

ALIBABA CLOUD

Alibaba Cloud

全站加速

Service Management

Document Version: 20201225

 Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions


Style	Description	Example
 Danger	A danger notice 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.
 Warning	A warning notice 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 restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.Features	05
2.Data monitoring	07
2.1. View the information about resource usage	07
2.2. Real-time monitoring	08
2.3. Statistical analysis	08
3.Logs	10
3.1. Download offline logs	10
3.2. Service-linked role for log delivery	11
4.Tool Management	15
4.1. Refresh and prefetch	15
4.2. Certificate Center	17
4.2.1. Configure an HTTPS certificate for multiple domain na...	17
4.2.2. Query domain name certificates	19
5.Real-time log delivery	21
5.1. Overview	21
6.WebSocket	22
6.1. What is WebSocket?	22
6.2. Configure the WebSocket protocol	23

1.Features

DCDN provides the service management module to support the monitoring, statistical analysis, refresh and prefetch, and log analytics features in the console. You can use these features to manage resources that are accelerated by DCDN. These features allow you to effectively analyze the status of DCDN in real time and make informed business decisions at the earliest opportunity.

 **Note** This topic describes the DCDN features that are classified into domain name management and service management. This allows you to understand and obtain up-to-date information about DCDN, this topic describes DCDN features. Features in the DCDN console are divided into domain name management and service management.

The following table describes the features of service management.

Feature	Documentation	Description	Default setting
Data monitoring	View the information about resource usage	You can view the information about the resource usage of all your domains for the current account and analyze the data to make informed business decisions. The usage data includes network traffic, bandwidth usage, back-to-origin traffic, the number of requests for static or dynamic content, cache hit ratio, and statistics of HTTP status codes.	None
	Real-time monitoring	You can view the basic data, back-to-origin statistics, and acceleration performance statistics of all your domains for the current account in real time. This allows you to make informed business decisions.	None
	Statistical analysis	You can view the statistics of accelerated domain names for the current day and the previous days for offline analysis. This allows you to obtain the up-to-date status information about your DCDN service.	None
Log management	Download offline logs	You can check logs by combining the following conditions: the time range and domain name. You can also download the logs.	None
Tools	Refresh and prefetch	The refresh feature allows you to force DCDN nodes to retrieve the latest files from the origins. The prefetch feature allows you to load frequently accessed resources to DCDN nodes before peak hours to accelerate content delivery.	None
	Configure an HTTPS certificate for multiple domain names at a time	DCDN supports HTTPS secure acceleration. You can upload a custom certificate or select a certificate from Alibaba Cloud SSL Certificates Service in the DCDN console. The certificate ensures data security during data transmission.	None

Feature	Documentation	Description	Default setting
Websocket	Configure the WebSocket protocol	You can enable WebSocket to minimize the usage of server and bandwidth resources and to facilitate real-time communication.	Disabled

