

CDN

# 最佳实践

文档版本 19  
发布日期 2024-05-21



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

---

# 目录

---

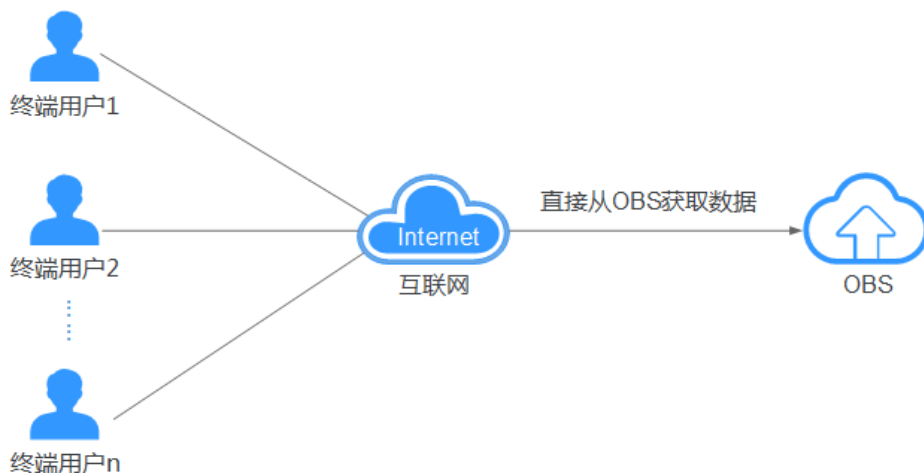
<b>1 CDN 加速 OBS 桶文件</b> .....	<b>1</b>
1.1 方案概述.....	1
1.2 CDN 加速 OBS 桶文件（CDN 控制台）.....	3
1.3 CDN 加速 OBS 桶文件（OBS 控制台）.....	6
1.4 自定义 OBS 私有桶策略配置.....	10
1.5 多云存储数据同步方案.....	12
1.6 CDN 加速 OBS 常见问题.....	13
<b>2 CDN 加速 ECS 资源</b> .....	<b>16</b>
<b>3 CDN 加速 WAF 防护资源</b> .....	<b>20</b>
<b>4 如何设置缓存过期时间</b> .....	<b>24</b>
<b>5 如何提高缓存命中率</b> .....	<b>30</b>
<b>6 推送 CDN 日志到云日志服务（LTS）</b> .....	<b>33</b>
<b>7 CDN 日志转存到 OBS</b> .....	<b>39</b>
<b>8 获取客户端真实 IP</b> .....	<b>48</b>
<b>9 CDN 加速云速建站 CloudSite</b> .....	<b>52</b>
<b>10 源站是 OBS 桶时如何配置自定义首页内容</b> .....	<b>54</b>
<b>11 通过日志分析恶意访问地址</b> .....	<b>56</b>
<b>12 客户端访问加速域名经过 Nginx 转发时，如何定期刷新 DNS 解析</b> .....	<b>58</b>
<b>A 修订记录</b> .....	<b>60</b>

# 1 CDN 加速 OBS 桶文件

## 1.1 方案概述

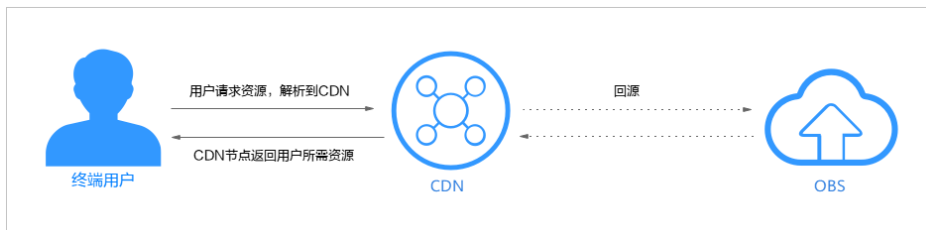
### 背景介绍

现在越来越多的行业使用OBS桶存储图片、视频、软件包等静态资源文件，并将OBS桶作为网站、论坛、APP、游戏等业务的存储源。在需要获取这些静态资源时，用户通过URL直接从OBS桶请求数据。OBS桶能够很好的解决本地存储不够用的难题，但一般情况下文件只存储在一个区域，不同区域的用户访问OBS桶的响应速度存在差异。在需要频繁访问的场景下，直接访问OBS桶来获取相应文件，还会消耗大量的流量费用。



### CDN 加速 OBS 文件方案

华为云CDN可以有效加速网站，为用户提供良好的体验，而OBS桶提供海量文件存储。将数据存放在OBS桶中然后通过配置CDN加速，这样构造的业务系统可以在降低成本的同时，提高终端用户使用感受。当终端用户发起访问请求时，会首先通过CDN查找对此域名响应速度较快的CDN节点，并查询此节点是否有缓存终端用户请求的内容。如果CDN节点有缓存用户所需资源，直接将资源返回给用户；如果CDN节点无缓存，则回源请求资源返回给用户，同时将资源缓存到CDN节点。



## 方案优势

1. 低成本
  - CDN加速OBS桶文件后，资源缓存在CDN节点，用户请求无需回源，而CDN加速的费用较低，二者配合使用可以节约50%到57%的带宽成本，详见[通过CDN减少OBS公网带宽费用](#)。
  - OBS桶提供CDN回源流量包折扣方式，使CDN从OBS桶获取数据时流量费用更低，计费详情请见[CDN加速OBS计费规则](#)。

### 📖 说明

CDN加速OBS桶不支持走内网。

2. 高效率
  - 华为云CDN具有加速资源丰富、节点分布广泛优势，保证将用户请求精准调度至较优边缘节点，提供有效且稳定的加速效果。
3. 自动刷新
  - 通过OBS控制台为您的桶绑定加速域名后，支持自动刷新配置，您可以参考[配置CDN自动刷新](#)完成相关配置。

## 适用场景

- 通过OBS桶提供文件下载业务的应用或服务。例如：通过HTTP/HTTPS提供文件下载业务的网站、工具下载、游戏客户端、APP商店等。
- 通过OBS桶提供音视频点播业务的应用或服务。例如：在线教育类网站、在线视频分享网站、互联网电视点播平台、音乐视频点播APP等。
- 通过OBS桶提供图片素材等的网站。例如：包括门户网站、电商平台、资讯APP、UGC应用（User Generated Content，用户原创内容）等

## 约束与限制

- 只有版本号为3.0及以上的桶支持此方案。桶版本号可以在OBS控制台上，进入桶概览页面后，在“基本信息”中查看。
- 当OBS配置了镜像回源且CDN侧开启Range回源时，如果镜像源站未遵循RFC Range Requests标准，对range请求响应非206，CDN会回源失败。如需支持该场景，请提工单申请。
- 当CDN源站类型为“OBS桶域名”且接入的是OBS私有桶时，不支持文件上传操作。如果您需要通过CDN将文件上传到OBS私有桶，需要以“源站域名”的形式将OBS私有桶接入CDN，同时，客户端携带鉴权请求头上传文件。

### 📖 说明

OBS私有桶以源站域名接入CDN后，因CDN无私有桶上传权限，此时客户端无法正常访问加速域名。使用GET/HEAD等方式通过此加速域名请求资源时，也需携带鉴权请求头。

## KMS 加密文件配置

CDN默认无法读取OBS桶中的加密文件，如果您的OBS桶存在此类文件，建议您慎重开启CDN加速，避免加密对象泄露。如果您因业务需求，需要加速OBS桶中的KMS加密文件，请注意：

- 如果您的OBS桶是公有桶，CDN将无法读取桶中的KMS加密文件，从而导致回源失败，用户无法访问到加密文件。  
解决方案：将公有桶中的加密文件转移到私有桶中，再接入CDN加速。
- 如果您的OBS桶是私有桶，需要为“CDNAccessPrivateOBS”委托配置“KMS Administrator”权限。如此，CDN才能读取OBS私有桶中的KMS加密文件并加速，配置过程详见[OBS委托授权](#)。

## 1.2 CDN 加速 OBS 桶文件（CDN 控制台）

### 场景介绍

某游戏网站目前已购买OBS桶服务，并存放了大量游戏软件、图片等文件在OBS中。随着用户不断增长，游戏下载、图片加载都存在响应较慢的问题，特别是离文件存放区域较远的用户。基于以上诉求，该网站决定采用CDN加速访问OBS方案，以最低成本实现游戏下载加速，提升用户访问体验。

### 数据准备

准备项	说明	示例
网站域名	游戏网站域名。如果您的加速范围为“中国大陆”或“全球”，根据中国《互联网管理条例》的要求，此域名必须在 <b>工信部备案并在有效期内</b> 才可以 <b>使用CDN加速</b> 。	download.game-apk1.com
OBS桶	版本号为3.0以上的OBS存储桶。	obs-doc-test

### 前提条件

已将网站所需图片、软件包等静态资源存储至已准备的OBS桶中。

#### 📖 说明

- 如果上述操作还未完成，可通过OBS控制台、OBS Browser、SDK等多种方式创建桶、上传文件，具体操作请参考[OBS帮助文档](#)。
- 如果您使用了2022年1月1日以后创建的OBS桶作为源站，并且需要支持在线预览功能，您要在CDN控制台>域名管理>高级设置>HTTP header配置，将“Content-Disposition”的值设为“inline”，详见[如何在浏览器中在线预览OBS中的对象？](#)。
- 如果您的OBS桶开启了镜像回源（数据回源），添加加速域名时请勿勾选“静态网站托管”功能，否则会造成数据回源不生效，详见[数据回源](#)。

## 配置步骤

### 1. 在CDN控制台添加加速域名

- a. 登录[华为云控制台](#)，选择“所有服务 > CDN与智能边缘 > 内容分发网络CDN”，进入CDN管理控制台。
- b. 单击左侧“域名管理”，进入域名管理页面。
- c. 在域名管理页面单击“添加域名”。
- d. 配置域名及CDN加速等信息。
  - 服务范围：根据您的业务需要选择服务范围。
  - 加速域名：输入游戏网站域名，此处以download.game-apk1.com为例。
  - 业务类型：实际业务结合[应用场景](#)选择合适的业务类型。
  - 源站配置：
    - 回源方式：根据需要选择合适的回源方式。
    - 源站类型：选择“OBS桶域名”。
    - 源站地址：选择本账号下的OBS桶域名或自定义OBS桶域名。
    - 静态网站托管：如果OBS桶开启了静态网站托管，同步勾选。
    - 桶类型：根据桶策略勾选公有桶或私有桶。
    - 优先级：主源站或备源站。
    - 回源HOST：默认为桶域名。

#### 说明

如果您使用[自定义OBS私有桶](#)作为源站，您需要为私有桶配置桶策略，配置详见[自定义OBS私有桶策略配置](#)。

- e. 单击“确定”，完成域名添加。

### 2. 配置CNAME

添加加速域名后，CDN会自动生成一条CNAME域名。加速域名在CDN服务中获得的CNAME域名不能直接访问，必须在加速域名的域名服务商处配置CNAME记录，将加速域名指向CNAME域名，访问加速域名的请求才能转发到CDN节点上，达到加速效果。本实践中自动生成的CNAME域名为“download.game-apk1.com.cdnhwc1.com”。不同DNS服务商的CNAME配置方式不同，此处以华为云云解析服务为例。其他DNS服务商的CNAME配置方法可参考[配置CNAME域名解析](#)。

- a. 登录[华为云控制台](#)，在控制台首页选择“网络 > 云解析服务DNS”，进入云解析服务页面。
- b. 在左侧菜单栏中，选择“公网域名”，进入公网域名列表页面。
- c. 在待添加记录集的域名所在行，单击“域名”列的域名名称。本实践中对应的域名为“game-apk1.com.”。
- d. 单击“game-apk1.com”，进入域名解析页面，然后单击右上角“添加记录集”，进入“添加记录集”弹出框。

### 添加记录集 ✕

主机记录  .game-apk1.com. ?

