CDN

Best Practices

Issue 08

Date 2024-11-14

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions

and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

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 Delivery of OBS Resources..... 1
1.1 Solution Overview..... 1
1.2 Configuration Process..... 4
1.3 Configuring a Policy for a Custom OBS Private Bucket..... 8
1.4 Synchronizing Data Stored on Multiple Clouds..... 9
1.5 FAQ..... 11
2 Accelerating Access to Websites Built on ECSs..... 14
3 Accelerating Delivery of Resources Protected by WAF..... 18
4 Setting the Cache TTL..... 25
5 Improving the Cache Hit Ratio..... 32
6 Obtaining Real IP Addresses of Users..... 36
A Change History..... 40

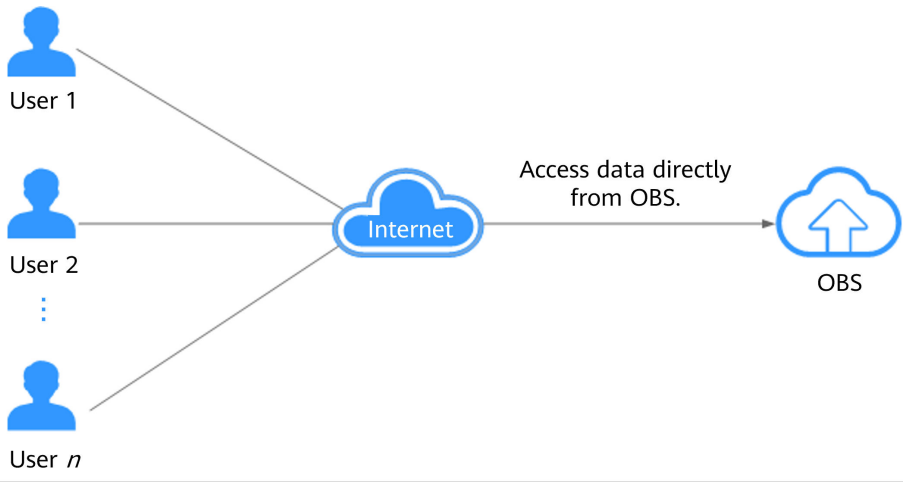
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1 Accelerating Delivery of 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.

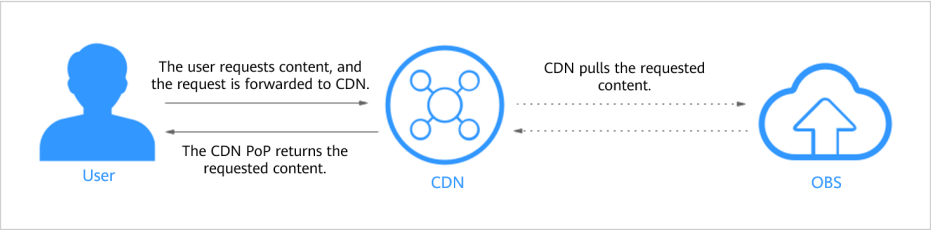


Solution

Huawei Cloud CDN can effectively accelerate distribution of website resources 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

point of presence (PoP) with the fastest response speed. If a CDN PoP has cached the content, it directly returns the content to the user. If the CDN PoP does not cache the content, it pulls the content from the origin server, returns the content to the user, and caches the content.



Resources and Costs

The following table lists the resources required for this practice.

Resource	Description	Monthly Fee
CDN	**Traffic**: traffic generated when users access CDN PoPs. You can purchase traffic packages to deduct it.	For billing details, see **Billing**.
OBS	**Traffic**: outgoing Internet traffic generated when CDN pulls content from OBS, billed in pay-per-use mode. If you set the origin server type to **OBS bucket** and select a bucket of version 3.0 or later, you can purchase pull traffic packages to deduct the traffic.	For details about OBS billing modes and standards, see **Billing**.

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 pull 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 stable acceleration.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Scenario

- 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 stores.
- 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** 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 **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. Therefore, 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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.2 Configuration Process

Background

A game website mainly serves users in the Chinese mainland. It has a large number of files such as software packages and pictures stored on OBS. As the number of users increased, game downloading and image loading became 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 cannot provide the acceleration service for the domain name. • For details about how to obtain a license for a domain name on Huawei Cloud, see **ICP License Service**.	download.game-apk1.com (licensed)
OBS bucket	The OBS bucket version is 3.0 or later, the bucket policy is public read, and static website hosting is not enabled.	obs-doc-test

Procedure

1. Store static resources such as images and software packages of the website in the prepared OBS bucket. You can create a bucket and upload files using OBS Console, OBS Browser, or SDK. For details, see **OBS documentation**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2. Add a domain name on CDN.
   a. Log in to **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 Names**.
   d. Configure the domain name and CDN acceleration information.
      - **Service Area**: Select **Chinese mainland**.
      - **Domain Names**: Enter **download.game-apk1.com**. If you add this domain name to CDN for the first time, verify its ownership.
      - **Service Type**: Select **File download**.
      - **Origin Server Settings**
        - **Origin Protocol**: Select **Same as user**.
        - **Type**: Select **OBS bucket**.
        - **Address**: Select the **obs-doc-test** bucket.
        - **Static website hosting**: Do not select this option.
        - **Bucket**: Select **Public bucket**.
        - **Priority**: Select **Primary origin server**.
        - **Host Header**: By default, the bucket domain name is used.