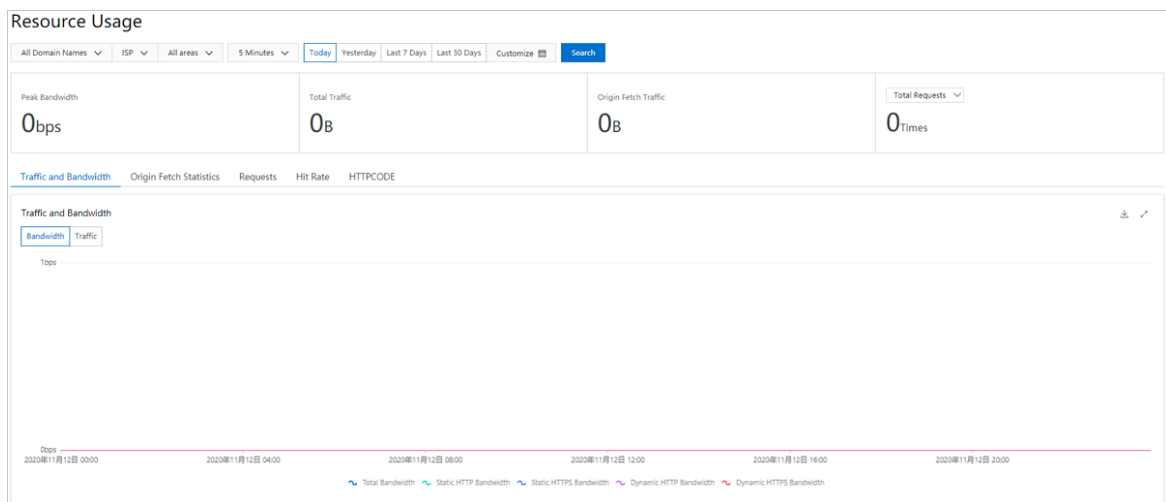
2.Data monitoring

2.1. View the information about resource usage

You can view the information about the resource usage of all your domains for the current account and analyze the data to make informed business decisions. The usage data includes network traffic, bandwidth usage, back-to-origin traffic, the number of requests for dynamic and static content, cache hit ratio, and statistics of HTTP status codes. This topic describes how to view the information about resource usage.

Procedure

1. Log on to the [DCDN console](#).
2. In the left-side navigation pane, choose **Monitoring > Resource Usage**.
3. On the **Resource Usage** page, select the monitoring item and metric that you want to view, and click **Search**.



You can check the details about the metrics by combining the following conditions: **domain name, ISP, region, and time range**. You can also download the required metric data for statistical analysis.

Item	Metric
Traffic and Bandwidth	Total bandwidth usage and network traffic, HTTP bandwidth usage and network traffic for static content, HTTPS bandwidth usage and network traffic for static content, HTTP bandwidth usage and network traffic for dynamic content, and HTTPS bandwidth usage and network traffic for dynamic content

Item	Metric
Origin Fetch Statistics	Total bandwidth usage and network traffic for back-to-origin requests, the bandwidth usage and network traffic of HTTP back-to-origin requests for static content, the bandwidth usage and network traffic of HTTPS back-to-origin requests for static content, the bandwidth usage and network traffic of HTTP back-to-origin requests for dynamic content, and the bandwidth usage and network traffic of HTTPS back-to-origin requests for dynamic content
Requests	Total requests and Query Per Second (QPS), HTTP requests and QPS for static content, HTTPS requests and QPS for static content, HTTP requests and QPS for dynamic content, and HTTPS requests and QPS for dynamic content
Hit Rate	Byte hit ratio and request hit ratio
HTTPCODE	Error codes 200, 301, and 403

2.2. Real-time monitoring

The real-time monitoring feature allows you to view the basic data, back-to-origin traffic, and acceleration performance statistics of all the domains for the current account in real time. This helps you make informed business decisions at the earliest opportunity. This topic describes the metrics for real-time monitoring in Dynamic Route for CDN (DCDN). This topic also describes how to view the metrics in the DCDN console.

Procedure

1. Log on to the [DCDN console](#).
2. In the left-side navigation pane, choose **Monitoring > Real-time Monitoring**.
3. On the **Real-time Monitoring** page, select the monitoring item and metric that you want to view, and click **Search**.

You can check the details about the metrics by combining the following conditions: **domain name**, **Region**, **Carrier**, and **time range**. The time range can be **Last 1 Hour**, **Last 6 Hours**, **Last 12 Hours**, or **Customize**.

Item	Metric
Basic Data	Bandwidth, Traffic, Requests, and QPS
Back-to-Origin Traffic	Back-to-Origin Bandwidth and Back-to-Origin Traffic
Quality Monitoring	Request Hit Ratio, Byte Hit Ratio, 4xx HTTP Status Codes, 5xx HTTP Status Codes, 3xx HTTP Status Codes, and 2xx HTTP Status Codes

2.3. Statistical analysis

You can use the statistical analysis feature to view and analyze the statistics of accelerated domain names for the current day and the previous days for offline analysis. This helps you obtain the up-to-date status information about your Dynamic Route for CDN (DCDN) service.

Context

The statistical analysis module displays the following monitoring items: **PV/UV**, **Regions and Carriers**, **Domains**, **Top Referers**, and **Top URLs**. You can export detailed raw data such as network bandwidth, network traffic, domain name rankings by traffic proportion, and request distribution by visitor or Internet service provider (ISP).

