Alibaba Cloud
dcdn

User Guide

Issue: 20190122

Legal disclaimer

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

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

al property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

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

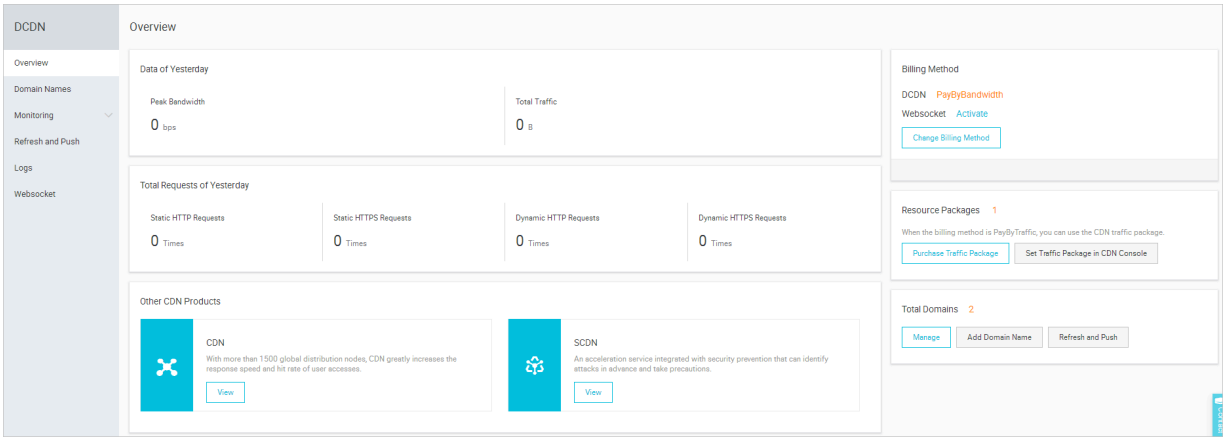
Contents

1 Introduction about the console

In the Dynamic Route for CDN (DCDN) console, you can add DCDN domain names, refresh the cache, and perform configurations. It also provides real-time resource monitoring based on data analytics. This article describes the DCDN console.

Overview

Logging on to the DCDN console directs you to an overview of your account's DCDN running status.



This page shows the following information:

- Yesterday's basic data
  - Peak bandwidth
  - Total traffic
- Yesterday's total number of requests
  - Number of static HTTP requests
  - Number of static HTTPS requests
  - Number of dynamic HTTP requests
  - Number of dynamic HTTPS requests

Left-side navigation pane:

Item	Description
Domain Names	Allows you to add, configure, delete, or modify information and configurations of DCDN domain names.

Item	Description
Resource Monitoring	Displays the real-time acceleration parameters of the basic CDN, including peak bandwidth, total traffic, and hit rate.
Refresh and Push	Allows you to perform the refresh and push operations.
Logs	Allows you to download DCDN logs.

2 Basic Settings

2.1 Set origin site

Origin types

The origin types include IP, OSS domain, and origin domain.

- IP: Enter the server outer network IP. You can enter multiple IPs and configure their priorities. Alibaba Cloud ECS IP can be exempted from verification.
- OSS domain: You can directly select OSS buckets under the same account, or manually enter the external domain name of the OSS, such as `xxx.oss-cn-hangzhou.aliyuncs.com`. You can view the external domain name of the OSS in the OSS console.
- Origin domain: Enter the domain name of your origin site. You can configure multiple origin site domain names and set their priorities.

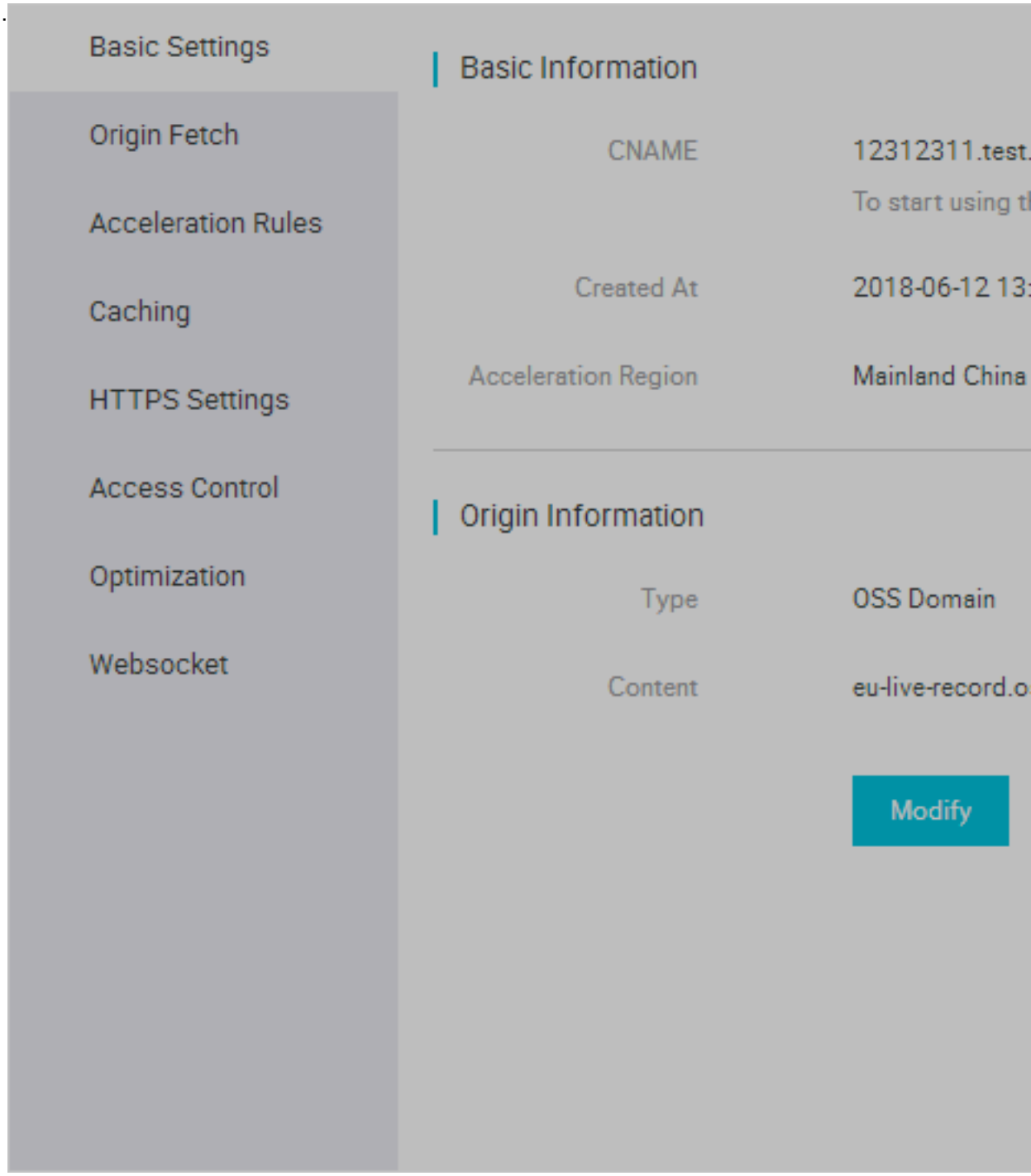
> **Note:**
> The origin domain name cannot be the same as the DCDN domain name. Otherwise, an origin fetch loop is caused. For example, if your DCDN domain name is `cdn.example.com`, we recommend that you set the origin site to `src.example.com`.

Multiple origin sites

When you set the origin type to IP or origin domain, you can configure multiple origin sites and set their priorities. Acceleration nodes perform origin fetch according to their priorities.

Ports

Ports 80 (for HTTP) and 443 (for HTTPS) are currently supported. Custom ports are not currently supported.



2.2 Set priorities for multiple sources

Introduction

DCDN allows you to set the origin priority for both **dynamic resources** and **static resources**.

- DCDN supports three types of origin domain names; OSS domain names, IP, and origin domain names. Multiple IP addresses and origin domain names are supported. You can set the origin priority when multiple origin sites exist.
- When you specify IP or origin domain as the origin type, you can configure multiple origin sites and set the origin priorities. The origin priority can be Primary or Secondary, and Primary has higher priority than Secondary.
- 100% of the user's origin fetch traffic is first sent back to the origin site with higher priority.
  - 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 origin priority, CDN round-robin takes place.

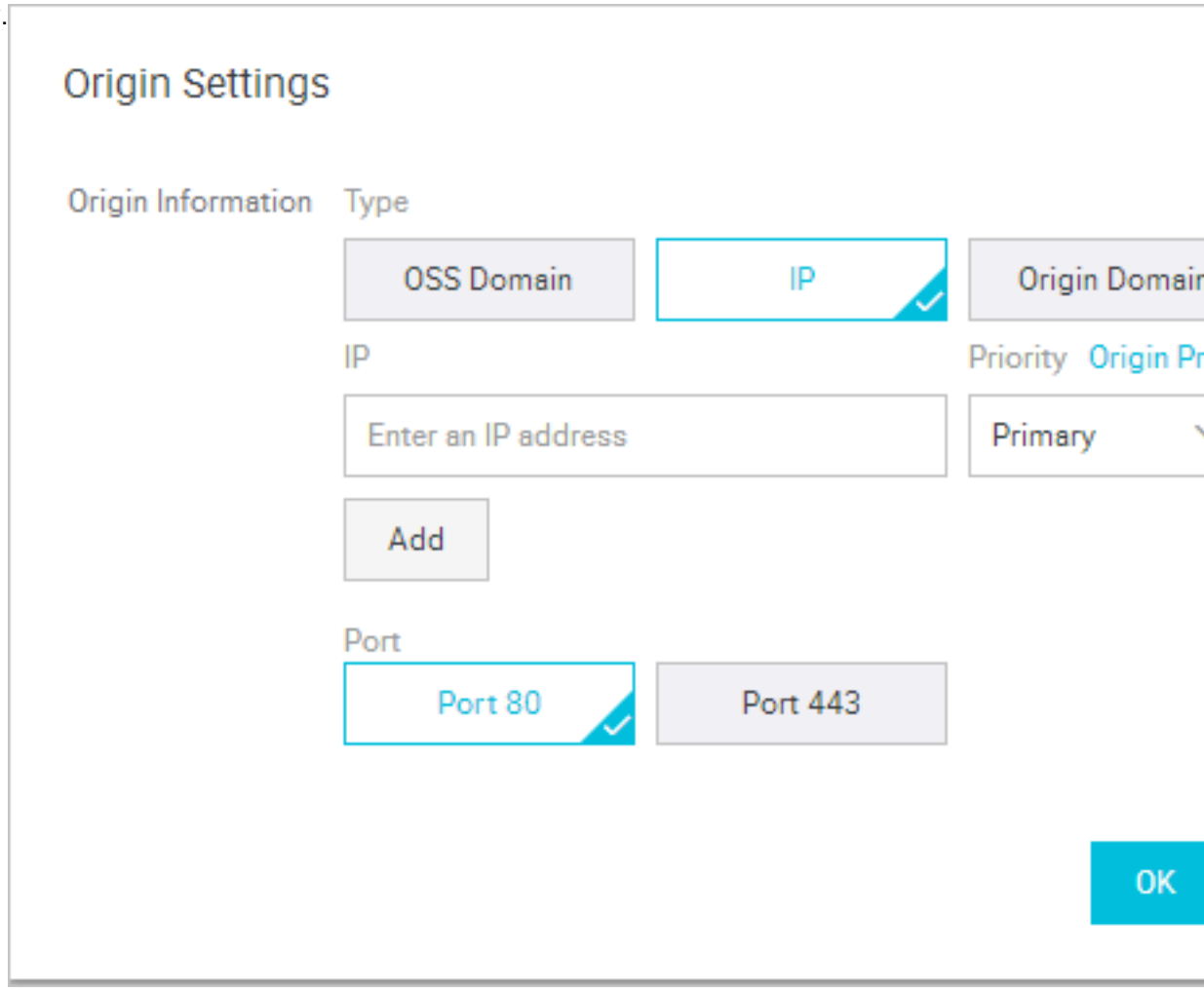
Origin site health check: 4-layer health check is automatically performed on origin sites every 5 seconds.