        NOTE

        - 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 Headers**, and set **Content-Disposition** to **inline**. For details, see **How Do I Preview Objects in OBS in a Browser Online?**
        - 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**.
   e. Click **OK**.
3. Configure a CNAME record on DNS.
   After the domain name is added, CDN automatically generates a CNAME for the domain name. The CNAME cannot be accessed directly. You must add it to your domain's DNS records. Then requests for your domain name will be redirected to CDN PoPs for acceleration. In this practice, the automatically generated CNAME 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. In the upper left corner of **Huawei Cloud console**, choose **Service List** > **Networking** > **Domain Name Service**.
      The DNS console is displayed.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

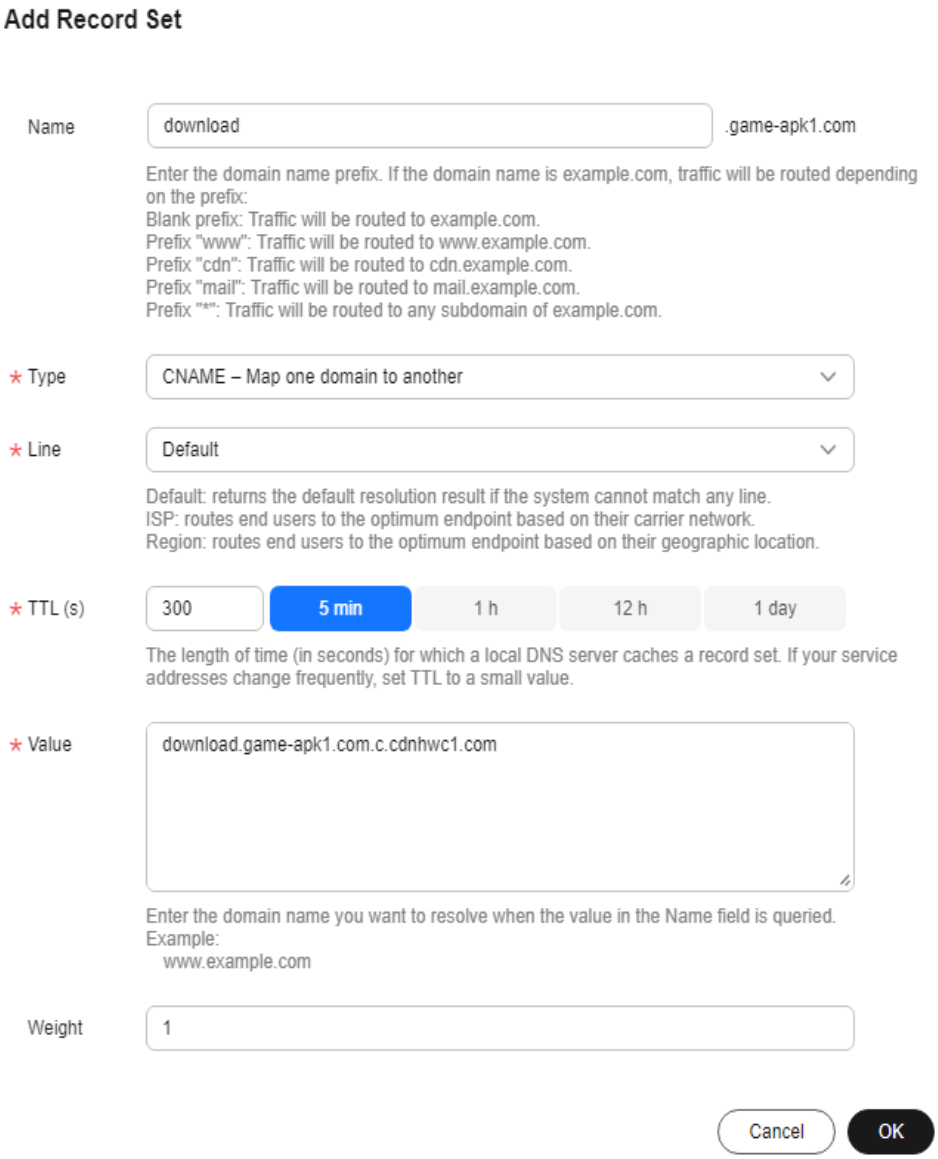
b. In the navigation pane, choose **Public Zones**.

   The public zone list is displayed.

c. Click the domain name you want to add a record set to. In this practice, 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.

Figure 1-1 Adding a record set



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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

f. Click **OK**.

