CDN

Best Practices

Issue 08

Date 2023-12-13

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

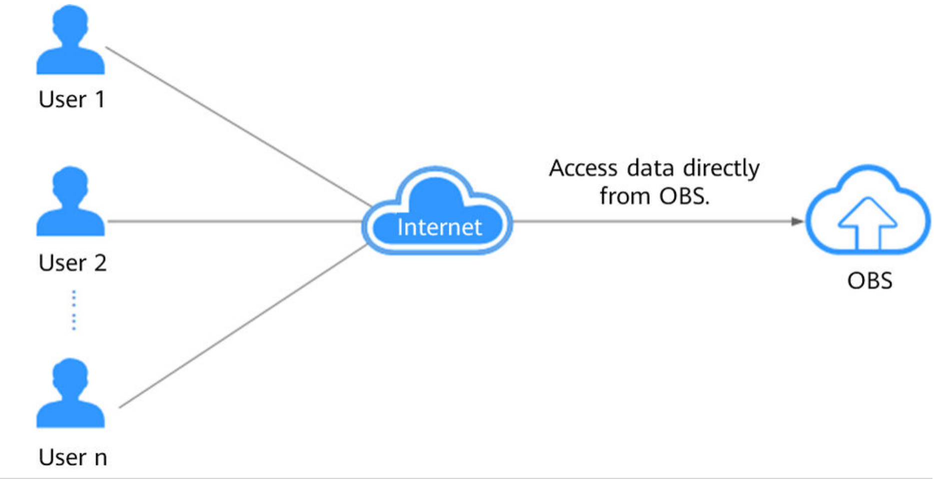
Contents

1 Accelerating OBS Resources

1.1 Solution Overview

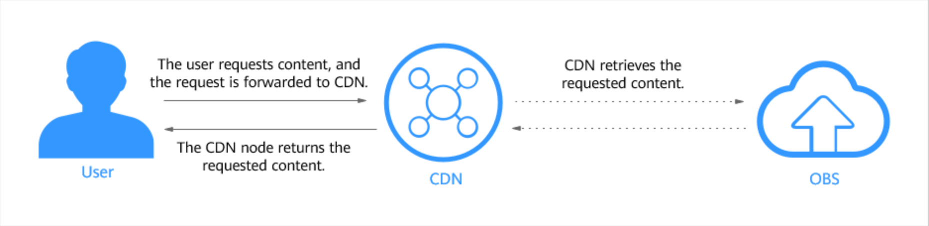
Background

More and more companies in different industries use OBS buckets to store static resource files such as images, videos, and software packages. They use the OBS buckets as the storage source for websites, forums, apps, and games. Users can directly request these static resources from OBS using URLs. OBS buckets can solve the problem of insufficient local storage. However, the response speeds for users accessing OBS buckets in other regions are different, since files are generally stored in only one region. In scenarios where frequent access is required, accessing OBS buckets to obtain files consumes a large amount of traffic.



Solution

Huawei Cloud CDN can effectively accelerate websites to deliver a better user experience. OBS buckets can store massive numbers of files. Storing data in OBS buckets and using CDN for service acceleration can both reduce costs and improve user experience. When a user initiates an access request, CDN checks whether the content requested by the user is cached on the CDN point of presence (PoP) with the fastest response speed. If the CDN PoP has cached the content, the CDN PoP directly returns the content to the user. If the CDN PoP does not cache the content, the CDN PoP retrieves the content from the origin server, returns the content to the user, and caches the content.


The user requests content, and the request is forwarded to CDN.
The CDN node returns the requested content.
CDN retrieves the requested content.
User
CDN
OBS

Solution Advantages

1. Low costs
   - Content in an OBS bucket with CDN acceleration enabled will be cached on CDN PoPs. CDN PoPs do not need to retrieve the content from the bucket when users request the content. The cost of CDN acceleration is low. With CDN acceleration, you can reduce bandwidth costs by 50% to 57%.
   - OBS provides pull traffic packages with preferential prices for CDN to request content from OBS. For details, see **OBS Billing for CDN Acceleration**.

   NOTE

   OBS buckets for CDN acceleration cannot be accessed through the intranet.
2. High efficiency
   - Huawei Cloud CDN has abundant acceleration resources and widely distributed PoPs. It ensures that user requests are precisely scheduled to the optimal PoP for effective and stable acceleration.

Scenarios

- Applications or services that provide download services via HTTP/HTTPS through OBS, for example, websites that provide download services based on HTTP or HTTPS, download tools, game clients, app store.
- Applications or services that provide audio on demand (AOD) or video on demand (VOD) services through OBS. On-demand services include online education, video sharing, music or video on demand, and other audiovisual content.
- Websites or applications that provide image materials through OBS, for example, portal websites, e-commerce platforms, news apps, and user-generated content (UGC) applications.

Limitations and Constraints

- This solution applies only to OBS buckets whose version is 3.0 or later. You can view the bucket version in the **Basic Information** area on OBS Console.
- When back-to-source by mirroring is configured on OBS and range requests are enabled on CDN, if the mirror origin server does not comply with the RFC

Range Requests standard, the response to range requests is not 206 and CDN fails to pull content. In this case, submit a service ticket.

- If the origin server type is set to **OBS bucket domain name** and the origin server is an OBS private bucket, file upload is not supported. To use CDN to upload files to the OBS private bucket, set the origin server type to **Origin server domain name** and enter the domain name of the private bucket when adding a domain name to CDN. In addition, force clients to carry the authentication header in requests for uploading files.

  NOTE

  After an OBS private bucket is connected to CDN using the bucket domain name, clients cannot access the acceleration domain name because CDN does not have the permission to upload files to the bucket. When GET or HEAD is used to request resources from the acceleration domain name, the authentication header must also be carried.

Accelerating Downloads of Files Encrypted by KMS

By default, CDN cannot read encrypted files in OBS buckets. If such files exist in your OBS bucket, enabling CDN acceleration may cause leakage of encrypted objects. If you need to accelerate downloads of files encrypted by KMS in your OBS bucket due to service requirements, pay attention to the following:

- If your OBS bucket is a public bucket, CDN cannot read files encrypted by KMS in the bucket. As a result, the retrieval fails and users cannot access the encrypted files.

  Solution: Move the encrypted files from the bucket to a private bucket, and then configure CDN acceleration for the private bucket.

- If your OBS bucket is a private bucket, assign the KMS Administrator permission to the CDNAccessPrivateOBS agency. In this way, CDN can read and accelerate downloads of files encrypted by KMS in the bucket. For details, see **OBS Authorization**.

1.2 Configuration Process

Background

A game website has stored a large number of files such as software packages and pictures on OBS. As the number of users increases, game downloading and image loading become slower, especially for users who are far away from the file storage area. To address this issue, the website decided to use the CDN service to accelerate game downloads at the lowest cost and improve user experience.

Required Data

Item	Description	Example
Domain Name	Domain name of the game website. If the service area of your website is Chinese mainland or global, the domain name **must be licensed by the Ministry of Industry and Information Technology (MIIT)** and **the license has not expired**, according to China's Internet Management Regulations. Otherwise, CDN does not accelerate the domain name.	download.game-apk1.com
OBS bucket	OBS bucket whose version is 3.0 or later.	obs-doc-test

Prerequisites

Static content, such as images and software packages, has been stored in an OBS bucket.

NOTE

- You can create a bucket and upload files to the bucket using OBS Console, OBS Browser, or SDK. For details, see **OBS Documentation**.
- If you use an OBS bucket created after January 1, 2022 as the origin server and want to enable online preview, log in to the CDN console, choose **Domains** in the navigation pane, click the target domain name, click the **Advanced Settings** tab, click **Edit** next to **HTTP Header**, and set **Content-Disposition** to **inline**. For details, see **How Do I Preview Objects in OBS Through a Browser?**
- If back-to-source by mirroring is enabled for your OBS bucket, do not select **Static website hosting** when adding an acceleration domain name. Otherwise, back to source does not take effect. For details, see **Back to Source**.

Procedure

1. **Add a domain name on CDN.**
   a. Log in to the **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

      The CDN console is displayed.

   b. In the navigation pane, choose **Domains**.
   c. On the **Domains** page, click **Add Domain Name**.
   d. Configure the domain name and CDN acceleration information.

- **Service Area**: Select a service area.
- **Domain Name**: Enter the domain name of the game website, for example, **download.game-apk1.com**.
- **Service Type**: Select a service type based on the **application scenario**.
- **Origin Protocol**: Select a protocol for origin pulls.
- **Origin Server Settings**
  - **Type**: Select **OBS bucket** and select the domain name of an OBS bucket under your account or customize an OBS bucket domain name.
  - **Static website hosting**: Select this checkbox if static website hosting has been enabled for the OBS bucket.
  - **Bucket**: Select **Public bucket** or **Private bucket** based on the bucket policy.
  - **Priority**: primary or secondary origin server.
  - **Host Header**: The default value is the bucket domain name.

  NOTE

  To use a **custom OBS private bucket** as the origin server, configure a policy for the private bucket. For details, see **Configuring a Policy for a Custom OBS Private Bucket**.

e. Click **OK**.