Supported scenario: Primary-secondary origin switchover.

Procedure

1. On the **Domain Names** page, select a domain name, and click **Configure**.
2. Go to **Basic Settings** > **Origin Information**, and click **Modify**.

3. Set the origin **IP** and **Priority**.



4. Click **OK** for the settings to take effect.

Note:

Priority settings for multiple origin sites only support the IP and origin domain names. OSS domain names do not support the origin priority setting. Select the origin type that suits your needs and set the priority appropriately.

3 Origin Fetch Settings

3.1 Back-to-Source settings

Introduction

You can configure the domain name of the web server to be accessed during the origin fetch process.

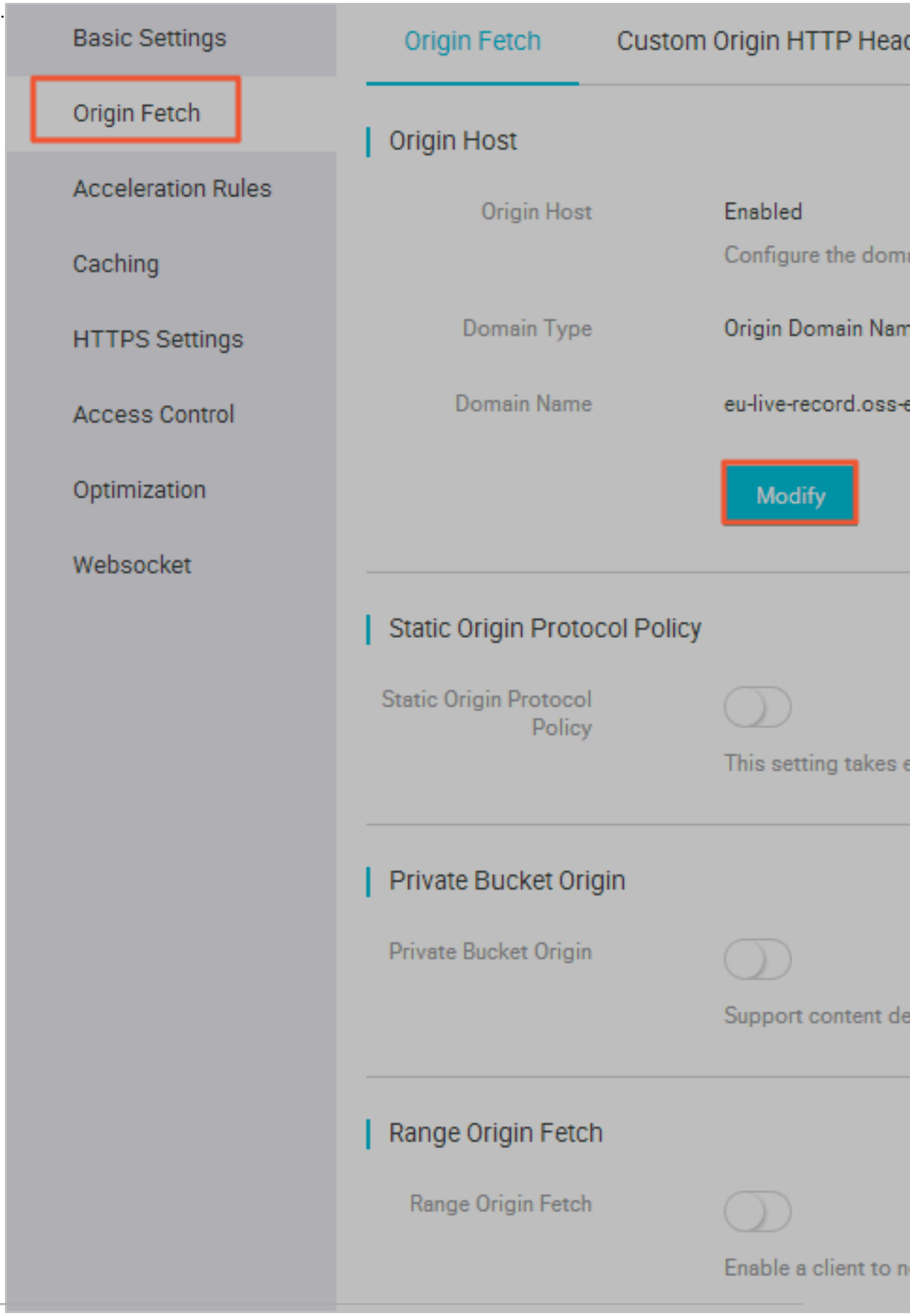
- The origin host configuration is optional. The default value is as follows:
  - If the origin site is an **IP** address, the origin host is the `DCDN domain name` by default.
  - If the origin site is an **OSS domain name**, the origin host is the `origin site domain name` by default.
- The options are: `DCDN domain names`, `origin domain names`, and `custom domain names`.

> **Note:**
> SNI origin fetch is not currently supported.

Procedure

1. On the **Domain Names** page, select a domain name, and click **Configure**.
2. Go to **Origin Fetch** > **Origin Host**, and click **Modify**.

3. Select the type of domain name to speed up, and click **OK**.



Difference between the origin site and the origin host

- Origin site: The origin site determines the specific IP address that is requested for origin fetch.
- Origin host: The origin host determines the specific website that is at the IP address accessed by the origin fetch request.

Case	Case 1	Case 2
Origin site	www.a.com	1.1.1.1
Origin host	www.b.com	www.b.com
In actual origin fetch, the request is forwarded to	Website www.b.com on the host corresponding to www.a.com	Website www.b.com on the host that is corresponding to 1.1.1.1

3.2 Use the same protocol as the back-to-source protocol

Introduction

When this feature is used, the client protocol for origin fetch is consistent with the protocol for accessing resources. That is, if a client uses HTTPS to request a resource, when the resource is not cached on the node, DCDN requests the resource from the origin using HTTPS. Similarly, if a client uses HTTP to request the resource, the node also uses HTTP to forward the request to the origin.

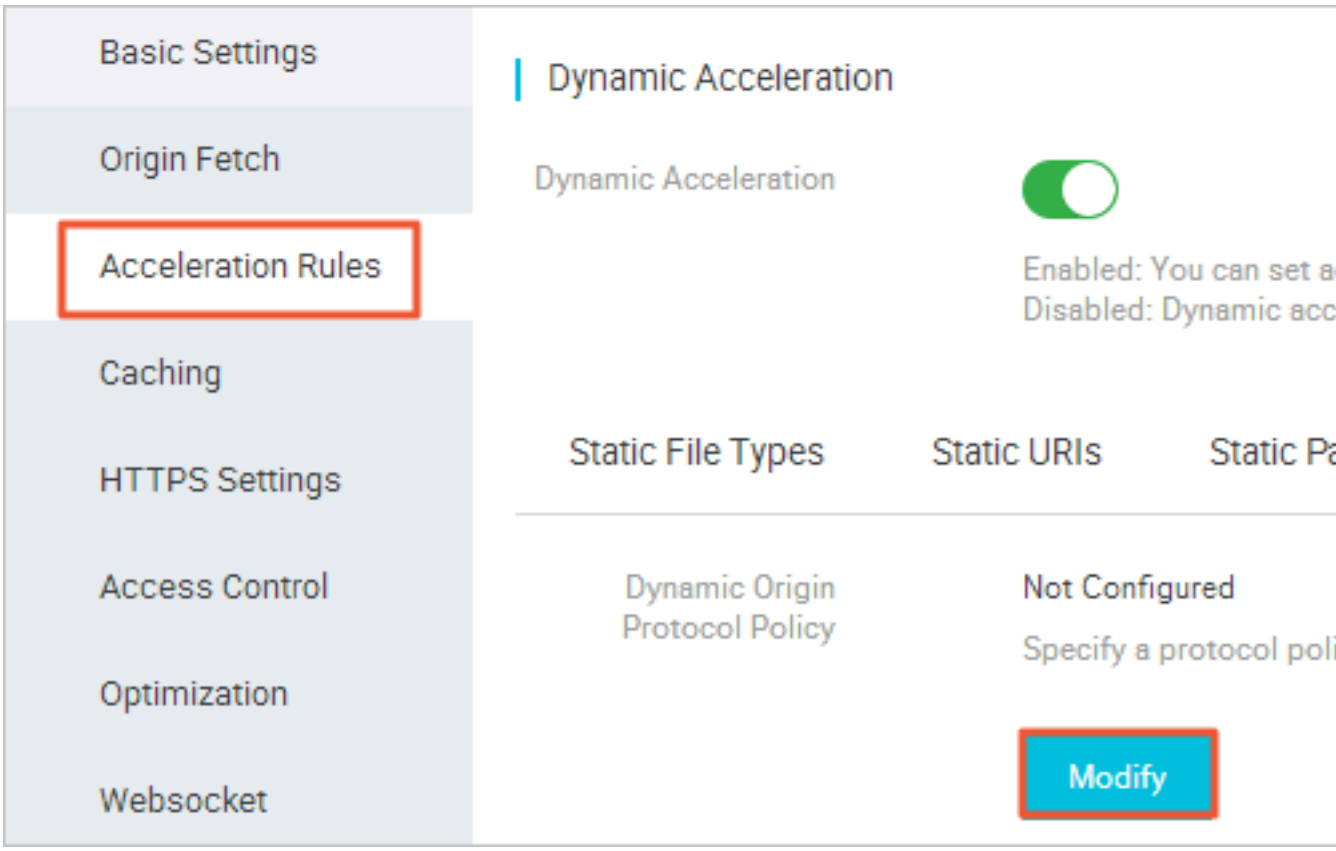
Currently, Dynamic Origin Protocol Policy and Static Origin Protocol Policy are supported.