\* 类型

\* 别名 ?  是  否

\* 线路类型  ?

\* TTL (秒)      ?

\* 值  ?

权重

其他配置

e. 根据界面提示填写参数配置，下表中未提到的参数可保持默认值。

参数	说明	示例
主机记录	主机记录指域名前缀。	本示例填写： download
类型	记录集的类型，此处为CNAME类型。	CNAME-将域名指向另外一个域名
别名	用于是否将此记录集关联至云服务资源实例。	否
线路类型	用于DNS服务器在解析域名时，根据访问者的来源，返回对应的服务器IP地址。 添加解析线路类型时，切记先添加默认线路类型，以保证网站可访问。	全网默认
TTL(秒)	TTL指解析记录在本地DNS服务器的有效缓存时间。如果您的服务地址经常更换，建议TTL值设置相对小些，反之，建议设置相对大些。	默认为“5分钟”，即300s。



参数	说明	示例
值	需指向的域名。 如果没有开启CDN加速，该值为桶访问域名；如果开启CDN加速后，该值为CDN分配的CNAME域名。	download.game-apk1.com.cdnhwc1.com

- f. 单击“确定”，完成添加。
- g. 验证CNAME配置是否生效。  
打开Windows操作系统中的cmd程序，输入如下指令：

```
nslookup -qt=cname 桶绑定的自定义域名
```

本实践中桶绑定的自定义域名为“download.game-apk1.com”。如果回显CDN分配的CNAME域名，则表示CNAME配置已经生效。

### 3. 开启OBS委托授权（公共读或公共读写的OBS桶跳过此步骤）

如果您的OBS桶是私有桶，您需要前往CDN控制台开启OBS委托授权，CDN才能从OBS中回源获取数据。具体请参见[OBS委托授权](#)。

#### 说明

- 如果您的私有桶中不希望被公开的资源，请将此部分资源移入其它私有桶中。

### 4. 配置文件下载URL

将代码中需要加速下载的文件URL地址配置为：游戏网站域名+文件在OBS桶中的存储路径+文件名称。

以配置的游戏网站域名download.game-apk1.com以及存储在obs-doc-test桶中的game/3.2.1/文件夹下的android.apk文件为例，文件下载URL的配置如下：

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

### 5. 验证业务

待游戏网站重新部署后，登录游戏网站，浏览网页图片、进行游戏下载。

如果图片可以成功显示、游戏可以成功下载，则表示加速配置成功。

## 1.3 CDN 加速 OBS 桶文件（OBS 控制台）

### 场景介绍

某游戏网站目前已购买OBS桶服务，并存放了大量游戏软件、图片、视频等文件在OBS中。随着用户不断增长，游戏下载、图片加载都存在响应较慢的问题，特别是离文件存放区域较远的用户。基于以上诉求，该网站决定采用CDN加速访问OBS方案，以最低成本实现游戏下载加速，提升用户访问体验。

## 数据准备

准备项	说明	示例
网站域名	游戏网站域名。如果您的加速范围是“中国大陆”或者“全球”，根据中国《互联网管理条例》的要求，此域名必须在 <b>工信部备案并在有效期内</b> 才可以 <b>使用CDN加速</b> 。	download.game-apk1.com
OBS桶	版本号为3.0以上的OBS存储桶。 <ul style="list-style-type: none"> <li>支持CDN加速的区域： 华北-北京一、华北-北京四、华东-上海一、华南-广州、华南-广州-友好用户环境、西南-贵阳一。</li> </ul>	obs-doc-test01

## 前提条件

已将网站所需图片、软件包等静态资源存储至已准备的OBS桶中。

### 说明

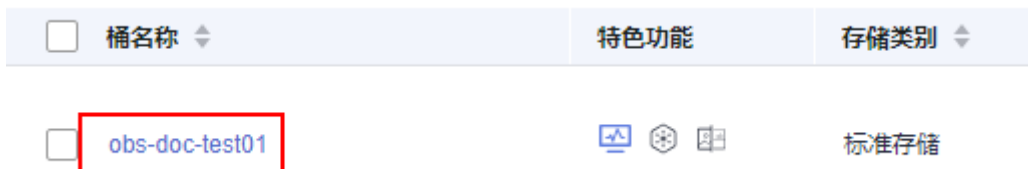
如果上述操作还未完成，可通过OBS控制台、OBS Browser、SDK等多种方式创建桶、上传文件，具体操作请参考[OBS帮助文档](#)。

## 配置步骤

### 1. 在OBS控制台中开启CDN加速

OBS支持域名管理功能，在OBS上绑定用户域名即可实现使用自定义域名访问OBS，且可以直接在绑定过程中开启CDN加速，不用前往CDN控制台开启。

- 登录[华为云控制台](#)，选择“所有服务 > 存储 > 对象存储服务 OBS”，进入OBS管理控制台。
- 单击存放软件包的桶名称，此处以obs-doc-test01为例，进入桶管理页面。



- 左侧导航栏选择“域名管理”，单击“配置加速域名”。
- 在“配置加速域名”弹框中配置域名及CDN加速等信息。
  - 服务范围：根据用户所在区域选择适合的服务范围。

- 用户域名：输入游戏网站域名，此处以download.game-apk1.com为例。
- 业务类型：实际业务结合[应用场景](#)选择合适的业务类型。

### 配置加速域名

- 1 添加加速域名  
使用CDN加速域名
- 2 解析CNAME  
解析域名后才可达到加速效果

#### 业务场景

\* 源站信息 OBS桶域名: obs-doc-test01.obs.cn-north-4.myhuaweicloud.com

\* 服务范围  中国大陆  中国大陆境外  全球

\* 业务类型

网站加速  
适用于门户网站、电商平台、资讯APP、UGC应用等有加速需求的网站

文件下载加速  
适用于下载工具、游戏客户端、APP商店等使用文件下载业务的网站

点播加速  
适用于在线教育、在线视频分享、视频点播等需要加速音频/视频的网站

域名信息 用户域名必须在工信部完成备案，请您确保域名已备案。 [前往备案](#)

\* 加速域名

(1/5)

#### 其他信息

静态网站托管  开启

#### 📖 说明

OBS侧配置加速域名暂时不支持HTTPS访问加速域名，只支持HTTP访问加速域名。

- 客户配置加速域名后，如果想使用HTTPS进行访问，需通过CDN管理控制台配置HTTPS证书，即可使用HTTPS访问。

e. 单击“确定”。

## 2. 配置CNAME

在OBS绑定用户域名时开启CDN加速后，CDN会自动生成一条CNAME域名。加速域名在CDN服务中获得的CNAME域名不能直接访问，必须在加速域名的域名服务商处配置CNAME记录，将加速域名指向CNAME域名，访问加速域名的请求才能

转发到CDN节点上，达到加速效果。本实践中自动生成的CNAME域名为“download.game-apk1.com.cdnhwc1.com”。不同DNS服务商的CNAME配置方式不同，此处以华为云解析服务为例。其他DNS服务商的CNAME配置方法可参考[配置CNAME域名解析](#)。

- 登录[华为云控制台](#)，在控制台首页选择“网络 > 云解析服务DNS”，进入云解析服务页面。
- 在左侧菜单栏中，选择“公网域名”，进入公网域名列表页面。
- 在待添加记录集的域名所在行，单击“域名”列的域名名称。本实践中对应的域名为“game-apk1.com。”。
- 单击“game-apk1.com”，进入域名解析页面，然后单击右上角“添加记录集”，进入“添加记录集”弹出框。

- 根据界面提示填写参数配置，下表中未提到的参数可保持默认值

参数	说明	示例
主机记录	主机记录指域名前缀。	本示例填写： download
类型	记录集的类型，此处为CNAME类型。	CNAME-将域名指向另外一个域名
别名	用于是否将此记录集关联至云服务资源实例。	否

参数	说明	示例
线路类型	用于DNS服务器在解析域名时，根据访问者的来源，返回对应的服务器IP地址。 添加解析线路类型时，切记先添加默认线路类型，以保证网站可访问。	全网默认
TTL(秒)	TTL指解析记录在本地DNS服务器的有效缓存时间。如果您的服务地址经常更换，建议TTL值设置相对小些，反之，建议设置相对大些。	默认为“5分钟”，即300s。
值	需指向的域名。 如果没有开启CDN加速，该值为桶访问域名；如果开启CDN加速后，该值为CDN分配的CNAME域名。	download.game-apk1.com.cdnhwc1.com

- f. 单击“确定”，完成添加。
- g. 验证CNAME配置是否生效。  
打开Windows操作系统中的cmd程序，输入如下指令：

```
nslookup -qt=cname 桶绑定的自定义域名
```

本实践中桶绑定的自定义域名为“download.game-apk1.com”。如果回显CDN分配的CNAME域名，则表示CNAME配置已经生效。

### 3. 开启OBS委托授权（公共读或公共读写的OBS桶跳过此步骤）

如果您的OBS桶是私有桶，您需要前往CDN控制台开启OBS委托授权，CDN才能从OBS中回源获取数据。具体请参见[OBS委托授权](#)。

#### 说明

- 如果您的私有桶中有不希望被公开的资源，请将此部分资源移入其它私有桶中。

### 4. 配置文件下载URL

将代码中需要加速下载的文件URL地址配置为：游戏网站域名+文件在OBS桶中的存储路径+文件名称。

以配置的游戏网站域名download.game-apk1.com以及存储在obs-doc-test桶中的game/3.2.1/文件夹下的android.apk文件为例，文件下载URL的配置如下：

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

### 5. 验证业务

待游戏网站重新部署后，登录游戏网站，浏览网页图片、进行游戏下载。

如果图片可以成功显示、游戏可以成功下载，则表示加速配置成功。

6. 配置自动刷新：您可以参考[配置CDN自动刷新](#)完成相关配置。

## 1.4 自定义 OBS 私有桶策略配置

如果您采用了自定义OBS私有桶作为CDN的源站，即：跨账号添加OBS私有桶作为源站，您需要前往OBS控制台为您的私有桶配置策略。

## 配置步骤

1. 在**OBS管理控制台**左侧导航栏选择“桶列表”。
2. 在桶列表单击待操作的桶名称，进入“对象”页面。
3. 在左侧导航栏，选择“访问权限控制 > 桶策略”。
4. 在桶策略界面单击“创建”，选择可视化视图。
  - 策略名称：自定义策略（可修改）
  - 效力：允许
  - 被授权用户：
    - 其他账号：domainId/userId，示例：  
0a0b0afb4\*\*\*\*\*019806272e0/\*。
    - 委托账号：domainId/\*，示例：0a0b0afb4\*\*\*\*\*019806272e0/\*。
  - 授权资源：可选整个桶（包括桶内对象）或当前桶。
  - 授权操作：选择自定义配置，动作选择“桶操作”下的“ListBucket”。

图 1-1 创建桶策略

创建桶策略 [如何配置?](#)