2. **Configure a CNAME record on DNS.**

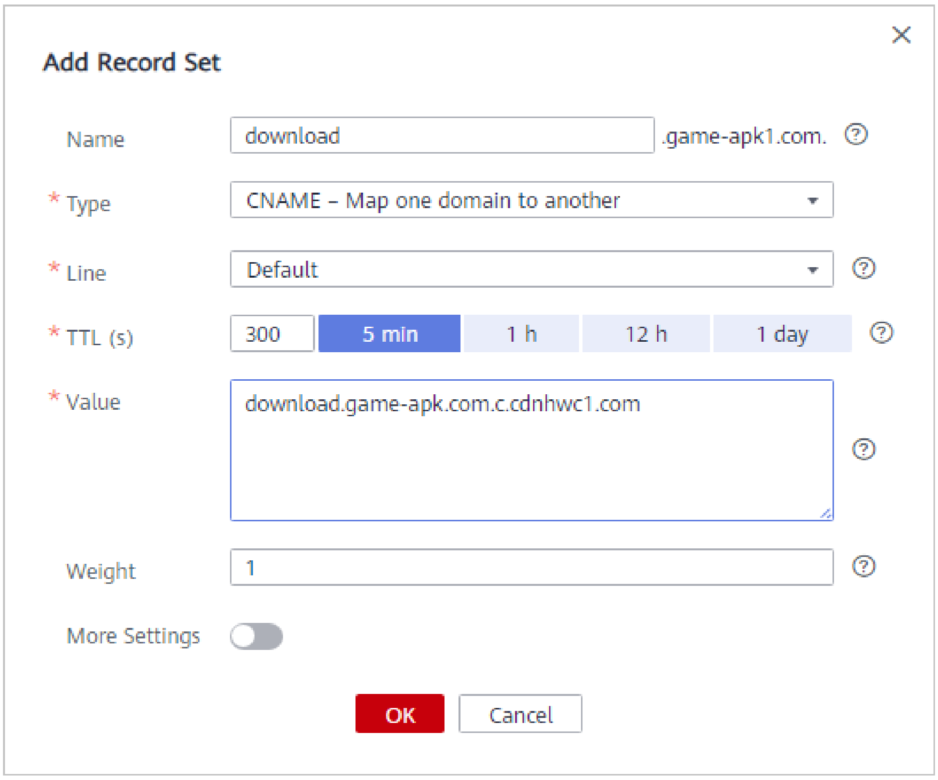
   After the domain name is added, CDN automatically generates a CNAME record for the domain name. The CNAME record cannot be accessed directly. You must add the CNAME record to your domain's DNS records. Then requests for your domain name will be redirected to CDN PoPs for acceleration. In this example, the automatically generated CNAME record is **download.game-apk1.com.c.cdnhwc1.com**. The CNAME configuration method varies depending on the DNS provider. In this document, DNS provided by Huawei Cloud is used as an example. For details about how to configure CNAME records on other DNS providers, see **Configuring a CNAME Record**.

   a. Log in to the **Huawei Cloud console**. Choose **Service List** > **Networking** > **Domain Name Service**. The DNS console is displayed.

   b. In the navigation pane, choose **Public Zones**. The public zone list is displayed.

   c. Click the domain name you want to add a record set to. In this example, the domain name is **game-apk1.com**.

   d. Click **game-apk1.com**. On the displayed page, click **Add Record Set** in the upper right corner. The **Add Record Set** dialog box is displayed.



Add Record Set

Name: download .game-apk1.com.

* Type: CNAME – Map one domain to another

* Line: Default

* TTL (s): 300

* Value: download.game-apk.com.c.cdnhwc1.com

Weight: 1

More Settings

e. Set the parameters as prompted. Use the default values for the parameters that are not listed in the following table.

Parameter	Description	Example
Name	Domain name prefix	download
Type	Type of the record set	CNAME – Map one domain to another
Line	Resolution line. The DNS server will return the IP address of the specified line based on the source of visitors. You must add a **Default** line to ensure that the website is accessible to users of all carriers.	Default
TTL (s)	Cache duration of the record set on a local DNS server. If your service address changes frequently, set TTL to a smaller value.	The default value is **300**, which is, 5 minutes.

Parameter	Description	Example
Value	Domain name alias If CDN acceleration is not enabled, the value is the bucket domain name. If CDN acceleration is enabled, the value is the CNAME record generated by CDN.	download.game-apk1.com.c.cdnhwc1.com

f. Click **OK**.

g. Check whether the CNAME record has taken effect.

Open the Windows command line interface and run the following command:

```
nslookup -qt=cname User-defined domain name bound to the bucket
```

In this example, the user-defined domain name bound to the bucket is **download.game-apk1.com**. If the CNAME record generated by CDN is displayed, the CNAME configuration has taken effect.

3. **Enable OBS authorization on CDN. (Skip this step for public read or public read/write OBS buckets.)**

   If your OBS bucket is a private bucket, you must enable OBS authorization on the CDN console so that CDN can pull data from OBS. For details, see **OBS Authorization**.

   NOTE

   - If your private bucket contains resources that you do not want to make public, move the resources to another private bucket.

4. **Configure the file download URL.**

   Set the URL of the file to be downloaded in the code as follows: ***Domain name of the game website*** + ***Storage path of the file in the OBS bucket*** + ***File name***.

   In the following example, the game website's domain name **download.game-apk1.com** and the **android.apk** file under the **game/3.2.1/** folder in the **obs-doc-test** bucket are used. Then the file download URL is as follows:

   ```
   https://download.game-apk1.com/game/3.2.1/android.apk
   ```

5. **Verify the services.**

   After the game website is redeployed, log in to the website, browse web pages, and download games.

   If images are displayed properly and the games are downloaded successfully, the acceleration configuration is successful.

1.3 Configuring a Policy for a Custom OBS Private Bucket

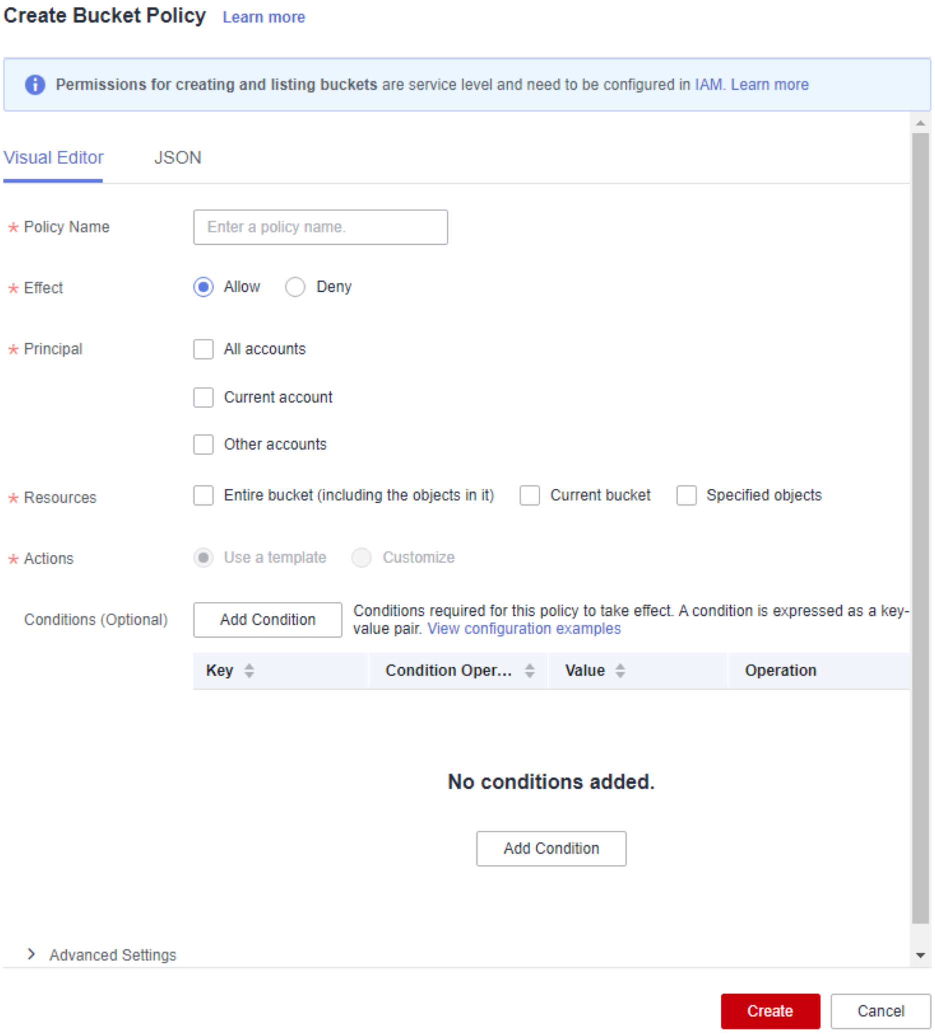
If you use a custom OBS private bucket as the CDN origin server, that is, use an OBS private bucket under another account as the origin server, you need to configure a policy for the private bucket on OBS Console.

Procedure

1. In the navigation pane of **OBS Console**, choose **Object Storage**.
2. In the bucket list, click the name of the bucket to be operated.

   The **Objects** page of the bucket is displayed.
3. In the navigation pane, choose **Permissions** > **Bucket Policies**.
4. On the **Bucket Policies** page, click **Create** and select **Visual Editor**.
   - **Policy Name**: Enter a name.
   - **Effect**: Select **Allow**.
   - **Principal**:
     - **Other accounts**: Enter an account ID in the format of *domainId*/*userId*. Example: 0a0b0afb4************019806272e0/*
     - **Delegated accounts**: Enter an account ID in the format of *domainId*/*. Example: 0a0b0afb4************019806272e0/*
   - **Resources**: Select **Entire bucket (including the objects in it)** or **Current bucket**.
   - **Actions**: Select **Customize** and select the **ListBucket** action.

Figure 1-1 Creating a bucket policy



Create Bucket Policy Learn more

Permissions for creating and listing buckets are service level and need to be configured in IAM. Learn more

Visual Editor | JSON

* Policy Name: Enter a policy name.

* Effect: ● Allow ○ Deny

* Principal: □ All accounts □ Current account □ Other accounts

* Resources: □ Entire bucket (including the objects in it) □ Current bucket □ Specified objects

* Actions: ● Use a template ○ Customize

Conditions (Optional): Add Condition — Conditions required for this policy to take effect. A condition is expressed as a key-value pair. View configuration examples

Key	Condition Oper...	Value	Operation

No conditions added.

Add Condition

> Advanced Settings

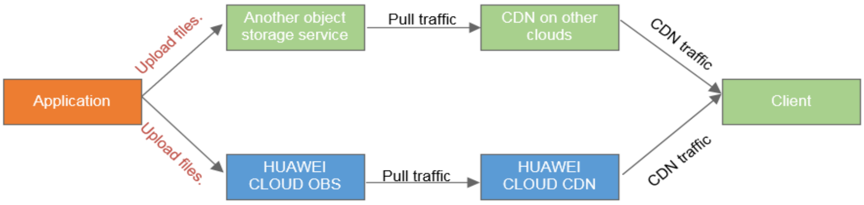
Create | Cancel

5. Click **Create**.

1.4 Synchronizing Data Stored on Multiple Clouds

Dual-write

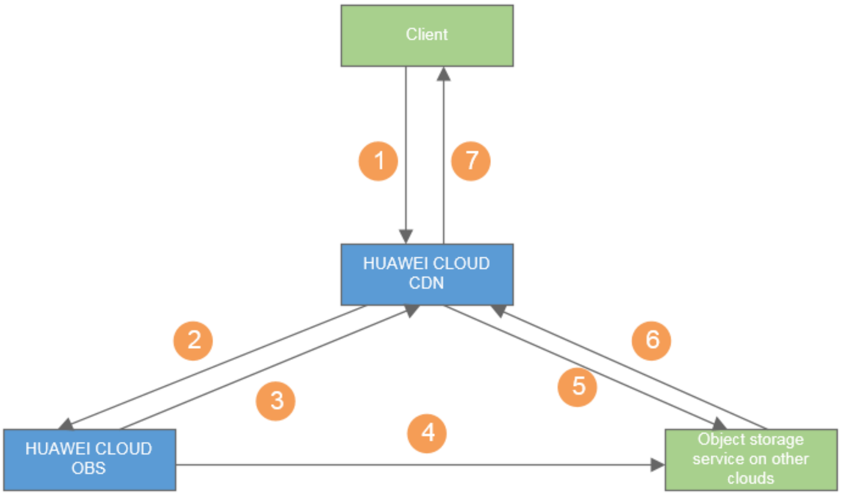
If data is generated on an application or generated on a client but written to an object storage service through the server, the dual-write solution is recommended. The architecture is as follows:



Applications can interconnect with SDKs of two object storage services to write files to the two object storage systems in synchronous or asynchronous mode. The upstream traffic of object storage services is free of charge. Therefore, using this architecture does not increase any cost.