 **Note** The time granularity of raw data collection varies based on the time range. The time granularity is 300 seconds for daily export tasks, 3,600 seconds for weekly export tasks, and 14,400 seconds for monthly export tasks.

Procedure

1. Log on to the [DCDN console](#).
2. In the left-side navigation pane, choose **Monitoring > Statistics Analysis**.
3. On the **Statistics Analysis** page, select the monitoring item and metric that you want to view, and click **Search**.

Item	Monitoring metric	Time range
PV/UV	The distribution of page views (PVs) and unique visitors (UVs) for the specified domain name.	Today, Yesterday, Last 7 Days, and Customize.
Regions and Carriers	Rank, Region, Total Traffic, Traffic Proportion, Visits, Visits (%) , and Response Time .	Today, Yesterday, Last 7 Days, and Customize.
Domains	Rank, Proportion, Peak Traffic / Peak Bandwidth, Peak Time , and Visits for each accelerated domain name.	Today, Yesterday, Last 7 Days, and Customize.
Top Referers	The referer traffic, Traffic Proportion, Visits , and Visits (%) for a specified domain name.	A date within the last three months.
Top URLs	URL traffic, Traffic Proportion, Visits , and Visits (%) for a specified domain name.	A date within the last three months.

3.Logs

3.1. Download offline logs

If failures or attacks occur when you use Dynamic Route for CDN (DCDN) to accelerate your domain names, you can troubleshoot issues based on log files. You can view operational logs for all the domain names that belong to the current account and download the logs to your on-premises storage. This topic describes the usage notes and the field formats of logs, and also how to view logs.

Context

Usage notes of logs:

- Log update delay: Log data is generated within 24 hours after an event occurs. However, in some cases, the log data may be generated after 24 hours.
- By default, you can download logs that are generated for up to 30 days. If you want to store logs for a longer period, use Log Service and save logs to Object Storage Service (OSS) buckets under your account.
- Log naming rules: accelerated domain name_year_monthh_day_start time_end time. Example: `www.test.com_2019_12_02_010000_020000.gz`.

Field formats of logs

- Sample log entry

```
[9/Jun/2019:01:58:09 +0800] 192.168.15.75 - 1542 "-" "GET http://www.aliyun.com/index.html" 200 191 283 0 MISS "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)" "text/html"
```

- Fields

Field	Description
<code>[9/Jun/2019:01:58:09 +0800]</code>	The start time of the log entry.
<code>192.168.15.75</code>	The IP address of the client that initiated the request.
<code>-</code>	The proxy IP address of the client.
<code>1542</code>	The response time of a request in milliseconds.
<code>"-"</code>	The referer header field in the HTTP request.
<code>GET</code>	The request method.
<code>http://www.aliyun.com/index.html</code>	The Uniform Resource Identifier (URI) of the request. No domain name information is included.

Field	Description
200	The HTTP status code.
191	The size of the request packet. Unit: bytes.
2830	The size of the response packet. Unit: bytes.
MISS	The cache hit status.
Mozilla/5.0(compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)	The information about the proxy of the client.
text/html	The type of the requested file.

Procedure

1. Log on to the [DCDN console](#).
2. In the left-side navigation pane, choose **Logs > Offline Log**.
3. On the **Offline Log Download** tab, select a domain name and a date, and then click **Search**.
4. Find the log file that you want to download and click **Download** in the **Actions** column.

3.2. Service-linked role for log delivery

When you enable the offline log delivery feature in Dynamic Route for CDN (DCDN), the system automatically creates the service-linked role `AliyunServiceRoleForDCDNLogDelivery` and grants the service-linked role the permissions to access resources in Object Storage Service (OSS) and Data Lake Analytics (DLA).


Overview

`AliyunServiceRoleForDCDNLogDelivery` is a service-linked role (SLR) of DCDN. When you enable the offline log delivery feature in DCDN, DCDN must assume the service-linked role to access resources in OSS and DLA. This allows DCDN to save log data to other services. Make sure that the geographic location where the log data is stored complies with the regulations. For more information, see [Service linked roles](#).