**i** 【创建桶】、【获取桶列表】两个服务级的操作权限，需要通过统一身份认证进行配置。如何配置?

可视化视图    JSON视图

\* 策略名称

\* 效力  允许  拒绝

\* 被授权用户  所有帐号  
 当前帐号  
 其他帐号

\* 授权资源  整个桶（包括桶内对象）  当前桶  指定对象

\* 授权操作  模板配置  自定义配置

授权条件（可选）  本规则生效的所需条件，以此限定规则的生效范围，通过键值表达式实现 [查看配置案例](#)

键	条件运算符	值	操作
暂无授权条件			
<input type="button" value="增加条件"/>			

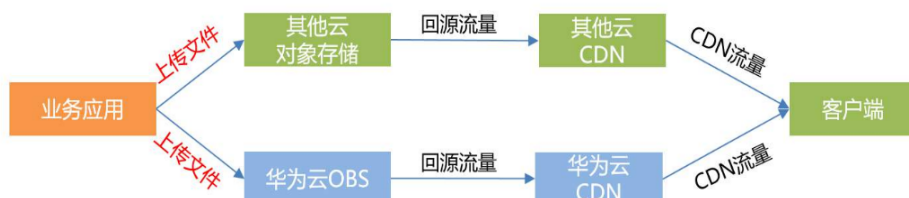
> 高级设置

5. 单击“创建”，完成桶策略创建。

## 1.5 多云存储数据同步方案

### 应用双写

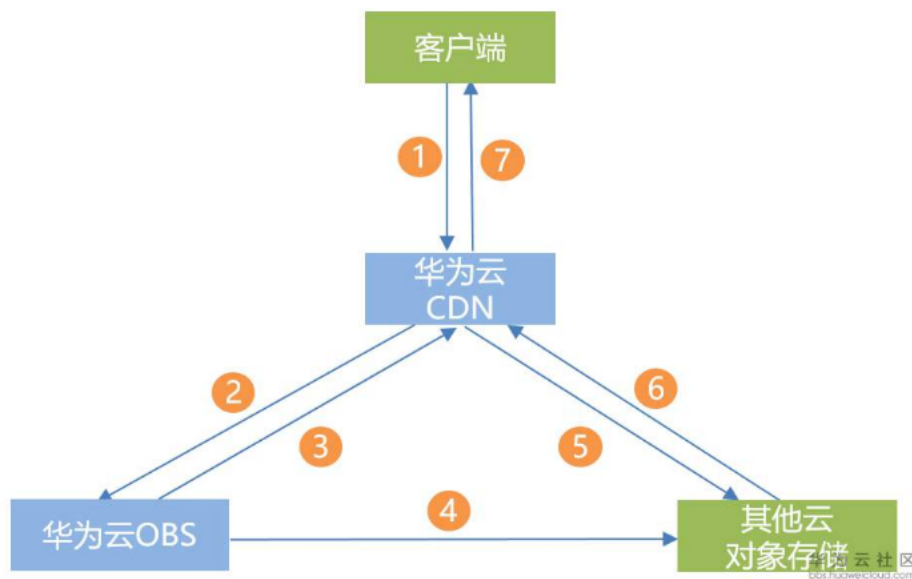
如果数据是在应用服务侧产生，或者数据在客户端产生但通过服务端将数据写入对象存储，则建议使用双写方案，架构如下：



此时业务应用可对接两家对象存储的SDK，将文件以同步模式或者异步模式写入两家对象存储。对象存储的上行流量免费，所以该架构不会增加任何成本。

### 数据回源

如果数据上传逻辑不做改变，则可使用OBS的“数据回源”功能，在文件访问请求到达OBS而OBS桶里没有该文件时，可通过“数据回源”将客户端请求重定向到设定的源站并异步地从源站将数据拉取到OBS存储下来，架构如下：



详细流程说明：

1. 客户端向华为CDN发起获取文件的请求
2. 华为CDN回源到华为OBS请求文件，OBS侧事先配置好数据回源，当请求的文件不存在时，会响应302重定向到配置的源站（此处为其他云对象存储）
3. 华为CDN接收到OBS返回的302请求
4. OBS异步从客户配置的源站请求文件
5. 华为CDN处理302跳转到其他云对象存储侧获取数据



6. 其他云对象存储响应华为CDN的文件请求
7. 华为CDN将文件内容返回给客户端，当下次客户端请求同样的文件时，华为CDN直接回源到OBS获取。

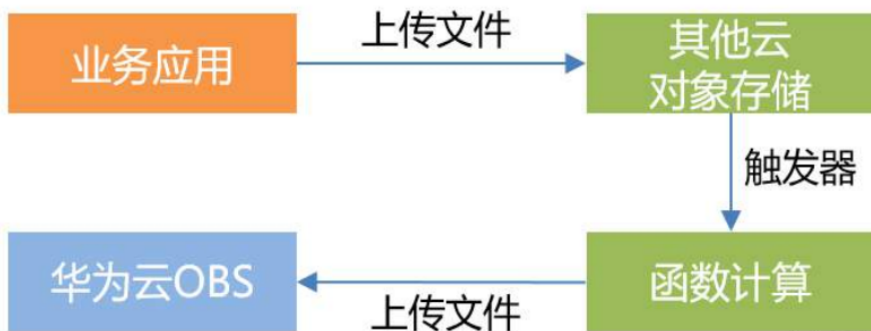
#### 📖 说明

“数据回源”功能是被动触发式，即只有向OBS发起请求后OBS才会到设置的源站将数据拉取过来，所以当一个新文件上传到其他云对象存储后，建议业务应用程序向OBS触发一个GET请求来请求数据（发起GET请求后可关闭连接，无需接收实体数据）。另外该架构会在其他云对象存储侧产生两份数据流量（针对同一个文件，CDN拉取一次，OBS拉取一次）。

## Serverless 触发式上传

不改变原有的上传逻辑，当文件上传到其他云对象存储后，触发函数计算服务，通过Serverless方式将文件同步到华为云OBS，架构如下：

图 1-2 Serverless 触发式上传



该架构需要客户在其他云启用函数计算服务并部署上传文件到OBS的代码，会产生函数计算服务的费用。

## 1.6 CDN 加速 OBS 常见问题

### 为什么回源流量没从回源流量包中扣除？

可能的原因：

1. 接入CDN的OBS桶和回源流量包不在同一区域，跨区购买将导致无法抵扣，请重新购买CDN回源流量包。
2. 源站类型请选择“OBS桶域名”，否则无法使用回源优惠。
3. 请确认您的OBS桶版本为3.0及以上，如果不是，将无法享受OBS针对CDN回源流量的特殊计费 and 流量包优惠，将按照公网流出费用进行结算。

### CDN 和 OBS 可以共用流量包吗？

不可以，CDN流量包抵扣CDN节点流入、流出的流量，OBS侧的流量由OBS流量包抵扣，各自单独计费。



## OBS 桶域名能否作为加速域名？

不可以，OBS桶域名是加速域名的源站，而加速域名和源站不能是一样的，否则访问将无限循环，您需要另外准备一个域名作为加速域名。

## 为什么 OBS 桶接入 CDN 后，访问域名会列出所有文件列表？

如果用户对OBS桶有读权限，就可以读取桶内对象列表。当用户请求的是CDN加速域名的时候，OBS就默认返回桶内对象列表。解决办法如下：

1. 如果您使用的是**OBS公有桶**，请参考以下操作步骤解决该问题：
  - a. 在OBS处开启静态网站托管，操作步骤请参考[配置静态网站托管](#)。
  - b. 同时在CDN域名的源站配置页面勾选“静态网站托管”。
    - i. 在CDN控制台域名管理页面，单击需要配置的域名。
    - ii. 在“源站配置”模块，单击对应源站“操作”列的“编辑”按钮。
    - iii. 勾选“静态网站托管”，完成配置。
2. 如果您使用的是**OBS私有桶**，请参考[通过CDN加速OBS视频点播](#)文档中实施步骤的第6步处理。
3. 如果您使用的是**OBS私有桶**，您还可以通过给“CDNAccessPrivateOBS”委托创建一条**拒绝列举桶内对象**的策略，达到不会列出桶文件列表的目的，步骤如下：
  - a. 前往IAM控制台，在左侧菜单栏选择“委托”，在“CDNAccessPrivateOBS”的“操作”列，单击“授权”。
  - b. 在授权页面单击“新建策略”，配置如下参数：

表 1-1 参数说明

参数		说明
策略名称		输入自定义的桶策略名称，例如：deny ListBucket。
策略配置方式		可视化视图。
策略内容	效力	拒绝。
	云服务	对象存储服务（OBS）。
	操作项	在列表一栏勾选“obs:bucket:ListBucket”。
	资源	所有资源
	请求条件	-

- c. 单击“下一步”，进入选择策略页面。
- d. 勾选刚创建的策略，此处示例为“deny ListBucket”，单击“下一步”，进入设置最小授权范围界面。
- e. 单击“确定”，完成授权，授权后15~20分钟生效。
- f. 授权生效后，请刷新CDN缓存后重试。

## 使用 CDN 加速 OBS 桶文件后访问变成强制下载

如果您需要支持在线预览功能，请前往CDN控制台>域名管理>高级设置>HTTP header配置，将“Content-Disposition”的值设为“inline”。

# 2 CDN 加速 ECS 资源

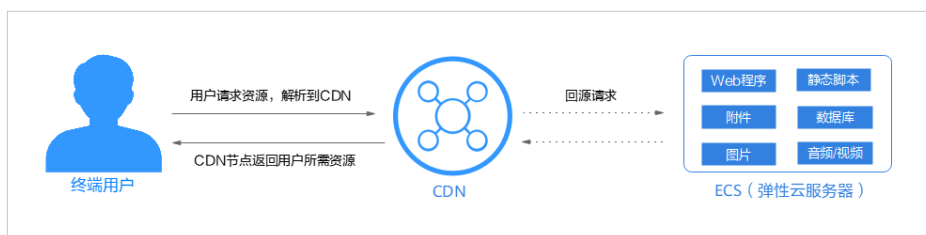
## 前提条件

- 已购买[弹性云服务器ECS](#)，且[绑定弹性公网IP](#)。
- 已经按照[使用限制](#)准备好需要接入的域名。
- 已[开通CDN服务](#)。

## 背景介绍

ECS（弹性云服务器）是由CPU、内存、操作系统、云硬盘组成的基础的计算组件，可以根据业务灵活配置，节约大量的硬件成本。ECS服务分区域，跨区域访问会存在网络延时的问题，影响用户体验。

华为云CDN可以有效加速网站，为用户提供良好的体验。通过CDN加速ECS资源，这样构造的业务系统可以在降低成本的同时，提高终端用户使用感受。当终端用户发起访问请求时，会首先通过CDN查找对此域名响应速度较快的CDN节点，并查询此节点是否有缓存终端用户请求的内容。如果CDN节点有缓存用户所需资源，直接将资源返回给用户；如果CDN节点无缓存，则回源请求资源返回给用户，同时将资源缓存到CDN节点。



## 方案优势

- 用户访问网站资源，全部通过CDN，降低源站压力。
- 使用CDN流量，单价低于ECS直接访问外网流量，可以节约50%到57%的带宽成本，详见[通过CDN减少公网带宽费用](#)。
- 终端用户从距离最近的CDN节点获取资源，减少网络传输距离，保证静态资源质量。