Back-to-Origin

If an OBS bucket does not have the requested file, enable the back-to-origin function to redirect the client's request to the configured origin server. The data will be asynchronously obtained from the origin server and stored on Huawei Cloud Object Storage Service (OBS).



The procedure is as follows:

1. A client requests a file from CDN.
2. CDN retrieves the requested file from OBS.
3. CDN receives an HTTP status code 302 from OBS if the requested file does not exist.
4. OBS asynchronously requests the file from the configured origin server (third-party object storage service).
5. CDN follows the redirect to obtain data from the third-party object storage service.
6. The third-party object storage service responds to the file request from CDN.
7. CDN returns the requested file to the client. When the client requests the same file next time, CDN directly fetches the file from OBS.

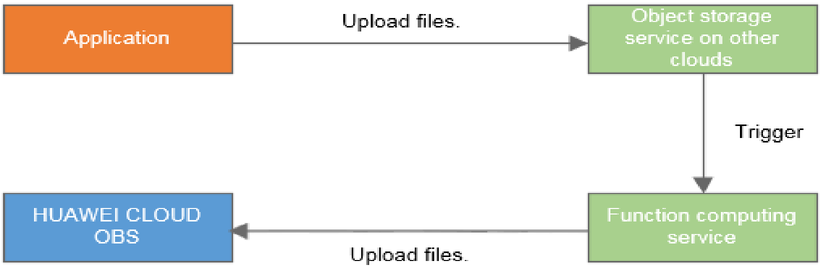
NOTE

The back-to-origin function is triggered only when OBS initiates a request. Therefore, after a new file is uploaded to another object storage service, it is recommended that the application sends a GET request to OBS. The connection can then be closed without receiving entity data. This mechanism generates two copies of data traffic on another object storage service side because CDN and OBS both request the file from the configured origin server.

Serverless Upload

After a file is uploaded to another object storage service, you can use the function computing service to synchronize the file to Huawei Cloud OBS in serverless mode.

Figure 1-2 Serverless upload


Application
Upload files.
Object storage service on other clouds
Trigger
HUAWEI CLOUD OBS
Upload files.
Function computing service

This architecture requires users to enable the function computing service in other clouds and deploy the code for uploading files to OBS, which will generate the function computing service fee.

1.5 FAQ

Why Is the Retrieval Traffic Not Deducted from a Pull Traffic Package?

Possible causes are as follows:

1. The OBS bucket connected to CDN and the pull traffic package are not in the same region. In this case, purchase a pull traffic package in the same region.

2. **OBS bucket** is not selected for **Origin Server Address** when the domain name is added to CDN.
3. The OBS bucket version is earlier than 3.0.

Can CDN and OBS Share a Traffic Package?

No. CDN traffic packages deduct the incoming and outgoing traffic of CDN PoPs. OBS traffic packages deduct OBS traffic.

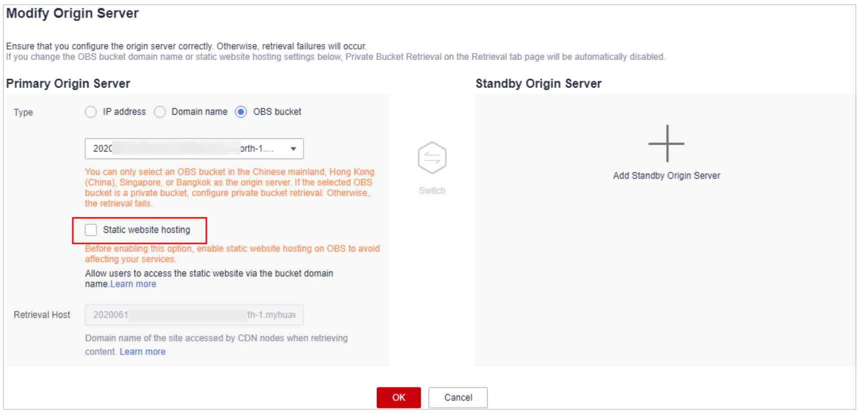
Can an OBS Bucket Domain Name Be Used as an Acceleration Domain Name?

No. The OBS bucket name is used as the origin server when you connect the bucket to CDN. If the OBS bucket domain name is also used as the acceleration domain name, an infinite loop will occur.

Why Are All Files in the Bucket Displayed When Users Request a File from an OBS Bucket Connected to CDN?

A user that has the read permission on an OBS bucket can read the object list of the bucket. When the user requests the domain name added to CDN, OBS returns the object list by default. The solution is as follows:

1. If you use an OBS public bucket, perform the following steps to rectify the fault:
   a. Enable static website hosting on OBS. For details, see **Configuring Static Website Hosting**.
   b. Select **Static website hosting** on the origin server settings page.
      i. Click the target domain name on the **Domains** page.
      ii. On the **Basic Settings** tab page, click **Edit** next to **Origin Server Settings**.
      iii. Select **Static website hosting** and click **OK**.



Modify Origin Server

Ensure that you configure the origin server correctly. Otherwise, retrieval failures will occur.
If you change the OBS bucket domain name or static website hosting settings below, Private Bucket Retrieval on the Retrieval tab page will be automatically disabled.

Primary Origin Server

Type ○ IP address ○ Domain name ● OBS bucket

2020[redacted]orth-1....

You can only select an OBS bucket in the Chinese mainland, Hong Kong (China), Singapore, or Bangkok as the origin server. If the selected OBS bucket is a private bucket, configure private bucket retrieval. Otherwise, the retrieval fails.

□ Static website hosting

Before enabling this option, enable static website hosting on OBS to avoid affecting your services.

Allow users to access the static website via the bucket domain name.Learn more

Retrieval Host 2020061[redacted]th-1.myhuav

Domain name of the site accessed by CDN nodes when retrieving content. Learn more

2. If you use an OBS private bucket, create a policy for the CDNAccessPrivateOBS agency to deny listing objects in the bucket.
   a. In the navigation pane of the IAM console, choose **Agencies**. In the **Operation** column of CDNAccessPrivateOBS, click **Authorize**.
   b. On the **Authorize Agency** page, click **Create Policy** and set required parameters.

Table 1-1 Parameters

Parameter		Description
Policy Name		Enter a policy name, for example, **deny ListBucket**.
Policy View		Select **Visual editor**.
Policy Content	Effect	Select **Deny**.
	Cloud service	Select **Object Storage Service (OBS)**.
	Actions	Select **obs:bucket:ListBucket**.
	Resources	Select **All**.
	Request condition	-

c. Click **Next**.

d. On the **Select Policy/Role** page, select the created policy and click **Next**.

e. On the **Select Scope** page, click **OK**. The authorization takes effect 15 to 20 minutes later.

f. After the authorization takes effect, refresh the CDN cache and try again.

Why Is a File in an OBS Bucket with CDN Acceleration Enabled Be Automatically Downloaded When I Access the File?

Online preview is not enabled. To enable it, log in to the CDN console and choose **Domains** in the navigation pane. Click the target domain name, click the **Advanced Settings** tab, click **Edit** next to **HTTP Header**, and set **Content-Disposition** to **inline**.

2 Accelerating ECS Resources

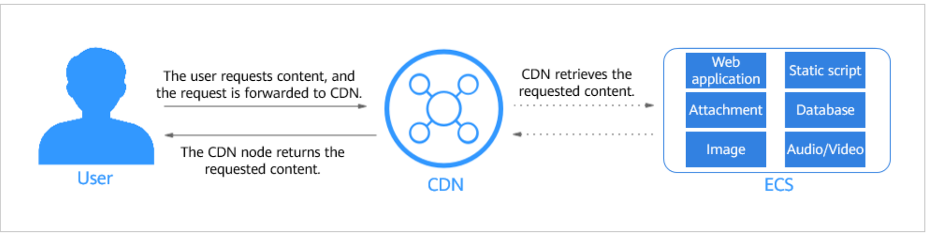
Prerequisites

- You have purchased an **Elastic Cloud Server (ECS)** and **bound an EIP**.
- You have prepared a domain name that meets **domain name access requirements**.
- You have **enabled CDN**.

Background

An ECS is a basic computing component that consists of CPUs, memory, OS, and Elastic Volume Service (EVS) disks. You can configure ECSs based on service requirements, saving a large amount of hardware costs. If ECSs are deployed in different regions, cross-region access may cause network latency, affecting user experience.

Huawei Cloud CDN can effectively accelerate websites to deliver a better user experience. If you use CDN to accelerate ECS resources, you can improve user experience at low costs. When a user initiates an access request, CDN checks whether the content requested by the user is cached on the CDN PoP with the fastest response speed. If the CDN PoP has cached the content, the CDN PoP directly returns the content to the user. If the CDN PoP does not cache the content, the CDN PoP retrieves the content from the origin server, returns the content to the user, and caches the content.


User
The user requests content, and the request is forwarded to CDN.
The CDN node returns the requested content.
CDN
CDN retrieves the requested content.
Web application
Static script
Attachment
Database
Image
Audio/Video
ECS

Solution Advantages

- Users access website content through CDN, reducing the pressure on the origin server.
- The unit price of CDN traffic is lower than that of the traffic generated when ECSs directly access the Internet, saving 50% to 57% of the bandwidth cost.

- Users can obtain content from the nearest CDN PoP, which shortens the network transmission distance and ensures the quality of static content.

