculation, no parameter is included in the URL. For example, during calculation of authentication signature for stream push is not included? `vhost=test.yourcompany.com`

Example:

Step	Content
Resource URL	`rtmp://video-center.alivecdn.com/app-name/video-name`
Authorization settings	Authentication method: Method A Authentication key: test123 valid time: 3, 600s
Stream push address	`rtmp://video-center.alivecdn.com/app-name/video-name? auth_key=1449030595-0-0-dee5f3819d7b62a9830ee2913caf111c&vhost=test.example.com`
Stream playback address (take the FLV format as an example)	`http://test.example.com/app-name/video-name.flv?auth_key=1449030834-0-0-5e1c604710241001fd7a367bc96a17b7`

- Notify_url settings, flow status real-time feedback, send a GET request to the user server through the HTTP interface, real-time feedback to the user on the status of successful streaming and successful streaming of video, the user server returns the result by 200 response to the interface returned by default. 1 indicates a success in receiving; 0 indicates a failure in receiving.

17.5 Type 5: Station-wide Acceleration

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 concurrenc y, 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.

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:
The station-wide acceleration is the default pure dynamic acceleration, which means that 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.

Operation Steps

1. Add a CDN domain name.

   Please refer to *Quick Start*, be aware to select a business type of: All Station acceleration.
2. Domain Name configuration.

After the domain name is added, the whole site is accelerated using pure dynamic acceleration by default, you need to specify a static file by configuring the dynamic static acceleration rule , and the specified static file uses static acceleration, the cache is on the CDN node for better acceleration. The specific configuration methods are as follows:

- Dynamic static acceleration rule settings:
  - *Static file type*
  - *Static URI settings*
  - *Static path settings*
  - *Special header settings*
  - *Dynamic Protocol follows back Source*
- Recommended Configuration:
  - HTTPS Security acceleration, just upload the accelerated Domain Name Certificate/ private key after you turn on secure acceleration mode, and supports viewing, disabling, enabling, editing of certificates to understand Certificate Format description.
  - Access control related settings to ensure the distribution of content security, prevent chain theft or malicious requests from causing unnecessary loss of traffic.
    - *Refer security chain*
    - *IP blacklist*
  - Performance Optimization related settings, smart compression distribution, ignore URL parameters to increase cache hit ratio.
    - *Page Optimization*
    - *Intelligent Compression*
    - *Filter parameters*
  - For more features, browse the CDN features list.

Billing rules

- The CDN all-station accelerated billing item is the base cost + the requested number of charges. The base cost is the base cost based on the Peak bandwidth selected by the CDN service or the flow meter fee. The cost of the number of requests includes the number of dynamic HTTP requests, the number of dynamic HTTPS requests, and the number of static HTTPS requests, respectively according to the unit price on a daily basis.

- For more details, please see the all-station accelerated billing rule.

17.6 类型6：移动加速

17.6.1 概述

前言

移动加速(Mobile Accelerator)是阿里云针对移动应用推出的动静态全网加速产品，旨在依托阿里云遍布全国的CDN节点，海量带宽网络等优越的基础设施资源，以及使用智能域名解析、无线协议优化、内容动态压缩、运营商级别优化等技术，为开发者提供更快、更稳定的网络接入能力，有效提升移动应用的可用性及用户体验。

功能特性

移动加速服务将主要通过以下几种技术手段来实现移动应用网络加速：

- 协议优化：采用深度优化定制的私有协议替换传统的HTTP协议，收获多路复用、请求头压缩、请求优先级支持等收益，防止内容劫持现象发生。同时我们也为云加速服务终端与加速节点间长连复用，最小化TCP的建连开销，提高连接利用率和请求响应速度；
- 链路优化：以阿里云遍布全国的优质边缘节点，海量的带宽资源为基础设施，结合HTTPDNS智能路由精准的调度，实现快速选路，就近接入；云加速节点会缓存热点内容，大大提高访问效率；云加速节点和ECS间搭建专线进行链路加速，如果您已经在使用阿里云ECS作为服务后端，加速结果更是锦上添花。
- 全站加速：支持HTTP/HTTPS的动态和静态请求的全站加速。

下载并安装SDK

移动加速通用版SDK提供 iOS和Android两个版本，支持动态加速域名列表管理，首次安装后即可对所有移动加速域名进行全网提速，可在CDN控制台管理移动加速域名的状态和配置，查看SDK开发指南。

- *iOS SDK*开发指南
- *Android SDK*开发指南
- 控制台使用说明

17.6.2 移动加速开通说明

开通服务

1. 申请移动加速资格。

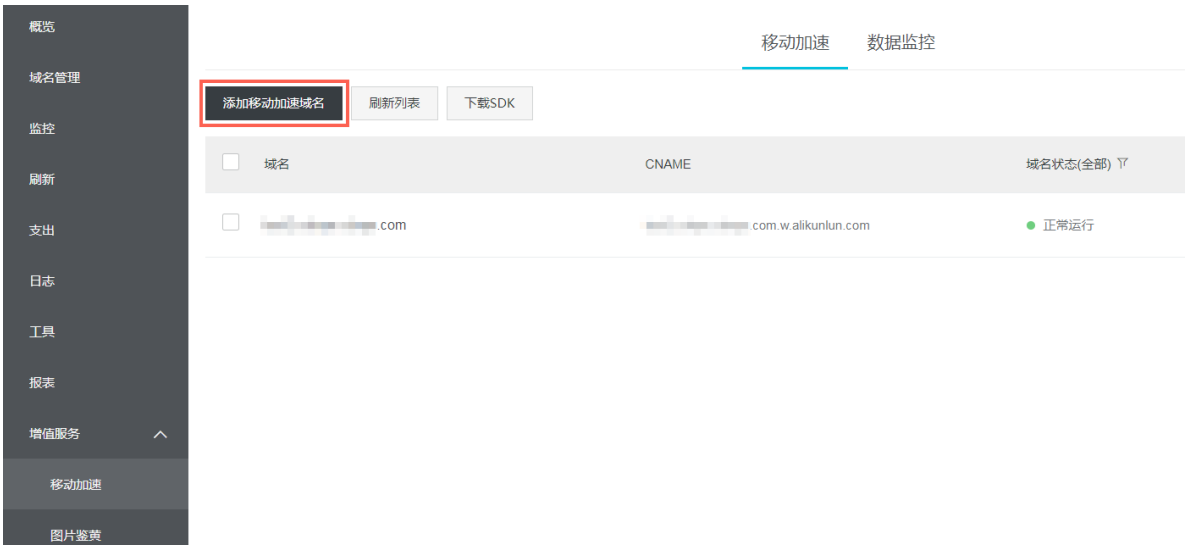
   目前CDN移动加速已全面公测，可在移动加速产品介绍页申请使用资格：

2. 开通后，进入移动加速控制台。

   在CDN控制台左侧导航栏的增值服务里可进入移动加速的控制台：

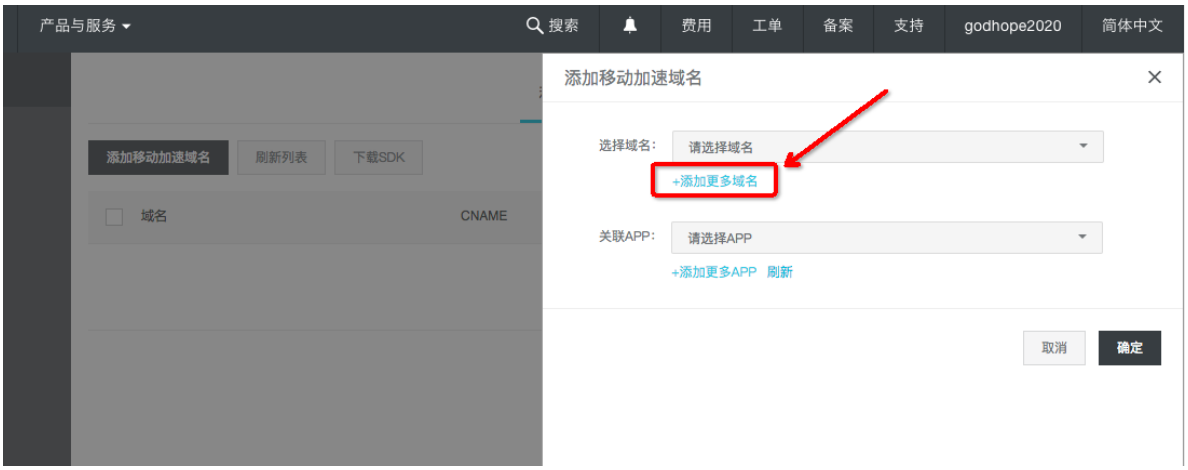
添加加速域名

1. 单击添加移动加速域名:



2. 在添加域名菜单里面，选择要加速的域名：

3. 如果没有域名可选择，先添加域名：



移动端SDK集成

SDK集成参考文档：*Android SDK开发指南*和 *iOS SDK开发指南*。

17.6.3 配置样例

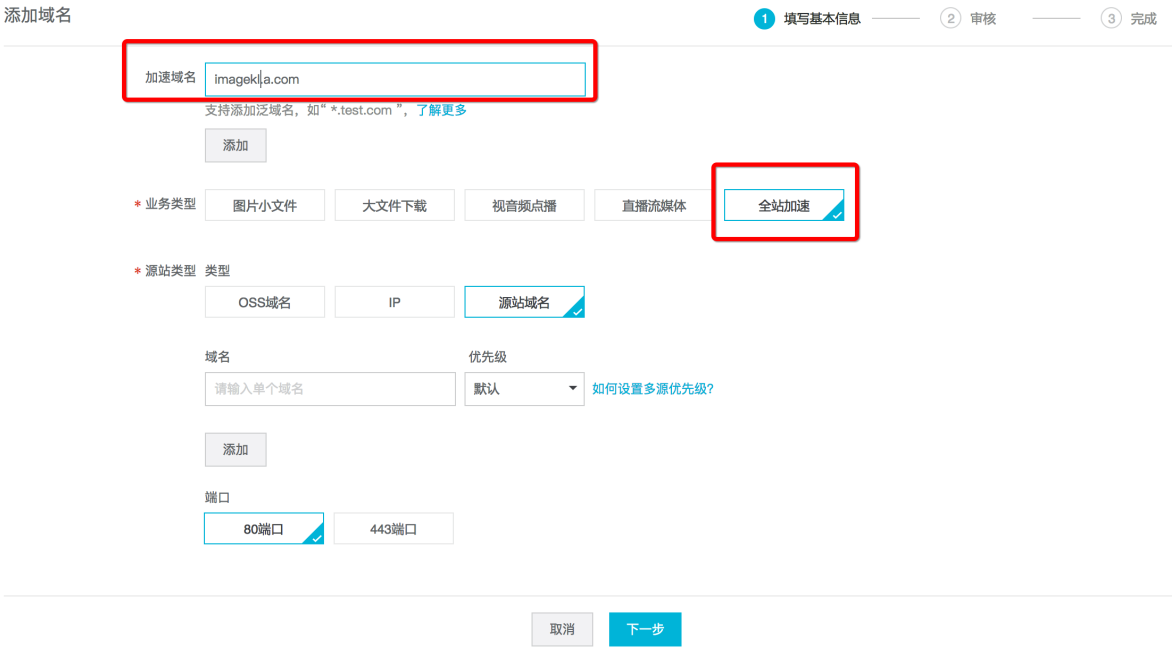
配置目标

- 配置加速域名，用于接入CDN移动加速系统；
- 保证流量逐步接入移动加速。

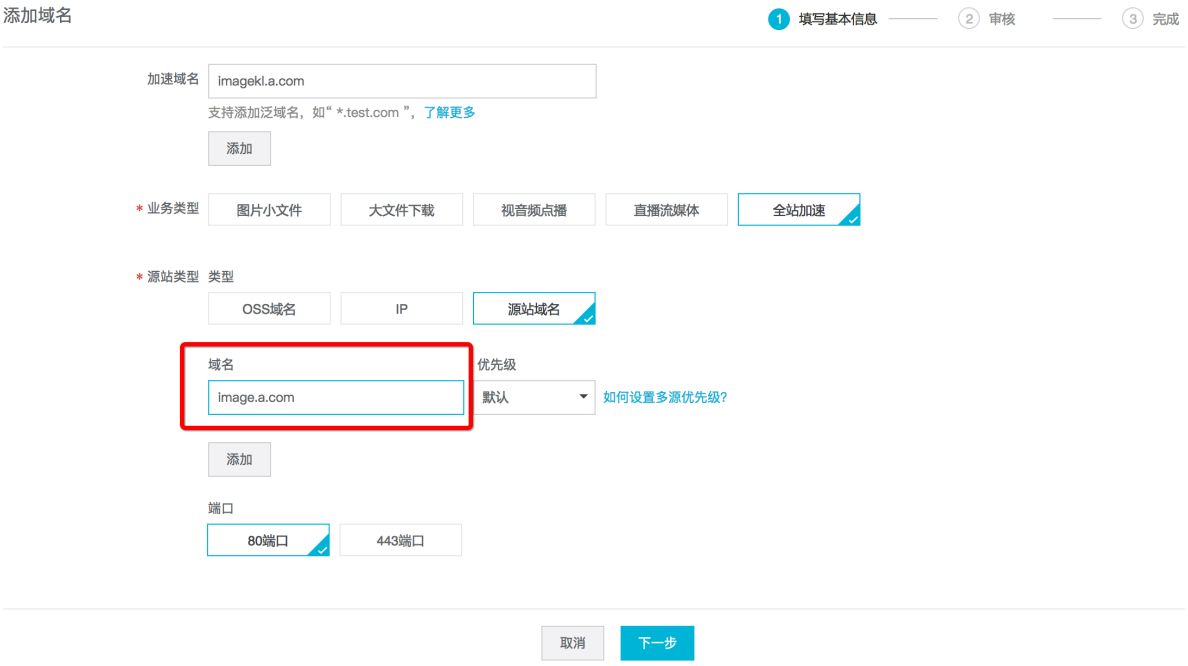
配置方案

假设待加速域名为`image.a.com`。

1. 新申请一个CDN移动加速域名（ 假设是`imagekl.a.com` ），配置到*CDN控制台*，业务类型选择全站加速。



2. 配置源站类型为源站域名，回源域名是`image.a.com`。



3. 上述配置完成后，CDN会为加速域名分配一个CNAME域名，如`imagekl.a.com.w.kunlunpi.com`（请以CDN实际分配的CNAME域名为准），修改`imagekl.a.com`的DNS权威服务器配置，将CDN分配的`imagekl.a.com.w.kunlunpi.com`添加成`imagekl.a.com`域名的CNAME记录。
4. 配置动静态加速规则。

   添加域名后，单击**配置**，进入加速域名配置界面，如下图所示：

移动加速相关的配置项为：**动静态加速规则**，配置规则如下：

- **静态文件类型**
  - 请求URL后缀名匹配时，为静态加速请求。
  - 例：配置为`.jpg,.txt,.html`，请求 /1.png、/1/2/3.txt、、/a.html均为静态加速请求。
- **静态URI设置**
  - 请求URL和配置内容完全匹配时，为静态加速请求。
  - 例：/1/2/3.jpg，请求 /1/2/3.jpg为静态加速请求，其余为动态加速请求。
- **静态路径设置**
  - 请求URL和配置内容正则匹配（仅支持`*`正则匹配，`*`匹配0个或多个任意字符）时，为静态加速请求。
  - 例：/*.py，请求 /a/b/c.py为静态加速请求，/a/b/c.py/d为动态加速请求。

验证方法

上述四个配置步骤完成后，等待2.4 DNS权威服务器解析结果生效后，可以通过以下两步验证CDN移动加速配置是否已经生效。

- `ping imagekl.a.com` 确认该域名已经解析到阿里CDN；
- 访问测试对象确认能正确返回。

至此，CDN控制台的相关配置工作已经完成，可以进入后续的SDK集成调试阶段。

备注

配置过程中注意事项参见概述。

17.6.4 iOS SDK开发指南

本文档介绍了MAC iOS SDK的使用方式。

说明：

集成前可参考移动加速 *iOS Demo*。

SDK集成

- 指定Master仓库和阿里云仓库：

```
source 'https://github.com/CocoaPods/Specs.git'
source 'https://github.com/aliyun/aliyun-specs.git'
```

- 添加依赖：

```
pod 'AlicloudMAC', '~> 1.0.0'
```

SDK使用

说明：

移动加速SDK内部Log查看Tips：可通过过滤字段[MAC查看。

1. 获取加速示例并初始化。

   `AppKey`和`AppSecret`可在 *App*列表页 获取。

```
AlicloudMACService *service = [AlicloudMACService sharedInstance];
[service initWithAppKey:@"******" appSecret:@"******" callback:^(
BOOL res, NSError *error) {
    if (res) {
        NSLog(@"MAC SDK init success.");
    } else {
        NSLog(@"MAC SDK init failed, error: %@", error);
    }
}];
```

2. 加速请求配置。

   - 若原生网络请求基于 NSURLConnection 或者 NSURLSession（session对象通过`sharedSession:`获取）发出，SDK可自动拦截原生网络请求，走到加速链路。

- 若原生网络请求基于 NSURLSession（session对象配置有自定义NSURLSessionConfiguration），需注册移动加速的 MACURLProtocol，如下所示：

```
NSURLSessionConfiguration *configuration = [NSURLSessionConfigur
ation defaultSessionConfiguration];
configuration.protocolClasses = @[ [MACURLProtocol class] ];
NSURLSession *session = [NSURLSession sessionWithConfiguration:
configuration];
```

- 移动加速SDK是通过注册 NSURLProtocol 拦截网络请求，需要注意 NSURLProtocol 的注册顺序。多个 NSURLProtocol 注册后，网络请求拦截为注册的相反顺序。移动加速 MACURLProtocol 的注册时机为SDK初始化时，调用停止和重启接口时，分别为注销和重新注册 MACURLProtocol。
- 示例：

```
[[AlicloudMACService sharedInstance] initWithAppKey:testAppKey
appSecret:testAppSecret callback:^(BOOL res, NSError *error) {
    if (res) {
        /* HookURLProtocol注册在SDK初始化之后，因此HookURLProtocol先拦
截到网络请求 */
        [NSURLProtocol registerClass:[HookURLProtocol class]];
    }
}
```

3. 自定义降级策略
   - 用户可设置降级策略，满足降级条件的网络请求，降级走原生网络库链路。
   - 基于下述接口配置：

```
- (void)setDegradationPolicy:(id)delegate;
```

4. 停止和重启移动加速。
   - 调用步骤 1所示的初始化接口，并按照步骤 2完成配置后，原生网络请求可自动被拦截，走到加速链路。
   - 调用停止接口，停止网络请求拦截。

```
/**
 停止移动加速
 */
- (void)stop:(MACCallbackHandler)callback;
```

   - 调用重启接口，重新恢复网络请求拦截。

```
/**
 重启移动加速
 */
```

```
- (void)restart:(MACCallbackHandler)callback;
```

5. 如何查看网络请求是否加速成功？

   - 打开移动加速SDK Log。
   - SDK初始化成功后，发出网络请求，可看到如下日志：

     ```
     [MACURLProtocol]-[I]: URL: [https://xxx.xxx.com/xx], accelerate
     type: [2]
     [MACURLProtocol]-[D]: Start loading request: <NSMutableURLRequest
     : 0xxxxxxxxxxxx> { URL: https://xxx.xxx.com/xx }
     ```

   - 网络请求结束后，可查看到如下日志，

     - `request result`
       - 1：网络请求成功
       - 0：网络请求失败
     - `accelerate result`
       - 1：网络请求加速成功
       - 0：网络请求加速失败

     ```
     [MACACCSNetworkRequest]-[I]: [https://xxx.xxx.com/xx] request
     result: [1], accelerate result: [1]
     ```

API接口

```
/**
降级策略定义
*/
@protocol MACDegradationDelegate
- (BOOL)shouldDegrade:(NSString *)hostName;
@end
/**
SDK回调Handler定义
@param res 回调结果
*/
typedef void (^MACCallbackHandler)(CallbackResult *res);
/**
SDK初始化并开启移动加速
@param appKey AppKey
@param appSecret AppSecret
@param callback 回调
*/
- (void)initWithAppKey:(NSString *)appKey
appSecret:(NSString *)appSecret
callback:(MACCallbackHandler)callback;
/**
设置自定义降级策略
@param delegate 降级策略
```

```
*/
- (void)setDegradationPolicy:(id)delegate;
/**
停止移动加速
*/
- (void)stop:(MACCallbackHandler)callback;
/**
重启移动加速
*/
- (void)restart:(MACCallbackHandler)callback;
/**
日志开关
@param enabled YES: 打开; NO: 关闭(默认)
*/
- (void)setLogEnabled:(BOOL)enabled;
```

示例

```
/**
初始化MAC SDK
*/
- (void)initMACSDK {
AlicloudMACService *service = [AlicloudMACService sharedInstance];
[service setDegradationPolicy:(id)self];
[service initWithAppKey:@"******" appSecret:@"******" callback:^(BOOL
res, NSError *error) {
if (res) {
NSLog(@"MAC SDK init success.");
} else {
NSLog(@"MAC SDK init failed, error: %@", error);
}
}];
}
/**
自定义降级策略
@param url 请求URL
@return YES: 降级到原生网络库; NO: 不降级
*/
- (BOOL)shouldDegrade:(NSURL *)url {
/* 若请求Host为a.b.com,降级走原生网络库 */
if ([[url host] isEqualToString:@"a.b.com"]) {
return YES;
}
return NO;
}
static NSURLSession *_session;
/**
发网络请求
*/
- (void)sendNetworkReqeust {
static dispatch_once_t onceToken;
dispatch_once(&onceToken, ^{
/* 若基于NSURLSession发网络请求并配置SessionConfiguration,需要注册
MACURLProtocol */
if (!_session) {
NSURLSessionConfiguration *configuration = [NSURLSessionConfiguration
defaultSessionConfiguration];
configuration.protocolClasses = @[ [MACURLProtocol class] ];
```

```
_session = [NSURLSession sessionWithConfiguration:configuration];
}
});
NSURL *url = [NSURL URLWithString:@"xxxxxx"];
NSURLRequest *request = [NSURLRequest requestWithURL:url];
NSURLSessionDataTask *task = [_session dataTaskWithRequest:request
completionHandler:^(NSData * _Nullable data, NSURLResponse * _Nullable
 response, NSError * _Nullable error) {
if (error) {
NSLog(@"Error: %@", error);
return;
}
NSLog(@"Content: %@", [[NSString alloc] initWithData:data encoding:
NSUTF8StringEncoding]);
}];
[task resume];
}
```

17.6.5 Android SDK开发指南

前言

本文旨在介绍MAC Android SDK的接入步骤和使用方法。

安装

1. 配置maven仓库。

   `build.gradle`添加阿里云maven仓库。

   ```
   allprojects {
       repositories {
           maven {
               url "http://maven.aliyun.com/nexus/content/repositories/
   releases"
           }
       }
   }
   ```