Note:
The origin site must support both port 80 and port 443. Otherwise, an origin fetch failure may occur.

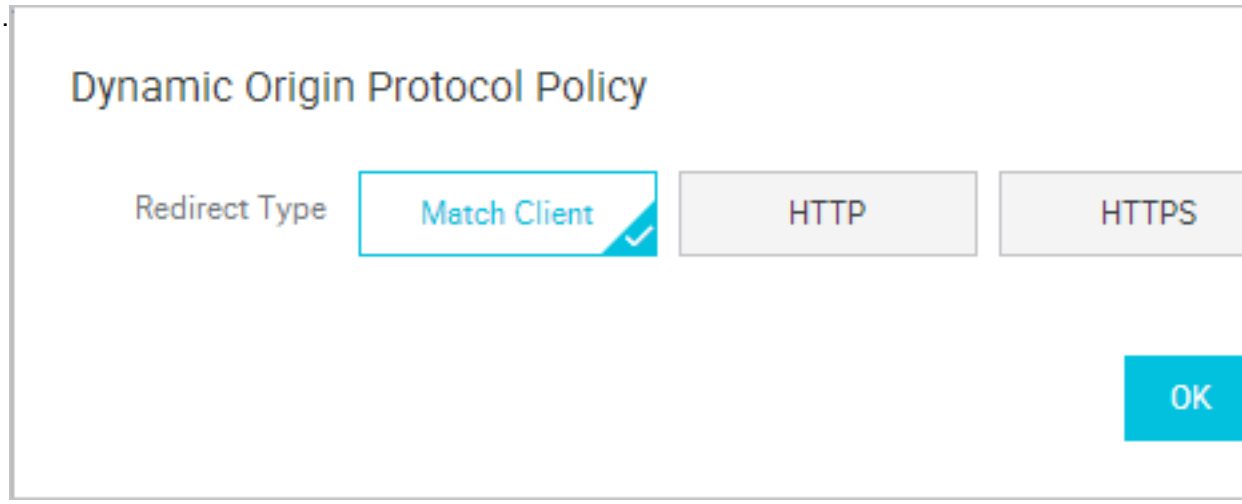
Procedure

Dynamic Origin Protocol Policy

1. On the **Domain Names** page, select a domain name, and click **Configure**.
2. Go to **Acceleration Rules** > **Dynamic Origin Protocol Policy**, and click **Modify**.

3. 

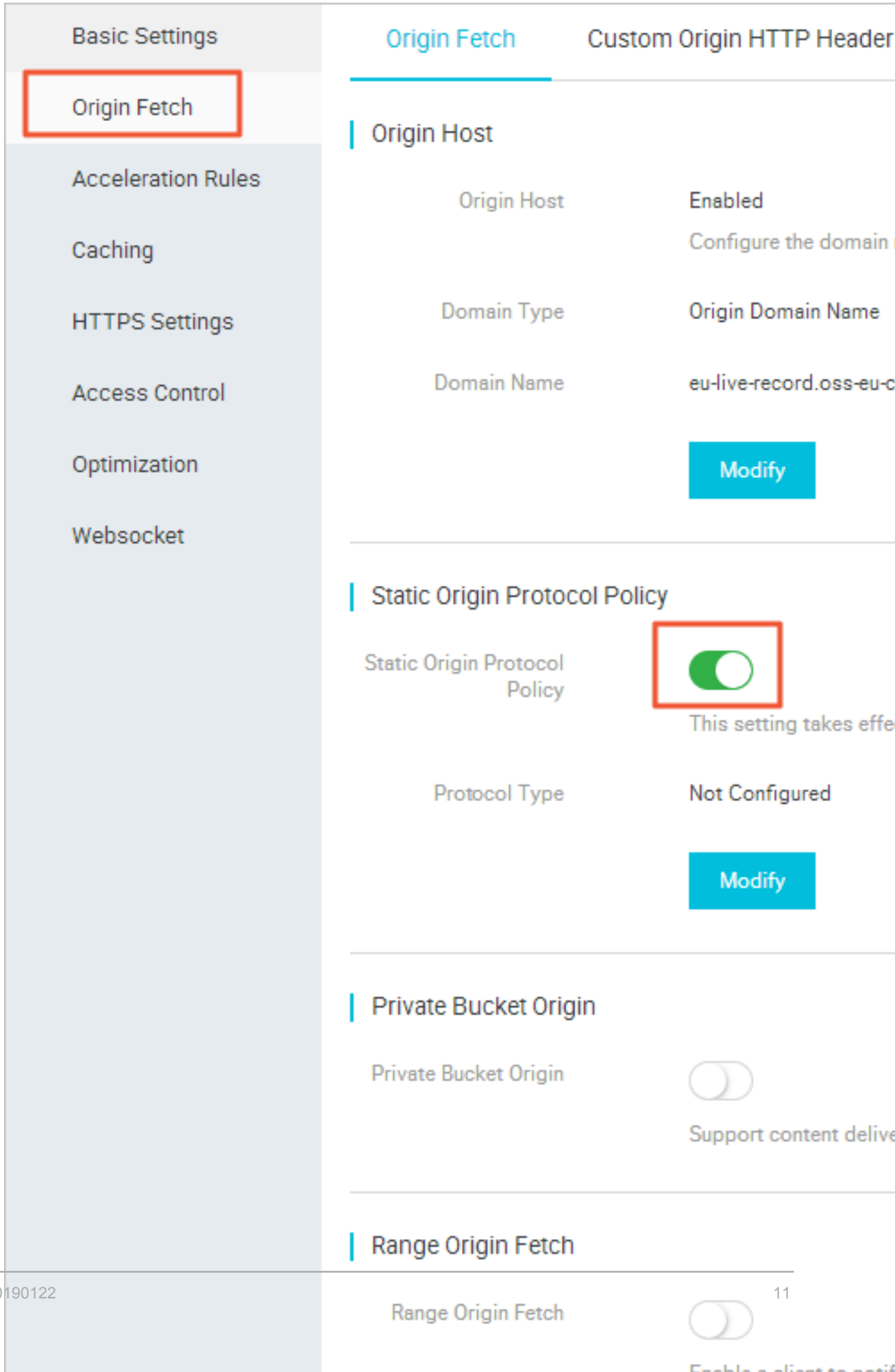
4. Select a Redirect Type: **Match Client**, **HTTP**, or **HTTPS**.



Static Origin Protocol Policy

1. On the **Domain Names** page, select a domain name, and click **Configure**.
2. Go to **Origin Fetch** > **Static Origin Protocol Policy** and click the switch.

3.


Basic Settings
Origin Fetch
Acceleration Rules
Caching
HTTPS Settings
Access Control
Optimization
Websocket
Origin Fetch
Custom Origin HTTP Header
Origin Host
Origin Host
Enabled
Configure the domain
Domain Type
Origin Domain Name
Domain Name
eu-live-record.oss-eu-c
Modify
Static Origin Protocol Policy
Static Origin Protocol Policy
This setting takes effe
Protocol Type
Not Configured
Modify
Private Bucket Origin
Private Bucket Origin
Support content delive
Range Origin Fetch
Range Origin Fetch

3.3 Private OSS bucket back-to-source

Function introduction

Private OSS bucket back-to-origin authorization means that if the acceleration domain name is to be returned to the user account and marked as a private OSS bucket (referred to as a private bucket), authorization must be performed first. If authorization is successful and authorization configuration is enabled, the user can access the private bucket only after the domain name is authorized by the private bucket.

Risk warnings

- If authorization succeeds and the private bucket feature of the corresponding domain name is enabled, the acceleration domain can access resources in your private bucket. Before you enable this function, carefully consider your business requirements.

   **Note:**
  bucket content is not suitable as a back-to-origin source for CDN acceleration domain names.
- You can use the functions provided by CDN, such as **OSS Anti-Leech(Referer)**, **Authentication** and so on, to effectively secure your resources.
- If your website is at risk of attack, we recommend that you purchase the Anti-DDoS Pro service . Moreover, do not authorize or enable the private OSS bucket function.

Procedure

Enable Private Bucket Back-to-Origin Authorization

1. On the **Domain Names** page, select a domain name, and click **Configure**.
2. Go to **Basic Settings** > **Origin Information**, and click **Modify**.
3. In **Back-to-Origin Settings** > **Private Bucket Back-to-Origin Settings** > **Service Access Authorization**, click **Immediate Authorization**.
4. Authorization successful. Click **OK** to enable private OSS bucket back-to-source for the domain name.
5. Operation successful.

Turn off private Bucket back-to-origin authorization

1. Go to **Resource Access Management** > **Role Management**.
2. **Delete** the roles you want to remove.
3. Private bucket authorization removal successful.

Note:
If your acceleration domain name is using a private bucket as the source site for back-to-origin, do not close or remove the private bucket authorization.

3.4 Back-to-source of range

Introduction

The range origin fetch feature allows a client to notify an origin site server to return partial content within a specified range. This feature accelerates delivery of large files by reducing the consumption of origin fetch traffic and improving the resource response speed.

- To use the range origin fetch feature, 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.
- When range origin fetch is enabled, a parameter request can be returned to an origin site. In this case, the origin site returns the file byte range according to the Range parameter and the CDN node returns the content in the byte range to the client.

  Note:
  For example, if a request sent from a client to a CDN node contains range:0-100, the range:0-100 parameter is also 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.
- When range origin fetch is disabled, a CDN higher-level node requests an origin site for all files. However, the requested files are not cached on the CDN node because a client automatically disconnects HTTP links after receiving bytes specified by Range. This causes a low cache hit rate and large origin fetch traffic.