Procedure

1. **Add a domain name on CDN.**

   a. Log in to the **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

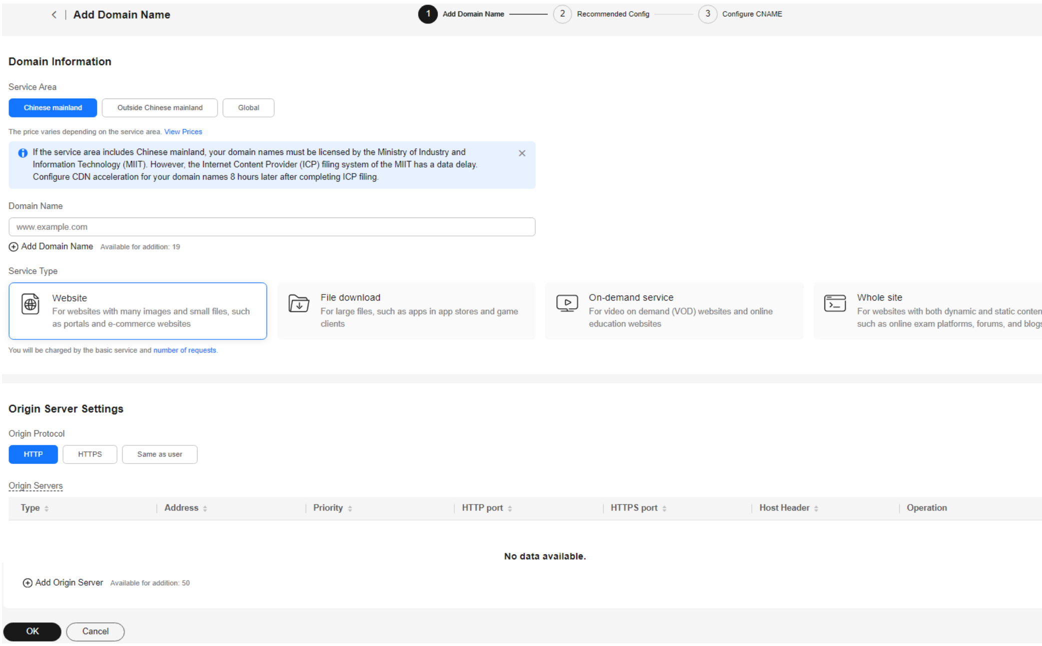
      The CDN console is displayed.

   b. In the navigation pane, choose **Domains**.

   c. On the **Domains** page, click **Add Domain Name**.

   d. In the **Add Domain Name** dialog box, specify the parameters. For details, see **Adding a Domain Name**.

      - **Domain Name**: download.game-apk1.com is used as an example.
      - **Service Area**: Select the service area based on your service requirements.
      - **Service Type**: Select a service type based on the **application scenario**.
      - **Type**: Select **IP address** or **Domain name**.



The price varies depending on the service area. View Prices

If the service area includes Chinese mainland, your domain names must be licensed by the Ministry of Industry and Information Technology (MIIT). However, the Internet Content Provider (ICP) filing system of the MIIT has a data delay. Configure CDN acceleration for your domain names 8 hours later after completing ICP filing.

Website: For websites with many images and small files, such as portals and e-commerce websites

File download: For large files, such as apps in app stores and game clients

On-demand service: For video on demand (VOD) websites and online education websites

Whole site: For websites with both dynamic and static conten such as online exam platforms, forums, and blog

You will be charged by the basic service and number of requests.

Type	Address	Priority	HTTP port	HTTPS port	Host Header	Operation
No data available.						

   e. Click **OK** and use recommended configurations as required.

      NOTE

      The configuration takes 5 to 10 minutes to take effect. When **Status** of the domain name becomes **Enabled**, the domain name has been added.

2. Test your domain name before adding a CNAME record to the domain's DNS records to ensure that your domain configurations are correct. For details, see **(Optional) Testing the Domain Name**.

3. **Configure a CNAME record on DNS.**

   After the domain name is added, CDN automatically generates a CNAME record for the domain name. The CNAME record cannot be accessed directly. You must add the CNAME record to your domain's DNS records. Then requests for your domain name will be redirected to CDN PoPs for acceleration. In this example, the automatically generated CNAME record is **download.game-apk1.com.c.cdnhwc1.com**. The CNAME configuration method varies depending on the DNS provider. In this document, DNS provided by Huawei Cloud is used as an example. For details about how to configure CNAME records on other DNS service providers, see **Configuring a CNAME Record**.

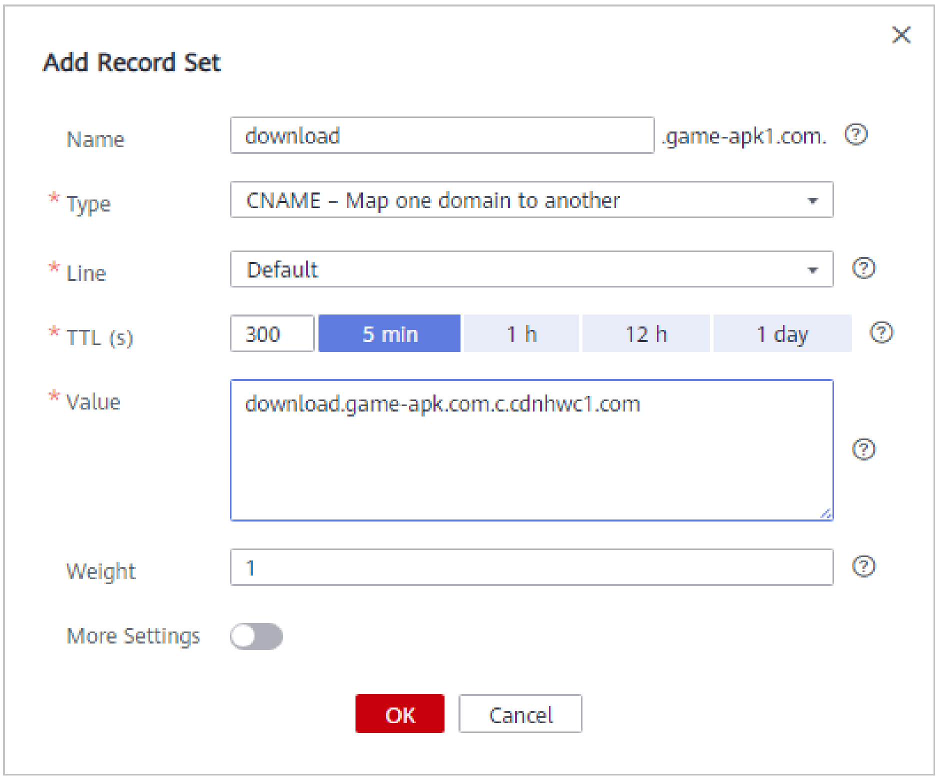
   a. Log in to the **Huawei Cloud console**. Choose **Service List** > **Networking** > **Domain Name Service**.

      The DNS console is displayed.

   b. In the navigation pane, choose **Public Zones**. The public zone list is displayed.

   c. Click the domain name you want to add a record set to. In this example, the domain name is **game-apk1.com**.

   d. Click **game-apk1.com**. On the displayed page, click **Add Record Set** in the upper right corner. The **Add Record Set** dialog box is displayed.



Name: download .game-apk1.com.
* Type: CNAME – Map one domain to another
* Line: Default
* TTL (s): 300
* Value: download.game-apk.com.c.cdnhwc1.com
Weight: 1
More Settings

   e. Set the parameters as prompted. Use the default values for the parameters that are not listed in the following table.

Parameter	Description	Example
Name	Domain name prefix	download

Parameter	Description	Example
Type	Type of the record set	CNAME – Map one domain to another
Line	Resolution line. The DNS server will return the IP address of the specified line based on the source of visitors. You must add a **Default** line to ensure that the website is accessible to users of all carriers.	Default
TTL (s)	Cache duration of the record set on a local DNS server. If your service address changes frequently, set TTL to a smaller value.	The default value is **300**, which is, 5 minutes.
Value	Domain name alias If CDN acceleration is not enabled, the value is the ECS domain name. If CDN acceleration is enabled, the value is the CNAME record generated by CDN.	download.game-apk1.com.c.cdnhwc1.com

f. Click **OK**.

g. Verify that the CNAME record has taken effect.

   Open the Windows command line interface and run the following command:

   ```
   nslookup -qt=cname Acceleration domain name
   ```

   In this example, the acceleration domain name is **download.game-apk1.com**. If the CNAME record generated by CDN is displayed, the CNAME configuration has taken effect.

3 Accelerating Resources Protected by WAF

Prerequisites

- You have a domain name that complies with the requirements described in **Domain Name Requirements** and a HUAWEI ID.
- You have **purchased a Web Application Firewall (WAF) instance**.
- You have **enabled CDN**.

Background

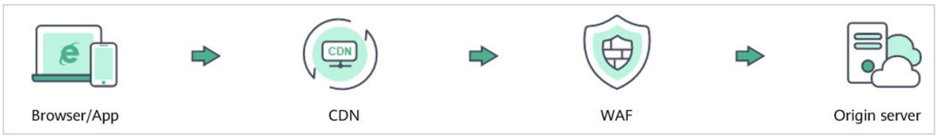
CDN is an intelligent virtual network built on top of the Internet. By deploying PoP servers across the network and distributing content from origin servers to these PoP servers, CDN enables users to obtain desired content nearby. Websites connected to CDN can quickly respond to user requests.

WAF keeps web services stable and secure. It examines all HTTP and HTTPS requests to detect and block attacks, including Structured Query Language (SQL) injection, cross-site scripting (XSS), webshells, command and code injections, file inclusion, sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawlers, and cross-site request forgery (CSRF).

If your websites have high requirements on security and acceleration, you can associate Huawei Cloud CDN with WAF to accelerate websites and defend against web attacks.

Principles

When CDN and WAF are connected, the traffic flow is as follows: CDN > WAF > origin server. CDN forwards the traffic to WAF, and WAF filters out unauthorized traffic and routes only authorized traffic back to your origin server.



Scenarios

This section uses Huawei Cloud WAF as an example to describe how to enable the connection between CDN and WAF. If your WAF service is provided by other service providers, configure it by referring to this section.

Scenario 1: You have purchased a WAF instance and added a domain name to WAF.

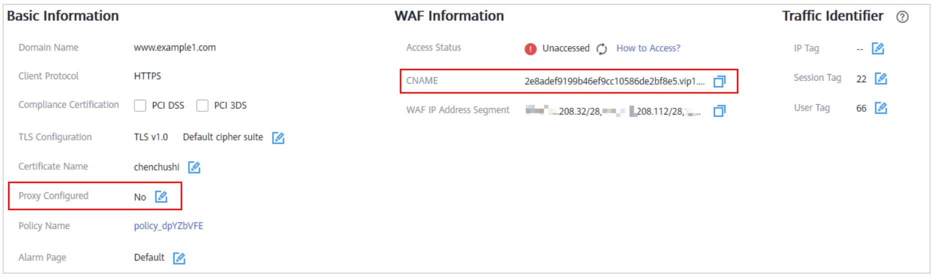
Set **Proxy Configured** to **Yes** in the basic information about the domain name to ensure that WAF security policies take effect on the real origin IP address. Then add the domain name to CDN and set the CNAME of WAF as the origin server in CDN. In this way, CDN can forward the traffic to WAF for acceleration and web attack defense.