2. 配置gradle依赖。

   ```
   dependencies {
       compile 'com.aliyun.ams:alicloud-android-mac:1.0.0'
   }
   ```

   目前MAC android sdk只支持arm架构，建议用真机进行测试。

3. Manifest配置。

   a. 添加组件。

   ```
   <service
               android:name="anetwork.channel.aidl.NetworkService"
               android:exported="false">
               <intent-filter>
   ```

```
                <action android:name="anetwork.channel.aidl.
IRemoteNetworkGetter" />
            </intent-filter>
        </service>
```

b. 添加权限。

```
<uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.ACCESS_NET
WORK_STATE" />
    <uses-permission android:name="android.permission.ACCESS_WIF
I_STATE" />
```

4. Proguard配置。

```
-keep class com.aliyun.ams.** {*;}
-keep public class org.android.spdy.** {*;}
-dontwarn com.alibaba.**
-dontwarn com.taobao.**
-dontwarn anetwork.channel.**
-dontwarn org.android.**
```

支持的版本

mac sdk支持的android最小版本为`10`。

```
minSdkVersion 10
```

API

- **`MacClient`**

  `MacClient`主要用来发起请求`Request`和得到响应`Response`，使用方法参见最佳实践：

```
public final class MacClient {
    // 用于MAC sdk的初始化
    public static void init(MacConfig config);
    // 根据输入的Request获得一个Call对象
    public Call newCall(Request request);
    // MacClient的Builder
    public static final class Builder {
        public MacClient build();
    }
}
```

- **`MacConfig`**

  MAC sdk在初始化时需要传入全局配置**`MacConfig`**，使用方法请参考最佳实践-初始化：

```
public final class MacConfig {
     // MacConfig的Builder
    public static final class Builder {
         // 设置Context
         public Builder context(Context context);
         // 设置appKey
```

```
        public Builder appKey(String appKey);
        // 设置appSecret
        public Builder appSecret(String appSecret);
        // 创建MacConfig对象
        public MacConfig build();
    }
}
```

- **Request**

  Request表示一个HTTP请求，每一个**Request**包含一个URL、method、请求header和body，使用方法请参考最佳实践-构建请求对象：

```
public final class Request {
     // 返回URL
    public String url();
    // 返回method，默认为Get
    public String method();
    // 返回请求头部
    public Map<String, String> headers();
    // 返回请求body
    public byte[] body();
    // Request的Builder
    public static final class Builder {
        // 设置URL
        public Builder url(String url);
        // 设置method
        public Builder method(String method, byte[] body);
        // 设置header
        public Builder headers(Map<String, String> headers);
        // 添加header
        public Builder addHeader(String name, String value);
        // 移除header
        public Builder removeHeader(String name);
        // 构建Request对象
        public Request build();
    }
}
```

- **Response**

  Response表示一个**Request**的响应，每一个**Response**包含状态码、响应头部以及响应body：

```
public final class Response {
     // 返回状态码
    public int code();
    // 返回响应头部
    public Map<String, String> headers();
    // 返回响应body
    public byte[] body();
    // 返回请求是否成功
    public boolean isSuccessful();
}
```

- **Callback**

MAC sdk允许用户使用异步**Callback**的方式，正常时返回Response，异常时返回MacException，使用方法请参考最佳实践-异步请求过程：

```
public interface Callback {
     // 正常时返回Response
    void onResponse(Call call, Response response);
    // 异常时返回MacException
    void onFailure(Call call, MacException exception);
}
```

最佳实践

1. 初始化。

   a. 调用MacConfig.init方法，设置AppKey，AppSecret，Context，建议在Application.onCreate时调用：

   ```
   public class DemoApplication extends Application {
       @Override
       protected void attachBaseContext(Context base) {
           super.attachBaseContext(base);
       }
       @Override
       public void onCreate() {
           super.onCreate();
           // 初始化MacConfig
           MacConfig config = new MacConfig.Builder()
                   .context(this)
                   .appKey(APP_KEY)
                   .appSecret(APP_SECRET)
                   .build();
           MacClient.init(config);
       }
   }
   ```

   其中，AppKey和AppSecret可在 *App列表页* 获取。

   b. 构造MacClient对象，通过该对象来进行网络操作：

   ```
   // 构造MacClient对象
   MacClient client = new MacClient.Builder().build();
   ```

2. 构建请求对象。

   请求对象Request可以设置url，header，method等，其中method默认为Get方法：

   ```
   Request req = new Request.Builder()
                               .url(url)
                               .headers(headers)
                               .addHeader("User-Agent", "Your UA")
                               .method("POST", body)
   ```

```
                                .build();
```

3. 同步请求过程。

   下面为移动加速的同步请求示例，使用时请确保同步请求方法在后台线程中执行:

```
new Thread(new Runnable() {
    @Override
    public void run() {
        Response rsp = null;
        try {
            rsp = client.newCall(req).execute();
        } catch (MacException e) {
            e.printStackTrace();
        }
        if (rsp != null) {
            int statusCode = rsp.code();
            byte[] data = rsp.body();
            Log.d(TAG, "[DemoActivity] execute statusCode: " +
statusCode + " data: " + new String(data));
        }
    }
}).start();
```

4. 异步请求过程。

   下面为移动加速的异步请求示例，使用时请确保异步请求方法在后台线程中执行:

```
new Thread(new Runnable() {
    @Override
    public void run() {
        client.newCall(req).enqueue(new Callback() {
            @Override
            public void onResponse(Call call, Response response) {
                int statusCode = response.code();
                byte[] data = response.body();
                Log.d(TAG, "[DemoActivity] onResponse statusCode: "
 + statusCode + " data: " + new String(data));
            }
            @Override
            public void onFailure(Call call, MacException e) {
                Log.d(TAG, e.getMessage(), e);
            }
        });
    }
}).start();
```

   如何判断加速是否成功

   - 过滤和查看tag为`mac`的日志，例如控制台通过adb logcat -s mac来过滤。
   - 请求成功后可以看到类似日志：

     ```
     [DHandler] url: https://xxx/xxx.html AccSuccess: 1 reqSuccess: 1
     ```

   其中，AccSuccess为1表示加速成功，reqSuccess为1表示请求成功

17.6.6 常见问题

同时集成多个阿里SDK，如移动加速，支付宝，移动推送等，遇到UTDID冲突如何解决？

*UTDID*冲突解决方案

18 Domain Names

18.1 HTTPS Acceleration

18.1.1 HTTPS Security Acceleration

Features

- HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) is an HTTP channel designed to ensure security, namely, the secure edition of HTTP. It encapsulates HTTP with the SSL/TLS protocol, so the foundation of HTTPS security is SSL/TLS.
- Advantages of HTTPS acceleration:
  - Key user information is encrypted during transmission, preventing leakage of sensitive information, such as session IDs or cookies, or other potential safety hazards;
  - Integrity verification is performed on all data during transmission, protecting the DNS or content from being hijacked, tampered with, or suffering from other "man in the middle" (MITM) attacks. For more information, see *Using HTTPS to Prevent Traffic Hijacking*.
- Alibaba Cloud CDN provides HTTPS secure acceleration. You only need to enable the secure acceleration mode and then upload the certificate and private key for the CDN domains. The service also supports viewing, disabling, enabling, and editing certificates. An uploaded user-defined only supports certificate in PEM format. For more information, see *Certificate format description and conversion method*.
- You can go to *Alibaba Cloud SSL Certificates Service* to apply for free certificate or buy advanced certificate.
- If your certificate is configured correctly and enabled, both HTTP access and HTTPS access are supported. If the certificate does not match with the private key or is disabled, only HTTP access is supported.

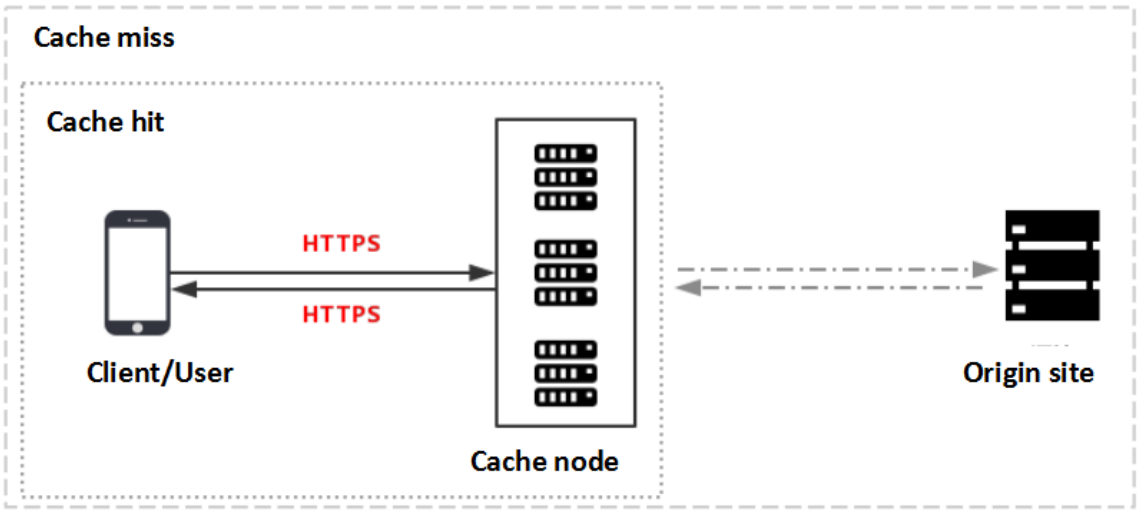
Note:

SNI back-to-origin is not supported.

Function Diagram

HTTPS enabled in the Alibaba Cloud CDN console can achieve HTTPS encryption requested between the user and the Alibaba Cloud CDN node. And the CDN node's request which returns

to the origin site to obtain the resource is still performed as configured in your origin site. We recommend that you configure and enable HTTPS in your origin site to realize full link HTTPS encryption:



Attentions:

Configuration

- **HTTPS Secure Acceleration** is supported for the following business scenarios:
  - Acceleration of images and small files
  - Acceleration of large file downloads
  - Acceleration of on-demand video/audio
  - Acceleration of live streaming media
  - Mobile acceleration is not supported.
- HTTPS security for wildcard domain names is supported.
- The options to :**Disable** and **Enable** are supported:
  - Enable: Certificate modification is supported, both HTTP and HTTPS requests are supported by default, and **force redirect** is supported.
  - Disable: No HTTPS requests are supported and no certificate/private key information will be retained. You must re-upload the certificate/private key to enable the certificate again.
- You are allowed to view the certificate, but the certificate only. The private key information cannot be viewed because it is sensitive information. Make sure you keep the certificate information safe.

- Modifications and edits can be made to the certificate. It takes up to 10 minutes for any modifications and edits to take effect, so proceed with caution.

Billing

HTTPS Secure Acceleration is a value-added offering. Once it is enabled, you are billed based on the number of HTTPS requests. For more information, see *HTTPS price details*.

> **Note:**
> The HTTPS cost is billed separately based on the number of requests, and is not included in the CDN traffic package. Ensure that you have adequate account balance before enabling HTTPS service, so as to avoid any arrears that may affect your CDN service.

Certificate

- You must upload a certificate for the CDN domains with the **HTTPS secured acceleration** enabled, including the certificate and the private key, both in the PEM format.