  Note:
  For example, if a request sent from a client to a CDN node contains range:0-100, the range:0-100 parameter isl not 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.

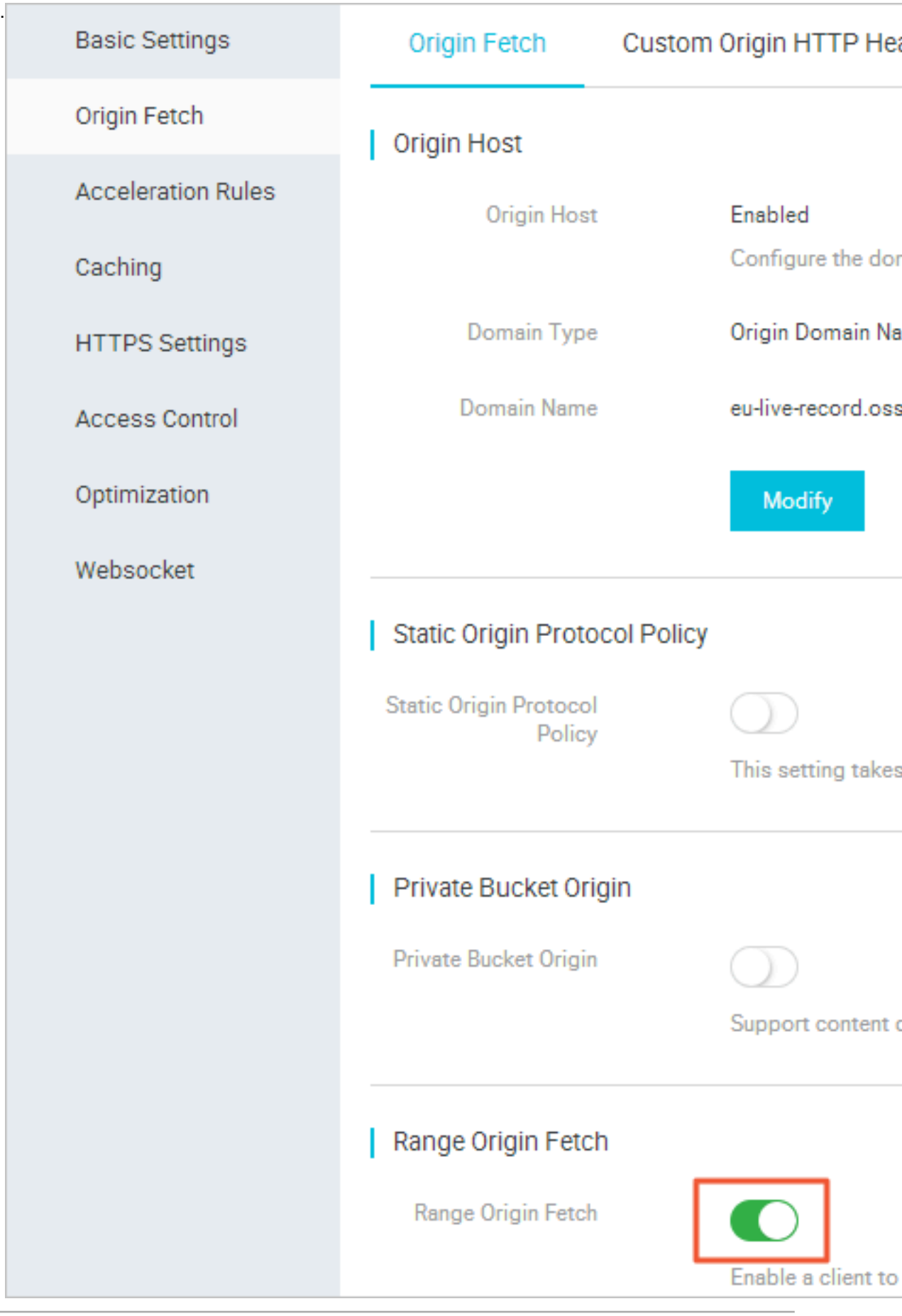
Note

To use the range origin fetch feature, 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.

Procedure

1. On the **Domain Names** page, select a domain name, and then click **Configure**.

2. Go to **Origin Fetch** > **Range Origin Fetch** to enable range origin fetch.



4 Acceleration Strategy

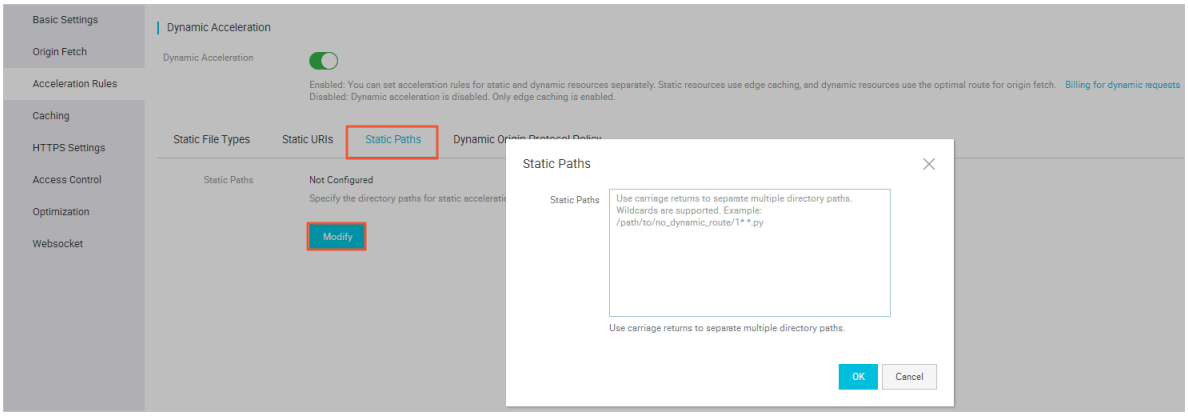
4.1 Set static file path

Introduction

The feature identifies static files by file path. The specified static files no longer use dynamic acceleration. Instead, they use static acceleration and allocate the best edge nodes for caching and distribution.

Procedure

1. On the **Domain Names** page, select a domain name, and click **Configure**.
2. Go to **Acceleration Rules** > **Static Paths**, and click **Modify**.
3. Specify the caching path.



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

4.2 Set static file type

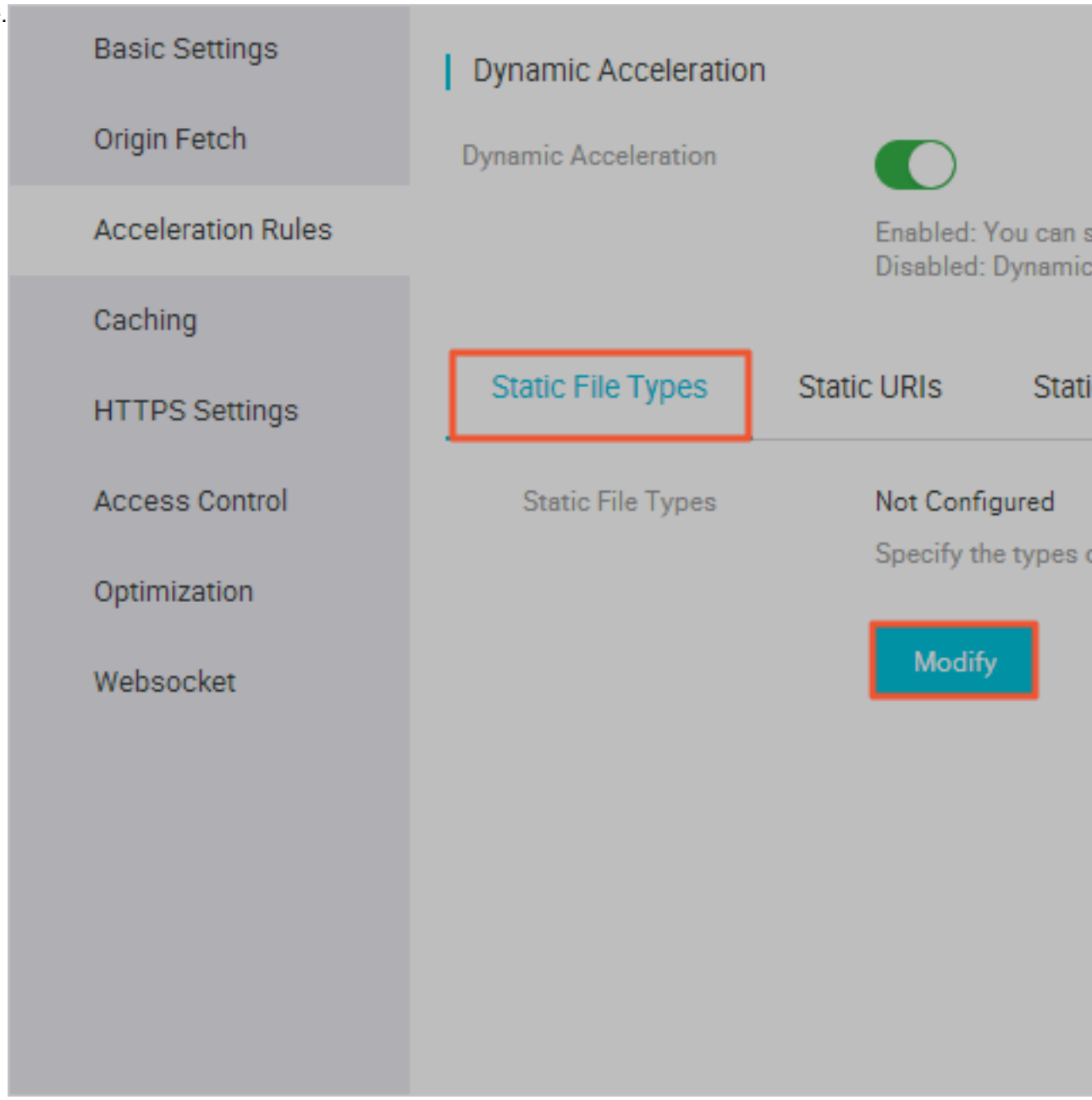
Introduction

The feature allows you to specify static file types by filename extension. The specified static files no longer use dynamic acceleration. Instead, they use static acceleration and allocate the best CDN nodes for caching and distribution.

Procedure

1. On the Domain Names page, select a domain name, and click **Configure**.
2. Go to **Acceleration Rules** > **Static File Types**, and click **Modify**.

3. Select static file types. The specified files are cached and CDN nodes do not need to request them from the origin site.