Create the service-linked role

If this is the first time you enable the offline log delivery feature in DCDN, the system automatically creates the service-linked role `AliyunServiceRoleForDCDNLogDelivery` and attaches the permission policy `AliyunServiceRoleForDCDNLogDelivery` to the service-linked role. DCDN can assume the service-linked role to access OSS and DLA after the offline log delivery feature is enabled. You can perform the following operations in OSS and DLA:

- OSS: Create and query OSS buckets, write to OSS buckets, query data in OSS buckets, and delete data from OSS buckets.
- DLA: Enable, query, and disable DLA tasks.

 **Note** If DCDN has assumed the service-linked role AliyunServiceRoleForDCDNLogDelivery, the system does not create the service-linked role again.

The following code block shows the content of the permission policy:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "openanalytics:CreateInstance",
        "openanalytics:UpgradeInstance",
        "openanalytics:ReleaseInstance",
        "openanalytics:ExecuteSQL",
        "openanalytics:QueryExecute",
        "openanalytics:DescribeVirtualCluster",
        "openanalytics:ListSparkJob",
        "openanalytics:GetJobStatus",
        "openanalytics:GetJobDetail",
        "openanalytics:GetJobLog",
        "openanalytics:KillSparkJob",
        "openanalytics:SubmitSparkJob"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "oss:PutBucket",
        "oss:GetBucketInfo"
      ],
      "Effect": "Allow",
      "Resource": "acs:oss:*:*:alicdn-log-delivery-*"
    },
    {
      "Action": [
        "oss:GetObject",
        "oss:PutObject"
      ],
      "Effect": "Allow",
      "Resource": "acs:oss:*:*:alicdn-log-delivery-*/alicdn-offline-log/*"
    }
  ]
}
```