## 配置步骤

### 1. 在CDN控制台添加加速域名

- a. 登录[华为云控制台](#)，选择“所有服务 > CDN与智能边缘 > 内容分发网络CDN”，进入CDN管理控制台。
- b. 单击左侧“域名管理”，进入域名管理页面。
- c. 在域名管理页面单击“添加域名”，配置域名及CDN加速等信息，参考[添加CDN加速域名](#)。
  - 加速域名：此处以download.game-apk1.com为例。
  - 服务范围：根据您的业务需要选择服务范围。
  - 业务类型：实际业务结合[应用场景](#)选择合适的业务类型。
  - 源站配置：
    - 回源方式：根据需要选择合适的回源方式。
    - 源站类型：选择源站IP或源站域名。
    - 源站地址：IP地址或域名。
    - 优先级：主源站或备源站。
    - 回源HOST：默认为加速域名。
- d. 单击“确定”，根据业务情况完成推荐配置。

#### 说明

配置过程大概需要5-10分钟，当“状态”为“已开启”时，表示域名添加成功

2. 添加加速域名后，为保证顺利切换不影响业务，建议先做测试再切换DNS解析，测试流程请参考[本地测试加速域名](#)。

### 3. 配置CNAME

添加加速域名后，CDN会自动生成一条CNAME域名。加速域名在CDN服务中获得的CNAME域名不能直接访问，必须在加速域名的域名服务商处配置CNAME记录，将加速域名指向CNAME域名，访问加速域名的请求才能转发到CDN节点上，达到加速效果。本实践中自动生成的CNAME域名为“download.game-apk1.com.cdnhwc1.com”。不同DNS服务商的CNAME配置方式不同，此处以华为云云解析服务为例。其他DNS服务商的CNAME配置方法可参考[配置CNAME域名解析](#)。

- a. 登录[华为云控制台](#)，在控制台首页选择“网络 > 云解析服务DNS”，进入云解析服务页面。
- b. 在左侧菜单栏中，选择“公网域名”，进入公网域名列表页面。
- c. 在待添加记录集的域名所在行，单击“域名”列的域名名称。本实践中对应的域名为“game-apk1.com.”。
- d. 单击“game-apk1.com”，进入域名解析页面，然后单击右上角“添加记录集”，进入“添加记录集”弹出框。

### 添加记录集 ✕

主机记录  .game-apk1.com. ?

\* 类型

\* 别名 ?  是  否

\* 线路类型  ?

\* TTL (秒)      ?

\* 值  ?

权重

其他配置

e. 根据界面提示填写参数配置，下表中未提到的参数可保持默认值。

参数	说明	示例
主机记录	主机记录指域名前缀。	本示例填写： download
类型	记录集的类型，此处为CNAME类型。	CNAME-将域名指向另外一个域名
别名	用于是否将此记录集关联至云服务资源实例。	否
线路类型	用于DNS服务器在解析域名时，根据访问者的来源，返回对应的服务器IP地址。 添加解析线路类型时，切记先添加默认线路类型，以保证网站可访问。	全网默认
TTL(秒)	TTL指解析记录在本地DNS服务器的有效缓存时间。如果您的服务地址经常更换，建议TTL值设置相对小些，反之，建议设置相对大些。	默认为“5分钟”，即300s。

参数	说明	示例
值	需指向的域名。 如果没有开启CDN加速，该值为ECS访问域名；如果开启CDN加速后，该值为CDN分配的CNAME域名。	download.game-apk1.com.cdnhwc1.com

f. 单击“确定”，完成添加。

g. 验证CNAME配置是否生效。

打开Windows操作系统中的cmd程序，输入如下指令：

```
nslookup -qt=cname 加速域名
```

本实践中加速域名为“download.game-apk1.com”。如果回显CDN分配的CNAME域名，则表示CNAME配置已经生效。

# 3 CDN 加速 WAF 防护资源

## 前提条件

- 已经按照[使用限制](#)准备好需要接入的域名和华为账号。
- 已[购买WAF](#)。
- 已[开通CDN服务](#)。

## 背景信息

CDN是构建在现有互联网基础之上的一层智能虚拟网络，通过网络各处部署节点服务器，实现将源站内容分发至所有CDN节点，使用户可以就近获得所需的内容，所以接入CDN的网站都能有比较快的响应速度。

Web应用防火墙（WAF：Web Application Firewall），通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。

如果您的网站对安全性能要求比较高，同时又有加速的需求，可以使用华为云CDN联动WAF配置，实现加速的同时防护Web攻击。

## CDN+WAF 的配置原理

CDN+WAF联动的业务流向为：CDN>WAF>源站，流量由CDN转发到WAF，WAF再将流量转到源站，实现网站加速、流量检测和攻击拦截。



## 配置场景

本文配置以您的WAF在华为云为例，为您介绍开通CDN+WAF联动部署。如果您的WAF在其它云服务，请参考本文完成配置。

### 场景1：已购买WAF并添加防护域名，配置CDN+WAF联动

如果您已经将域名接入WAF防御，要配置CDN+WAF联动，您需要先将WAF域名基本信息中的“是否已使用代理”修改为“是”，WAF才能够针对真实源IP进行安全策略

防御；然后在CDN侧添加加速域名，将WAF的CNAME作为CDN的源站，CDN才能将流量转发给WAF，实现加速和Web攻击防御联动。

### 使用限制：

- CDN的加速域名仅支持默认端口，以非标端口的方式接入WAF的防护域名将无法接入CDN。
- 如果您在WAF侧为防护域名配置了HTTPS证书，请同步在CDN侧完成证书配置，否则会导致域名无法访问。

### 操作步骤

1. 根据[修改WAF防护域名基本信息](#)指导修改防护域名的代理设置。

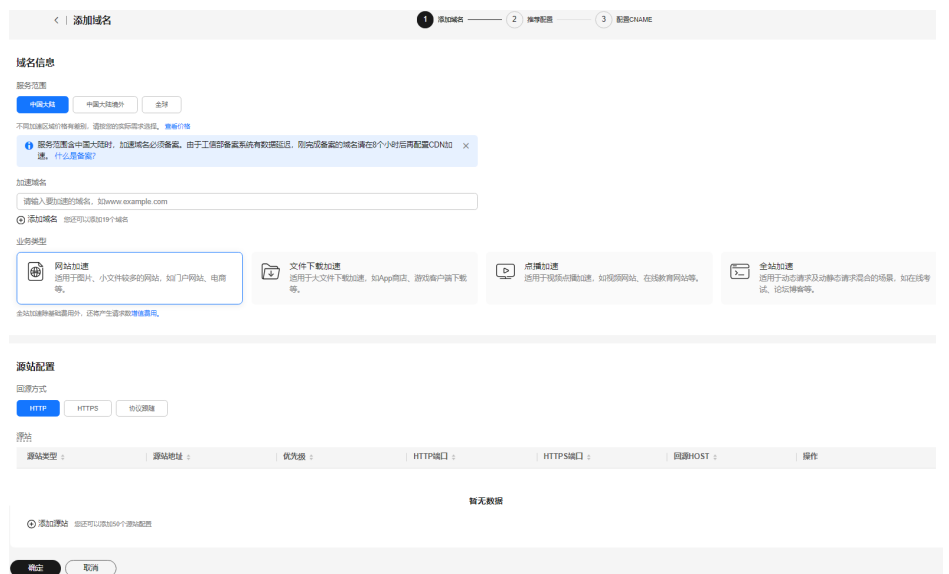
- 是否已使用代理：是



2. 复制WAF的CNAME。

3. 在CDN侧添加加速域名（即WAF的防护域名）

- a. 登录[华为云控制台](#)，在控制台首页中选择“CDN与智能边缘 > 内容分发网络 CDN”，进入CDN控制台。
- b. 在左侧导航栏选择“域名管理”，进入域名管理页面。
- c. 在域名管理界面，单击“添加域名”，配置域名参数。
  - 添加源站时，“源站类型”选择“源站域名”，“源站地址”输入WAF的CNAME域名。



d. 单击“确定”完成域名的添加，CDN会为加速域名生成专属CNAME。



### 📖 说明

- 如果您的WAF是独享模式，需要使用“源站IP”接入CDN，“源站”文本框中请输入**为弹性负载均衡绑定弹性公网IP**。
4. （可选）添加加速域名后，为保证顺利切换不影响业务，建议先做测试再切换DNS解析，请参考[本地测试加速域名](#)。
  5. 在DNS域名服务商处修改解析记录，配置CDN提供的CNAME，详情请参见[配置CNAME](#)。
  6. 验证CNAME是否生效。

打开Windows操作系统中的cmd程序，输入如下指令：

```
nslookup -qt=cname 加速域名
```

如果回显CNAME，则表示CNAME配置已经生效，如下图：

```
C:\Users\localhost>nslookup -qt=cname www.example.com net
服务器: localhost.t.huawei.com
Address:
非权威应答:
www.example.com canonical name = www.example.com c.cdnhwcl.com
```

### 📖 说明

如果您暂未使用CDN和WAF，也建议您按照场景1的方式先接入WAF，再配置联动。

### 场景2：加速域名已经接入CDN加速，配置CDN+WAF联动

如果您的域名已经接入CDN加速，现在需要配置CDN+WAF联动，您需要先在WAF添加防护域名，“是否已使用代理”选项选择“是”，WAF才能够针对真实源IP进行安全防护；然后将CDN侧加速域名的源站修改WAF的CNAME，CDN才能将流量转发给WAF，实现加速和Web攻击防御联动。

### 使用限制：

如果您在CDN侧为加速域名配置了HTTPS证书，请同步在WAF侧完成证书配置，否则会导致域名无法访问。

### 操作步骤

1. 将网站信息（源站服务器的IP、端口等信息）[添加到WAF](#)。配置要点如下。
  - 防护域名端口：标准端口。
  - 是否已使用代理：七层代理。
2. 配置完成后，WAF会为该域名生成一个专属的CNAME。

为避免修改DNS解析后业务异常，建议先在本地验证无误后，再修改DNS解析，[验证参考](#)

请复制以下CNAME值，然后前往该域名代理(高防、CDN、云加速等)，将代理的回源IP改为CNAME值

CNAME: .....waf.huaweicloud.com

[复制](#)

修改完成后，待DNS生效，即可为您的网站提供防护

[下一步](#) [取消](#)

### 📖 说明

建议您在配置好WAF后先验证业务是否正常，再修改CDN源站。

3. 将CDN加速域名的源站地址修改为WAF的CNAME域名。
  - a. 登录[华为云控制台](#)，在控制台首页中选择“CDN与智能边缘 > 内容分发网络CDN”，进入CDN控制台。
  - b. 在左侧菜单栏中，选择“域名管理”。
  - c. 在域名列表中，单击需要修改的域名或域名所在行的“设置”，进入域名配置页面。
  - d. 选择“基本配置”页签。
  - e. 在源站配置模块，单击“编辑”，将源站修改为如下配置：
    - 源站类型：源站域名。
    - 源站地址：填写WAF生成的CNAME域名。
    - 回源端口：默认端口。

#### 说明

- 如果您的WAF是独享模式，需要使用“源站IP”接入CDN，“源站”文本框中输入[为弹性负载均衡绑定弹性公网IP](#)。

完成以上配置后，流量经过CDN转发到WAF，达到加速和Web攻击防护的目的。

# 4 如何设置缓存过期时间

CDN加速的本质是缓存加速，把源站资源缓存在遍布全球的节点上，用户可以就近从边缘节点获取资源，从而达到加速的效果。CDN控制台可以设置源站资源在节点上缓存的时间，方便您根据业务需要对不同的文件设置相应的缓存过期时间。

## 源站对 CDN 节点缓存的影响

### 1. 源站设置了缓存过期时间

- 源站设置了no-cache、private、no-store，CDN侧同时开启了“缓存遵循源站”功能：CDN节点不缓存源站资源，用户每次访问都需要回源，无法达到加速的目的。