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

5. 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
   ```

6. 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

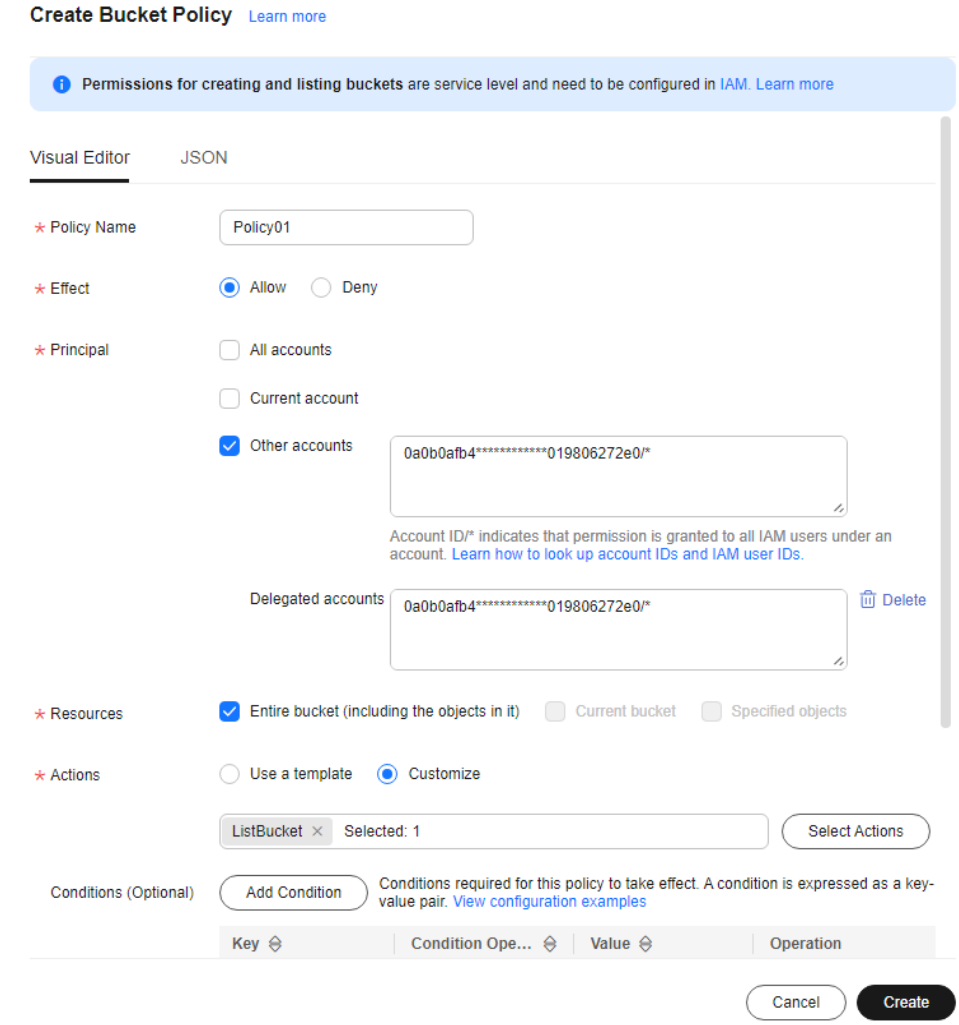
Procedure

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 under **Operations on Buckets**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 1-2 Creating a bucket policy

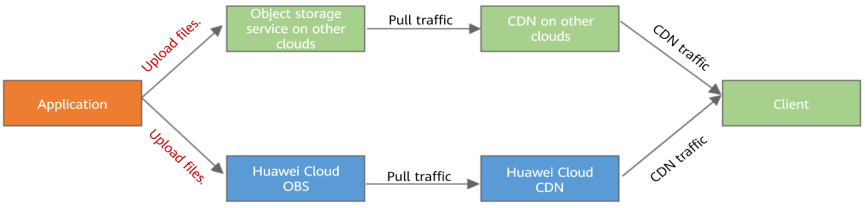


5. Click **Create**.

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 a server, the dual-write solution is recommended. The following figure shows the architecture.



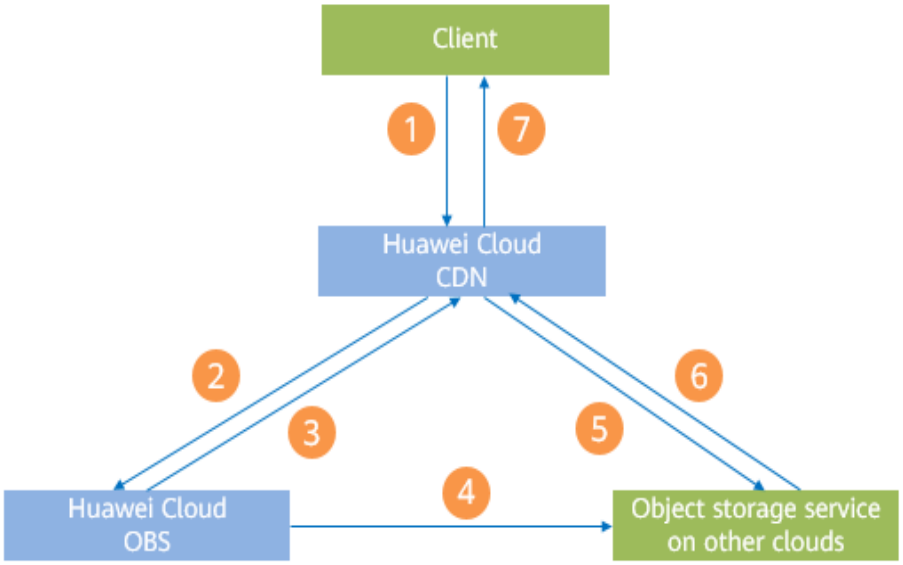
Applications can interconnect with SDKs of two object storage services to write files to the two object storage systems in synchronous or asynchronous mode. The

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

upstream traffic of object storage services is free of charge. Therefore, using this architecture does not increase any cost.

Back to Source

If an OBS bucket does not have a requested file, enable the back-to-source function to redirect the client 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 pulls 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

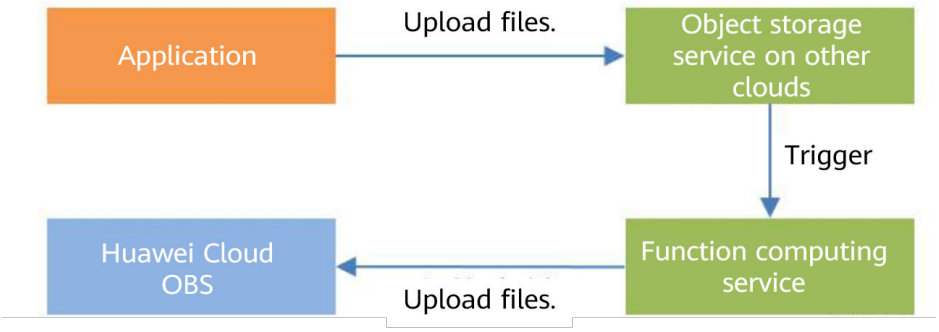
The back-to-source function is triggered only when OBS initiates a request. Therefore, after a new file is uploaded to another object storage service, it is recommended that the application sends a GET request to OBS. The connection can then be closed without receiving entity data. This mechanism generates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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 1-3 Serverless upload



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 Pull 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 as the origin server type 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 of the CDN console.
      i. Click the target domain name on the **Domains** page.
      ii. In the **Origin Server Settings** area, locate the row that contains the target origin server and click **Edit** in the **Operation** column.
      iii. Select **Static website hosting** and click **OK**.
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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Why Is a File in an OBS Bucket with CDN Acceleration Enabled 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 Headers**, and set **Content-Disposition** to **inline**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2 Accelerating Access to Websites Built on ECSs

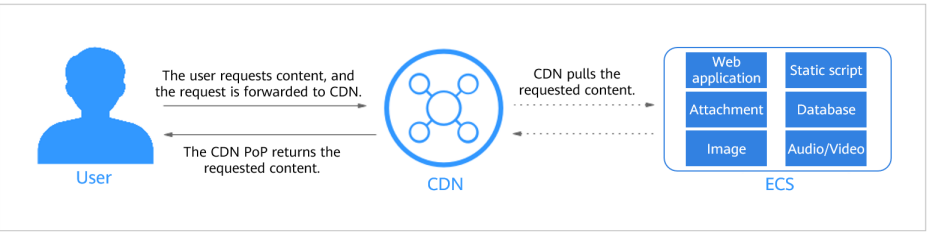
Background

An ECS is a basic computing component that consists of CPUs, memory, OS, and Elastic Volume Service (EVS) disks. Flexible ECS configuration helps save a large amount of hardware costs. Assume that a customer deployed a forum website accessible through a domain name on Huawei Cloud ECS. The initial service volume was small, and user access was smooth. As the services grew, the access traffic increased sharply. Users complained about problems such as slow access. To improve the access speed and user experience, the customer decided to use Huawei Cloud CDN.

Solution Overview

Using Huawei Cloud CDN to accelerate content delivery for websites built on ECSs can reduce costs and improve user experience.

Service process: 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 a CDN PoP has cached the content, it directly returns the content to the user. If the CDN PoP does not cache the content, it pulls the content from the origin server, returns the content to the user, and caches the content.



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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

Procedure

1. Set up a forum website on an ECS. For details, see **Setting Up a Discuz Forum**.
   - The IP address of the server is 192.168.1.1.
   - The domain name of the website is discuztest.com.
2. Enable CDN.
   a. Log in to **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

      The CDN console is displayed.
   b. Click **Enable Now**.