```
},
{
  "Action": "ram:CreateServiceLinkedRole",
  "Resource": "*",
  "Effect": "Allow",
  "Condition": {
    "StringEquals": {
      "ram:ServiceName": "openanalytics.aliyuncs.com"
    }
  }
},
{
  "Action": "ram>DeleteServiceLinkedRole",
  "Resource": "*",
  "Effect": "Allow",
  "Condition": {
    "StringEquals": {
      "ram:ServiceName": "logdelivery.dcdn.aliyuncs.com"
    }
  }
}
]
```

Delete the service-linked role

If you no longer use the offline log delivery feature for DCDN and want to delete the service-linked role `AliyunServiceRoleForDCDNLogDelivery`, perform the following steps.

1. Close the offline log delivery task.
 - i. Log on to the [DCDN console](#).
 - ii. In the left-side navigation pane, choose **Logs > Offline Log**.
 - iii. On the **Logs** page, click the **Offline Log Delivery** tab.
 - iv. Click **Close Delivery Task**.
 - v. Click **OK**.
2. Delete the service-linked role.
 - i. Log on to the [RAM console](#).
 - ii. In the left-side navigation pane, click **RAM Roles**.

- iii. In the **RAM Role Name** column, find the service-linked role `AliyunServiceRoleForDCDNLogDelivery` and click **Delete**.

 **Note** If the service-linked role fails to be deleted, check whether the offline log delivery task has been closed.

4.Tool Management

4.1. Refresh and prefetch

Dynamic Route for CDN (DCDN) allows you to refresh and prefetch resources from origin servers. The refresh feature allows you to force DCDN nodes to retrieve the latest files from the origin servers. The prefetch feature allows you to load frequently accessed resources to DCDN nodes before peak hours to improve the efficiency of resource accesses. This topic describes how to configure the refresh and prefetch features and how to view refresh and prefetch records.

Context

The following section describes the concepts of refresh and prefetch in DCDN:

- Refresh: After a URL refresh or directory refresh request is submitted, the requested resource that is cached on the DCDN nodes forcibly expires. When a DCDN node receives a request for the resource, the node retrieves the resource from origin servers. Then, the DCDN node caches the resource and returns it to the requester. The refresh feature reduces the cache hit ratio.
- Prefetch: After a URL prefetch request is submitted, the origin server automatically caches the resource for the URL to DCDN nodes. When a DCDN node receives a request for the resource for the first time, the node returns the resource from the cache. This eliminates the need to retrieve the resource from the origin server. The prefetch feature increases the cache hit ratio.

The following table describes the refresh and prefetch features.

Category	How it works	Limit	Time to take effect
URL-based object refresh	DCDN nodes are forced to retrieve the latest versions of the specified files from origin servers.	Each URL must start with <code>http://</code> or <code>https://</code> . You can refresh up to 2,000 URLs with each Alibaba Cloud account per day. A maximum of 1,000 URLs can be submitted at a time.	Within five minutes
Directory-based object refresh	DCDN nodes are forced to retrieve the latest files in the specified directories from origin servers.	Each URL must start with <code>http://</code> or <code>https://</code> , and end with a forward slash <code>/</code> . You can refresh up to 100 directories with each Alibaba Cloud account per day. A maximum of 100 directories can be submitted at a time.	

Category	How it works	Limit	Time to take effect
URL-based object prefetch	DCDN fetches the specified resources from origin servers before DCDN receives requests for these resources and caches them to Layer 2 (L2) nodes. When these resources are requested for the first time, the L2 nodes return them from the cache.	Each URL must start with <code>http://</code> or <code>https://</code> . You can prefetch up to 500 URLs with each Alibaba Cloud account per day. A maximum of 100 URLs can be submitted at a time.	

Note The time that is required to complete a refresh or prefetch task is based on multiple factors. The factors include the file quantity, the file size, the bandwidth of origin servers, and network conditions.

Procedure

1. Log on to the [DCDN console](#).
2. In the left-side navigation pane, choose **Tools > Refresh and Prefetch**.
3. On the Refresh and Prefetch page, click the **Refresh Cache** tab and set the following parameters to refresh or prefetch resources based on your business requirements.

Note If you want to submit URLs by using a file when you configure the refresh or prefetch feature, the file must be in the TXT format.


Refresh and Push

Refresh Cache
Operation Records

Operation Type

Refresh Type

URL Daily URL refresh limit 2000, daily URL push limit 500, daily directory refresh limit 100. It takes about 5 minutes for a refresh operation to take effect.


 Enter texts or drag a file here.

500 Refresh Items Left

4. Click **Submit**.
5. Click the **Records** tab.
6. On the **Records** tab, specify a time range and an operation type, enter a domain name or a URL, and then click **Search**.

You can check the refresh and prefetch records, including the refreshed or prefetched object, type, time, status, and progress of each operation.