#### 📖 说明

CDN默认关闭“缓存遵循源站”功能。

- 设置了其它缓存过期时间：CDN控制台默认或者新设置的缓存过期时间会覆盖源站的缓存过期时间。

### 2. 源站未设置缓存过期时间

- 遵循CDN控制台默认或者新设置的缓存过期时间。

## 根据业务类型设置缓存过期时间

### CDN默认缓存过期时间：

1. 业务类型选择的是网站加速、文件下载加速或点播加速，且源站类型为源站IP或源站域名的加速域名，会有两条默认缓存规则。
  - 常规动态文件（如：.php .jsp .asp .aspx）默认缓存过期时间为0，对此类动态文件请求会直接回源，此默认规则允许修改和删除。
  - 除常规动态文件外的其他“所有文件”默认缓存过期时间30天，允许修改，不允许删除。
2. 如果您在添加域名里源站类型选择的是“OBS桶”，会有一条默认缓存规则。
  - 默认有“所有文件”默认缓存过期时间30天，允许修改，不允许删除。

#### 📖 说明

所有文件默认缓存30天，此规则允许修改但不允许删除。您可以将自定义缓存规则设置为更高优先级（数值更大），该自定义规则将会被优先匹配。

- 业务类型为全站加速时，默认有“所有文件”、缓存过期时间为“0”的缓存规则，允许修改和删除。

**您可以根据业务类型配置缓存过期时间：**

- 网站加速类型，建议设置缓存过期时间：
  - 对php、aspx、asp、jsp、do、dwr、cgi、fcgi、action、ashx、axd、json等动态文件不缓存。
  - 对以shtml、html、htm、js结尾的文件，建议缓存7天。
  - 其他静态文件建议缓存30天。
- 下载加速类型，建议设置缓存过期时间：
  - 对php、aspx、asp、jsp、do等动态文件不缓存。
  - 对7z、apk、wdf、cab、dhp、exe、flv、gz、ipa、iso、mpk、MPQ、pbcv、pxl、qnp、r00、rar、xy、xy2、zip、CAB等文件缓存30天。
- 视频点播加速类型，建议设置缓存过期时间：
  - 对php、aspx、asp、jsp、do等动态文件不缓存。
  - 对mww、html、htm、shtml、hml、gif、swf、png、bmp、js等缓存7天。
  - 对MP3、wma、7z、apk、wdf、cab、dhp、exe、flv、gz、ipa、iso、mpk、MPQ、pbcv、pxl、qnp、r00、rar、xy、xy2、zip、CAB等文件缓存30天。

## 操作步骤

- 登录[华为云控制台](#)，在控制台首页中选择“CDN与智能边缘 > 内容分发网络CDN”，进入CDN控制台。
- 在左侧菜单栏中，选择“域名管理”。
- 在域名列表中，单击需要修改的域名或域名所在行的“设置”，进入域名配置页面。
- 选择“缓存配置”页签。
- 在缓存规则模块，单击“编辑”，系统弹出“配置缓存策略”对话框。
- 单击“添加”，根据业务需求配置缓存策略，如[图4-1](#)所示。具体配置参数说明如[表4-1](#)所示。

**图 4-1 配置缓存策略**



表 4-1 缓存策略配置参数

参数	说明	配置规则
所有文件	设置CDN节点所有缓存资源的过期时间。	对于新添加的加速域名，CDN默认添加一条“所有文件”缓存过期时间为30天的规则，此默认规则允许修改，不允许删除。
文件名后缀	设置指定文件类型的缓存资源的缓存规则。 对于新添加的业务类型为网站加速、文件下载加速和点播加速，且源站为自有源站的加速域名，CDN默认添加一条常规动态文件（如.php .jsp .asp .aspx）缓存过期时间为0的规则，对此类动态文件请求会直接回源。此默认规则允许修改和删除。	<ul style="list-style-type: none"> <li>支持所有格式的文件类型。</li> <li>输入首字符为“.”，以“;”进行分隔。</li> <li>字符总数不能超过255。</li> <li>输入的文件后缀名总数不能超过20个。</li> <li>文件名后缀英文字符支持大写和小写。</li> </ul> <b>示例：</b> .JPG;.zip;.exe。
目录路径	设置某一指定路径下的缓存资源的缓存规则。	输入要求以“/”作为首字符，以“;”进行分隔，输入的目录路径总数不能超过20个，且字符总数不能超过255。 <b>示例：</b> /test/folder01;/test/folder02。
全路径	设置完整路径下某一文件的缓存规则。	输入要求以“/”作为首字符，“*”不能在结尾。支持匹配指定目录下的具体文件或者带通配符“*”的文件。单条全路径缓存规则里仅支持配置一个全路径。 <b>示例：</b> 如/test/index.html或/test/*.jpg
首页	设置根目录缓存规则	网站的根目录就是网站的顶层文件目录，目录下放着网站所有的子文件夹。 <b>示例：</b> 以目录“abc/file01/2.png”为例，“abc/”就是根目录，缓存首页就是对“abc/”设置缓存规则。
优先级	缓存规则的优先级。 优先级设置具有唯一性，不支持多条缓存规则设置同一优先级，且优先级不能输入为空。多条缓存规则下，不同缓存规则中的相同资源内容，CDN按照优先级高的缓存规则执行缓存内容过期。	取值为1~100之间的整数，数值越大优先级越高。

参数	说明	配置规则
缓存过期时间	达到设置的缓存过期时间后，当用户向CDN节点请求资源时，CDN会直接回源站请求对应的最新资源返回给用户，并缓存到CDN节点中。	<p>时间设置不能超过365天，建议参考如下规则进行配置：</p> <ul style="list-style-type: none"> <li>对于不经常更新的静态文件（如.jpg、.zip等），建议将缓存过期时间设置成1个月以上。</li> <li>对于频繁更新的静态文件（如js、css等），请根据实际业务情况设定。</li> <li>对于动态文件（如php、jsp、asp等），建议设置成0秒，回源获取。</li> </ul>
URL参数	<p>目前大多数的网页请求都携带URL参数信息，参数以“？”开始，如果参数没有包含重要信息（如版本信息等），可以设置忽略部分参数，从而提高缓存命中率，提升分发效率。</p> <p><b>配置原则：</b></p> <ul style="list-style-type: none"> <li>URL参数变化，资源不变，可以配置忽略参数。</li> <li>URL参数变化，资源变化，不可配置忽略参数。</li> <li>如果您开通了“视频拖拽”功能，请将您视频资源对应的“URL参数”设置为“忽略参数”。</li> </ul>	<ul style="list-style-type: none"> <li><b>不忽略参数：</b>不忽略“？”之后的参数。</li> <li><b>忽略参数：</b>忽略所有URL参数，CDN缓存时忽略请求URL中“？”之后的参数，提高缓存命中率。</li> <li><b>忽略指定URL参数：</b>CDN缓存时将忽略您在控制台配置的参数，保留其它参数。</li> <li><b>保留指定URL参数：</b>CDN缓存时将保留您在控制台配置的参数，忽略其它参数。</li> </ul>
URL参数值	需要忽略或保留的指定参数值，当“URL参数”选择“不忽略参数”或“忽略参数”时不填。	<ul style="list-style-type: none"> <li>最多可填写10个参数名，多个参数之间用“;”分割。</li> <li>支持数字0-9、字符a-z、A-Z，及特殊符“.”、“_”、“~”。</li> </ul>

参数	说明	配置规则
缓存遵循源站	<p>如果源站配置了缓存过期时间，即源配置了Cache-Control:max-age或Expires，您希望CDN的缓存过期时间与源站配置一致，可以选择开启“缓存遵循源站”功能，CDN将执行源站的缓存过期时间。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>如果源站同时配置了Cache-Control和Expires，优先遵从Cache-Control配置的过期时间。</li> <li>如果开启了缓存遵循源站，但是源站没有配置Cache-Control和Expires，此时节点缓存遵循CDN配置的缓存规则。</li> </ul>	默认关闭缓存遵循源站功能。

- （可选）通过单击缓存规则所在行的“删除”，删除不需要的缓存规则。
- 单击“确定”，完成缓存规则配置。

#### 📖 说明

##### 如果您修改了缓存规则：

- 新的规则仅对后面缓存的资源生效，已经缓存的资源需要等缓存过期后，再次缓存才会遵循新的缓存规则。
- 如果您想要立即生效，请在修改缓存规则后执行缓存刷新操作。

## 配置示例

**配置场景1：**有一个门户网站，配置了华为云CDN加速，客户希望不缓存首页需要在CDN控制台增加一条类型为“首页”，缓存过期时间为“0”的规则。

类型	内容	优先级	缓存过期时间	URL参数
首页		2	0天	不忽略参数
所有文件		1	30天	忽略参数

**配置场景2：**设置某个类型的文件或者某个页面不缓存

- 某客户配置了CDN加速，设置了对“.do”格式的文件缓存1天，由于业务需求，需要对“.do”格式的文件不缓存。

需要在CDN控制台增加一条文件名后缀为“.do”的缓存规则，缓存过期时间设置为“0”。

类型	内容	优先级	缓存过期时间	URL参数
所有文件		1	30天	忽略参数
文件名后缀	.do	3	0天	不忽略参数

#### 📖 说明

新规则仅对后续资源缓存生效，新规则配置完成后，建议您刷新“.do”文件所在的URL或者目录，新规则才可以对所有“.do”文件生效。

2. 某客户配置了CDN加速，发现登录界面无限循环，无法登录，停用CDN加速后，可以正常登录。

这是因为CDN节点缓存了登录界面导致的，需要在控制台增加一条针对登录界面的缓存规则，缓存过期时间设置为“0”。以华为云控制台登录界面为例，华为云控制台的登录页面为“https://auth.huaweicloud.com/authui/login.html#/login”，在控制台增加一条全路径：/authui/login.html#/login，缓存过期时间为“0”的缓存规则。

类型	内容	优先级	缓存过期时间	URL 参数
全路径	/authui/login.html#/login	4	0天	不忽略参数
所有文件		1	30天	忽略参数

**配置场景3：**某客户加速域名www.example.com设置了如下图的缓存规则，不知道哪一个规则生效。

类型	内容	优先级	缓存过期时间
全路径	/test/*.jpg	8	3天
目录路径	/test/folder01	6	5天
文件名后缀	.jpg	2	1天
所有文件		1	30天

用户访问www.example.com/test/cdn.jpg，虽然所有文件、文件名后缀、全路径三条规则都匹配到了，但是由于全路径的优先级为8，在三条规则里优先级最高，所以系统最终匹配全路径/test/\*.jpg这条规则。



# 5 如何提高缓存命中率

## 背景信息

CDN缓存命中率低，会导致源站压力大，静态资源访问效率低。您可以针对导致CDN缓存命中率低的具体原因，选择对应的优化策略，来提高CDN的缓存命中率。CDN缓存命中率包括流量命中率和请求命中率。

- **流量命中率** = 命中缓存产生的流量 / 请求总流量
- **请求命中率** = 命中缓存的请求数 / 请求总数

### 📖 说明

流量命中率越低，回源流量越大，源站的流出流量越大，源站带宽资源占用越大，其代表了源站服务器收到的负载压力，请重点关注流量命中率。

## 查看缓存命中率

您可以登录CDN控制台查看流量命中率和请求命中率。

1. 登录[华为云控制台](#)，在控制台首页中选择“CDN与智能边缘 > 内容分发网络CDN”，进入CDN控制台。
2. 在左侧菜单栏中，选择“统计分析”。
3. 分别选择“使用量统计”和“访问情况统计”查看“流量命中率”和“请求命中率”。