Restrictions

- CDN supports only domain names with the default ports. If the domain name is added to WAF using a non-standard port, the domain name cannot be added to CDN.
- If you have uploaded an HTTPS certificate for the domain name on WAF, upload the certificate to CDN. Otherwise, the domain name cannot be accessed.

Procedure

1. Modify the proxy settings of the domain name in WAF by following the instructions provided in **Viewing Basic Information**.
   - **Proxy Configured**: Select **Yes**.



Basic Information

Domain Name www.example1.com
Client Protocol HTTPS
Compliance Certification □ PCI DSS □ PCI 3DS
TLS Configuration TLS v1.0 Default cipher suite
Certificate Name chenchushi
Proxy Configured No
Policy Name policy_dpYZbVFE
Alarm Page Default

WAF Information

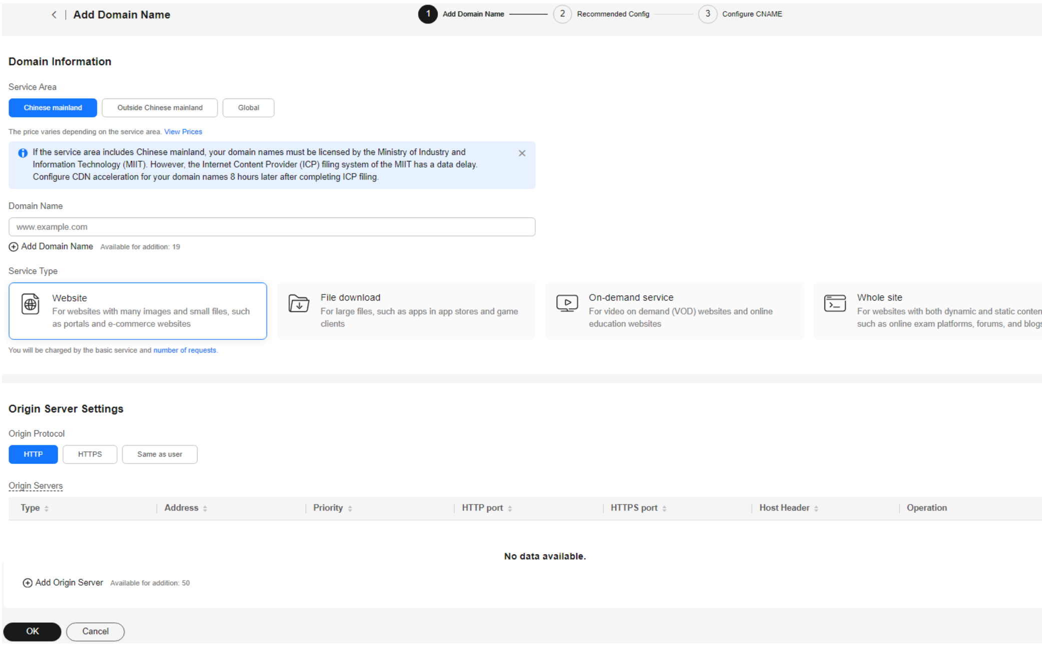
Access Status Unaccessed How to Access?
CNAME 2e8adef9199b46ef9cc10586de2bf8e5.vip1....
WAF IP Address Segment [redacted].208.32/28,[redacted]208.112/28,[redacted]...

Traffic Identifier

IP Tag --
Session Tag 22
User Tag 66

2. Copy the CNAME record generated by WAF.
3. Add the domain name to CDN.
   a. Log in to the **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

      The CDN console is displayed.
   b. In the navigation pane, choose **Domains**.
   c. On the **Domains** page, click **Add Domain Name**. In the dialog box displayed, specify domain parameters.
      - When adding an origin server, set **Type** to **Domain name** and **Address** to the CNAME record generated by WAF.



Domain Information

Service Area

The price varies depending on the service area. View Prices

If the service area includes Chinese mainland, your domain names must be licensed by the Ministry of Industry and Information Technology (MIIT). However, the Internet Content Provider (ICP) filing system of the MIIT has a data delay. Configure CDN acceleration for your domain names 8 hours later after completing ICP filing.

Domain Name

www.example.com

Add Domain Name Available for addition: 19

Service Type

Website
For websites with many images and small files, such as portals and e-commerce websites

File download
For large files, such as apps in app stores and game clients

On-demand service
For video on demand (VOD) websites and online education websites

Whole site
For websites with both dynamic and static conten
such as online exam platforms, forums, and blog

You will be charged by the basic service and number of requests.

Origin Server Settings

Origin Protocol

Origin Servers

Type	Address	Priority	HTTP port	HTTPS port	Host Header	Operation
No data available.						

Add Origin Server Available for addition: 50

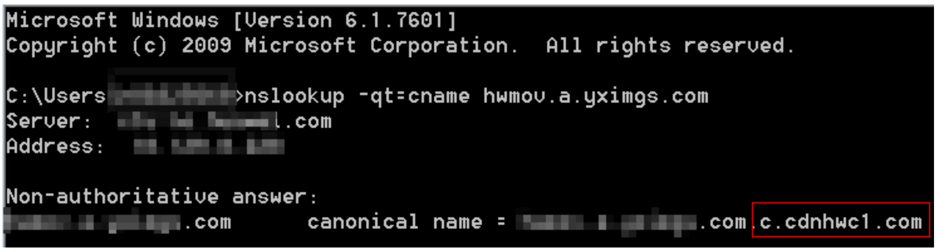
d. Click **OK**. CDN generates a dedicated CNAME record for the domain name.

4. (Optional) Test your domain name before adding a CNAME record to the domain's DNS records to ensure that your domain configurations are correct. For details, see **(Optional) Testing the Domain Name**.
5. Add the CNAME record provided by CDN to your domain's DNS records. For details, see **Configuring a CNAME Record**.
6. Verify that the CNAME record has taken effect.

   Open the Windows command line interface and run the following command:

   ```
   nslookup -qt=cname Domain name
   ```

   If the CNAME record is displayed, the CNAME record has taken effect. A typical command output is shown in the following figure.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users[redacted]>nslookup -qt=cname hwmov.a.yximgs.com
Server:  [redacted].com
Address:  [redacted]