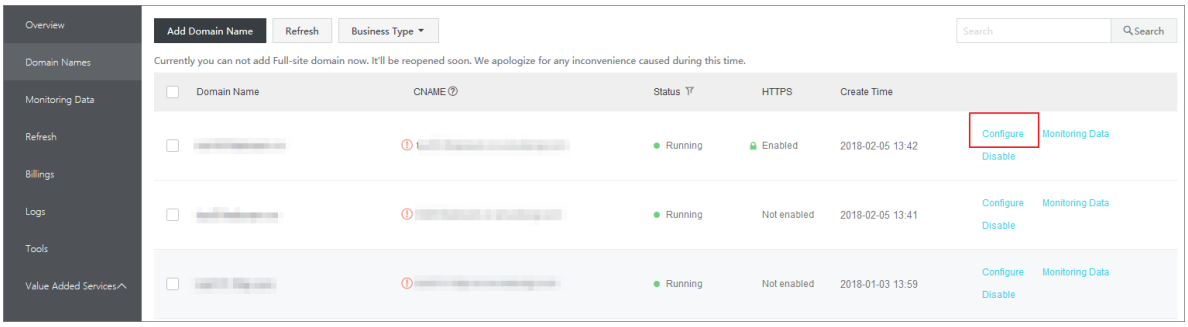
  > **Note:**
  > CDN adopts the Tengine service which is based on Nginx. Therefore, only certificates that are readable by Nginx are supported, namely, PEM certificates. For more information, see *Certificate format and conversion method*.

- Only SSL/TLS handshake with SNI information is supported.
- The certificate and private key that you upload must match each other. Otherwise, the verificati on fails.
- It takes 10 minutes for any certificate updates to take effect.
- Private key with a password is not supported.

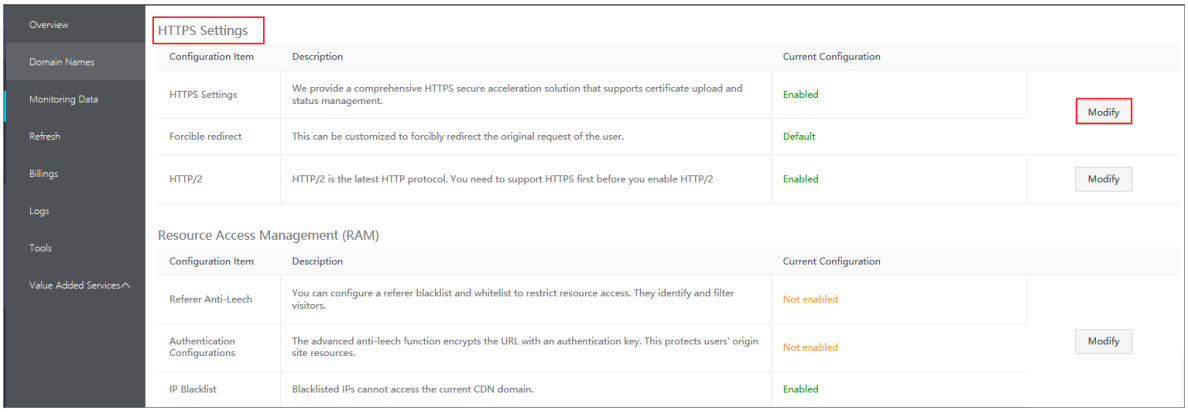
Configuration guide

1. Purchase a certificate To enable HTTPS Secure Acceleration, you must have a certificate associated with the CND domains. *You can purchase a certificate with Alibaba Cloud Certificat es Service*.
2. configure CDN domain name

   Log on to the *CDN console*, go to the Domain Names and select the desired domain name to go to the configuration page, HTTPS Settings, Modify Configuration



Click **Modify Configuration**to perform the settings.



1. Click if **HTTPS Setting** is enabled. Click **Modify Configuration** to enter the setting page and click **Enable**.

   Note:
   HTTPS Secure Acceleration is a value-added offering. Once it is enabled, you are billed based on the number of HTTPS requests. For more information, see *Billing details*.

2. Select certificate:

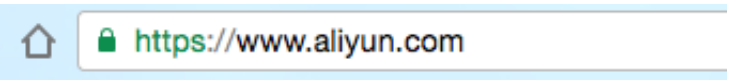
   - You can *quickly apply for free certificate or buy advanced certificate in Alibaba Cloud SSL certificate service*. For a certificate purchased with Alibaba Cloud Certificates Service, you can select to associate the CND domain by using the certificate name directly.
   - You can use custom upload if no associated certificate is available in the certificate list. In this case, you must set the certificate name, and then upload the certificate information and the private key. This certificate is saved in Alibaba Cloud Certificates Service and can be viewed in the **My Certificates** section.

3. Only the PEM certificate format is supported. For more information, see *About Certificate Formats*.

4. **Force redirect** is supported: You can enable this function to force redirect users' original request method.
   - For example, when **Force HTTPS Redirect** is enabled and you initiate an HTTP request, the server returns a 302 redirect response and the original HTTP request is forcibly redirected to an HTTPS request.
   - Default: supports both HTTP and HTTPS requests.
   - Force HTTPS redirect: User requests are forcibly redirected to HTTPS requests.
   - Force HTTP Redirect: User's requests are forcibly redirected to HTTP requests.

3. Verify whether the certificate is effective.

   After the certificate is set up and becomes effective (about one hour after the HTTPS certificate is set up), visit resources by means of HTTPS. If the green HTTPS mark appears in the browser, it indicates that a private connection is established with the website and HTTPS Secure Acceleration has taken effect.



18.1.2 Certificate Format

Before *Enabling the HTTPS* service, you must configure certificates. You can directly select *https://yundun.console.aliyun.com* managed or purchased certificates in Alibaba Cloud Security, 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//C3hWn0uIVGdg76626gg0oJSaj48R2n0MnVcC
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 CERTIFICATE-----` and `-----END CERTIFICATE-----` content together.
- Each line has 64 characters, but the last line can have less then 64 characters.

Certificate links issued by intermediate CAs:

`-----BEGIN CERTIFICATE-----`

```
-----END CERTIFICATE-----

-----BEGIN Certificate -----

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
```