   c. Select a billing option, read and agree to the service agreement, and click **Enable Now**.
3. Add a domain name on CDN.
   a. In the navigation pane of the CDN console, choose **Domains**.
   b. On the **Domains** page, click **Add Domain Names** and configure the acceleration domain name and origin server information.
      - **Domain Names**: Enter **discuztest.com**.
      - **Service Area**: Select **Chinese mainland**.
      - **Service Type**: Select **Website**.
      - **Origin Server Settings**
        - **Origin Protocol**: Select **HTTP**.
        - **Type**: Select **IP address**.
        - **Address**: Enter **192.168.1.1**.
        - **Priority**: Select **Primary origin server**.
        - **Host Header**: By default, the acceleration domain name is used.
   c. 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.
4. 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. Configure CNAME resolution. CDN automatically generates a CNAME after you add a domain name. The CNAME cannot be accessed directly. You must add it to your domain's DNS records. Then requests for your domain name will be redirected to CDN PoPs for acceleration.

   In this practice, the generated CNAME is **discuztest.com.c.cdnhwc1.com**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

a. In the upper left corner of **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 practice, the domain name is **discuztest.com**.

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

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.	www
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.	5 min
Value	Domain name to be pointed to. If CDN acceleration is not enabled, the value is the ECS domain name. If CDN acceleration is enabled, the value is the CNAME generated by CDN.	discuztest.com.c.cdnhwc1.com

f. Click **OK**.

6. Check whether 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 practice, the acceleration domain name is **discuztest.com**. If the CNAME generated by CDN is displayed, the CNAME configuration has taken effect.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

7. Check whether the configuration is successful.

   Log in to the forum website and browse web pages. If the website can be visited, the acceleration configuration is successful.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3 Accelerating Delivery of Resources Protected by WAF

Scenario

CDN is a smart virtual network on the Internet infrastructure. 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), web shells, 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 delivery of website resources, defend against web attacks, and secure your websites.

NOTE

- In this practice, **CDN has been enabled**, the acceleration domain name is **www.example.com**, and the domain name is resolved on Huawei Cloud.
- The domain name has been **licensed**.

Solution Overview

The CDN+WAF solution protects your domain names and accelerates response speed of the websites regardless of their locations, on Huawei Cloud or not. 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Solution Advantages

This solution shortens website content access latency, speeds up website response, and improves website availability. You can stop worrying about low network bandwidth, large user access traffic, and uneven distribution of branches. Besides that, this combination protects your website from web application attacks, such as SQL injections, XSS, web shells, command/code injections, file inclusion, sensitive file access, third-party application vulnerability exploits, CC attacks, malicious crawlers, and cross-site request forgery.

Resources and Costs

The following table lists the resources required for this practice.

Resource	Description	Monthly Fee
CDN	• Billing mode: pay-per-use • Resource packages available	For billing details, see **Billing**.
WAF	Cloud - Standard edition • Billing mode: Yearly/Monthly • Domain name quota: 10, including a maximum of one top-level domain name • QPS quota: 2,000 QPS • Peak bandwidth: 100 Mbit/s inside the cloud and 30 Mbit/s outside the cloud	For billing details, see **Billing**.