Non-authoritative answer:
[redacted].com       canonical name = [redacted].com.c.cdnhwc1.com
```

NOTE

If your domain name has not been added to neither CDN nor WAF, you are advised to add the domain name to WAF and then configure the connection according to scenario 1.

Scenario 2: You have added a domain name to CDN for acceleration.

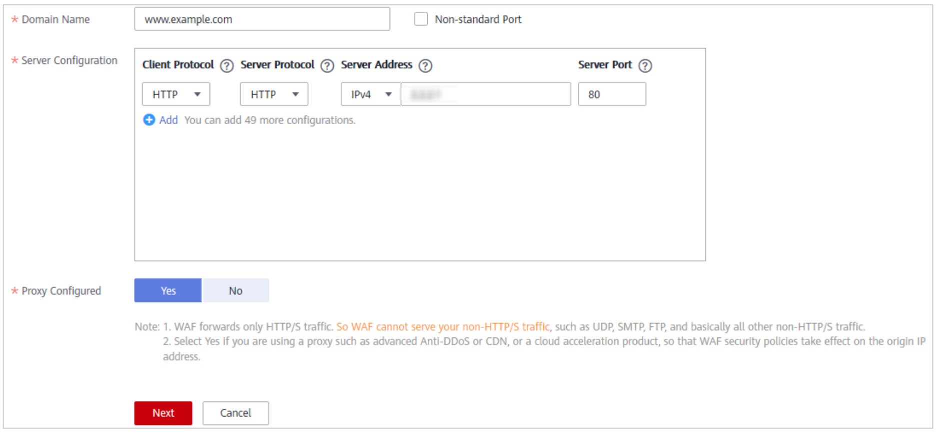
Add the domain name to WAF and set **Proxy Configured** to **Yes**. In this way, WAF can perform security defense for real IP addresses of clients. Then set the CNAME generated by WAF as the origin server in CDN to allow CDN to forward the traffic to WAF, achieving acceleration and web attack defense.

Restrictions

If you have uploaded an HTTPS certificate for the domain name on CDN, upload the certificate to WAF. Otherwise, the domain name cannot be accessed.

Procedure

1. Add the domain name information, including the IP address and port of your origin server, to WAF. For details, see **Adding a Domain Name to WAF**. Pay attention to the following key settings:
   - **Non-standard Port**: Deselect it.
   - **Proxy Configured**: Select **Yes**.



* Domain Name: www.example.com
□ Non-standard Port

* Server Configuration

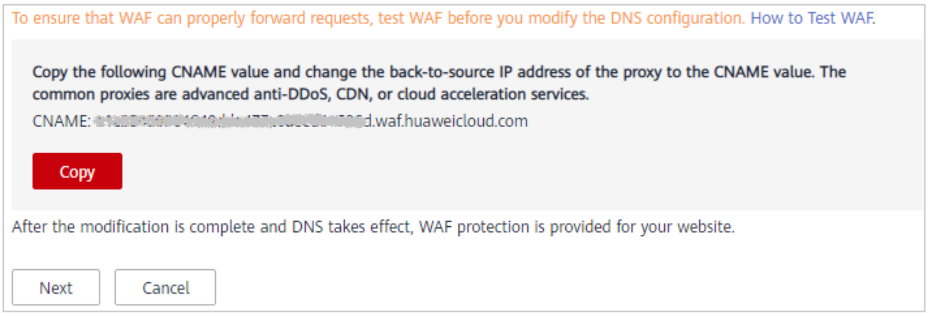
Client Protocol	Server Protocol	Server Address	Server Port
HTTP	HTTP	IPv4 [redacted]	80

Add You can add 49 more configurations.

* Proxy Configured: [✓ Yes] No

Note: 1. WAF forwards only HTTP/S traffic. So WAF cannot serve your non-HTTP/S traffic, such as UDP, SMTP, FTP, and basically all other non-HTTP/S traffic.
2. Select Yes if you are using a proxy such as advanced Anti-DDoS or CDN, or a cloud acceleration product, so that WAF security policies take effect on the origin IP address.

2. When the configuration is complete, WAF generates a dedicated CNAME for the domain name.



To ensure that WAF can properly forward requests, test WAF before you modify the DNS configuration. How to Test WAF.

Copy the following CNAME value and change the back-to-source IP address of the proxy to the CNAME value. The common proxies are advanced anti-DDoS, CDN, or cloud acceleration services.

CNAME: [redacted]d.waf.huaweicloud.com

After the modification is complete and DNS takes effect, WAF protection is provided for your website.

NOTE

You are advised to check whether services are normal after adding the domain name to WAF, and then modify the origin server configuration in CDN.

3. Change the origin server address of the domain name added to CDN to the CNAME generated by WAF.
   a. Log in to the **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

      The CDN console is displayed.
   b. In the navigation pane, choose **Domains**.
   c. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
   d. Click the **Basic Settings** tab.
   e. In the **Origin Server Settings** area, click **Edit** in the **Operation** column of the origin server and modify the origin server settings.

- **Type**: Select **Domain name**.
- **Address**: Enter the CNAME generated by WAF.
- **Origin Port**: Retain the default port.

When the configuration is complete, CDN forwards traffic to WAF for acceleration and web attack defense.

4 Setting the Maximum Cache Age

CDN caches origin content on globally distributed PoPs so that users can obtain the content from nearby PoPs. On the CDN console, you can set the maximum cache age for origin content of different file types based on service requirements.

Impact of Origin Servers on CDN PoP Caches

- If you have configured a cache rule on the origin server, the following scenarios are possible:
  - If you have set **Cache-Control** to **no-cache**, **private**, or **no-store** on the origin server and enabled **Origin Cache Control** on the CDN console, CDN PoPs do not cache origin content. Instead, CDN PoPs retrieve content from the origin server each time the content is requested. This does not achieve acceleration.

    NOTE

    By default, **Origin Cache Control** is disabled on the CDN console.
  - If you have set a specific maximum cache age on the origin server, this maximum cache age will be overwritten by that set on the CDN console.
- If no cache rules are set on the origin server, cache rules set on the CDN console are used.

Setting the Maximum Cache Age Based on Service Type

Default maximum cache age

- If the service type is website acceleration, file download acceleration, or on-demand service acceleration, and the origin server address is an origin IP address or origin domain, the following default cache rules are available:
  - The default maximum cache age for common dynamic files (for example, .php, .jsp, .asp, and .aspx files) is 0. CDN pulls content from the origin server directly when receiving requests for such dynamic files. You can modify and delete this rule.
  - The default maximum cache age for files other than common dynamic files is 30 days. You can modify but cannot delete this rule.
- If your origin server is an OBS bucket, the default maximum cache age for all files is 30 days. You can modify but cannot delete this rule.

NOTE

You can add a custom cache rule with a higher priority so that custom rule will be used.

- If the service type is whole site acceleration, a cache rule with **Type** set to **All files** and **Maximum Age** set to **0** is available by default. You can modify and delete this rule.

You can configure the maximum cache age based on the service type.

- You are advised to set the maximum cache age for website acceleration so that CDN PoPs proceed as follows:
  - Do not cache dynamic files such as .php, .aspx, .asp, .jsp, .do, .dwr, .cgi, .fcgi, .action, .ashx, .axd, and .json files.
  - Cache .shtml, .html, .htm, and .js files for 7 days.
  - Cache other static files for 30 days.
- You are advised to set the maximum cache age for download acceleration so that CDN PoPs proceed as follows:
  - Do not cache dynamic files such as php, aspx, asp, jsp, and .do files.
  - Cache the following file types for 30 days: .7z, .apk, .wdf, .cab, .dhp, .exe, .flv, .gz, .ipa, .iso, .mpk, .mpq, .pbcv, .pxl, .qnp, .r00, .rar, .xy, .xy2, .zip, and .cab.
- You are advised to set the maximum cache age for VOD acceleration so that CDN PoPs proceed as follows:
  - Do not cache dynamic files such as .php, .aspx, .asp, .jsp, and .do files.
  - Cache the following file types for 7 days: .mwv, .html, .htm, .shtml, .hml, .gif, .swf, .png, .bmp, and .js.
  - Cache the following file types for 30 days: .mp3, .wma, .7z, .apk, .wdf, .cab, .dhp, .exe, .flv, .gz, .ipa, .iso, .mpk, .mpq, .pbcv, .pxl, .qnp, .r00, .rar, .xy, .xy2, .zip, and .cab.

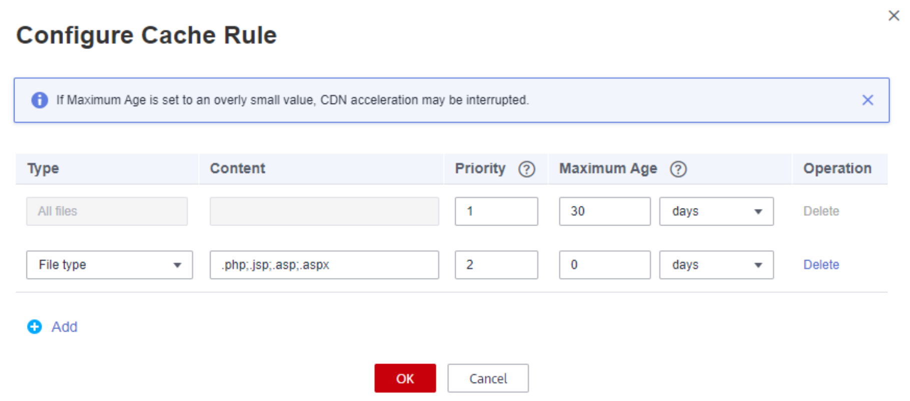
Procedure

1. Log in to the **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

   The CDN console is displayed.
2. In the navigation pane, choose **Domains**.
3. In the domain list, click the target domain name or click **Configure** in the **Operation** column.
4. Click the **Cache Settings** tab.
5. In the **Cache Rules** area, click **Edit**.

   The **Configure Cache Rule** dialog box is displayed.
6. Click **Add** to add cache rules. See **Figure 4-1**. **Table 4-1** describes the parameters.

Figure 4-1 Configuring a cache rule



Configure Cache Rule

If Maximum Age is set to an overly small value, CDN acceleration may be interrupted.

Type	Content	Priority	Maximum Age		Operation
All files		1	30	days	Delete
File type	.php;.jsp;.asp;.aspx	2	0	days	Delete

Table 4-1 Cache rule parameters

Parameter	Description	Configuration Rule
All files	All cached resources on CDN PoPs	By default, CDN has a rule for every new domain name. The rule specifies that the maximum cache age for **All files** is 30 days. You can modify but cannot delete this rule.
File type	Files of a specific type If the service type of a new domain name is **Website**, **File download**, or **On-demand service** and its origin server is a private one, CDN adds a rule to it by default. The rule specifies that the maximum cache age is 0 for common dynamic files, such as .php .jsp .asp, and .aspx files. CDN pulls such files from the origin server for every request. You can modify and delete this rule.	- All file types are supported. - Start each file name extension with a period (.), and separate file name extensions with semicolons (;). - Enter up to 255 characters. - Enter up to 20 file name extensions. - File name extensions are case-insensitive. Example: **.JPG;.zip;.exe**
Directory	All files in a directory	Start a directory with a slash (/), and separate multiple directories with semicolons (;). Enter a maximum of 20 directories with a maximum of 255 characters in total. Example: **/test/folder01;/test/folder02**

Parameter	Description	Configuration Rule
Full path	A specific file	Start a full path with a slash (/) and do not end it with an asterisk (*). A file in the specified directory or file with the wildcard * can be matched. Enter only one full path. Examples: **/test/index.html** or **/test/*.jpg**
Homepage	Root directory	The root directory of a website is the top-level directory of the website folder, which contains all subfolders of the website. For example, for **abc/file01/2.png**, **abc/** is the root directory, and a cache rule is configured for **abc/**.
Priority	Priority of a cache rule Each cache rule must have a unique priority. If a resource is specified in multiple cache rules, the rule with the highest priority is applied.	Enter an integer ranging from 1 to 100. A greater number indicates a higher priority.
Maximum Age	Duration that a file can be cached. If the maximum age of the file has reached, CDN requests the most recent content of the file from the origin server when a user requests the file from a CDN PoP. In addition, the CDN caches that content on the CDN PoP.	The age of a cached file cannot exceed 365 days. You are advised to set the time according to the following rules: ● For static files (such as .jpg and .zip files) that are not frequently updated, set the maximum age to more than one month. ● For static files (such as .js and .css files) that are frequently updated, set the maximum age based on service requirements. ● For dynamic files (such as .php, .jsp, and .asp files), set the maximum age to 0 seconds.