图 5-1 流量命中率

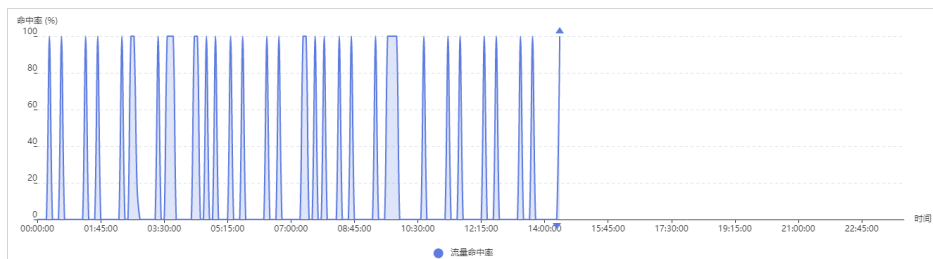
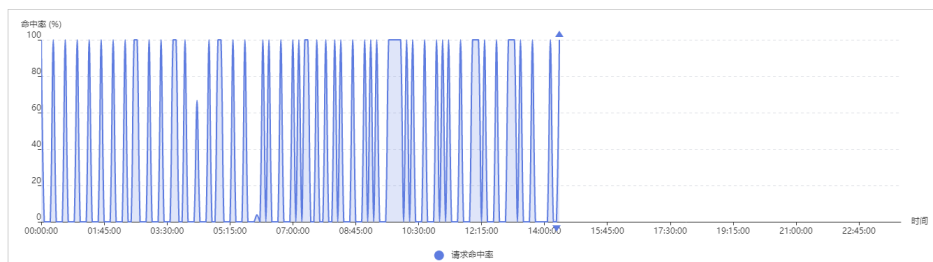


图 5-2 请求命中率



## 优化缓存命中率

### 1. 合理设置缓存过期时间

CDN加速的本质是缓存加速，把源站资源缓存在遍布全球的节点上，用户可以就近从边缘节点获取资源，从而达到加速的效果。您可以通过CDN控制台合理设置缓存过期时间来提高缓存命中率，建议如下：

- 对于不经常更新的静态文件（如图片类型、应用下载类型等），建议您将缓存时间设置为1个月以上。
- 对于频繁更新的静态文件（如JS、CSS等），您可以根据实际业务情况设置。
- 对于动态文件（如PHP、JSP、ASP等），建议您将缓存时间设置为0，即不缓存。

详细的设置步骤和注意事项请见[如何设置缓存过期时间](#)。

#### 说明

- 如果源站设置了s-maxage=0、max-age=0、no-cache、no-store、private，CDN侧同时开启了“缓存遵循源站”功能（此功能默认关闭），CDN节点将无法缓存源站资源，导致频繁回源。
- 如果您的源站有多个主机，某个相同的资源在多个主机中的Last-modified、Etag、Content-Length不一致，CDN节点将无法缓存该资源，导致重复回源。
- 如果源站资源更新，请刷新资源对应的URL，以保证用户可以获得最新的资源。
- **如果您修改了缓存规则：**
  - 新的规则仅对后面缓存的资源生效，已经缓存的资源需要等缓存过期后，再次缓存才会遵循新的缓存规则。
  - 如果您想要立即生效，请在修改缓存规则后执行缓存刷新操作。

### 2. 配置URL参数

目前大多数的网页请求都携带URL参数信息，参数以“？”开始，如果参数没有包含重要信息（如版本信息等），是否携带该参数访问不会影响用户获得正确的资源，可以选择将“URL参数”功能配置为“忽略参数”或“忽略指定参数”，提高缓存命中率，提升分发效率，详见[URL参数](#)。

#### 典型应用：

- 终端用户首次访问URL “http://www.example.com/1.txt?test1” 时，CDN无缓存，回源请求资源；第二次访问 “http://www.example.com/1.txt?test2” 时，由于配置了“URL参数”的“忽略参数”功能，所以“？”之后的参数不匹配，直接命中缓存 “http://www.example.com/1.txt”。
- 终端用户首次访问URL “http://www.example.com/1.txt?test1” 时，CDN无缓存，回源请求资源；第二次访问 “http://www.example.com/1.txt?test2” 时，由于“URL参数”功能配置为“不忽略参数”，所以“？”之后的参数也需要匹配，要重新回源请求 “http://www.example.com/1.txt?test2”。

### 3. 预热URL

CDN可以通过缓存预热将源站资源主动缓存到CDN节点，用户访问时就能直接从CDN节点获取到最新的资源，详见[缓存预热](#)。

当您的域名初次接入CDN加速、活动发布时您可以将源站资源预热到CDN节点，用户访问资源时直接从CDN节点获取，从而提升CDN的缓存命中率。

#### 典型场景：

- 初次接入CDN：域名初次接入CDN时，节点暂未缓存源站资源，此时，您可以将源站资源预热至CDN节点。后续用户访问资源将直接从就近的CDN节点获取资源，提升访问速度。
- 安装包发布：新版本安装包或是升级包发布前，提前将资源预热至CDN节点。正式上线后，海量用户的下载请求将直接由全球加速节点响应，提升下载速度的同时，大幅度降低源站压力。
- 运营活动：运营活动发布前，提前将活动页涉及到的静态资源预热至CDN节点。活动开始后，用户访问中所有静态资源均由加速节点响应，海量带宽储备保障用户服务可用性，提升用户体验。

### 4. 开启Range回源

Range回源是指源站在收到CDN节点回源请求时，根据HTTP请求头中的Range信息返回指定范围的数据给CDN节点。Range回源能有效缩短大文件的分发时间，提升回源效率，提高缓存命中率，详见[Range回源](#)。

#### 典型场景：

- 未开通Range时，用户想观看指定片段的视频，而CDN回源时需要获取整个视频，所以回源流量大于响应给用户的流量，从而造成缓存命中率降低。开启Range回源后，CDN将分片回源获取资源返回给用户，从而提升缓存命中率。

### 5. 其它

- 缓存资源需要更新时，尽量避免刷新目录

当源站某个资源更新时，一般需要通过刷新相应的URL来强制节点缓存资源过期。刷新目录会将目录内所有的资源全部置为过期，用户下次访问时将无法命中缓存，全部回源站请求资源，因此尽量避免刷新整个目录，尤其慎重刷新根目录。

- 避免在URL中携带动态参数

如果您的URL中包含动态参数，如时间戳，CDN无法缓存该资源，导致频繁回源。

## 判断 URL 是否命中缓存

1. 在浏览器Chrome上，按F12。
2. 选择“Network”。
3. 查看指定URL的响应头，查看头部信息，进行如下判断：
  - 如果有“x-hcs-proxy-type”头部，值为“1”即命中缓存，值为“0”即未命中缓存，不再查看其它头部；
  - 如果无“x-hcs-proxy-type”头部，而有“X-Cache-Lookup”头部，值为“Hit From MemCache”、“Hit From Disktank”或“Hit From Upstream”即为命中缓存，其它值表示未命中缓存，不再查看其它头部；
  - 如果同时无“x-hcs-proxy-type”、“X-Cache-Lookup”头部，有“age”头部，则值大于“0”即命中缓存，值为“0”即未命中缓存。

# 6 推送 CDN 日志到云日志服务 (LTS)

在使用CDN对资源进行加速时，CDN会产生大量日志数据，每一次终端用户访问都会产生对应的日志，以便分析业务情况。华为云CDN通过与云日志服务（LTS）融合，将实时采集到的日志推送至云日志服务进行分析。

## 为什么要看实时日志

实时日志可以帮助您分析加速域名遇到的异常问题，也可以帮助您了解用户的访问情况。实时日志的优势如下：

1. 当前CDN控制台可为用户展示的离线日志是延时了6个小时的日志，而实时日志延时较小，可以帮助您更快速的对终端用户访问日志进行分析。
2. 传统离线日志需要您先将离线日志包下载、解压再对日志进行分析处理，过程比较繁琐。华为云已打通与云日志服务间的通信链路，采用流式传输，免去了传统日志繁琐的下载分析流程。
3. 云日志服务已部署CDN专属的可视化仪表盘，您可以一键开启，将CDN原始日志可视化呈现。
4. 离线日志目前默认提供访问时间、状态码等13个字段，实时日志默认提供日志分析常用的25个字段，详见[实时日志字段](#)。

## 注意事项

1. CDN目前仅支持推送中国大陆节点的日志到云日志服务的北京四region。CDN其余地区节点的日志推送功能正在规划，请关注产品动态。
2. CDN节点实时日志推送暂不收费（后续是否会收费请关注产品动态），基础存储与分析相关费用由云日志服务（LTS）收取。
3. 受网络、节点物理硬件等的影响，引起的部分日志有延迟属于正常波动，实时日志也会存在小概率的延迟。
4. 实时日志不可用于计费、对账等场景。
5. 对接LTS后，如果您的域名上量超过20%，请提前5天提交工单请运维人员介入，以免影响正常使用。

## 如何开通实时日志

目前已实现对接LTS服务，控制台暂未开通自助配置功能，您可以[提交工单](#)申请开通实时日志功能，提交工单时请提供项目（cn-north-4）、[项目ID](#)、[日志组](#)、[日志流](#)信息。示例如下：

- 项目：cn-north-4。
- 项目ID：81b6\*\*\*\*\*bcf543ea。
- 日志组：test-cdn-log-prod。
- 日志组ID：95\*\*\*\*53-3a81-49ed-9003-c24\*\*\*\*\*de8
- 日志流：test-cdn-log-data-flow-prod。
- 日志流ID：a9\*\*\*\*63-5b82-4126-80c9-212\*\*\*\*\*534

日志推送成功后可通过云日志服务控制台查看CDN日志，云日志服务为CDN定制了如下功能：

图 6-1 日志服务仪表盘

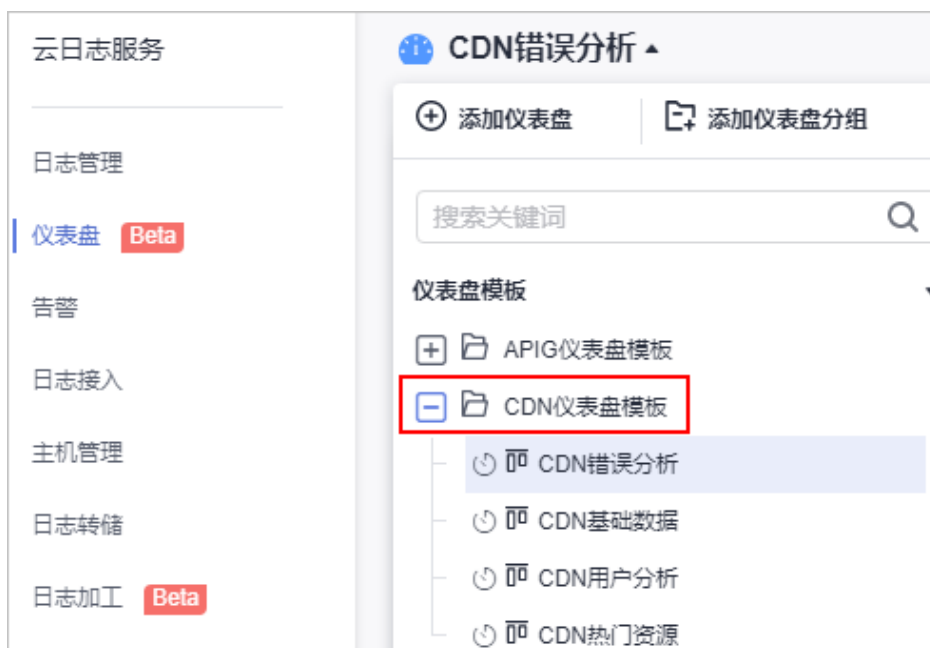


表 6-1 功能详情

功能	说明
<a href="#">CDN错误分析</a>	支持查看和导出错误访问信息，可按照域名、URI、请求状态、运营商、错误码等维度分析，帮助您快速定位和分析错误信息。
<a href="#">CDN基础数据</a>	支持查看和导出CDN的基础数据，如缓存命中率、下载速度、访问状态、访问延时、请求命中率、请求带宽、访问平均延时等，帮助您了解CDN的整体运行状态，及时发现和处理异常情况。
<a href="#">CDN用户分析</a>	支持查看和导出CDN的用户访问数据，如访问次数、访问人数、访问客户端、运营商次数统计、访问地区分布、有效访问用户TOP、下载量TOP用户等信息，帮助您更好的了解用户特点。
<a href="#">CDN热门资源</a>	支持查看和导出CDN的热门资源，如域名访问次数TOP5、域名下载流量Top5、热门访问（URI）、热门访问（来源）、运营商流量和速度、运营商统计等，帮助您根据热门访问情况及时调整运营策略。