Procedure

1. Purchase the standard edition of cloud WAF.
   a. Log in to **Huawei Cloud console**.
   b. Choose **Service List** > **Security & Compliance** > **Web Application Firewall**.
   c. In the upper right corner, click **Buy WAF**. On the displayed page, set **WAF Mode** to **Cloud Mode**.
      - **Region**: Select the region nearest to your services to be protected.
      - **Edition**: Select **Standard**.
      - **Standard Expansion Package** and **Required Duration**: Set them as required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

d. Confirm the details and click **Buy Now**.

e. Check the order details, read and agree to the *Huawei Cloud WAF Disclaimer*, and click **Pay Now**.

f. On the payment page, select a payment method and pay for your order.

2. Add website information to WAF.

a. In the navigation pane of the WAF console, choose **Website Settings**.

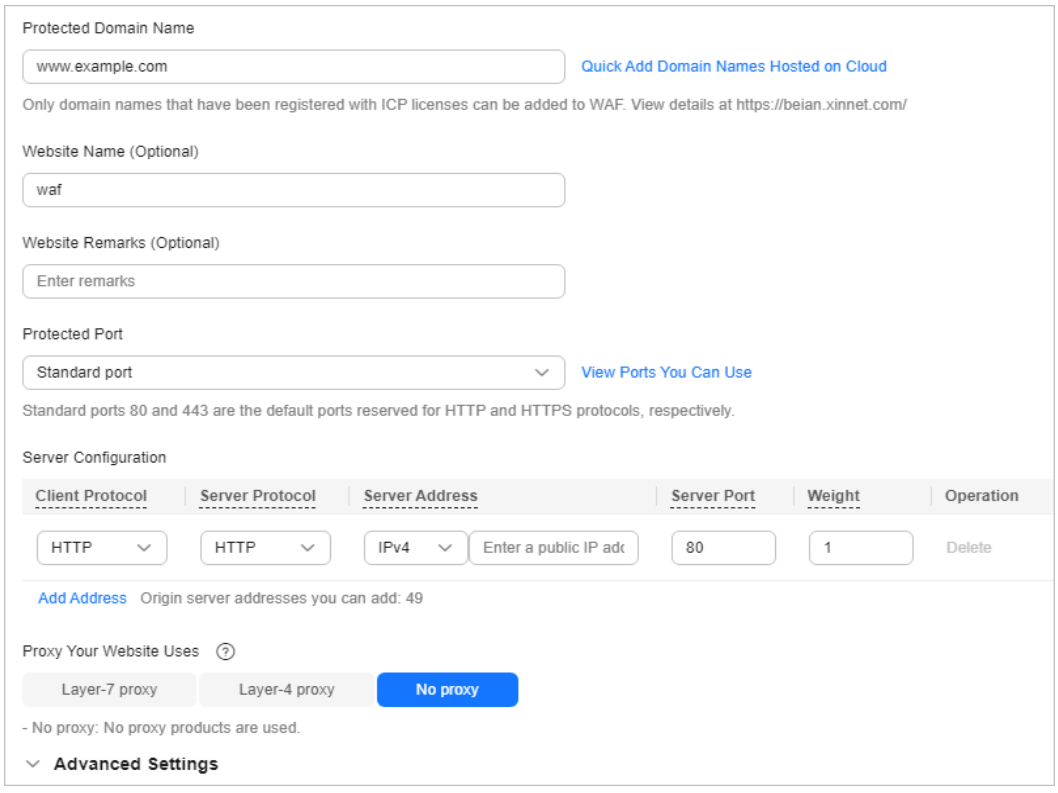
b. In the upper left corner of the website list, click **Add Website**.

c. Select **Cloud - CNAME** and click **OK**.

- For details about the **Cloud - Load balancer** mode, see **Connecting a Website to WAF (Cloud Mode - Load Balancer Access)**

d. Configure website information based on **Table 3-1**.

Figure 3-1 Basic information configuration



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-1 Key parameters

Parameter	Description	Example
Domain Name	Domain name you want WAF to protect. • The domain name has been licensed. • You can enter a top-level single domain name, like example.com, a second-level domain name, like www.example.com, or a wildcard domain name, like *.example.com.	www.example.com
Protection Port	Service port corresponding to the domain name of the website you want to protect.	Standard port

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example
Server Configuration	Configurations of your web server address. You need to configure the client protocol, server protocol, server address, server port, and server weight. • **Client Protocol**: protocol used by a client to access a server. The options are **HTTP** and **HTTPS**. • **Server Protocol**: protocol used by WAF to forward client requests. The options are **HTTP** and **HTTPS**. • **Server Address**: public IP address (generally corresponding to the A record of the domain name configured on DNS) or domain name (generally corresponding to the CNAME of the domain name configured on DNS) of the web server that a client accesses. • **Server Port**: service port over which the WAF instance forwards client requests to the origin server. • **Weight**: Requests are distributed across backend origin servers based on the load balancing algorithm you select and the weight you assign to each server.	**Client Protocol**: **HTTP** **Server Protocol**: **HTTP** **Server Address**: **IPv4** *XXX.XXX.1.1* **Server Port**: **80**
Proxy Your Website Uses	Other proxies you deploy in front of WAF. In this example, **Layer-7 proxy** is selected.	Layer-7 proxy

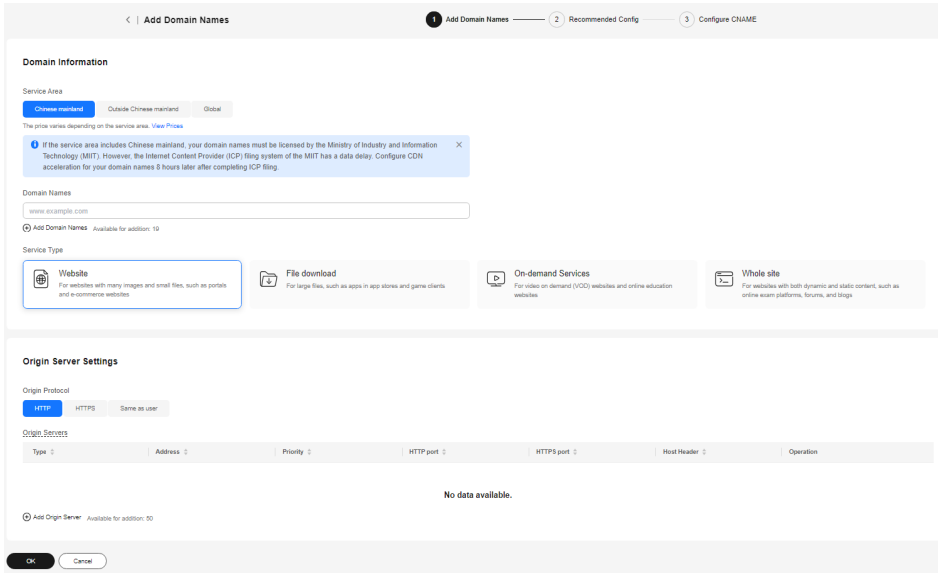
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

- 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.

e. Click **Next** and finish configuration by referring to **Whitelist WAF Back-to-Source IP Addresses** and **Verification**.

3. Copy the CNAME generated by WAF. On the basic information page of the domain name, click under **CNAME**.
4. Add the domain name to CDN.
   a. In the upper left corner of **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 Names** and specify domain parameters.
      - When adding an origin server, set **Type** to **Domain name** and **Address** to the CNAME generated by WAF.



   d. Click **OK**. CDN generates a dedicated CNAME for the domain name.
5. (Optional) Test your acceleration 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**.
6. Configure CNAME resolution.
   a. In the upper left corner of **Huawei Cloud console**, choose **Service List** > **Networking** > **Domain Name Service**.
      The DNS console is displayed.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