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_certs -in incertificat.p7b -out outcertificate.
cer
```

In outcertificat.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 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.

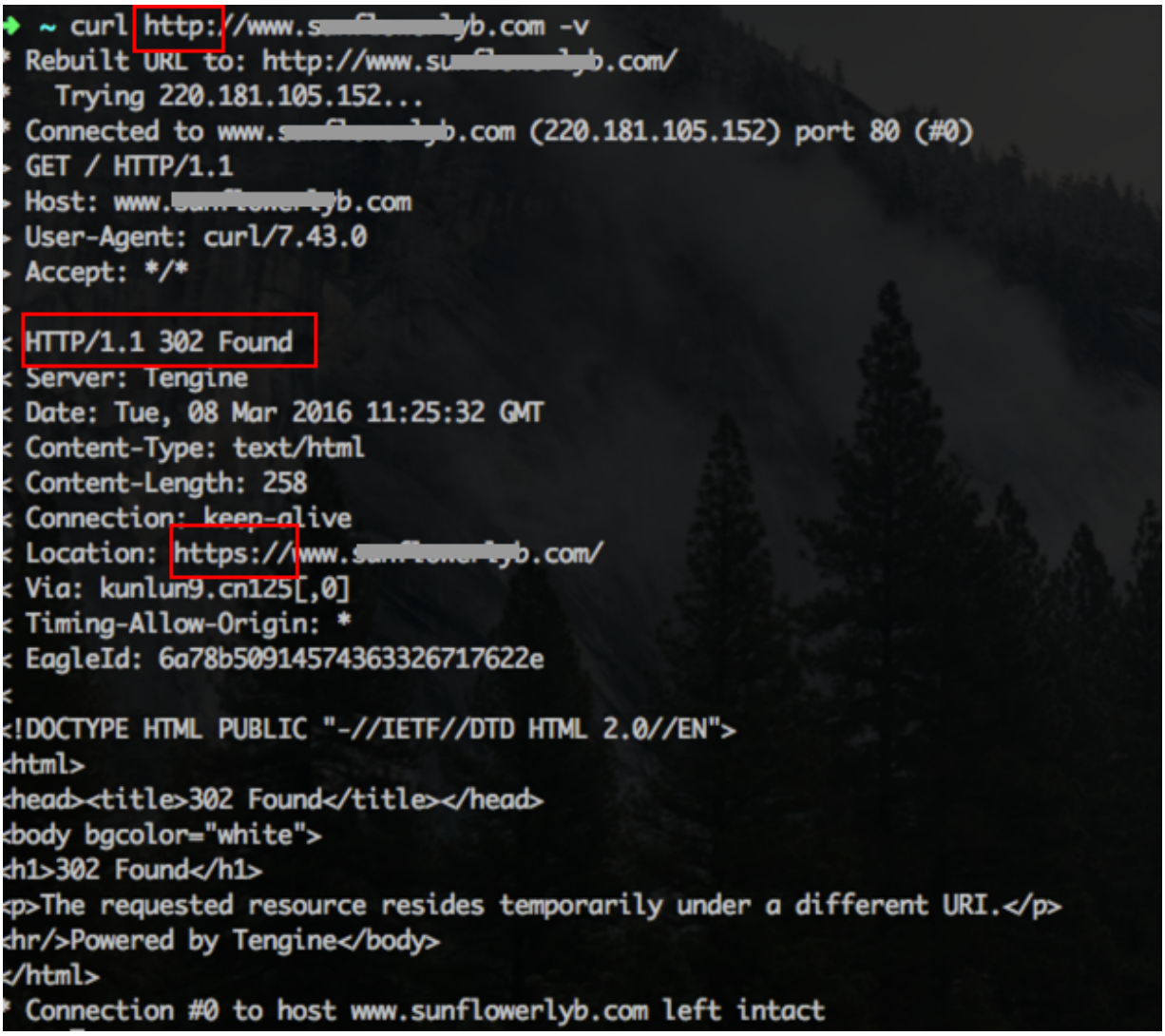
For more certificate-related FAQs, see *More certificate questions*.

18.1.3 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 Names**page, select the domain name, then click **Manage**.
2. Enable the function in **HTTPS Configuration** > .

18.1.4 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

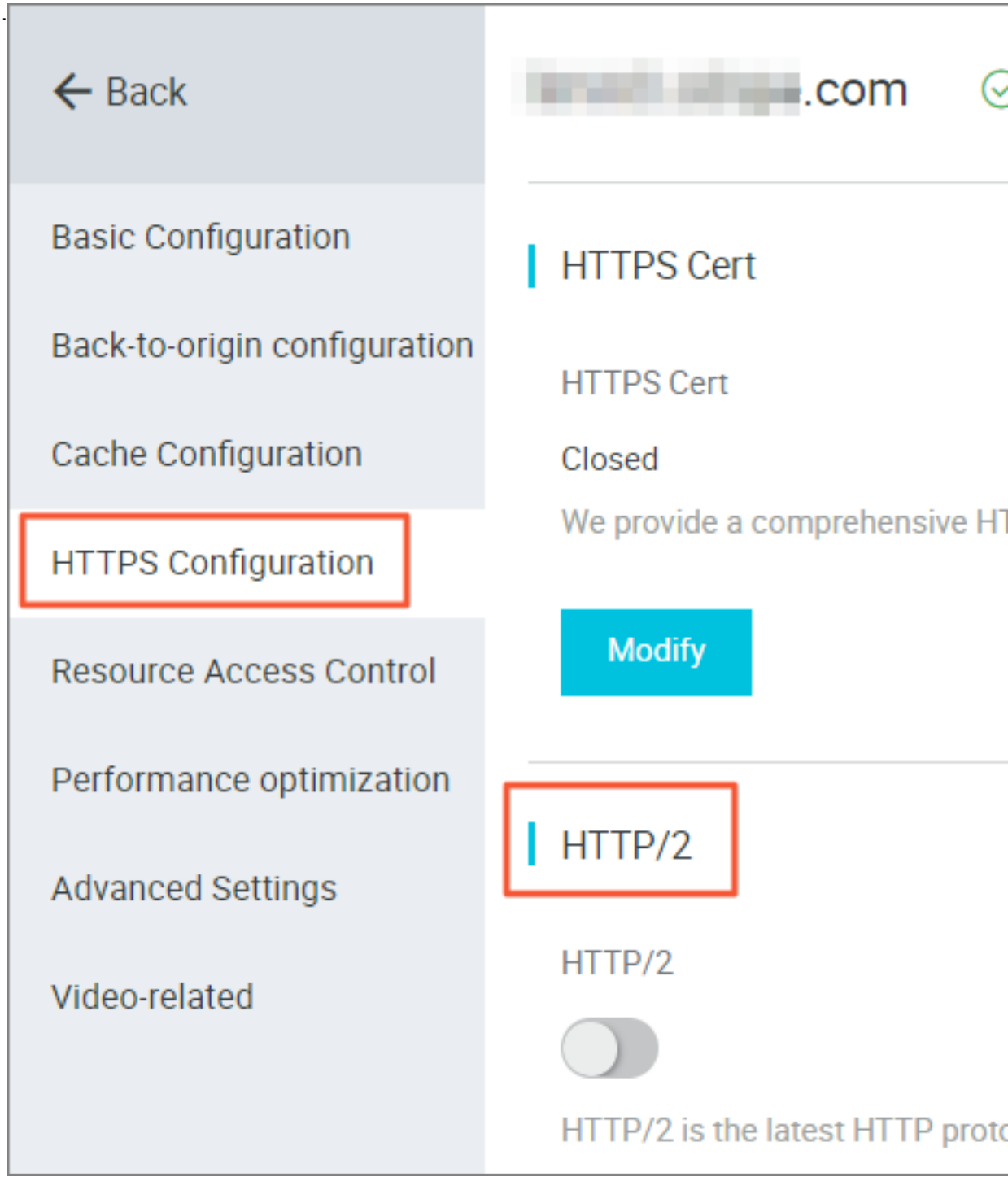
1. Log on to the *CDN console*.
2. On the **Domain Names** page, select a domain name and click **Configure**.

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**.



18.2 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.

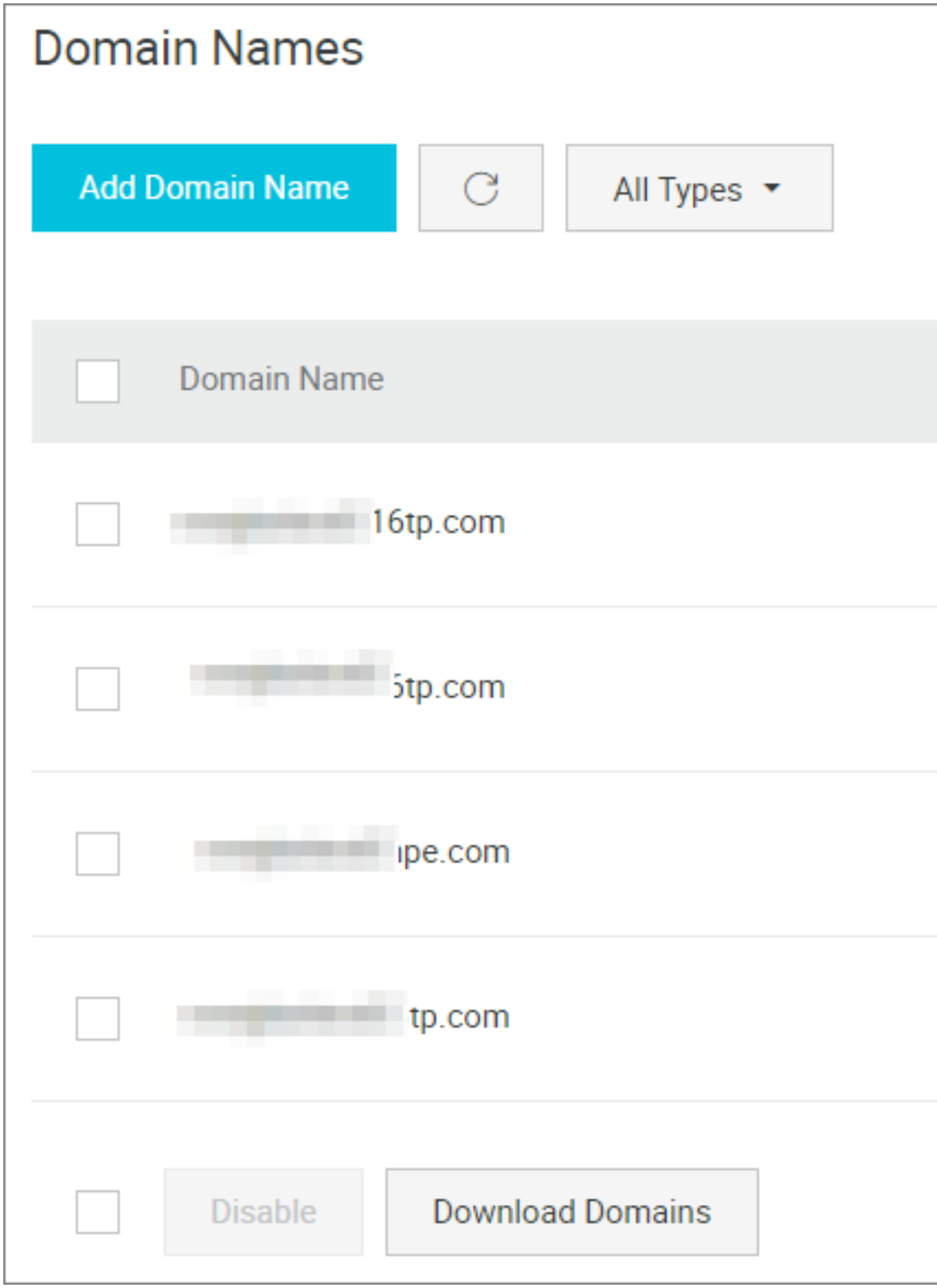
Note:

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 wish 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 wish 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.

18.3 Content back-to-source settings

18.3.1 Set Priorities of Multiple Origin Sites and Custom Port

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 "standby", and the priority is "main"> "standby".

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 5 seconds.

Main supported scenario: Master/Slave origin site switch.

Procedure

1. Go to **Domain Names**page, select the domain name, then click **Manage**.
2. Go to **Basic configuration** > **Origin site infoOrigin Site Configuration**, set origin site types, address, and port. (Now you can set the back-to-origin port to Port 80, Port 443, or Custom.)
   - If you set your Origin site information to **IP** or **Origin Site**, pay as the internet-caused traffic.
   - If you set your Origin site information to **OSS domain**, pay as the intranet-caused traffic. *OSS Pricing Details*.
   - If you have set an OSS domain name for your **origin site**, still pay as the intranet-caused traffic.
3. Click **OK** to complete the configuration.

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 protocal is set to **Follow**.
- Make sure that your back-to-origin protocol and custom port are properly in use if you wish 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.

18.3.2 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. Go to **Domain Names**page, select the domain name, then click **Manage**.
2. Enable the function in**Origin Site Configuration,** > **Private Bucket Authorization**.
3. Click **Authorize Now**.
4. 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.

18.3.3 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 Names**page, select the domain name, then click **Manage**.
2. Click **Modify** in**Cache Configuration** > **Back-to-origin with the Same Protocol**.
3. Choose your **Redirect Type**: **Follow HTTPS**, or **HTTP**.

18.3.4 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.

18.3.5 Back-to-source host

Introduction

You can customize a Web server domain name that a CDN node accesses in the back-to-source process.

Origin site: The origin site determines which IP the request is returned to during back-to-source.

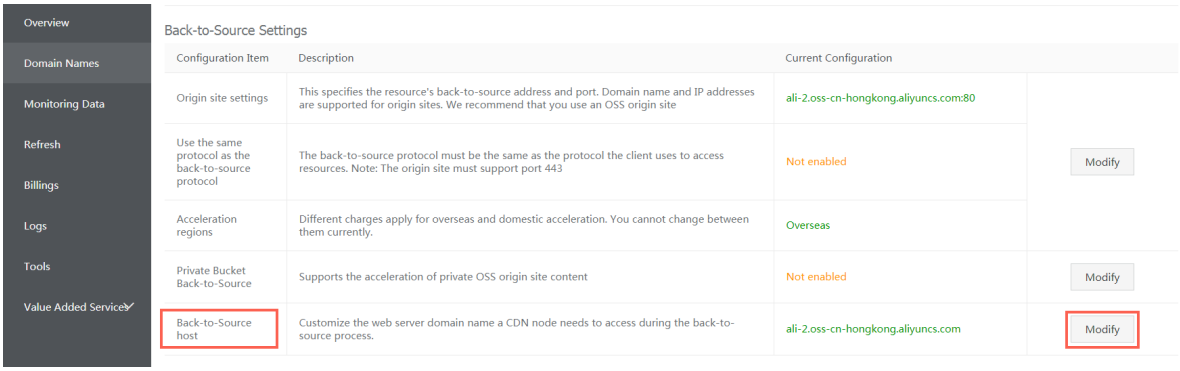
Back-to-source host: The back-to-source host determines which site on the IP to access when the request is returned to source.

- Example 1: The origin site of the domain name is `www.a.com`, the back-to-source host is `www.b.com`. then the request is returned to the actual IP resolved through `www.a.com` corresponding to the host site `www.b.com`.
- Example 2: origin site is IP origin site `1.1.1.1` Back-to-source host is `www.b.com` then the request is actually returned to `www.b.com` of the host corresponding to `1.1.1.1`.

Note:
Currently, sni back-to-source is not supported.

Procedure

- **Back-to-source host** is optional, and default value is:
  - If the origin site is **IP**, the back-to-source host is `CDN domain name` by default.
  - If the origin site is **OSS origin site**, back-to-source host is `origin site domain name` by default.