4.2. Certificate Center

4.2.1. Configure an HTTPS certificate for multiple domain names at a time

Dynamic Route for Content Delivery Network (DCDN) supports Hypertext Transfer Protocol Secure (HTTPS) acceleration. You can upload a custom certificate or select a certificate from Alibaba Cloud SSL Certificates Service in the DCDN console. The certificate ensures data security during transmission. This topic describes how to configure or update an HTTPS certificate for multiple domain names at a time.

Context

HTTPS is an HTTP channel that is designed to enhance security. The integration of HTTPS into DCDN secures content transmission. This allows clients to browse website content in a secure and efficient manner.

SSL certificate files must be in the PEM format. For more information about how to convert certificate files to the PEM format, see [Certificate formats](#).

HTTPS acceleration is a value-added service. After you enable HTTPS, the service is charged based on the number of HTTPS requests that DCDN has received. You cannot use DCDN data transfer plans to offset the fee. For more information about the HTTPS pricing, see [Requests billing](#).

Procedure

1. Log on to the [Dynamic Route for CDN console](#).
2. In the left-side navigation pane, click **Tools**. Then, click **Certificate Center**.
3. On the **Certificate Center** page, click **Add Certificate**.
4. On the **Add Certificate** pane, set the certificate parameters.

Parameter	Description
-----------	-------------

Parameter	Description
Certificate Source	<ul style="list-style-type: none"> ◦ SSL Certificates Service You can apply for certificates of various providers and types in the SSL Certificates Service console. ◦ Custom Certificate (Certificate + Private Key) If you cannot find a certificate that meets your requirements from the certificate list, upload a custom certificate. You must enter the certificate name, the public key, and the private key of the certificate. The certificate is saved to SSL Certificates Service. You can view information about the certificate in the SSL Certificates Service console. ◦ Free Certificate Free certificates are used only for HTTPS acceleration. You cannot manage free certificates or view the public or private keys of free certificates in the SSL Certificates Service console. <ul style="list-style-type: none"> ▪ A free certificate is issued within one to two business days after you apply for it. During this period of time, you can also upload a custom certificate or select a certificate from Alibaba Cloud SSL Certificates Service. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 10px; margin: 10px 0;"> <p>Note After you submit the application, the certificate may be issued within several hours or two business days. The amount of time it takes depends on the verification process that is required by the certificate authority.</p> </div> <ul style="list-style-type: none"> ▪ A free certificate is valid for one year. Before it expires, you do not need to apply for a new certificate each time you enable HTTPS acceleration. If the free certificate expires, you must apply for a new one. <p>You can switch between certificates from SSL Certificates Service, custom certificates, and free certificates.</p>
Certificate Name	You must specify the certificate name if you set Certificate Source to SSL Certificates Service or Custom Certificate (Certificate + Private Key) .
Certificate (Public Key)	This parameter is required if you set Certificate Source to Custom Certificate (Certificate + Private Key) . For more information, see PEM Encoding Reference below the Certificate (Public Key) field.
Private Key	This parameter is required if you set Certificate Source to Custom Certificate (Certificate + Private Key) . For more information, see PEM Encoding Reference below the Private Key field.

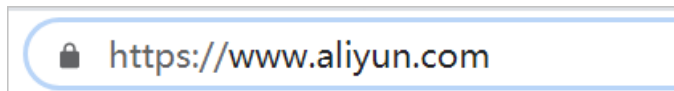
5. Click **Next**.
6. Associate domain names with the certificate.

Note If you use a certificate from SSL Certificates Service or a custom certificate, you can associate multiple domain names with the certificate at a time. If you use a free certificate, you can associate only one domain name with the certificate.

7. Click **OK** to deploy or update the certificate.

What to do next

After a certificate is uploaded, it takes effect within one minute. To verify that the HTTPS certificate takes effect, send HTTPS requests to access resources. If the URL is displayed with a lock icon in the address bar of the browser, HTTPS secure acceleration is working as expected.



Related API operations

You can call the related API operation to configure or update the certificate of a domain name. For more information, see [SetDcdnDomainCertificate](#).

Note If you want to update the certificates of multiple domain names, call this operation multiple times.

4.2.2. Query domain name certificates

This topic describes how to query the domain name certificates under your Alibaba Cloud account.

Prerequisites

An HTTPS certificate is configured. For more information about how to configure an HTTPS certificate, see [Configure an HTTPS certificate for multiple domain names at a time](#).

Procedure

1. Log on to the [Dynamic Route for CDN console](#).