b. In the navigation pane, choose **Public Zones**.

c. Click the domain name you want to add a record set to. Configure the following parameters:

- **Name**: Enter **www**.
- **Type**: Select **CNAME – Map one domain to another**.
- **Alias**: Select **No**.
- **Line**: Select **Default**.
- **TTL (s)**: The recommended value is **5 min**. The larger the TTL value, the slower the update of DNS records.
- **Value**: Enter the CNAME generated in **4**.
- Keep other settings unchanged.

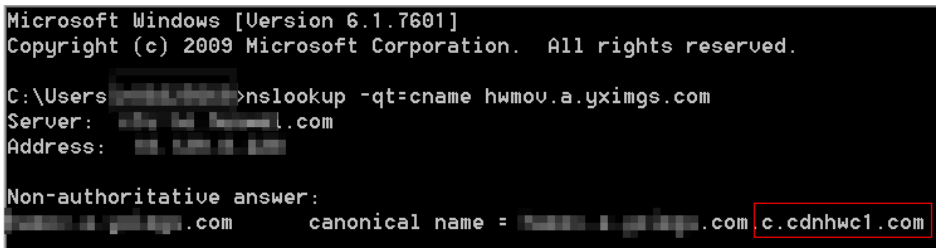
d. Click **OK**.

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



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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4 Setting the Cache TTL

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 cache TTL 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 pull 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 TTL on the origin server, this TTL 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 a Cache TTL Based on Service Type

Default cache TTL

- If the service type is website acceleration, file download acceleration, or on-demand service acceleration, and the origin server address is an IP address or domain name, the following default cache rules are available:
  - The default cache TTL 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 cache TTL for other files is 30 days. You can modify but cannot delete this rule.
- If your origin server is an OBS bucket, the default cache TTL for all files is 30 days. You can modify but cannot delete this rule.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 **TTL** set to **0** is available by default. You can modify and delete this rule.

You can configure a cache TTL based on the service type and the following suggestions.

- Website acceleration
  - 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 seven days.
  - Cache other static files for 30 days.
- Download acceleration
  - Do not cache dynamic files such as php, aspx, asp, jsp, and .do files.
  - Cache files of the following 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.
- On-demand service acceleration
  - Do not cache dynamic files such as .php, .aspx, .asp, .jsp, and .do files.
  - Cache the following file types for seven 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 **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. **Table 4-1** describes the parameters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-1 Configuring a cache rule

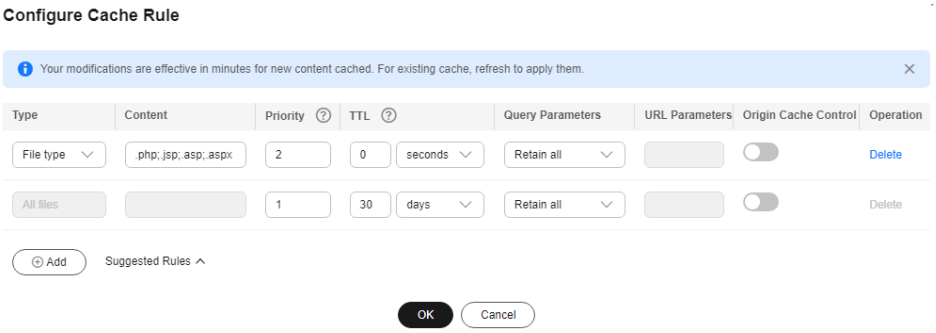


Table 4-1 Cache rule parameters

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 cache TTL 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 cache TTL 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**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Configuration Rule
Full path	A specific file	A full path must start with a slash (/) and cannot end with a wildcard (*). 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.
TTL	Duration that a file can be cached. If the cache TTL 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 cache TTL 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 TTL to more than one month. ● For static files (such as JS and CSS files) that are frequently updated, set the TTL based on service requirements. ● For dynamic files (such as PHP, JSP, and ASP files), set the TTL to 0 seconds.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Configuration Rule
Query Parameters	Most web page requests carry URL parameters starting with a question mark (?). If parameters do not contain important information (such as version), you can ignore them to improve the cache hit ratio and speed up delivery. **Configuration rules:** • If resources do not change with URL parameters, ignore query parameters. • If resources change with URL parameters, retain query parameters. • If you have enabled video seek, set **Query Parameters** to **Ignore all** for your video resources.	• **Retain all**: CDN retains all parameters following the question mark (?). • **Ignore all**: CDN ignores all parameters following the question mark (?) in request URLs, improving the cache hit ratio. • **Ignore specific**: CDN ignores the specified parameters in request URLs but retains other parameters. • **Retain specific**: CDN retains the specified parameters in request URLs but ignores other parameters.