- The value options include`CDN domain name`, `origin site domain name`, and `custom domain name`.
- Configuration change: Go to CDN **Domain Names**, select the desired domain name to go to management page, back-to-source configuration to modify the configuration of the back-to-source host.



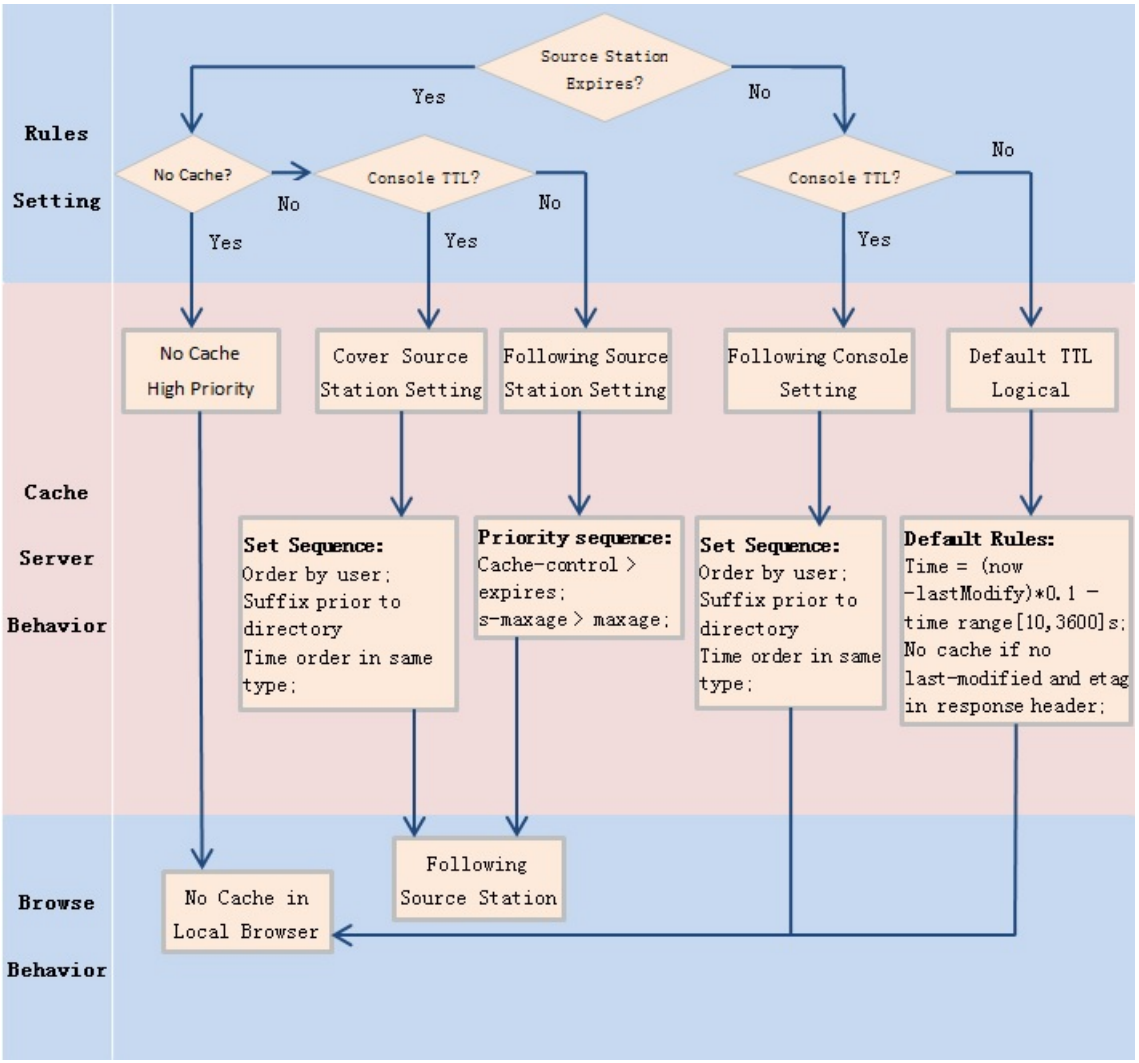
18.4 Node Cache Settings

18.4.1 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 filename 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 filename 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.

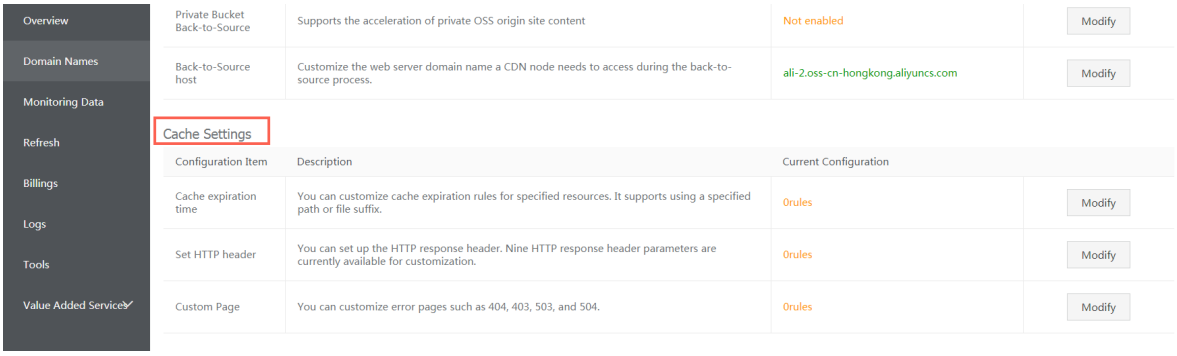
Notes

- For infrequently updated static files (e.g. image files or application download files), we suggest you set a cache time of 1 month or more;

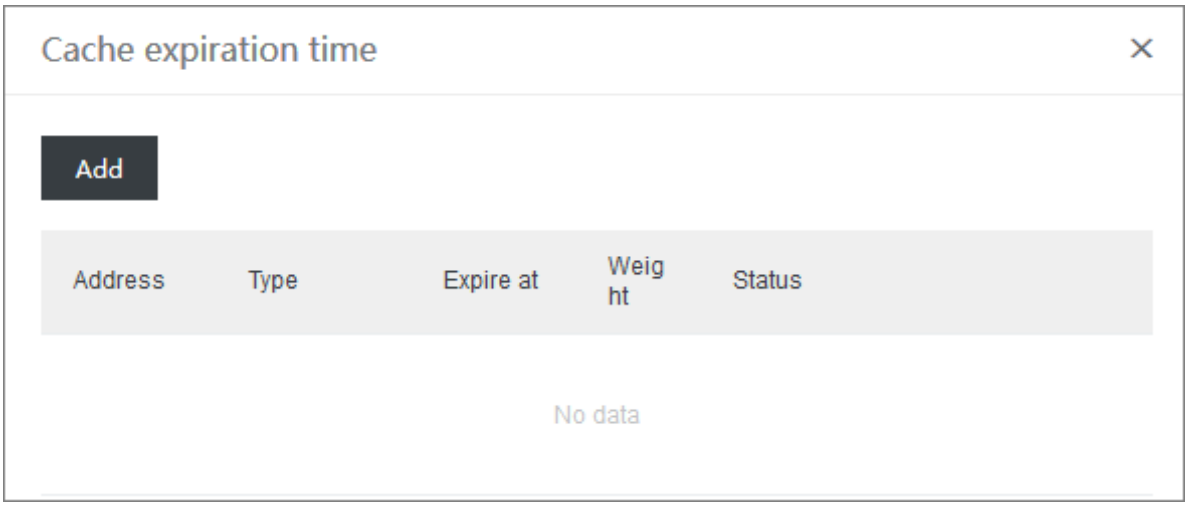
- For static files that must be updated or are updated frequently (e.g. js and css files), you can set a shorter cache time based on the actual situation;
- For dynamic files (for example, PHP files, JSP files, and ASP files), we recommend that you set the cache duration as 0s, indicating that the files are not cached. If dynamic files such as PHP files are not updated frequently, we recommend that 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

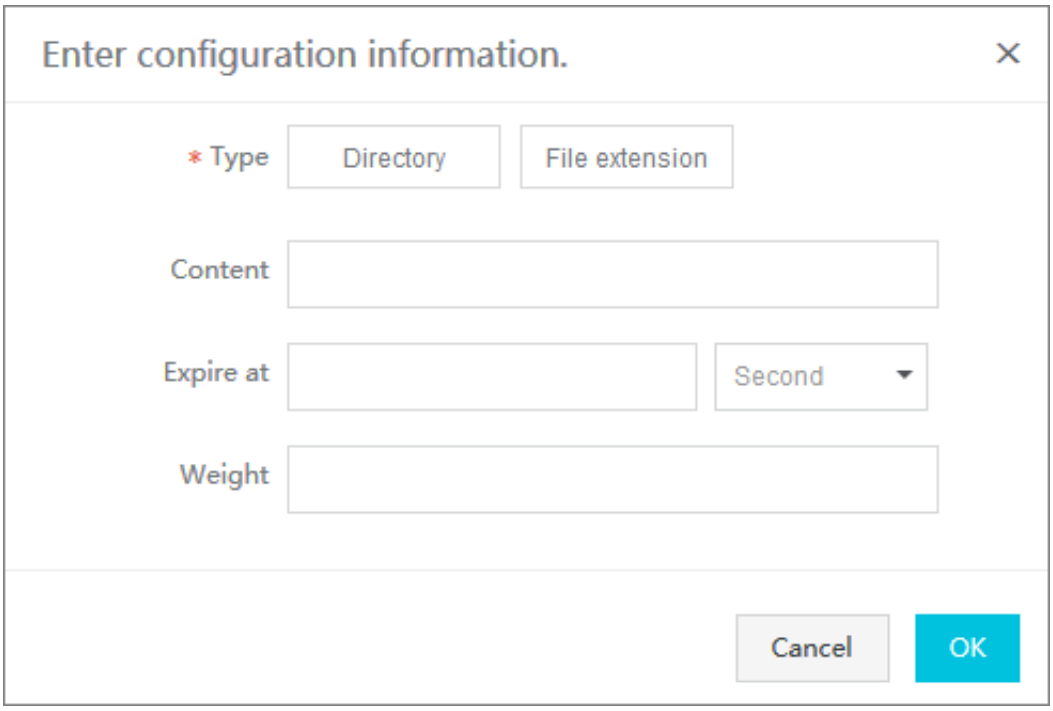
1. Go to CDN Domain Names page, select a domain name to enter the **Domain Names** page and find Cache setting:



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 filename 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.

18.4.2 Customize the 404 page

Introduction

You can customize the page that is displayed when a 404 status code is returned. The following three options are available:

Take return Code 404 as an example:

- Default 404 page: when an HTTP 404 error is returned, the server returns the default 404 Not Found page.
- Public welfare 404 page: when an HTTP an HTTP 404 error is returned, the server returns to the real-time update of the public welfare 404 page, view the *public welfare 404 page*.
- Custom 404 page: when an HTTP 404 error is returned, the server returns to the 404 page designed and edited by the user. You must costomize complete URL address of the error page.

Attentions:

- The public welfare 404 page is a public welfare resource of Alibaba Cloud. It is free and generates no traffic fees.
- Custom 404 pages are personal resources which are billed based on normal delivery.

Procedure

1. Go to the CDN domain name overview page, select a domain name to enter the **Domain Names** page, and set the **Custom page**.
2. Click **Modify**, and you can view and manage the custom error pages.
3. Click **Add** to add the page content of the custom return code.

If you choose **Custom page 404**, you need to store the page resources, like other static files, under the origin site domain. You can access the page through a CDN domain by entering the complete URL (including `http://`) of the CDN domain.
For example, if the CDN domain name is `exp.aliyun.com`, and the 404 page is `error404.html` you can store the `error404.html` page to the origin site. Select the "Custom 404", and enter `http://exp.aliyun.com/error404.html`.

18.4.3 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-Disposition	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.
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

18.5 Access Control Settings

18.5.1 鉴权方式A

工作原理

用户访问加密 URL 构成

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

鉴权字段描述

- `PrivateKey` 字段用户可以自行设置
- 有效时间1800s指用户访问客户源服务器时间超过自定义失效时间（timestamp字段指定）的1800s后，该鉴权失效。例如用户设置访问时间为2020-08-15 15:00:00，则链接的真正失效时间为2020-08-15 15:30:00。

字段	描述
timestamp	失效时间，整形正数，固定长度为10，是1970年1月1日以来的秒数。 控制失效时间，10位整数，有效时间1800s。
rand	随机数，建议使用UUID (不能包含中划线”-“，如: 477b3bbc253f467b8def6711128c7bec 格式)。
uid	暂未使用（设置成0即可)
md5hash	通过md5算法计算出的验证串，由数字和小写英文字母混合组成0-9a-z，固定长度32。

CDN服务器拿到请求后，会首先判断请求中的 `timestamp` 是否小于当前时间。

- 如果小于当前时间，则认为过期失效并返回HTTP 403错误。
- 如果 `timestamp` 大于当前时间，则构造出一个同样的字符串(参考以下sstring构造方式)。然后使用MD5算法算出 `HashValue` ，再和请求中带来的 `md5hash` 进行比对。比对结果一致，则认为鉴权通过，返回文件。否则鉴权失败，返回HTTP 403错误。

- `HashValue` 是通过以下字符串计算出来的：