7. (Optional) Delete a cache rule if you no long use it.
8. Click **OK**.

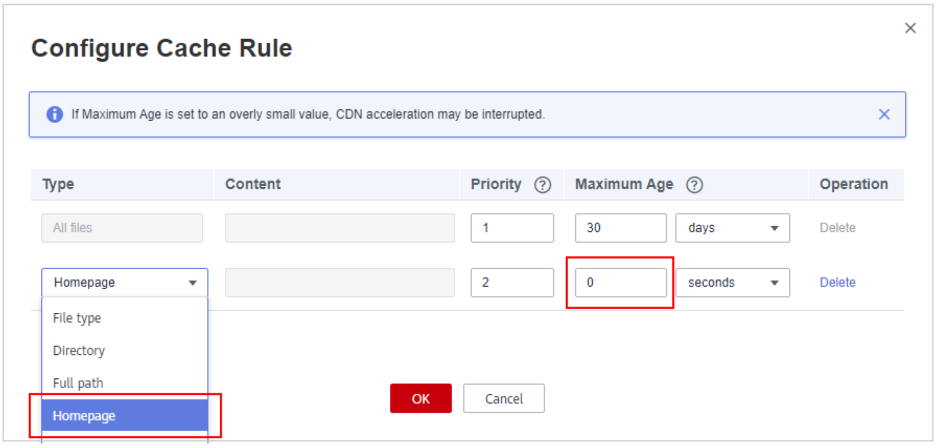
NOTE

If you have modified a cache rule, the new rule does not apply to content that has been cached but only applies to new content. If you want the modification to take effect immediately, refresh the cache after modifying the cache rule.

Examples

Scenario 1: Assume that you have added a web portal to Huawei Cloud CDN for acceleration, but you do not want to cache it.

You can add a cache rule for this web portal on the CDN console, with **Type** set to **Homepage** and **Maximum Age** to **0**.



Configure Cache Rule

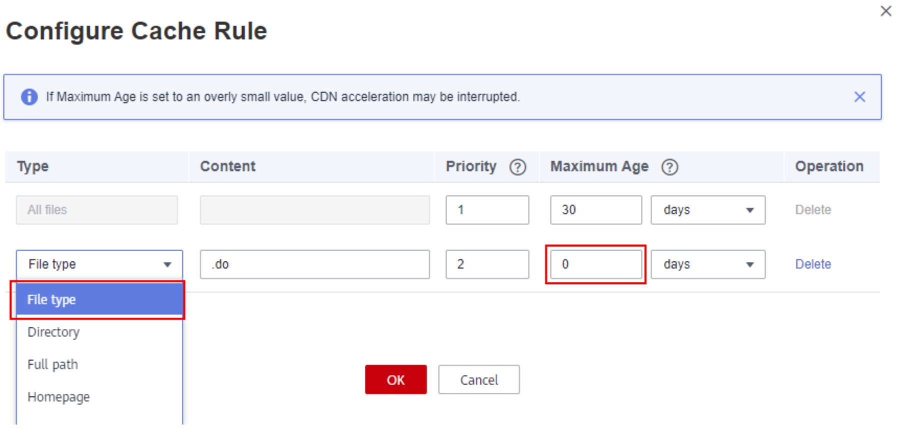
If Maximum Age is set to an overly small value, CDN acceleration may be interrupted.

Type	Content	Priority	Maximum Age		Operation
All files		1	30	days	Delete
Homepage		2	0	seconds	Delete

Scenario 2: Assume that you do not want to cache files of a specific type or a specific web page.

1. You have configured CDN acceleration for your website and set the maximum cache age of .do files to one day. However, due to service requirements, you do not need to cache .do files anymore.

   You can add a cache rule for your website on the CDN console, with **Type** set to **File type**, **Content** to **.do**, and **Maximum Age** to **0**.



Configure Cache Rule

If Maximum Age is set to an overly small value, CDN acceleration may be interrupted.

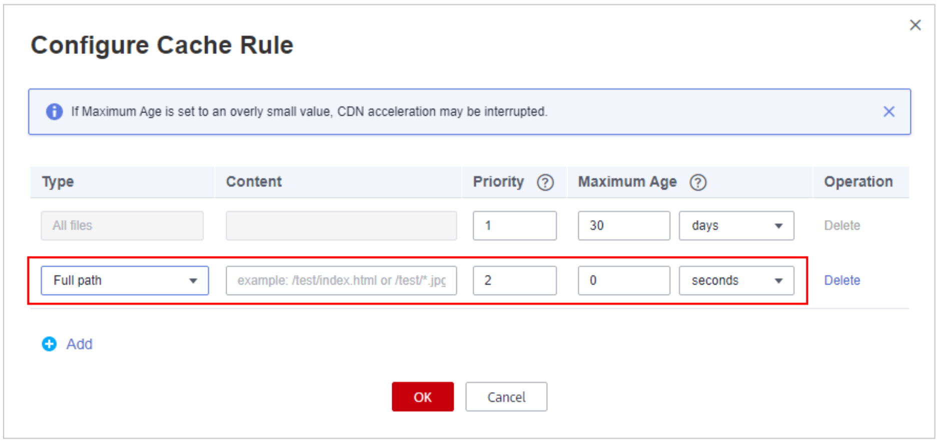
Type	Content	Priority	Maximum Age		Operation
All files		1	30	days	Delete
File type	.do	2	0	days	Delete

NOTE

The new rule only applies to new content. After the new rule is added, refresh the cached URL or directory where the .do file is located on the CDN console so that the new rule can take effect for all .do files.

2. You have configured CDN acceleration for your website, the login page of your website is displayed cyclically, and your customers cannot log in to the website. After CDN acceleration is disabled, customers can log in to the website.

   This is because CDN PoPs have cached the login page. To resolve the issue, add a cache rule for your website on the CDN console and set the maximum cache age of the login page to **0** in the rule. Take the login page of the Huawei Cloud console as an example. The login page of the Huawei Cloud console is **https://auth.huaweicloud.com/authui/login.html#/login**. You can add a cache rule on the CDN console, with **Type** set to **Full path**, **Content** to **/authui/login.html#/login**, and **Maximum Age** to **0**.

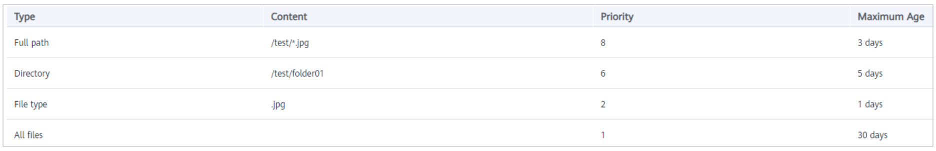


Configure Cache Rule

If Maximum Age is set to an overly small value, CDN acceleration may be interrupted.

Type	Content	Priority	Maximum Age		Operation
All files		1	30	days	Delete
Full path	example: /test/index.html or /test/*.jpg	2	0	seconds	Delete

Scenario 3: Assume that you have configured the following cache rules for your acceleration domain name www.example.com but do not know which rule takes effect.



Type	Content	Priority	Maximum Age
Full path	/test/*.jpg	8	3 days
Directory	/test/folder01	6	5 days
File type	.jpg	2	1 days
All files		1	30 days

When a user requests **www.example.com/test/cdn.jpg**, rules of the **All files**, **File type**, and **Full path** type are all matched. The priority of the **Full path** rule is 8, which is the highest among the three rules. Therefore, the rule of the **Full path** type (**/test/*.jpg**) is used.

5 Improving the Cache Hit Ratio

Background

If the CDN cache hit ratio is low, the pressure on the origin server is high and the static resource access efficiency is low. You can select an optimization policy based on the cause of the low cache hit ratio to improve the cache hit ratio. In CDN, the cache hit ratio includes the traffic hit ratio and request hit ratio.

- **Traffic hit ratio** = Traffic generated by requests that hit the cache/Total traffic of requests
- **Request hit ratio** = Number of requests that hit the cache/Total number of requests

  NOTE

  The traffic hit ratio indicates the load on the origin server. A lower traffic hit ratio means a larger retrieval traffic, which leads to a larger output traffic and higher bandwidth consumption on the origin server.

Viewing the Cache Hit Ratio

You can log in to the CDN console to view the traffic hit ratio and request hit ratio.

1. Log in to the **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

   The CDN console is displayed.
2. In the navigation pane, choose **Statistical Analysis**.
3. Choose **Utilization Statistics** and **Access Statistics** to view the traffic hit ratio and request hit ratio.

Figure 5-1 Traffic hit ratio

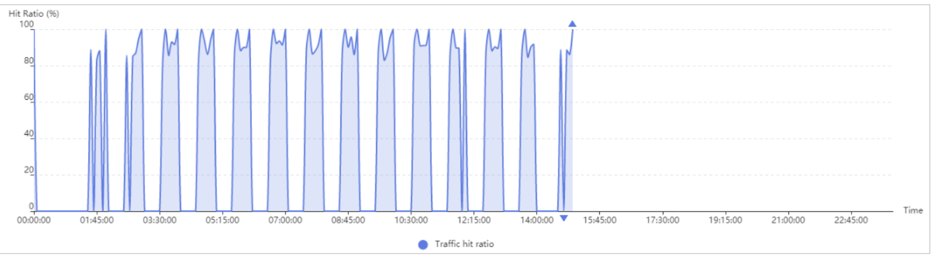
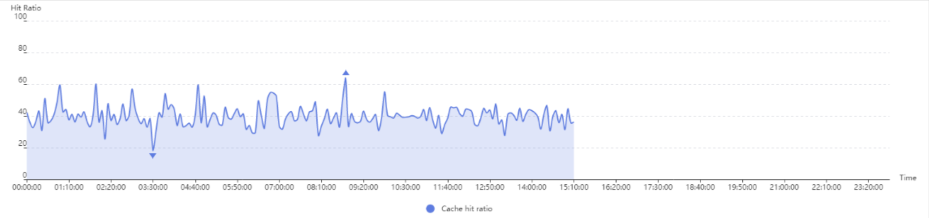


Figure 5-2 Request hit ratio



Optimizing the Cache Hit Ratio

1. **Set an appropriate maximum cache age.**

   CDN caches origin content on globally distributed PoPs so that users can obtain the content from nearby PoPs. You can set a proper maximum cache age for different content on the CDN console to improve the cache hit ratio.

   – For static files (such as images and app packages) that are not frequently updated, set the maximum cache age to more than one month.

   – For static files (such as JS and CSS files) that are frequently updated, set the maximum age based on service requirements.

   – For dynamic files (such as PHP, JSP, and ASP files), set the maximum cache age to **0**, so these files will not be cached on CDN PoPs.

   For details, see **Setting the Maximum Cache Age**.

   NOTE

   - If you have set **Cache-Control** to **s-maxage=0**, **max-age=0**, **no-cache**, **no-store**, or **private** on the origin server and enabled **Origin Cache Control** on the CDN console, CDN PoPs cannot cache origin content and will frequently retrieve content from the origin server. By default, **Origin Cache Control** is disabled.
   - If your origin server has multiple hosts and the **Last-modified**, **Etag**, and **Content-Length** parameters of a resource on these hosts are set to different values, CDN PoPs cannot cache the resource and frequently retrieves the resource.
   - If origin content has been updated, refresh the URLs of the content to ensure that users can obtain the latest content.
   - **If you have modified a cache rule,** the new rule does not apply to content that has been cached but only applies to new content. If you want the modification to take effect immediately, refresh the cache after modifying the cache rule.

2. **Enable URL parameter filtering.**

   Currently, most web page requests carry URL parameters following a question mark (?). Parameters that do not contain important information (such as version) do not affect users' access to the correct content. You can configure URL parameter filtering to improve the cache hit ratio and distribution efficiency. For details, see "URL Parameter Filtering" in **Cache Rules**.

   Typical applications

   – When a user requests **http://www.example.com/1.txt?test1** for the first time, the content is not cached on CDN, and CDN needs to retrieve that content from the origin server. If **Ignore URL Parameters** is enabled on CDN, when another user requests **http://www.example.com/1.txt?test2**, the parameter behind the question mark (?) will be ignored. As a result, the cache of **http://www.example.com/1.txt** is hit.

   – When a user requests **http://www.example.com/1.txt?test1** for the first time, the content is not cached on CDN, and CDN needs to retrieve that content from the origin server. If **Ignore URL Parameters** is disabled, when another user requests **http://www.example.com/1.txt?test2**, the full URL, including the parameter behind the question mark (?) will be matched. As a result, no cache is hit and CDN has to retrieve **http://www.example.com/1.txt?test2** from the origin server.

3. **Preheat URLs.**

   CDN can proactively cache origin content to CDN PoPs through cache preheating. When users access the content, they can directly obtain the latest content from CDN PoPs. For details, see **Cache Preheating**.

   When your domain name is connected to CDN for the first time, you can preheat origin content to CDN PoPs so that users can directly obtain the content from CDN PoPs, improving the cache hit ratio.

   Typical scenarios

   – Initial access to CDN: When a domain name is connected to CDN for the first time, the origin content is not cached on CDN PoPs. In this case, you can preheat the origin content to CDN PoPs. Then users can directly obtain the content from the nearest CDN PoP, improving the access speed.

   – Installation package release: Before releasing a software installation package or upgrade package, you can preheat the content to CDN PoPs. After the software or upgrade is launched, the CDN PoPs directly respond to the download requests of a large number of users, which improves the download speed and greatly reduces the pressure on your origin server.

   – Promotional activity: Before releasing a promotional campaign, you can preheat the static content involved on the activity page to CDN PoPs. After the activity starts, the CDN PoPs respond to user requests for accessing all static content, which ensures service availability and improves user experience.

4. **Enable range requests.**

   A range request allows the origin server to send a specific range of data to a CDN PoP using the range information in the HTTP request header. Range requests accelerate large file distribution and improve origin pull efficiency and cache hit ratio. For details, see **Range Requests**.

   Typical scenarios

   – If a user requests a clip of a video, CDN needs to retrieve the entire video from the origin server when Range-based retrieval is disabled. As a result, the retrieval traffic is greater than the traffic used for returning the content to the user, decreasing the cache hit ratio. When Range-based retrieval is enabled, CDN only needs to retrieve the clip of the video and returns the clip to the user, improving the cache hit ratio.