2. In the left-side navigation pane, click **Tools**. Then, click **Certificate Center**.
3. On the **Certificate Center** page, you can view certificate information such as the accelerated domain name, the certificate name, and the certificate status.

Certificates

[Add Certificate](#)

HTTPS is an extension of HTTP for secured communication. HTTPS secures data transmitted over DCDN and allows users to visit websites quickly and safely.

Accelerated Domain Name	Certificate Name	Certificate Status	Certificate Issued At	Certificate Expires At	Primary Domain Name	Certificate Type
...	...	The domain name does not match the certificate.	May 12, 2020 8:00 AM	May 12, 2021 8:00 PM	...	Upload Custom Certificate (Certificate+Private Key)
...	...	Valid	May 12, 2020 8:00 AM	May 12, 2021 8:00 PM	...	Alibaba Cloud Security Certificate
...	...	Valid	Sep 11, 2020 8:00 AM	Sep 12, 2021 8:00 PM	...	Free Certificate

The following table describes the states that domain name certificates support.

Certificate state	Description
Valid	The domain name certificate is valid.

Certificate state	Description
The domain name does not match the certificate.	If the domain name and the certificate do not match, you must update the certificate. For more information about how to update a certificate, see Configure an HTTPS certificate for multiple domain names at a time .
Expiring	The certificate is about to expire. Renew your certificate at the earliest opportunity. For more information, see Renewal upon expiration .
Expired	The certificate has expired. You can update the certificate. For more information, see Configure an HTTPS certificate for multiple domain names at a time .

Related API operations

You can call the related API operation to query your domain name certificates. For more information, see [DescribeDcdnHttpsDomainList](#).

5. Real-time log delivery

5.1. Overview

This topic describes the features, scenarios, benefits, and billing methods of real-time log delivery.

What is real-time log delivery?

When you use Dynamic Route for CDN (DCDN) to accelerate content delivery, a large amount of logs are generated. You can use DCDN to collect logs that are dynamically generated and deliver the logs to Log Service or a specified location for log analytics in real time. You can analyze the collected logs to troubleshoot issues and make business decisions at the earliest opportunity.

For more information, see [Log Service](#).

Scenarios

You can use real-time log delivery to troubleshoot issues that may occur when you use DCDN to accelerate your domain name. You can also use the collected logs to analyze user statistics.

Benefits

For traditional log analytics, you must download logs, upload the logs to a data warehouse, perform data scrubbing and modeling, and then analyze the logs. These steps consume large amount of effort and time. The real-time log delivery feature of DCDN can be used to collect logs with low latency and monitor your DCDN service. After you activate DCDN, logs of DCDN are automatically delivered to Log Service. This simplifies the data analysis process and allows you to view the analysis results at your convenience.

Differences between real-time log delivery and log downloads

The following list shows the differences between real-time log delivery and log downloads:

- Real-time log delivery is used to dynamically collect logs. The delay between the time when logs are generated and when logs are collected is at most three minutes. DCDN integrates with Log Service to implement log analysis. This allows you to analyze logs, troubleshoot issues, and make business decisions at the earliest opportunity.
- When you download offline logs, the delay is usually less than 24 hours. However, the delay may also exceed 24 hours.

Billing methods

You are charged based on the number of logs that are pushed in real time. For more information about the pricing of real-time log collection, see [Pricing of value-added services](#).

You are separately charged for Log Service. For more information about the billing methods of Log Service, see [Pricing of value-added services](#).

6. WebSocket

6.1. What is WebSocket?

This topic describes the concept, benefits, and application scenarios of WebSocket.

Overview

WebSocket is a new network protocol that enables interaction between a web browser and a web server over a persistent Transmission Control Protocol (TCP) connection. WebSocket supports full-duplex communications that allow the server to actively send data to the client. Therefore, WebSocket requires only one handshake to establish a bi-directional, full-duplex, and persistent connection between the browser and the server. This simplifies the data exchanges between the client and the server.

Benefits

Many websites are using Asynchronous JavaScript and XML (AJAX) polling to implement push technologies. Based on the polling technique, the browser sends HTTP requests to the server at specific intervals, such as every second. Then, the server returns the most recent data to the browser of the client.

The disadvantage of this model is that the browser has to continuously send requests to the server. HTTP requests may have a large header and a small payload. The HTTP requests of this type result in a waste of bandwidth and other resources.