```
sstring = "URI-Timestamp-rand-uid-PrivateKey" （URI是用户的请求对象相对地址，不包含参数，如 /Filename）
HashValue = md5sum(sstring)
```

鉴权实例

1. 通过 `req_auth` 请求对象:

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

2. 设置密钥为：aliyuncdnexp1234（您可以自行配置）
3. 设置鉴权配置文件有效时间为：2015年10月10日00:00:00，计算出秒数为1444435200。
4. CDN服务器会构造一个用于计算Hashvalue的签名字符串：

```
/video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234"
```

5. 根据该签名字符串，CDN服务器会计算HashValue：

```
HashValue = md5sum("/video/standard/1K.html-1444435200-0-0-
aliyuncdnexp1234") = 80cd3862d699b7118eed99103f2a3a4f
```

6. 则请求时url为：

```
http://cdn.example.com/video/standard/1K.html?auth_key=1444435200-0-
0-80cd3862d699b7118eed99103f2a3a4f
```

如果计算出的HashValue与用户请求中带的 md5hash = 80cd3862d699b7118eed99103f2a3a4f 值一致，则鉴权通过。

18.5.2 鉴权方式B

原理说明

用户访问加密 URL 格式

用户访问的 URL 如下:

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

加密URL的构造:域名后跟生成URL的时间（精确到分钟）(timestamp)再跟md5值(md5hash)，最后拼接回源服务器的真实路径(FileName)，URL有效时间为1800s。

当鉴权通过时，实际回源的URL是:

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

鉴权字段描述

- 注意：`PrivateKey` 由CDN客户自行设置
- 有效时间1800s是指，用户访问客户源服务器时间超过自定义失效时间(timestamp字段指定)的1800s后，该鉴权失效；例如用户设置访问时间2020-08-15 15:00:00，链接真正失效时间是2020-08-15 15:30:00

字段	描述
DomainName	CDN客户站点的域名
timestamp	资源失效时间，作为URL的一部分，同时作为计算 `md5hash` 的一个因子，格式为：`YYYYMMDDHHMM` ,有效时间1800s
md5hash	以timestamp、FileName和预先设定好的PrivateKey 共同做MD5获得的字符串，即 md5(`PrivateKey` + `timestamp` + `FileName`)
FileName	实际回源访问的URL (注意，鉴权时候FileName要以/开头)

示例说明

1. 回源请求对象:

   ```
   http://cdn.example.com/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
   ```

2. 密钥设为：aliyuncdnexp1234 (用户自行设置)。
3. 用户访问客户源服务器时间为 201508150800（格式为： YYYYMMDDHHMM ）。

4. 则CDN服务器会构造一个用于计算 md5hash 的签名字符串：

```
aliyuncdnexp1234201508150800/4/44/44c0909bcfc20a01afaf256ca99a8b8b.
mp3
```

5. 服务器会根据该签名字符串计算 md5hash：

```
md5hash = md5sum("aliyuncdnexp1234201508150800/4/44/44c0909bcf
c20a01afaf256ca99a8b8b.mp3") = 9044548ef1527deadafa49a890a377f0
```

6. 请求CDN时url：

```
http://cdn.example.com/201508150800/9044548ef1527deadafa49a890a377f0
/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
```

计算出来的 md5hash 与用户请求中带的 md5hash = 9044548ef1527deadafa49a890a377f0 值一致，于是鉴权通过。

18.5.3 鉴权方式C

原理说明

用户访问加密 URL 格式

格式1

```
http://DomainName/{/}/FileName
```

格式2

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

- 花括号中的内容表示在标准的URL基础上添加的加密信息。
- `<md5hash>`是验证信息经过 MD5 加密后的字符串;
- `<timestamp>`是未加密的字符串，以明文表示。固定长度10，1970年1月1日以来的秒数，表示为十六进制。
- 采用格式一进行URL加密，例如：

```
http://cdn.example.com/a37fa50a5fb8f71214b1e7c95ec7a1bd/55CE8100/
test.flv
```

`<md5hash>` 为 a37fa50a5fb8f71214b1e7c95ec7a1bd`<timestamp>` 为 55CE8100。

鉴权字段描述

- `<md5hash>` 部分字段描述。

字段	描述
PrivateKey	干扰串，不同客户采用不同的干扰串
FileName	实际回源访问的URL (注意，鉴权时候path要以/开头)
time	用户访问源服务器时间，取 UNIX 时间，以十六进制数字字符表示。

- PrivateKey 取值 `aliyuncdnexp1234`
- FileName 取值 `/test.flv`
- time 取值 `55CE8100`
- 因此 md5hash 值为：

```
md5hash = md5sum(aliyuncdnexp1234/test.flv55CE8100) = a37fa50a5f
b8f71214b1e7c95ec7a1bd
```

- 明文: `timestamp = 55CE8100`

  这样生成加密 URL:

  格式一：

```
http://cdn.example.com/a37fa50a5fb8f71214b1e7c95ec7a1bd/55CE8100/
test.flv
```

  格式二：

```
http://cdn.example.com/test.flv?KEY1=a37fa50a5fb8f71214b1e7c95ec7a1
bd&KEY2=55CE8100
```

示例说明

用户使用加密的 URL 访问加速节点,CDN服务器会先把加密串 1 提取出来, 并得到原始的 URL 的 `<FileName>` 部分，用户访问时间，然后按照定义的业务逻辑进行验证：

1. 使用原始的 URL 中的 `<FileName>` 部分,请求时间及 PrivateKey 进行 MD5 加密得到一个加密串2。
2. 比较加密串 2 与加密串 1 是否一致，如果不一致则拒绝。
3. 取加速节点服务器当前时间，并与从访问 URL 中所带的明文时间相减，判断是否超过设置的时限 t(时间域值 t 默认为 1800s)。

4. 有效时间1800s是指，用户访问客户源服务器时间超过自定义时间的1800s后，该鉴权失效；例如用户设置访问时间2020-08-15 15:00:00，链接真正失效时间是2020-08-15 15:30:00。
5. 时间差小于设置时限的为合法请求，CDN加速节点才会给予正常的响应，否则拒绝该请求，返回 http 403错误。

18.5.4 鉴权配置

URL鉴权功能主要用于保护用户站点的内容资源不被非法站点下载盗用。虽然，通过防盗链方法添加 Referer 黑、白名单的方式可以解决一部分盗链问题。但是，由于 Referer 内容可以伪造，所以Referer 防盗链方式无法彻底保护站点资源。因此，采用URL鉴权方式保护用户源站资源更为安全有效。

工作原理

URL鉴权功能通过阿里云CDN加速节点与客户资源站点配合，实现了一种更为安全可靠的源站资源防盗方法。

1. CDN客户站点提供加密 URL（包含权限验证信息）。
2. 您使用加密后的 URL 向加速节点发起请求。
3. 加速节点对加密 URL 中的权限信息进行验证以判断请求的合法性。正常响应合法请求，拒绝非法请求。

鉴权方式

阿里云CDN 兼容并支持鉴权方式*A*、鉴权方式*B*、鉴权方式*C*三种鉴权方式。您可以根据自己的业务情况，选择合适的鉴权方式，来实现对源站资源的有效保护。

鉴权代码示例

您可以查看 鉴权代码示例。

配置引导

1. 在CDN控制台页面下的域名管理 页，选择需要设置的域名，单击配置。

2. 在访问控制 > 鉴权配置栏，单击修改配置。

3. 单击开启URL鉴权配置，选择鉴权类型，并主**KEY**。

18.5.5 Anti-leech

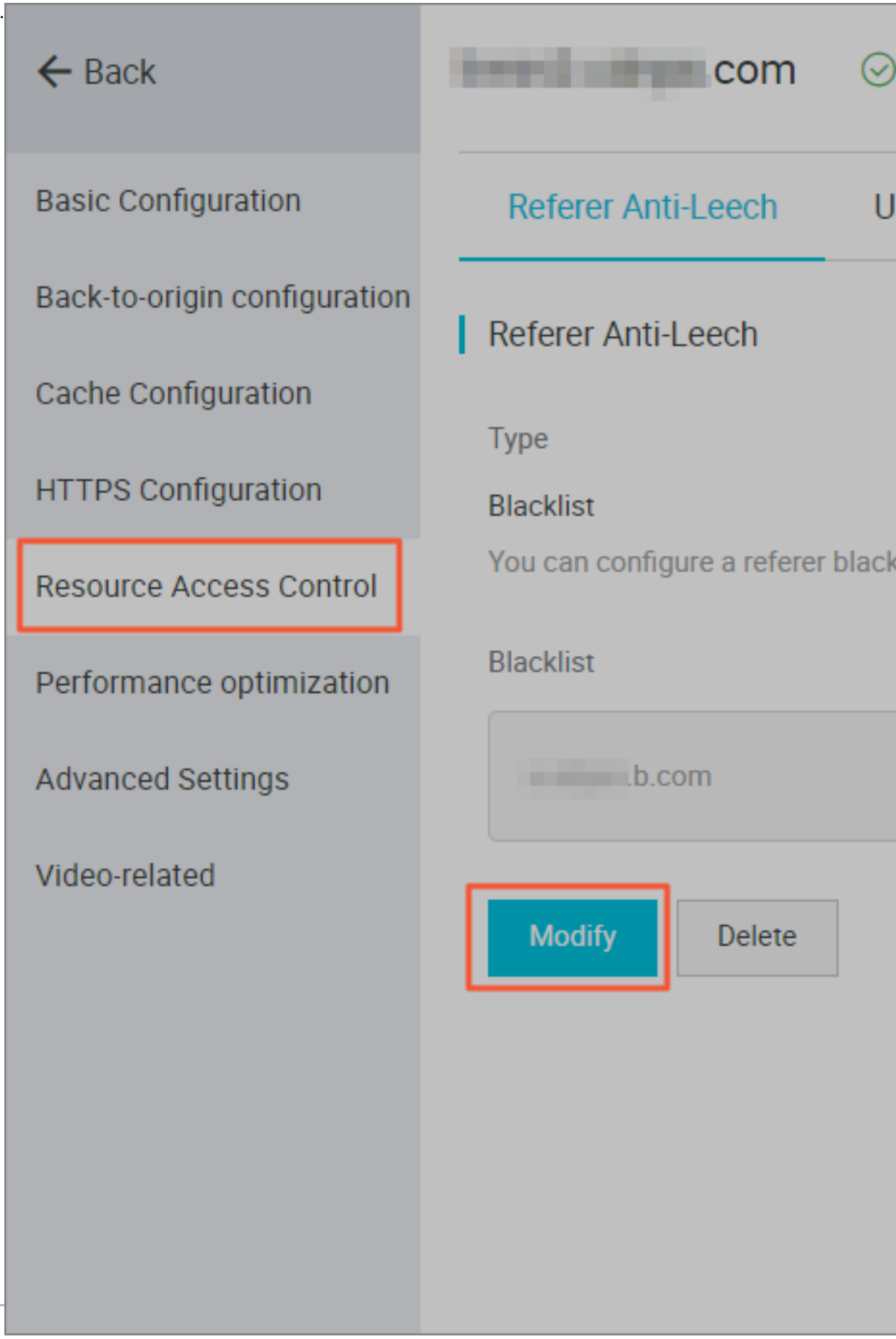
Introduction

- 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 Names**page, select the domain name, then click **Manage**.

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



3. Choose**Blacklist** 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).

18.5.6 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.

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

Note:

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 Names**page, select the domain name, then click **Manage**.
2. On **Access Control** > **IP Blacklist/Whitelist**, click **Modify**.
3. Choose**Blacklist** or **Whitelist**, and add the IP network segment in the box below.
4. Click **Confirm**.

18.5.7 鉴权代码示例

URL鉴权规则请查阅 *URL鉴权*，通过这个 demo 您可以根据业务需要，方便的对URL进行鉴权处理。以下Python Demo包含三种鉴权方式：A鉴权方式、B鉴权方式、C鉴权方式，分别描述了三种不同鉴权方式的请求URL构成、哈希字符串构成等内容。

Python版本

```
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.fromtimestamp(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 authorization
    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()
```

18.6 Video Service Configuration

18.6.1 Notify_URI 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=cdnvideocenter010207116011.cm3
```

Parameter	Value description
time	unix timestamp

Parameter	Value description
usrargs	User streaming parameters
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

18.6.2 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 Names**page, select the domain name, then click **Manage**.
2. Enable the function in **Video-related** > **Drag/Drop Playback**.