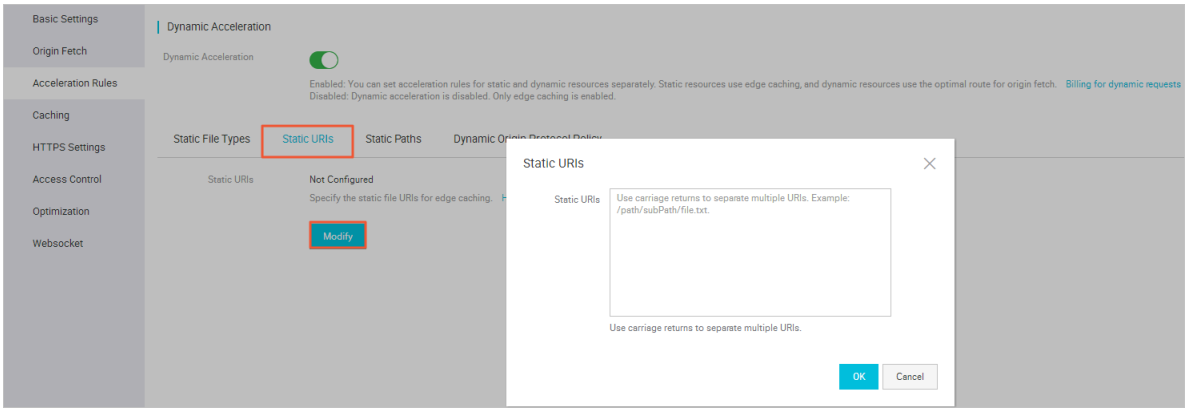
4.3 Set static file URI

Introduction

This feature identifies static files by file URI. The specified static files no longer use dynamic acceleration. Instead, they use static acceleration and allocate the best edge nodes for caching and distribution.

Procedure

1. On the **Domain Names** page, select a domain name, and click **Configure**.
2. Go to **Acceleration Rules** > **Static URIs**, and click **Modify**.
3. Enter URIs. Resources on the specified static URIs use static acceleration and are cached in the edge node.



5 Node Cache Settings

5.1 Set HTTP header

Introduction

Parameter	Description
Content-Type	Specifies the content type of a client response object.
Cache-Control	Specifies the caching method followed by client requests and responses.
Content-Disposition	Specifies the default file name for activating the file download settings when the client responds to objects.
Content-Language	Specifies the language for the client to respond to objects.
Expires	Specifies the expiration time for the client to respond to objects.
Access-Control-Allow-Origin	Specifies the sources of allowed cross-origin requests.
Access-Control-Allow-Methods	Specifies the method of allowed cross-origin requests.
Access-Control-Max-Age	Specifies the caching duration for the client program to return results for an origin fetch request for a specific resource.
Access-Control-Expose-Headers	Specifies custom header information of allowed access.

You can set an HTTP response header. Currently, nine HTTP request header parameters are available for customization. The parameters are as follows:

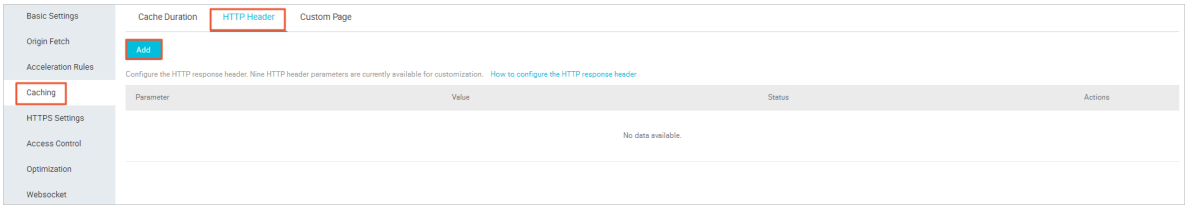
Restrictions and guidelines

- The configuration of HTTP response header will affect the response actions of all resources' client program under the DCDN domain name, rather than the actions of the cache server.
- Currently, you can set the HTTP head only to the above mentioned parameters. To request other HTTP header parameter settings, open a ticket.

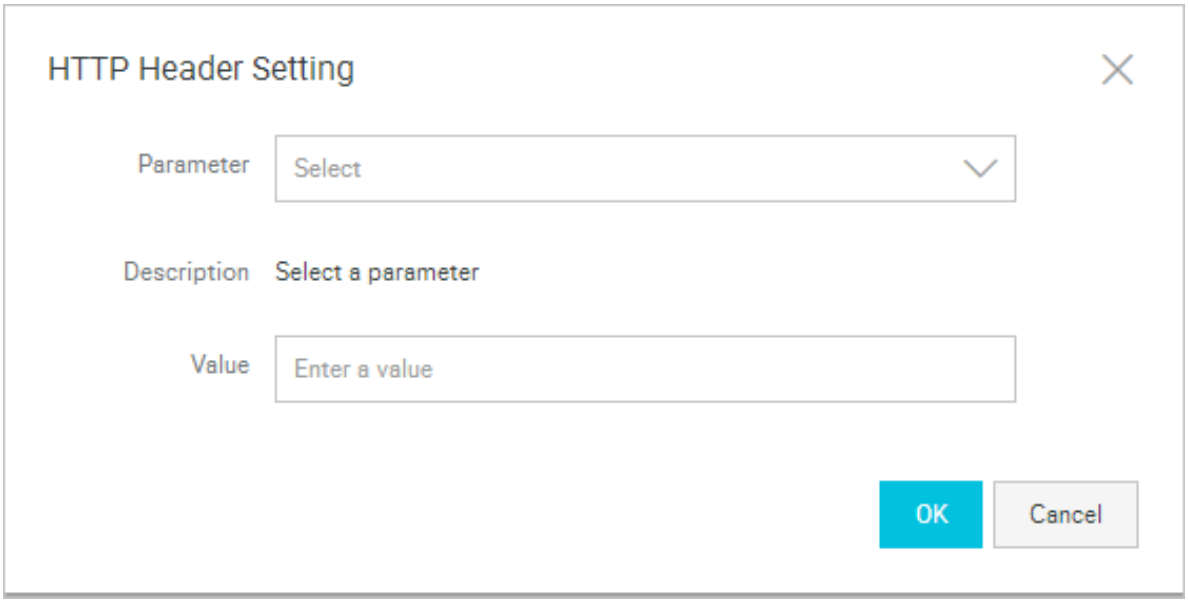
- You can enter * to indicate all domain names or enter an absolute domain name for the **Access-Control-Allow-Origin** parameter. For example: www.aliyun.com. Currently, wildcard domain names are not supported.

Procedure

1. On the **Domain Names** page, select a domain name, and click **Configure**.
2. Go to **Caching** > **HTTP Header**, and click **Add**.



3. You can set custom parameters for the HTTP header.



6 HTTPS Configuration

6.1 Force redirect

Introduction

When **SSL acceleration** is enabled for a DCDN domain, DCDN can redirect user requests according to the force redirect setting.

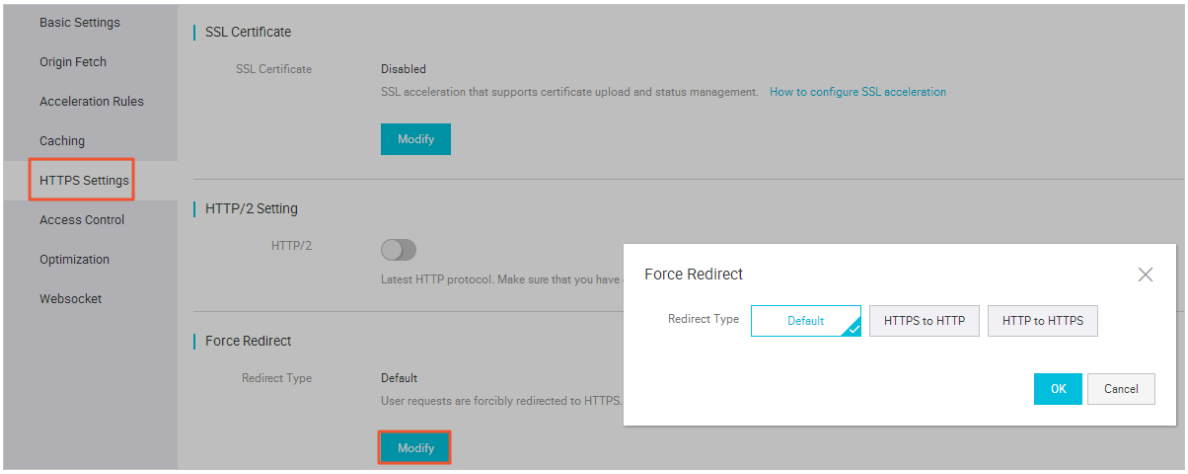
For example, you set the redirect type to **HTTP to HTTPS**. When the user initiates an HTTP request, the server returns a 302 redirect response, and the original HTTP request is redirect to the HTTPS, as shown in the following figure:

Note:

- For the force redirect setting to take effect, make sure that **SSL acceleration** has been enabled. You can redirect HTTP to HTTPS or redirect HTTPS to HTTP.
- User request are not redirected by default.

Procedure

1. On the **Domain Names** page, select a domain name, and click **Configure**.
2. Go to **HTTPS Settings** > **Force Redirect**, and click **Modify**.
3. Select a Redirect Type.



- The force redirect setting is optional. The default setting supports both HTTP and HTTPS requests.
- The options are Default, HTTPS to HTTP, HTTP to HTTPS.

- HTTP to HTTPS: HTTP requests are redirected to HTTPS.
- HTTPS to HTTP: HTTPS requests are redirected to HTTP.

6.2 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 *DCDN console*.
2. On the **Domain Names** page, select a domain name and click **Configure**.