URL Parameters	Parameters to be ignored or retained. Leave this parameter blank when **Query Parameters** is set to **Retain all** or **Ignore all**.	• Enter up to 10 parameter names separated by semicolons (;). • Only letters, digits, periods (.), underscores (_), and tildes (~) are supported.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Configuration Rule
Origin Cache Control	If **Cache-Control: max-age** or **Expires** has been configured on the origin server and you want the cache TTL on the CDN side to be the same as that configured on the origin server, you can switch on **Origin Cache Control**. Then **Cache-Control: max-age** or **Expires** determines how long content is cached on CDN PoPs. **NOTE** • If both **Cache-Control** and **Expires** are configured on the origin server, **Cache-Control** is preferentially used. • If origin cache control is enabled on CDN but neither **Cache-Control** nor **Expires** is configured on the origin server, CDN PoPs use the cache rules configured on CDN.	By default, this function is disabled.

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

NOTE

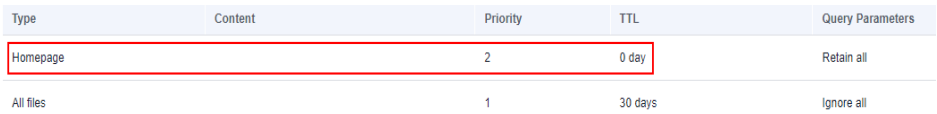
If you have modified a cache rule,

- Your modifications are effective for new content cached.
- You can purge to apply modifications to the existing cache.

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 **TTL** to **0**.

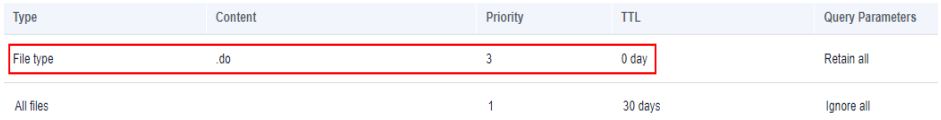


Scenario 2: Assume that you do not want to cache files of a specific type or a specific web page.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1. You have configured CDN acceleration for your website and set the cache TTL 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 **TTL** to **0**.

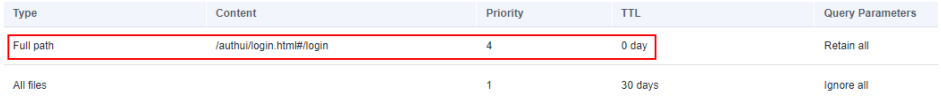
Type	Content	Priority	TTL	Query Parameters
File type	.do	3	0 day	Retain all
All files		1	30 days	Ignore all

   NOTE

   The new rule only applies to new content. After the new rule is added, purge 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.

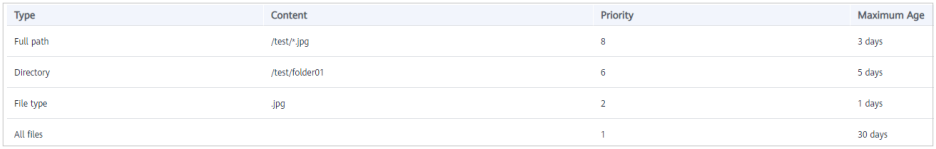
2. You have configured CDN acceleration for your website, the login page of your website is displayed cyclically, and your customers cannot log in to the website. After CDN acceleration is disabled, customers can log in to the website.

   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 cache TTL 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 **TTL** to **0**.

Type	Content	Priority	TTL	Query Parameters
Full path	/authui/login.html#/login	4	0 day	Retain all
All files		1	30 days	Ignore all

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 origin pull 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.

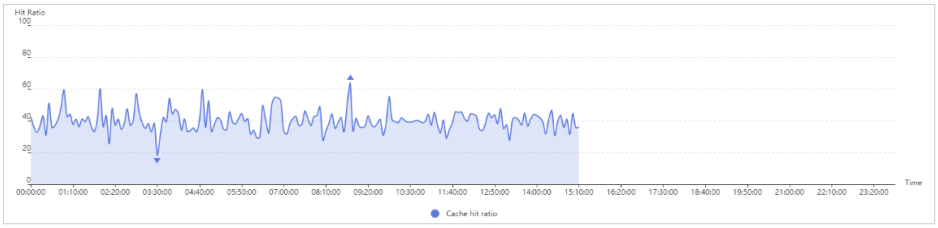
1. Log in to **Huawei Cloud console**. Choose **Service List** > **Content Delivery & Edge Computing** > **Content Delivery Network**.

   The CDN console is displayed.
2. In the navigation pane, choose **Analytics**.
3. Choose **Traffic** and **Requests** under **Analytics** to view the traffic hit ratio and request hit ratio.

Figure 5-1 Traffic hit ratio

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 5-2 Request hit ratio



Optimizing the Cache Hit Ratio

1. Set an appropriate cache TTL.

   CDN caches origin content on globally distributed PoPs so that users can obtain the content from nearby PoPs. You can set a proper TTL 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 TTL to more than one month.
   - For static files (such as JS and CSS files) that are frequently updated, set the TTL based on service requirements.
   - For dynamic files (such as PHP, JSP, and ASP files), set the TTL to **0**, so these files will not be cached on CDN PoPs.

   For details, see **Setting the Cache TTL**.

   NOTE