如果以上功能不能满足您的需求，您可以定制仪表盘，请在提交工单时提出您的需求。

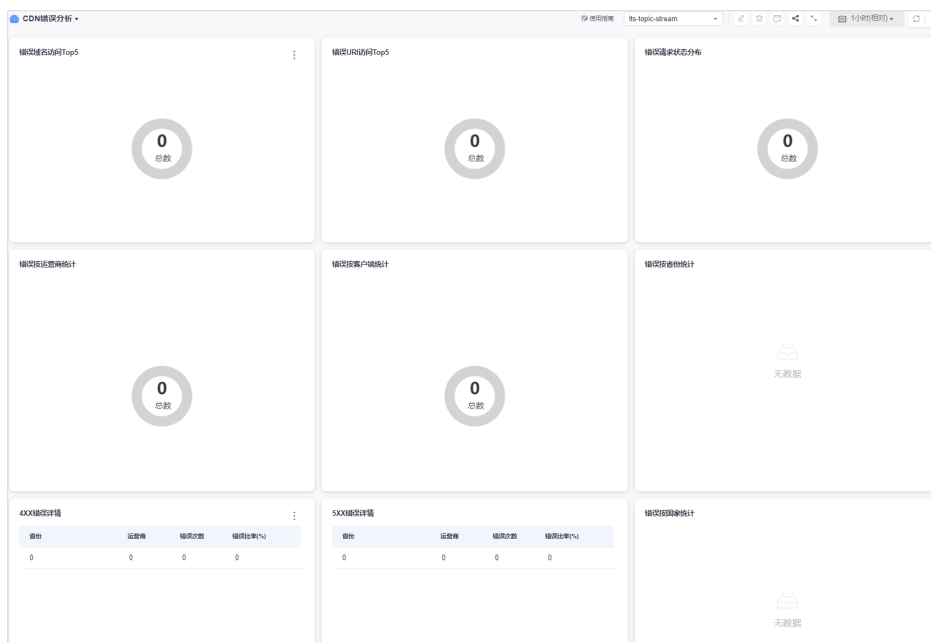
您还可以根据业务情况创建告警规则，以便及时跟进和处理异常事件，配置请参考[日志告警](#)。

## CDN 错误分析

通过CDN错误分析报表，您可以查看用户访问异常信息，帮助您快速定位异常访问源头。通过本报表您可以查看以下数据：

- 错误域名访问Top5：按照域名维度统计访问错误Top域名。
- 错误URI访问Top5：按照URI维度统计访问错误Top URI。
- 错误请求状态分布：统计错误请求状态码的数量和占比。
- 错误按运营商统计：统计各个运营商的错误和占比。
- 错误按客户端统计：统计客户端访问错误的数量和占比。
- 错误按省份统计：统计访问错误的省份。
- 4XX错误详情：统计4XX类错误的次数、占比、运营商及所在省份。
- 5XX错误详情：统计5XX类错误的次数、占比、运营商及所在省份。
- 错误按国家统计：按照国家维度统计访问错误所在地。

图 6-2 错误分析



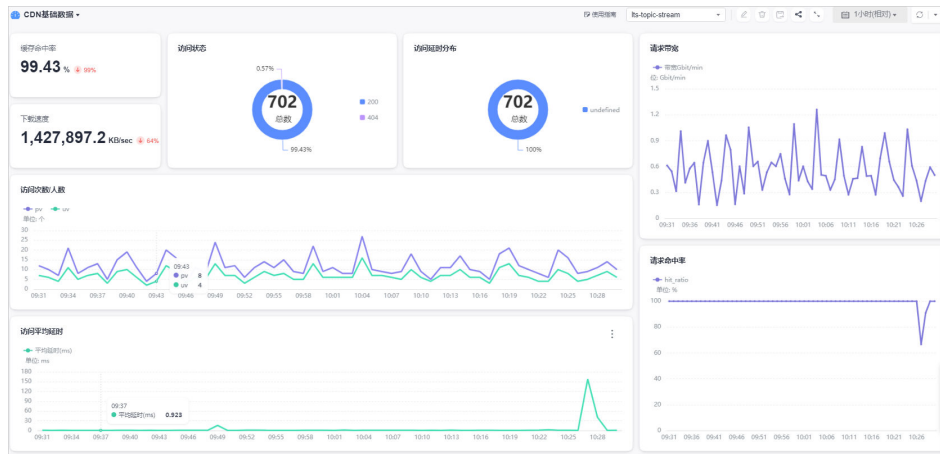
## CDN 基础数据

基础数据报表可以帮助您快速了解CDN服务的性能，包含以下数据：

- 缓存命中率：用户请求资源命中CDN缓存的概率（按字节）。
- 请求命中率：用户请求资源命中CDN缓存的概率（按请求数）。
- 下载速度：用户通过CDN下载资源的速度。

- 访问状态：按照返回的状态码（200、4xx、5xx）统计用户的请求状态及占比。
- 访问延时分布：不同延时时段的占比。
- 请求带宽：展示不同时段的用户请求带宽。
- 访问次数/人数：展示不同时段的访问次数和人数。
- 访问平均延时：终端用户访问页面延时的平均值。

图 6-3 基础数据

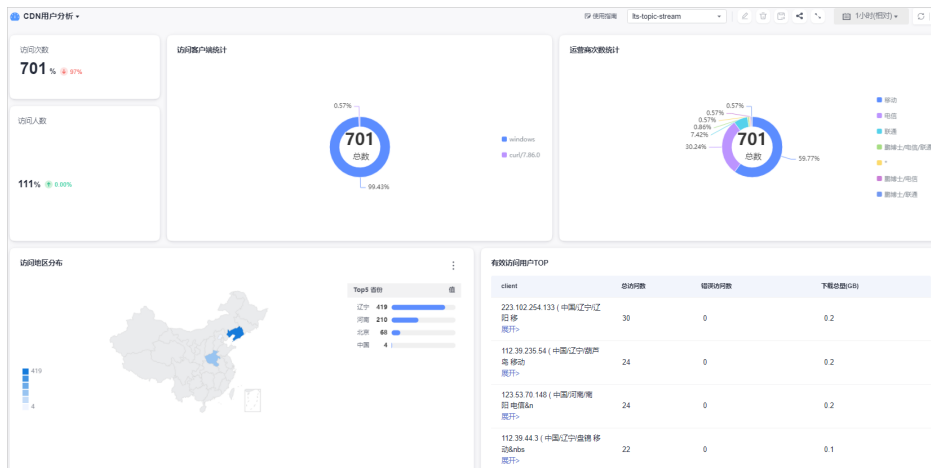


## CDN 用户分析

用户行为分析报表可以帮助您快速了解当前用户的结构，主要包含以下数据：

- 访问次数：总访问次数，PV。
- 访问人数：总访问人数，UV。
- 访问客户端统计：统计客户端访问的数量和占比。
- 运营商次数统计：统计各个运营商的访问次数和占比
- 访问地区分布：统计访问的地区分布及Top值。
- 有效访问用户TOP：统计有效访问用户的Top值。
- 下载量TOP用户：统计通过CDN下载的用户Top值。

图 6-4 用户分析



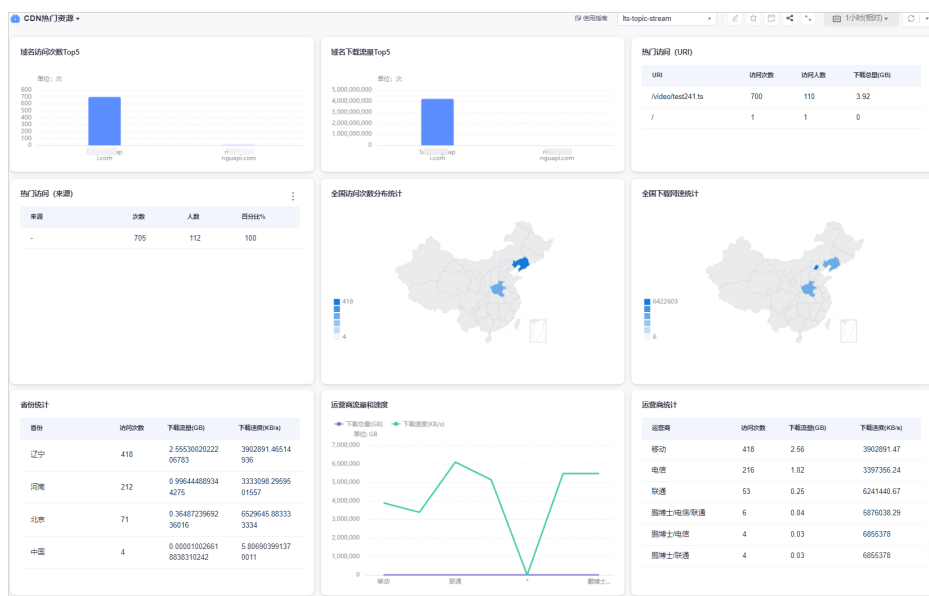


## CDN 热门资源

热门资源数据可以帮助您了解热门资源详情，也可以从热门数据了解到您的运营活动效果是否正常、热点时间内流量的上涨是否符合预期，以便及时调整运营策略。通过热门资源可以查看以下数据：

- 域名访问次数Top5：统计用户访问量较多的域名Top5。
- 域名下载流量Top5：统计用户下载量较多的域名Top5。
- 热门访问（URI）：统计用户访问量较多的URI Top。
- 热门访问（来源）：统计热门Referer来源域名，并且记录访问次数、人数、占比。
- 全国访问次数分布统计：按省份统计全国各地访问的次数。
- 全国下载网速统计：按省份统计全国各地下载的速度。
- 省份统计：按省份统计访问次数、下载速度、下载总量。
- 运营商流量和速度：统计各运营商在不同时段的流量和下载速度。
- 运营商统计：统计不同运营商的访问次数、下载速度、下载流量。

图 6-5 热门资源



## 实时日志字段

表 6-2 实时日志字段说明

字段	字段含义	是否一定有值	缺省值
request_time	请求时间戳，单位：毫秒	是	无
domain	请求的域名	是	无
method	请求方法	是	无
scheme	请求协议	是	无