The WebSocket protocol that is defined by HTML5 has the following benefits:

- Each message that is exchanged between the client and the server contains a small header. The size of the header is about 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.
- When a WebSocket connection is established, the browser continuously communicates with the server.

The WebSocket protocol helps you minimize the usage of server and bandwidth resources, reduce the amount of the transferred data, and facilitate real-time communication.

Scenarios

Scenario	Description
Live commenting	User A sends a live comment through a mobile phone and wants to use the mobile phone to view the live comments that are sent by other clients. To meet the requirements, you can use WebSocket to push the live comments that are sent by other clients to the mobile phone of User A. Then, User A can view the live comments that are sent by other users.
Online education	When a teacher offers courses to students online, the teacher can use a client to send data to the clients of the students in real time based on WebSocket communication. The examples of the sent data include notes and outlines.


Scenario	Description
Real-time quotes for financial products	To handle the fluctuating prices of financial products, such as stock and gold, WebSocket pushes the up-to-date prices to the clients of global traders in real time. This helps the traders make informed decisions at the earliest opportunity.
Live sportscast	Live sportscasts are the top concern for a large number of sports lovers all over the world. WebSocket allows for real-time updates in live sportscasts to ensure optimal user experience.
Video conferencing	Video conferencing is widely used in diverse scenarios. In a video conference, WebSocket helps to deliver real-time information to participants who join the conference through multiple ends.
Location-aware applications	An increasing number of developers apply the GPS feature of mobile devices to location-aware applications. You can use WebSocket to keep tracking the location of a user. For example, your WebSocket-based application can record the movement trails of the user. This allows you to collect more details about the user.

6.2. Configure the WebSocket protocol

The WebSocket protocol simplifies data exchanges between clients and servers, and allows servers to actively push data to clients. You can enable WebSocket to minimize the usage of server and bandwidth resources, and to facilitate real-time communication. This topic describes how to enable and configure WebSocket.

Procedure

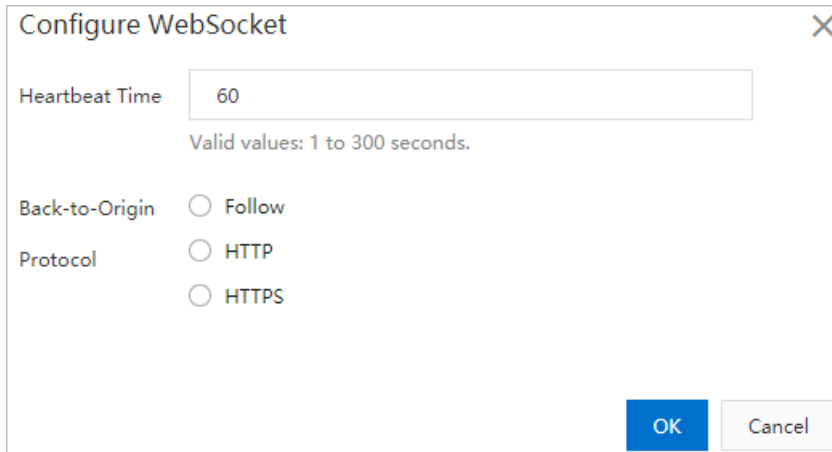
1. Enable WebSocket. Before you use WebSocket, you must specify the billing method of WebSocket and wait until the billing method takes effect. For more information, see [Activate the DCDN service](#).

 **Note**

- If you are a new user, the billing method of WebSocket immediately takes effect.
- If you have used WebSocket before, the time when the WebSocket billing method takes effect depends on the Dynamic Route for CDN (DCDN) billing method. If DCDN uses the **daily billing** method, the WebSocket billing method takes effect at 00:00 on the next day. If DCDN uses the **monthly billing** method, the WebSocket billing method takes effect at 00:00 on the first day of the next month.

2. Configure the WebSocket protocol.
 - i. In the left-side navigation pane, click **WebSocket**.
 - ii. Find the domain name that you want to manage. Then, click **Modify** for the domain name.
 - iii. Turn on **Websocket**.
 - iv. Click **Modify**.

- v. In the **Configure WebSocket** dialog box, specify the **Heart beat Time** and **Back-to-Origin Protocol** parameters.



Parameter	Description
Heart beat Time	<p>The heartbeat time is the interval at which the client sends data packets to the server to indicate the status of the client. The default value is 60 seconds. We recommend that you set the heartbeat time based on the following rule: $A \leq B \leq C$.</p> <div style="background-color: #e0f2f1; padding: 5px; border: 1px solid #ccc;"> <p>? Note A represents the heartbeat time of the client. B represents the heartbeat time of DCDN. C represents the heartbeat time of the origin server.</p> </div> <p>If the heartbeat time of the client is longer than that of DCDN, DCDN may be disconnected when the client is active. This results in service errors. Assume that A is 80 seconds, B is 60 seconds, and C is 80 seconds. If no data is transferred at the sixty-first second or earlier, DCDN is disconnected because its 60-second heartbeat time has elapsed. If the client sends status data to DCDN at the seventieth second, a service error occurs.</p>
Back-to-Origin Protocol	<p>The protocol policy to be used when DCDN communicates with the origin server over WebSocket.</p> <ul style="list-style-type: none"> HTTP DCDN uses only HTTP to communicate with the origin server over WebSocket. HTTPS DCDN uses only HTTPS to communicate with the origin server over WebSocket. Follow DCDN uses HTTP or HTTPS to communicate with the origin server over WebSocket. The protocol that DCDN uses depends on the protocol of client requests.

- vi. Click **OK**.