   - By default, **Origin Cache Control** is disabled. 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 frequently pulls content from the origin server.
   - 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 pulls the resource.
   - If origin content has been updated, purge the URLs of the content to ensure that users can obtain the latest content.
   - **If you have modified a cache rule,**
     - Your modifications are effective for new content cached.
     - You can purge to apply modifications to the existing cache.

2. Set URL parameter rules.

   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. When setting a cache rule, you can set **Query Parameters** to **Ignore all** or **Ignore specific** to improve the cache hit ratio and distribution efficiency. For details, see **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 pulls that content from the origin server. If **Query Parameters** is set to **Ignore all** 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- When a user requests **http://www.example.com/1.txt?test1** for the first time, the content is not cached on CDN, and CDN pulls that content from the origin server. If **Query Parameters** is set to **Retain all** on CDN, 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 pull **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 prefetch. When users access the content, they can directly obtain the latest content from CDN PoPs. For details, see **Cache Prefetch**.

   Content prefetch can help you improve 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 prefetch 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 prefetch 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 prefetch 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 pull the entire video from the origin server when range requests are disabled. As a result, the pull traffic is greater than the traffic used for returning the content to the user, decreasing the cache hit ratio. When range requests are enabled, CDN only needs to pull the requested video clip and returns it 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 purge the URL of the cached content to force the cache on CDN PoPs to expire. Purging the entire directory will force the cache of all content in the directory to expire. When a user accesses a resource in the directory, no cache is hit and CDN needs to pull the resource from the origin server. Therefore, do not purge the entire directory, especially the root directory.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- Do not carry dynamic parameters in URLs.

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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. Obtain real IP addresses of users from the value of the **X-Forwarded-For** field in the **localhost_access_log** file.

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. Obtain real IP addresses of users from the value of the **X-Forwarded-For** field in the **access.log** file.

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**). Ensure that the IIS process has the read permission on the destination directory.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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. Obtain real IP addresses of users from the value of the **X-Forwarded-For** field in 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).

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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- **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. Obtain real IP addresses of users from the value of the **X-Forwarded-For** field in 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).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

A Change History

Released On	Description
2024-06-13	This issue is the ninth official release. • Added section "Periodically Purging the Cache Using FunctionGraph."
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."

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Released On	Description
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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.