18.6.3 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 to**Domain Name**page，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.

18.7 Performance Optimization settings

18.7.1 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.

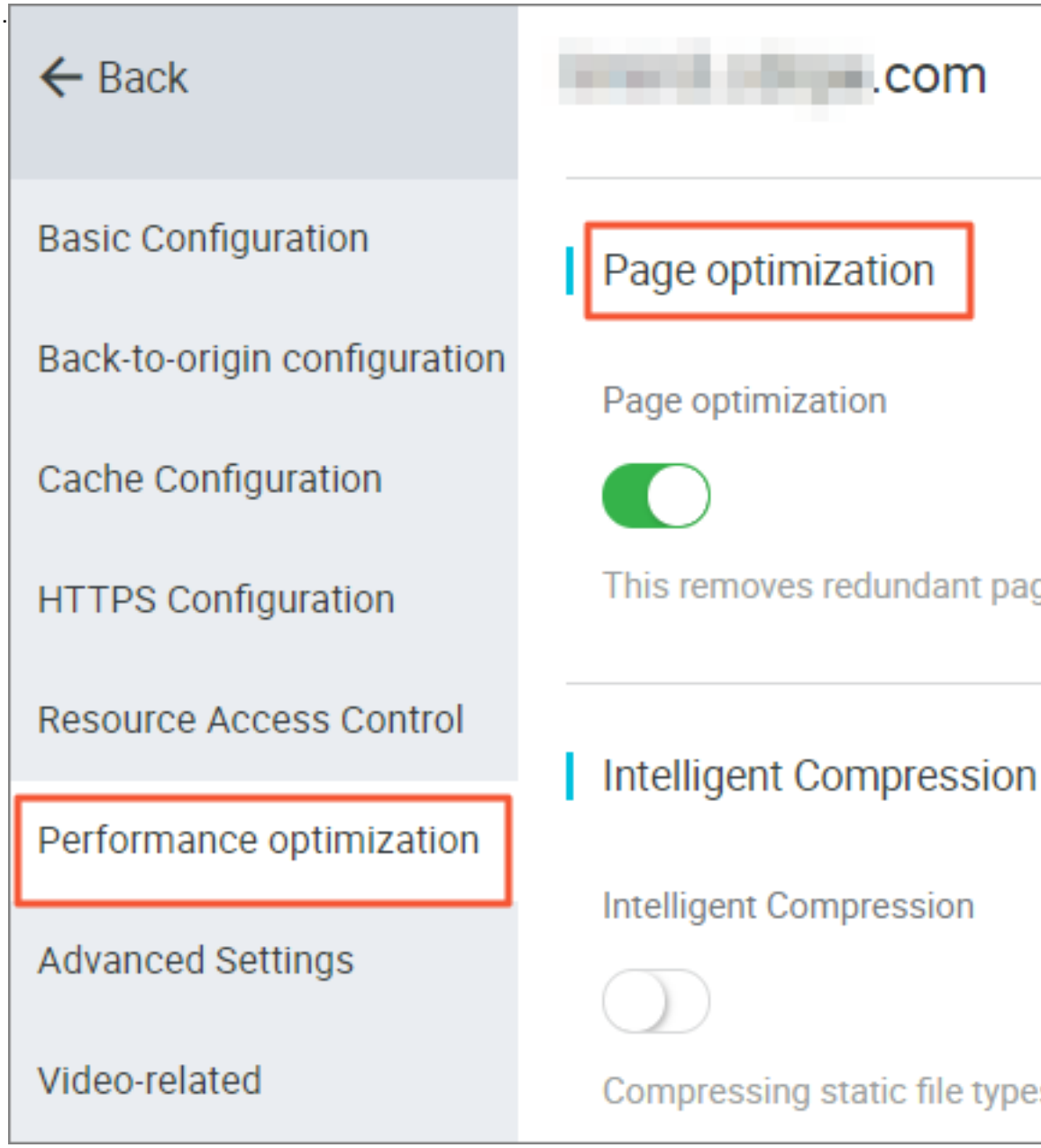
Contents in the following formats can be compressed: text/xml, text/plain, text/css, application/javascript, application/x-javascript, application/rss+xml, text/javascript, image/tiff, image/svg+xml, and application/json.

Applicable business type: All.

Procedure

1. Go to **Domain Names**page, select the domain name, then click **Manage**.

2. Enable the function in **Performance Optimization** > **Smart Compression**.



18.7.2 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

1. Go to **Domain Names**page, select the domain name, then click **Manage**.

2. Enable the function in **Performance Optimization** > **Page Optimization**.

18.7.3 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 Names**page, select the domain name, then click **Manage**.
2. Enable the function in **Performance Optimization** > **Filter Parameter**.

18.8 Advanced settings

18.8.1 Peak Bandwidth

Introduction

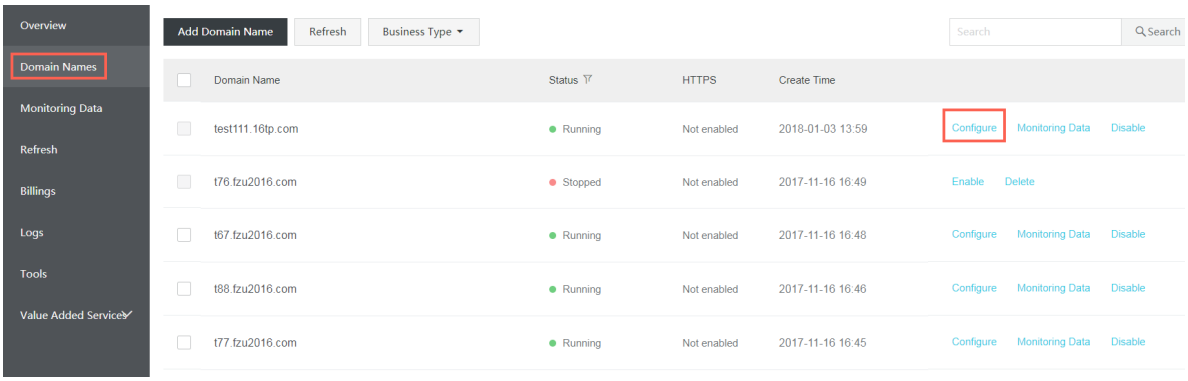
The bandwidth cap function sets the maximum bandwidth value for average bandwidth measured during each statistical cycle (five minutes). If the average bandwidth exceeds the maximum, the domain name automatically goes offline to protect your domain name security. In this situation, all requests are sent 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.

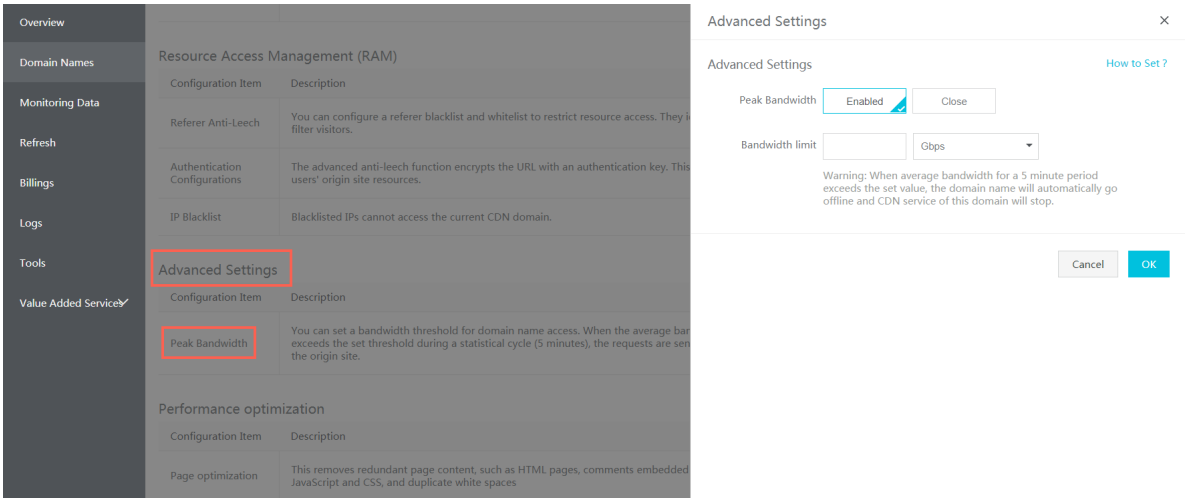
Note:
The bandwidth cap function is not currently available for wildcard domain names, so the function has no effect even it is enabled.

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

How do I enable the bandwidth cap function?

1. Click **Configure** in Domain Names page, go to **Security Settings** on the configuration page of the selected domain name, and click **Modify Configuration**.

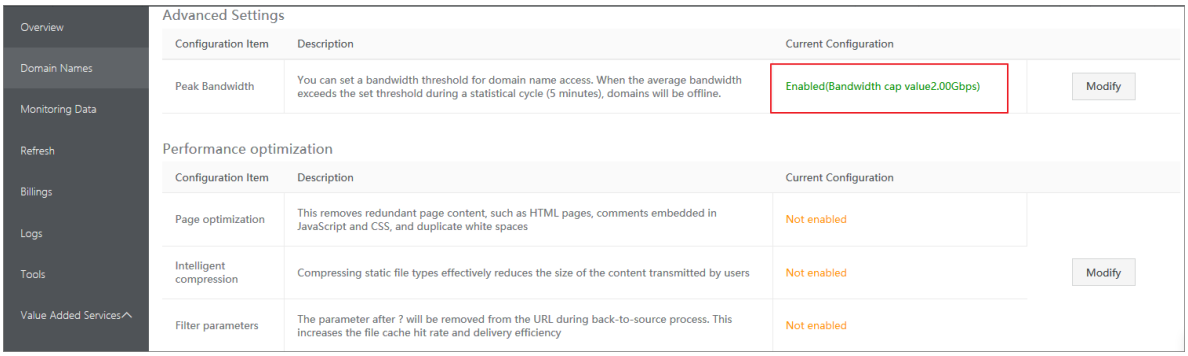




2. Enable the bandwidth cap function. The bandwidth is measured in Mbps, Gbps, or Tbps.

> **Note:**
> bandwidth value can be set in powers of thousand.

3. The bandwidth cap function is successfully enabled.



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

Attentions:

After you enable the bandwidth cap function, your services are limited by the bandwidth cap and go offline if it is exceeded. To avoid affecting the services on your domain name, we recommend you set the cap value with discretion based on reasonable estimation.