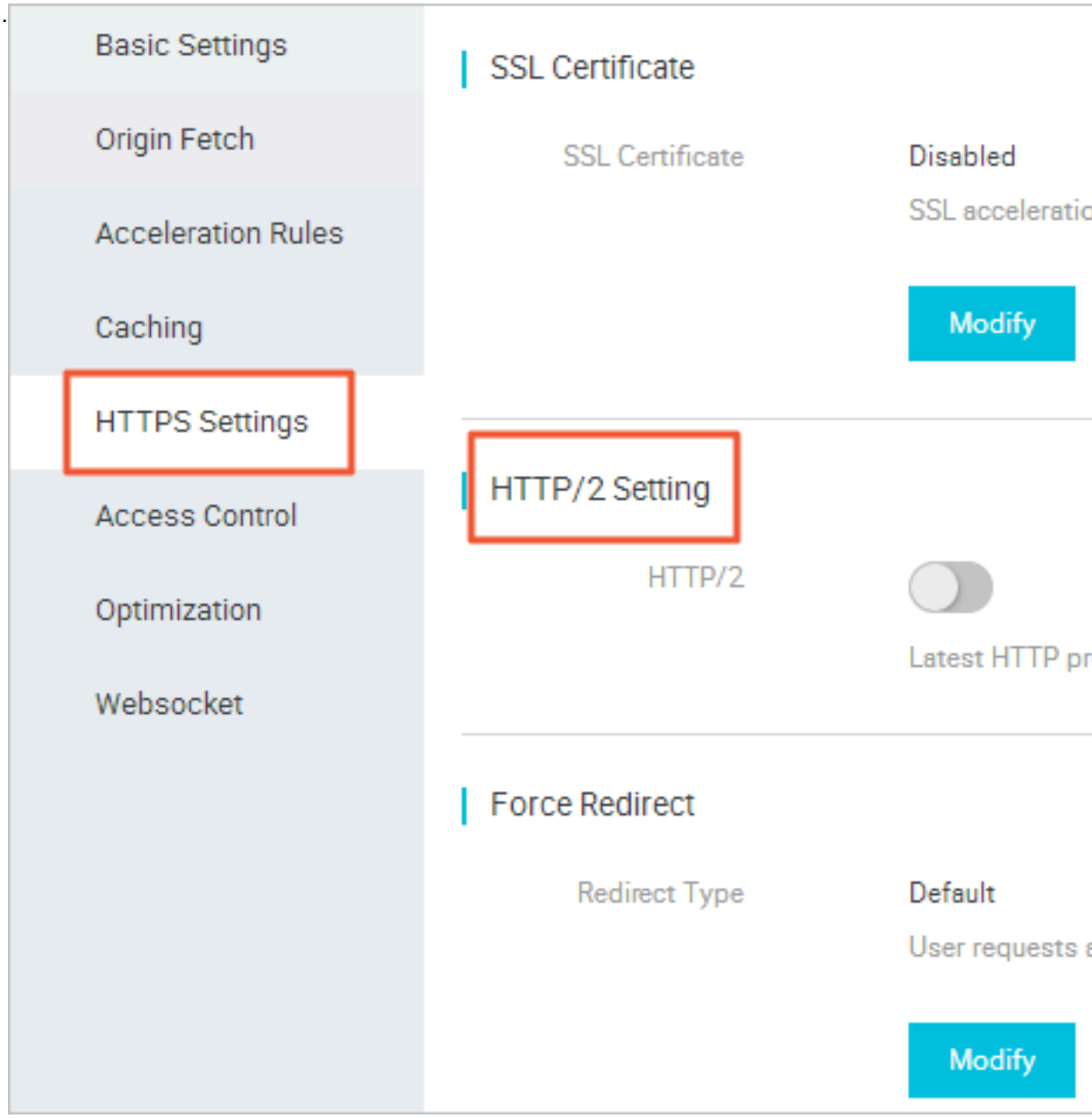
Note:

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**.



7 Access Control

7.1 IP blacklist and whitelist

Introduction

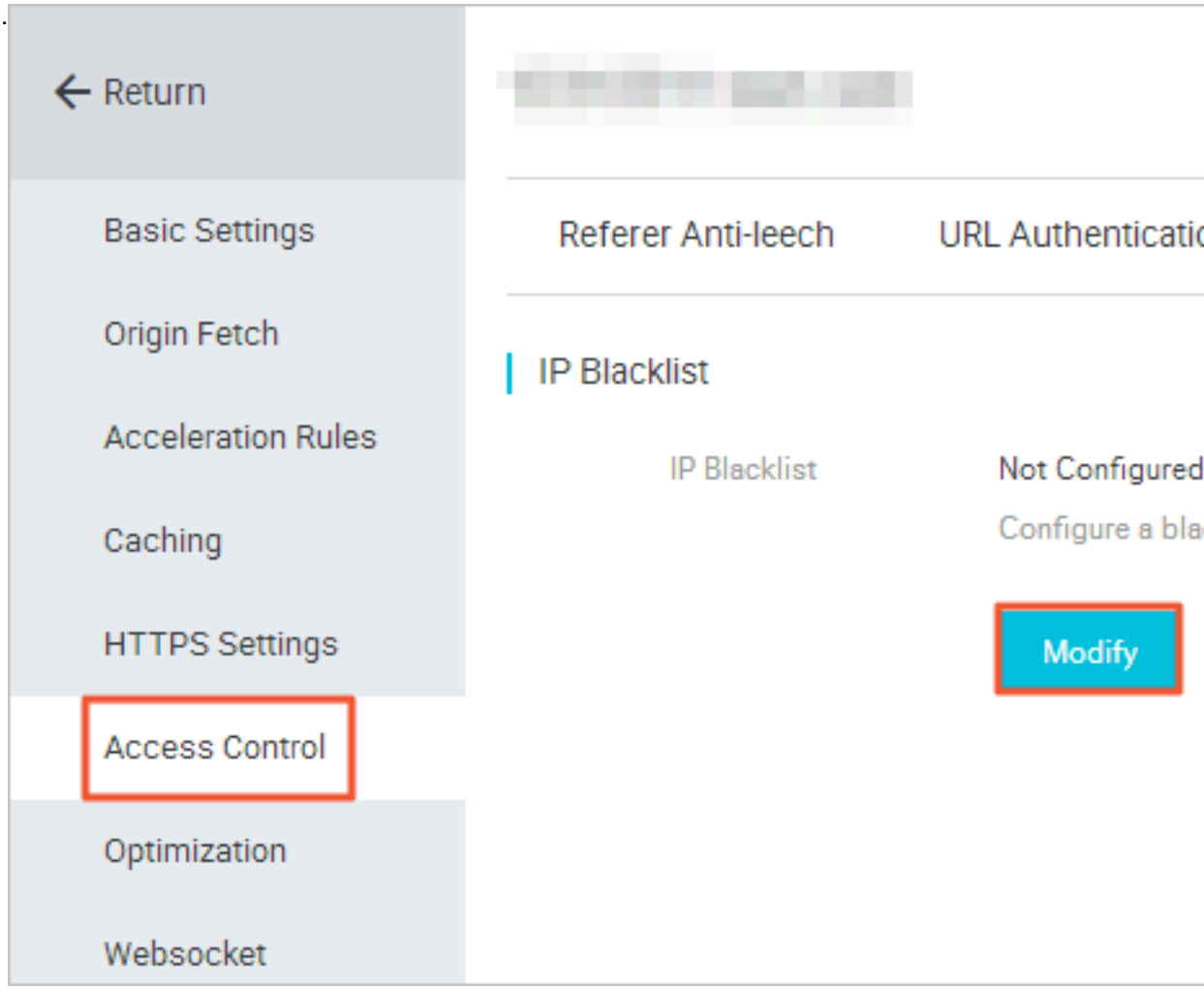
DCDN supports blacklist rules. An IP address that is listed on the blacklist cannot access the corresponding domain.

- IP blacklist currently supports blacklisting entire IP address ranges, for example: 127.0.0.1/24.
- For example, 127.0.0.1/24. 24 indicates that the first 24 bits in the subnet mask are used as effective bits,and 32-24=8 bits are used to express host numbers. In this way, the subnet can accommodate 2 ^ 8-2 = 254 hosts. 127.0.0.1/24 indicates the IP network segment in the range of 127.0.0.1 to 127.0.0.255.

Procedure

1. On the **Domain Names** page, select a domain name and click **Configure**.

2. Go to **Access Control** > **IP Blacklist**, and click **Modify**.



3. Configure the IP blacklist and then click OK.

7.2 Referer anti-leech

Introduction

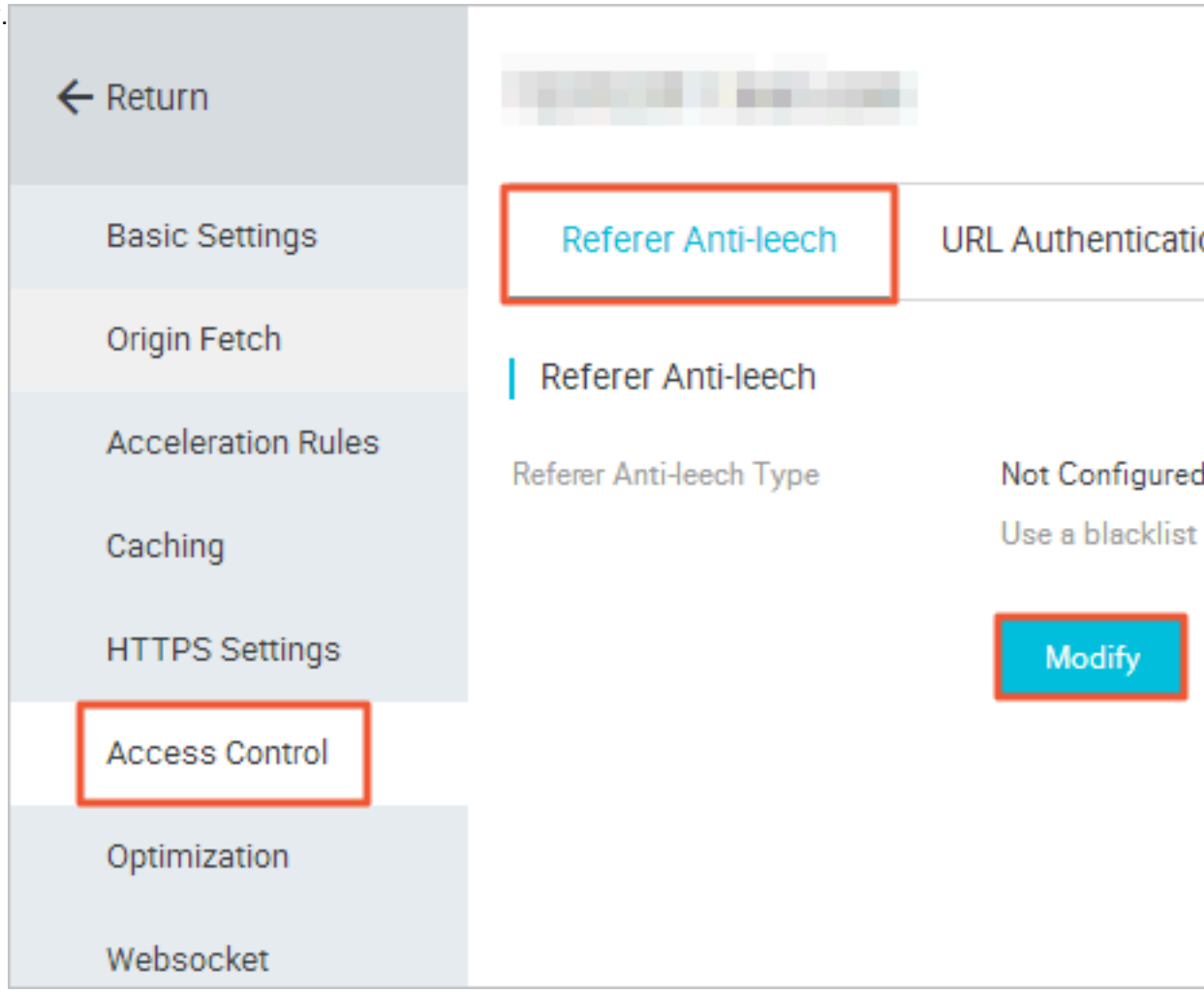
- The anti-leech feature is based on the referer information supported by HTTP. It uses the referer to track, identify, and judge sources. Users can configure the referer blacklist and whitelist for accesses to identify and filter a visitor's identity, limiting their access to DCDN resources.
- The anti-leech feature supports blacklist or whitelist. After a visitor initiates a request for a resource, the request reaches the DCDN node. The DCDN node filters the visitor's identity according to the preset anti-leech blacklist or whitelist. Visitors with an identity that is either included in the whitelist or not excluded in the blacklist can obtain the resource. Otherwise, the visitor request is rejected and a 403 response code is returned.