5. **Perform further operations.**

   – Do not update an entire directory when a specific cached content needs to be updated.

     You can refresh the URL of the cached content to force the content cached on CDN PoPs to expire. Refreshing the entire directory will force all content in the directory to expire. When a user accesses a resource in the directory, no cache will be hit and CDN will need to retrieve content from the origin server. Therefore, do not refresh the entire directory, especially the root directory.

- Do not carry dynamic parameters in URLs.

  If your URLs contain dynamic parameters, such as timestamps, CDN cannot cache the content and frequently retrieves the content.

Checking Whether Requests for a URL Hit the Cache

1. Open Google Chrome and press **F12**.
2. Choose **Network**.
3. Enter the website to be accessed in the address box and press **Enter**. View the response headers of the URL of a specific resource and perform the following operations:
   - If the **x-hcs-proxy-type** header exists, check its value. The value **1** indicates that the cache is hit, and the value **0** indicates that the cache is not hit.
   - If the **x-hcs-proxy-type** header does not exist, check the value of the **X-Cache-Lookup** header. Value **Hit From MemCache**, **Hit From Disktank**, or **Hit From Upstream** indicates that the cache is hit, whereas other values indicate that the cache is not hit.
   - If neither the **x-hcs-proxy-type** nor **X-Cache-Lookup** header exists, check the value of the **age** header. Values greater than 0 indicate that the cache is hit, and the value **0** indicates that the cache is not hit.

6 Obtaining Real IP Addresses of Users

This section describes how to obtain real IP addresses of users on different types of web servers (including Tomcat, Apache, Nginx, IIS 6, and IIS 7).

Background

After a website is connected to CDN for acceleration, IP addresses obtained by the origin server from IP address headers are not the real IP addresses of users. You can configure your web server to obtain the real IP addresses of users.

When a proxy server (such as CDN and WAF) forwards an HTTP, WebSocket, or WSS request to the next server, the proxy server adds the **X-Forwarded-For** field to the request header to record the real IP address of the user. The format of the record is **X-Forwarded-For:** *Real IP address of the user*, *IP address of the proxy server 1*, *IP address of the proxy server 2*, *IP address of the proxy server 3*, ..., *IP address of the proxy server N*.

You can obtain the real IP address of the user by obtaining the first IP address from the **X-Forwarded-For** field.

Nginx

If an Nginx reverse proxy is deployed on your origin server, you can configure location information on the Nginx reverse proxy so that the backend web server can use similar functions to obtain real IP addresses of users.

1. Configure the following information in the corresponding location of the Nginx reverse proxy to obtain the information about real IP addresses of users:
   ```
   Location ^ /<uri> {
       proxy_pass  ....;
       proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
   }
   ```
2. Enable the backend web server to use similar functions to obtain real IP addresses of users.
   ```
   request.getAttribute("X-Forwarded-For")
   ```

Tomcat

If Tomcat is deployed on your origin server, you can enable the **X-Forwarded-For** function of Tomcat to obtain real IP addresses of users.

1. Open the **server.xml** file in the **tomcat/conf/** directory. Partial information about the AccessLogValve logging function is as follows:

   ```
   <Host name="localhost"  appBase="webapps" unpackWARs="true" autoDeploy="true">
           <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
                  prefix="localhost_access_log." suffix=".txt"
                  pattern="%h %l %u %t "%r" %s %b"/>
   ```

2. Add **%{X-Forwarded-For}i** to **pattern**. Part of the modified **server.xml** file is as follows:

   ```
   <Host name="localhost"  appBase="webapps" unpackWARs="true" autoDeploy="true">
           <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
                  prefix="localhost_access_log." suffix=".txt"
                  pattern="%{X-Forwarded-For}i %h %l %u %t "%r" %s %b" />
   </Host>
   ```

3. View the **localhost_access_log** file to obtain real IP addresses of users from the value of the **X-Forwarded-For** field.

Apache

If Apache is deployed on your origin server, you can run commands to install the third-party module mod_rpaf of Apache, and modify the **http.conf** file to obtain real IP addresses of users.

1. Run the following commands to install the third-party module mod_rpaf of Apache:

   ```
   wget https://github.com/gnif/mod_rpaf/archive/v0.6.0.tar.gz
   tar xvfz mod_rpaf-0.6.tar.gz
   cd mod_rpaf-0.6
   /usr/local/apache/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
   ```

2. Open the **httpd.conf** configuration file and modify the file content as follows:

   ```
   LoadModule rpaf_module   modules/mod_rpaf-2.0.so ##Load module mod_rpaf.
   <IfModule mod_rpaf.c>
   RPAFenable On
   RPAFsethostname On
   RPAFproxy_ips 127.0.0.1 <Reverse proxy IP address>
   RPAFheader X-Forwarded-For
   </IfModule>
   ```

3. Define the log format.

   ```
   LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
   common
   ```

4. Enable custom logs.

   ```
   CustomLog"[Apache server directory]/logs/$access.log"common
   ```

5. Restart the Apache server for the configuration to take effect.

   ```
   /[Apache server directory]/httpd/bin/apachectl restart
   ```

6. View the **access.log** file to obtain real IP addresses of users from the value of the **X-Forwarded-For** field.

IIS 6

If IIS 6 is deployed on your origin server, you can install the **F5XForwardedFor.dll** plug-in to obtain real IP addresses of users from access logs recorded by the IIS 6 server.

1. Download the F5XForwardedFor module.
2. Copy the **F5XForwardedFor.dll** file in the **x86\Release** or **x64\Release** directory based on the OS version of your server to a specific directory (for example, **C:\ISAPIFilters**) and ensure that the IIS process has the read permission on the destination directory.

3. Open the Internet Information Services (IIS) Manager, right-click the website that is currently open, and choose **Properties** from the shortcut menu.
4. In the **Properties** dialog box, click the **ISAPI Filters** tab, and click **Add**. In the dialog box that is displayed, configure the following information:
   - **Filter name**: Enter **F5XForwardedFor**.
   - **Executable**: Enter the full path of the **F5XForwardedFor.dll** file, for example, **C:\ISAPIFilters\F5XForwardedFor.dll**.
5. Click **OK** to restart the IIS 6 server.
6. View the access logs recorded by the IIS 6 server (the default log path is **C:\WINDOWS\system32\LogFiles\**, and the IIS log file name extension is .log) to obtain real IP addresses of users from the value of the **X-Forwarded-For** field.

IIS 7

If IIS 7 is deployed on your origin server, you can install the **F5XForwardedFor** module to obtain real IP addresses of users from access logs recorded by the IIS 7 server.

1. Download the F5XForwardedFor module.
2. Copy the **F5XFFHttpModule.dll** and **F5XFFHttpModule.ini** files in the **x86\Release** or **x64\Release** directory based on the OS version of the server to the specific directory (for example, **C:\x_forwarded_for\x86** or **C:\x_forwarded_for\x64**) and ensure that the IIS process has the read permission on the destination directory.
3. Double-click **Modules** in the IIS server option.
4. Click **Configure Native Modules**. In the dialog box that is displayed, click **Register**.
5. In the dialog box that is displayed, register the downloaded DLL file based on the OS and click **OK**.
   - x86: Register the module **x_forwarded_for_x86**.
     - **Name**: Enter **x_forwarded_for_x86**.
     - **Path**: Enter **C:\x_forwarded_for\x86\F5XFFHttpModule.dll**.
   - x64: Register the module **x_forwarded_for_x64**.
     - **Name**: Enter **x_forwarded_for_x64**.
     - **Path**: Enter **C:\x_forwarded_for\x64\F5XFFHttpModule.dll**.
6. After the registration is complete, select the newly registered module (x_forwarded_for_x86 or x_forwarded_for_x64) and click **OK**.
7. In **ISAPI and CGI Restrictions**, add the registered DLL file based on OS and set **Restriction** to **Allowed**.
   - x86
     - **ISAPI or CGI path**: Enter **C:\x_forwarded_for\x86\F5XFFHttpModule.dll**.

        - **Description**: Enter **x86**.

    - x64

        - **ISAPI or CGI path**: Enter **C:\x_forwarded_for\x64\F5XFFHttpModule.dll**.

        - **Description**: Enter **x64**.

8. Restart the IIS 7 server and wait for the configuration to take effect.
9. View the access logs recorded by the IIS 7 server (the default log path is **C:\WINDOWS\system32\LogFiles\**, and the IIS log file name extension is .log) to obtain real IP addresses of users from the value of the **X-Forwarded-For** field.

A Change History

Released On	Description
2023-12-07	This issue is the eighth official release. ● Updated section "Configuring a Policy for a Custom OBS Private Bucket."
2022-03-10	This issue is the seventh official release. ● Added section "Configuring a Policy for a Custom OBS Private Bucket."
2021-12-28	This issue is the sixth official release. ● Updated section "Improving the Cache Hit Ratio."
2021-04-21	This issue is the fifth official release. ● Added the section "Improving the Cache Hit Ratio."
2021-04-02	This issue is the fourth official release. ● Added the section "Accelerating ECS Resources."
2021-03-19	This issue is the third official release. ● Updated the section "Accelerating File Downloads from OBS." ● Added the section "Setting the Maximum Cache Age."
2020-04-15	This issue is the second official release. ● Updated the procedure. ● Optimized some descriptions.
2019-06-27	This issue is the first official release.