Restrictions and guidelines

- The anti-leech feature is disabled by default. You can configure it as needed.
- Blacklist and whitelist are mutually exclusive. You can use this feature to edit only the referer blacklist or whitelist at a time.
- You can set whether to allow **empty referer field** to access DCDN resources. This allows direct access to the resource URL from the browser address bar.
- After configuration, support for wildcard domains is automatically added. For example, if you enter example.com, the effective configuration is *.example.com, applying to all subdomains of example.com.

Procedure

1. On the **Domain Names** page, select a domain name and click **Configure**.
2. Go to **Access Control** > **Referer Anti-leech**, and click **Modify**.



3. Configure a **Blacklist** or **Whitelist**.

8 Performance Optimization

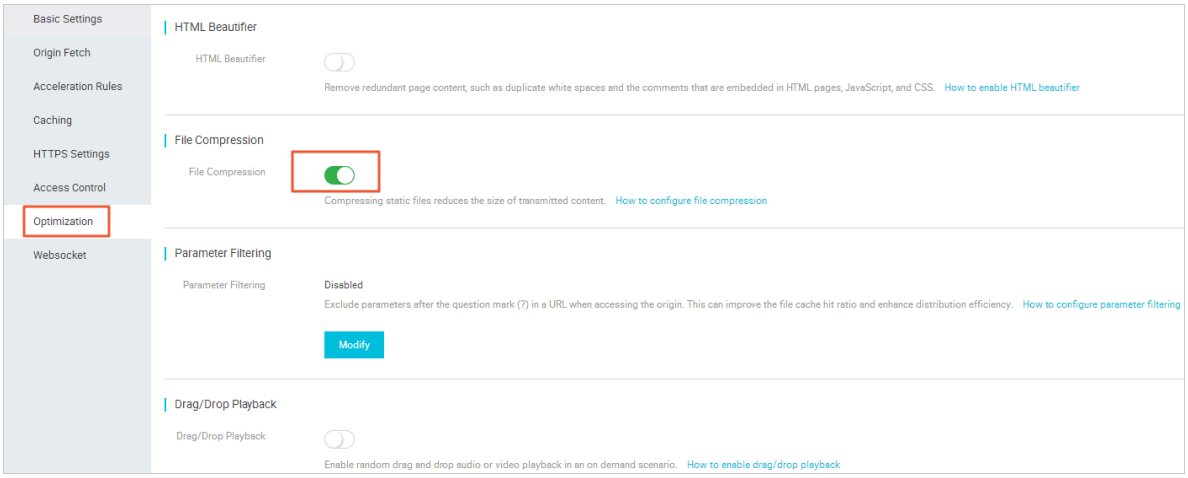
8.1 Intelligent compression

Introduction

- The file compression feature can be used to compress majority of static files in order to reduce the size of content transmitted by users, accelerating content delivery.
- The currently supported compression formats are: content-type: `content-type:text/xml`, `text/plain`, `text/css`, `application/javascript`, `application/x-javascript`, `application/rss+xml`, `text/javascript`, `image/tiff`, `image/svg+xml`, and `application/json`.

Procedure

1. On the **Domain Names** page, select a domain name, and click **Configure**.
2. Go to **Optimization** > **File Compression** to enable this function.



8.2 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. Files of MP4 and FLV format are supported.

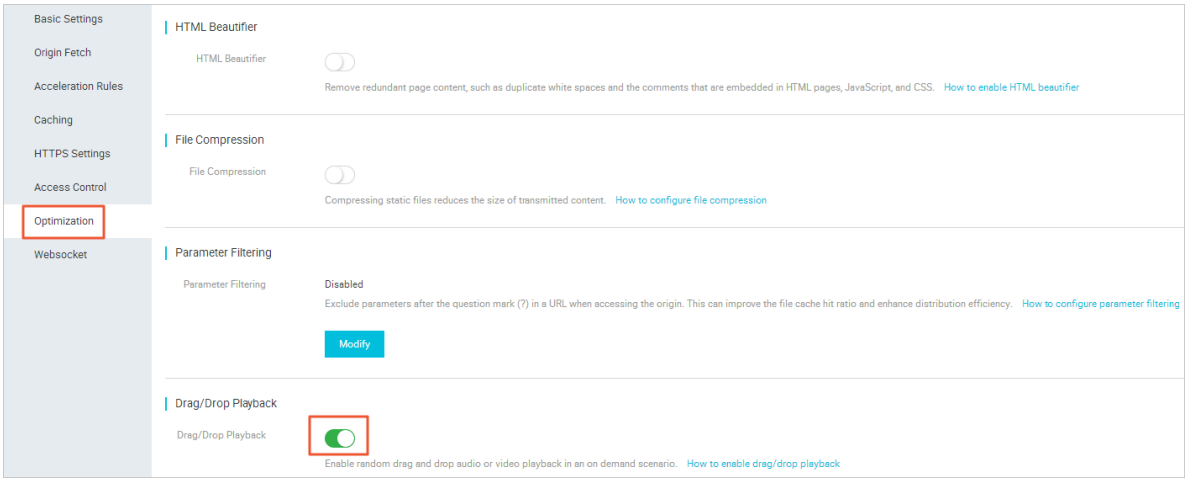
File Format	Meta Information	start Parameter	Example
MP4	Meta information of an origin site video must be contained in the file header. A video with its meta information contained in the file tail is not supported.	The start parameter specifies the time in seconds. Decimals are supported to indicate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

Note

- To use the drag/drop playback feature, 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.
- Files of MP4 and FLV format are supported.
- Currently, flv format only supports audio aac and video avc coding formats. Drag and drop are not supported for other coding formats.

Procedure

1. On the **Domain Names** page, select a domain, and click **Configure**.
2. Go to **Optimization >** > **Drag/Drop Playback** to enable this function.



8.3 Filter parameters

Introduction

When a URL request that carries a question mark (?) and request parameters is sent to a CDN node, the CDN node determines whether to send the request to the origin site.

- If parameter filtering is enabled, 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.
- If parameter filtering is disabled, different copies are cached on the CDN node for different URLs.

Recommendations

- An HTTP request typically contains the parameters. If the content of a parameter has low priority and the parameter overview file can be ignored, we recommend that you enable the parameter filtering. This improves the file cache hit rate and the delivery efficiency.
- If a parameter carries important information, for example, the file version information, we recommend that you set it as a reserved parameter. The system supports multiple reserved parameters. If the request contains any reserved parameters, the reserved parameters are included in the request to the origin site and are not ignored.

Usage example

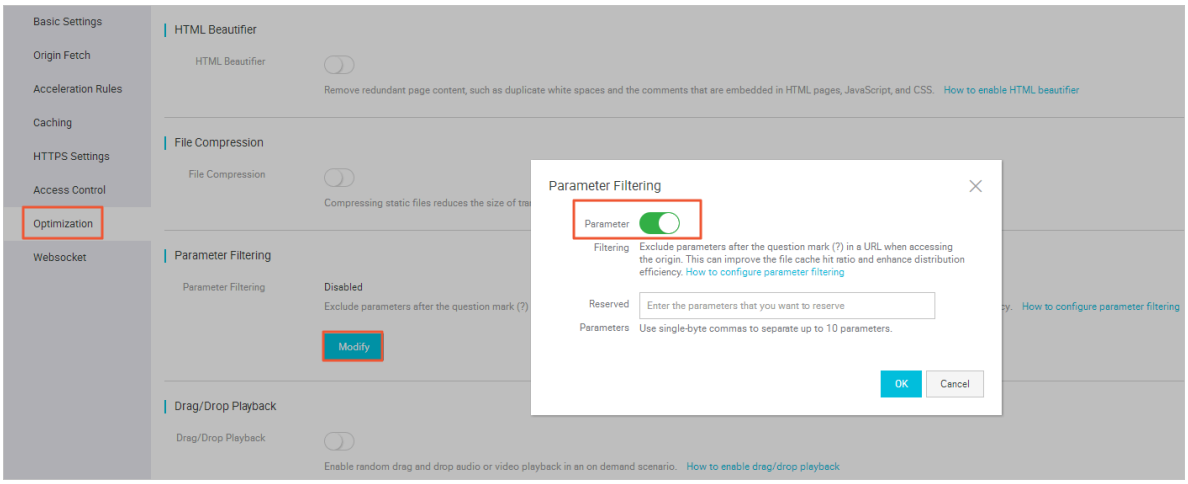
For example: `http://www.abc.com/a.jpg?x=1`. Request the URL to the CDN node.

- Using the parameter filtering feature, the CDN node initiates a request `http://www.abc.com/a.jpg` to the origin site ignoring parameter x=1.

- After the origin site responds to the request, the response arrives at the CDN node. The CDN node keeps a copy and continues to respond the content of `http://www.abc.com/a.jpg` to the terminal. All similar requests `http://www.abc.com/a.jpg?parameters` respond the content of the CDN copy `http://www.abc.com/a.jpg`.
- After you have disabled the parameter filtering feature, each URL caches a different copy on the CDN node. For example, different response content will be returned for `http://www.abc.com/a.jpg?x=1` and `http://www.abc.com/a.jpg?x=2` from the origin site.

Procedure

1. On the **Domain Names** page, select a domain, and click **Configure**.
2. Go to **Optimization** > **Parameter Filtering**, and click **Modify**.
3. Click the **Parameter Filtering** switch.



8.4 Page optimization

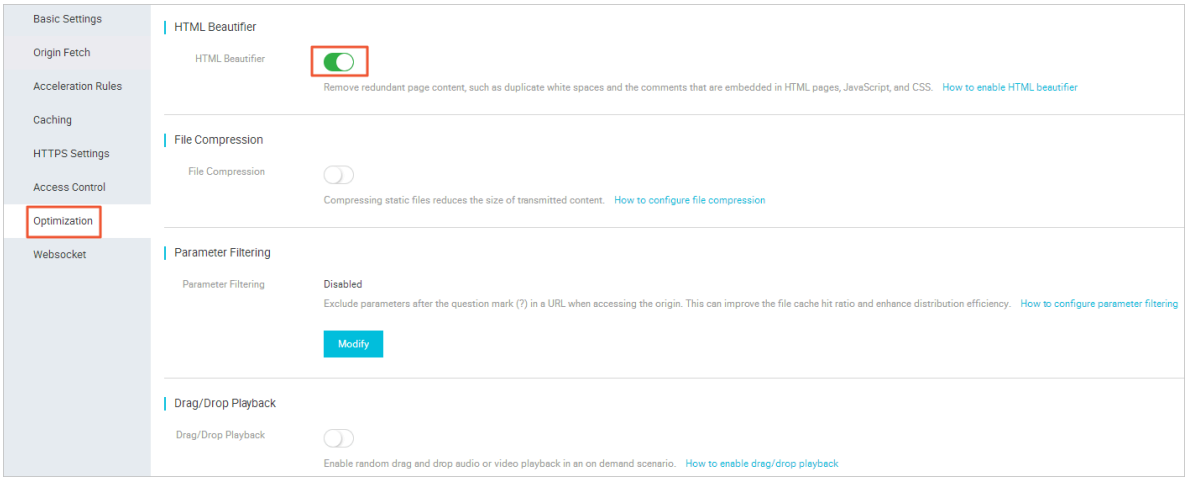
Introduction

The HTML beautifier feature allows you to delete comments and duplicate blank spaces in webpage HTML. This can reduce the file size by removing redundant content from the page and improve the acceleration distribution efficiency.

Procedure

1. On the **Domain Names** page, select a domain name, and click **Configure**.
2. Go to **Optimization** > **HTML Beautifier** to enable HTML Beautifier.

3.


Basic Settings
Origin Fetch
Acceleration Rules
Caching
HTTPS Settings
Access Control
Optimization
Websocket
HTML Beautifier
HTML Beautifier
Remove redundant page content, such as duplicate white spaces and the comments that are embedded in HTML pages, JavaScript, and CSS. How to enable HTML beautifier
File Compression
File Compression
Compressing static files reduces the size of transmitted content. How to configure file compression
Parameter Filtering
Parameter Filtering
Disabled
Exclude parameters after the question mark (?) in a URL when accessing the origin. This can improve the file cache hit ratio and enhance distribution efficiency. How to configure parameter filtering
Modify
Drag/Drop Playback
Drag/Drop Playback
Enable random drag and drop audio or video playback in an on demand scenario. How to enable drag/drop playback

9 Websocket

This document describes the technical details, benefits, and applicable scenarios of Websocket and how to use Websocket.

What is Websocket

WebSocket is a protocol for creating a bi-directional message exchange between browsers and servers over a persistent TCP connection. WebSocket supports full-duplex communications that allow the server to send data to the client actively. Therefore, WebSockets requires only one handshake to establish a bi-directional, full-duplex, persistent connection from a web browser to a server. This makes the message exchange between clients and servers much simpler.

Benefits

- Short header: The data exchanged between clients and servers contains a very short header. The header has a minimum size of 2 Bytes.
- Instead of returning data after receiving a request from the browser, the server actively pushes data to the browser when new data is available.

Many websites are using Ajax polling to facilitate push technologies. With the polling technique , the browser sends HTTP requests to the server at specific intervals, for example, every one second, and the server returns the most recent data to the browser of the client.

The disadvantage of this model is that the browser has to send the HTTP request to the server every time a request occurs. However, the HTTP request can have a long header, and the valid data can be only a small part of the header. Sending such HTTP requests is a waste of bandwidth and other resources. The WebSocket protocol defined by HTML5 can conserve server resources and bandwidth, and facilitate real-time communication.

The WebSocket protocol defined by HTML5 can conserve server resources and bandwidth, and facilitate real-time communication.

Scenarios

- Live comments

  End user A sends a live comment through a mobile phone. At the same time, the user A wants to view live comments sent by other clients on the mobile phone. In this scenario, you can use Websocket to push the live comments sent by other clients to the mobile phone of the user A. So the user A can also view the live comments sent by other users.

- Online education

  In one-to-many online education, the teacher can use Websocket to push the notes and syllabuses edited on the teacher's client to the students' clients in real time.

- Real-time quotes for financial products

  The price of financial products such as stocks and gold changes quickly. With Websocket, the real-time price of financial products can be pushed to clients around the world to help traders make quick trading decisions.

- Live sportscast

  Live sportscast is the top concern for numerous sports lovers all over the world. Websocket allows for real-time updates in live sportscast to ensure the best viewing experience.

- Video conferences

  Video conferences are widely used in multiple scenarios. In a video conference, participants join the conference through multiple ends. Websocket helps to deliver real-time information to these participants.

- Geo-location-based applications

  An increasing number of developers are using the GPS feature of mobile devices to facilitate geo-location-based applications. If you have kept a record of the end user's location, for example, the user's movement trails recorded by an app, you can use Websocket to collect more detailed data.

Activate Websocket

You must first specify the billing method of Websocket and wait until the billing method takes effect before you use Websocket.

1. Log on to the *DCDN console*.
2. Click **Change Billing Method**.
3. Click **Activate** to activate Websocket.
4. Wait until Websocket is activated.

Note:

- If you are a new user, the billing of Websocket takes effect immediately.
- If you have purchased Websocket before, when the billing method is **Pay By Day**, Websocket takes effect on the next natural day. When the billing type is **Pay By Month**,

Websocket takes effect at 00:00 on the first day of the next month. Keep the current billing items if the billing method has not changed.

For more information about Websocket billing, see *Billing methods*.

Use Websocket

You can configure Websocket after it takes effect.

1. On the **Domain Names** page, select a domain name, and click **Configure**.
2. In the left-side navigation pane, click **Websocket**.
3. Click the Websocket toggle, and set the interval for sending and receiving heartbeats and specify the protocol used for sending back-to-origin requests.

Note:

The interval is set to 60 seconds by default. The protocol used for sending back-to-origin requests is not specified by default. Specify it based on your needs.

- Heartbeat interval: A heartbeat is a periodic signal generated to indicate normal operation . The client sends a message to the server at intervals to indicate the status of the client. The server returns a message to the client to indicate the status of the server. In this way, the client and the server can know whether the other end is connected properly. The time between heartbeat flows is referred to as a heartbeat interval.
- The protocol type used for sending back-to-origin requests can be HTTP, HTTPS, or Follow .

Websocket statistics

Granularity supported by different statistics types on multiple time dimensions are as follows:

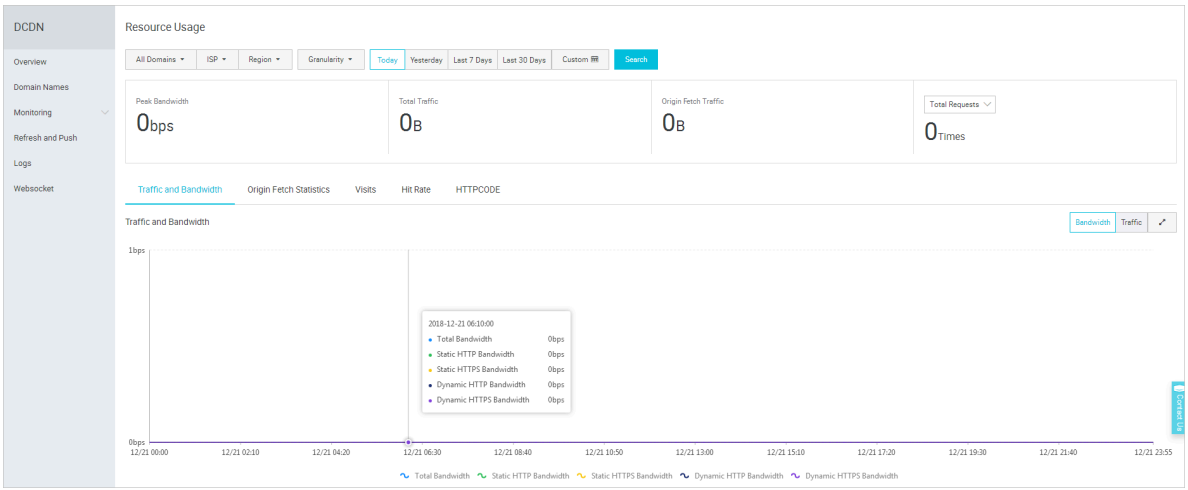
Type of statistics	Within 3 days	4 - 31 days	Greater than or equal to 32 days
Bandwidth and traffic statistics	Five minutes or one hour	One hour or one day	One day
HTTP code statistics			

Queries by region, service provider, domain name, and time range are supported. You can query a maximum time range of three months.

10 Resource monitoring

Functions

- Resource monitoring covers traffic bandwidth, origin fetch statistics, access times, hit rate, and HTTP code. Users can search for information by domain name, region, ISP, time granularity, and custom time interval.
- Users can download detailed raw data, such as network bandwidth, traffic, traffic percentage of domain names, visitor regions, and ISPs.
- The resource monitoring data is different from the billing data. For example, a 30-day statistical curve takes a granularity of 14,400 seconds, but the billing statistical curve takes a granularity of 300 seconds. 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:

The granularity of raw data changes according to the time interval. Data exported by day has a granularity of 300 seconds, and the data exported by week and month have granularities of 3600 seconds and 14,400 seconds, respectively .