字段	字段含义	是否一定有值	缺省值
uri	请求资源	是	无
uri_param	请求参数	否	"-"
client_ip	用户真实IP	是	无
client_port	和CDN节点建连客户端端口	是	无
refer_protocol	HTTP refer中的协议	否	"-"
refer_domain	HTTP refer中domain信息	否	"-"
refer_uri	HTTP refer中uri信息	否	"-"
refer_param	HTTP refer中的参数信息	否	"-"
request_size	请求大小	是	无
response_time	请求响应时长, 单位: 毫秒	是	无
response_size	请求返回大小, 单位: 字节	是	无
http_code	请求响应码	是	无
response_range	应答头里表示的range信息 (由源站创建), 如bytes: 0~99/200	是	无
request_range	用户请求中Header头中range字段取值, 如bytes: 0~100	是	无
request_body_bytes	实际发送body大小, 单位: 字节	是	无
content_type	请求的资源类型	是	无
hit_info	命中信息, 取值为HIT (命中)、MISS (未命中)	是	无
user_agent	UA	否	"-"
uuid	请求唯一标识 (全网唯一请求ID, 即traceid)	是	无
via_info	via头信息	否	"-"
X-Forwarded-For	请求头中X-Forwarded-For字段	否	"-"

# 7 CDN 日志转存到 OBS

CDN记录了所有域名（包括已删除域名，如果您开通了企业项目，则已删除域名不支持此功能）被网络用户访问的详细日志，您可以通过CDN控制台查看和下载最近30天的日志，对您的业务资源被访问情况进行详细分析。

日志转存储服务是华为云CDN配合函数工作流，将CDN日志存储到OBS桶，可以帮助您将日志存储更长的时间，便于您基于长时间的日志做出自定义的数据分析，有助于您更好地了解您CDN的服务质量，以及您的终端客户的访问详情，提高您的业务决策能力。

本文以Python3.6为例，为您介绍通过API创建FunctionGraph函数和Timer触发器，实现定时将CDN日志转存到OBS。

## 前提条件

暂时仅支持日志转存到北京四的OBS桶，请您提前准备好位于北京四的OBS桶。

## 操作步骤

### 1. 创建自定义策略

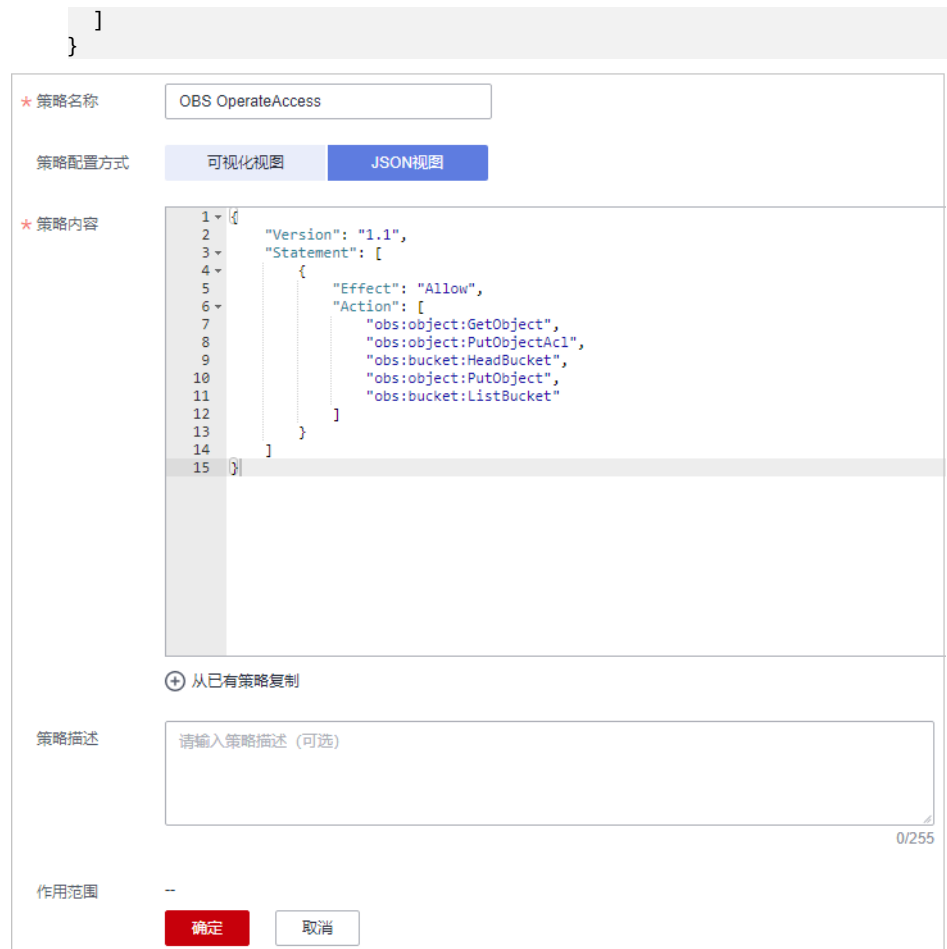
- a. 登录[华为云控制台](#)，在左侧导航栏，选择“管理与监管>统一身份认证服务”。
- b. 在左侧导航栏，选择“权限管理>权限”页签，单击右上方的“创建自定义策略”。

- 策略名称：OBS OperateAccess。

- 策略配置方式：JSON视图。

- 策略内容：

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "obs:object:GetObject",
        "obs:object:PutObjectAcl",
        "obs:bucket:HeadBucket",
        "obs:object:PutObject",
        "obs:bucket:ListBucket"
      ]
    }
  ]
}
```



- c. 单击“确定”，完成策略配置。
2. **创建委托**
    - a. 登录[华为云控制台](#)，在左侧导航栏，选择“管理与监管>统一身份认证服务”。
    - b. 在左侧导航栏，选择“委托”页签，单击右上方的“+ 创建委托”。
    - c. 在创建委托页面，按照如下参数设置委托。
      - 委托名称：FG\_TO\_CDN。
      - 委托类型：云服务。
      - 云服务：函数工作流FunctionGraph。
      - 持续时间：永久。

\* 委托名称: FG\_TO\_CDN

\* 委托类型:  普通帐号  
将帐号内资源的操作权限委托给其他华为云帐号。  
 云服务  
将帐号内资源的操作权限委托给华为云服务。

\* 云服务: 函数工作流 FunctionGraph

\* 持续时间: 永久

描述: 请输入委托信息。  
0/255

下一步 取消

- d. 单击“下一步”，进入为“FG\_TO\_CDN”委托配置权限界面。
  - 权限选择：OBS OperateAccess（第一步创建的策略）、CDN LogsReadOnlyAccess。

名称	类型
<input checked="" type="checkbox"/> OBS OperateAccess	自定义策略
<input checked="" type="checkbox"/> CDN LogsReadOnlyAccess	系统策略

- e. 单击“下一步”，配置作用范围。
  - i. 帐号未开通企业项目，配置如下：

- 作用范围：所有资源。

根据当前您所选择的策略，系统推荐以下授权范围方案，更便于您最小化授权，可进行选择。了解如何根据您的应用场景选择合适的授权范围方案

选择授权范围方案

所有资源  
不设置最小授权范围，授权后，用户根据权限使用帐号中所有资源。

展开其他方案

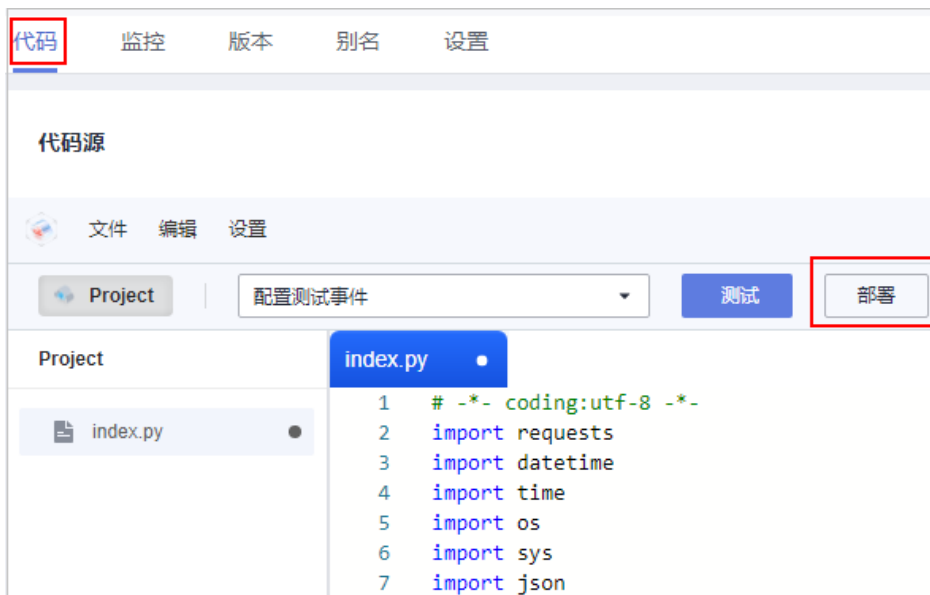
- ii. 帐号已开通企业项目，配置如下：
    - 作用范围：指定企业项目资源。



- iii. 选择存放日志的OBS桶所在的企业项目。
  - f. 单击“确认”，完成委托配置。
3. 准备函数 workflow 环境
- a. 登录[华为云控制台](#)，在左侧导航栏，选择“计算>函数 workflow”，region选择“北京四”。
  - b. 单击右上方“创建函数”，进入创建函数界面，选择“空白模板”。
    - 函数类型：事件函数。
    - 输入函数名称：cdn\_to\_obs（可自定义）。
    - 委托名称：选择已创建好的委托“FG\_TO\_CDN”。
    - 企业项目：选择“default”。
    - 运行时语言：选择“Python 3.6”。



- c. 单击“创建函数”，进入代码编辑界面，将[代码示例](#)的代码内容贴入在线IDE。



### 说明

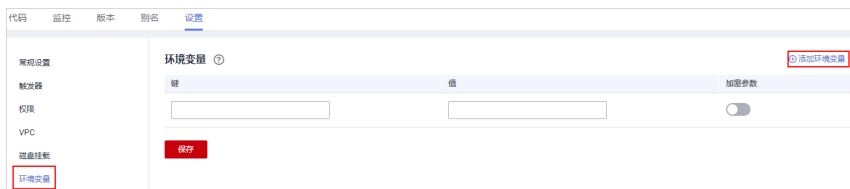
如果有多个域名的日志需要转存，您需要分别为每个域名创建一个函数工作流。

- d. 单击“配置”，进入函数配置界面，修改常规设置。
  - 执行超时时间：函数运行的超时时间，超时的函数将被强行停止，建议设置为900。

### 说明

如果您发现转存的日志数量不对，请向“函数工作流”服务提工单，增大执行超时时间。

- e. 添加环境变量，在设置界面左侧单击“环境变量”。
  - url：https://cdn.myhuaweicloud.com/v1.0/cdn/logs（CDN日志下载的url）。
  - domain\_name：xxx.com（需要转存日志的CDN加速域名）。
  - obsAddress：xxx.com（用于存日志的OBS桶域名）。
  - destBucket：\*\*\*\*\*（用于存日志的OBS桶名称）。



- 单击下方“保存”。
- f. 在设置界面左侧单击“权限”。
    - 选择已创建好的“FG\_TO\_CDN”委托，单击“保存”。
  - g. 创建“触发器”。在函数配置界面选择“触发器”，单击右侧“创建触发器”。

- 触发器类型：定时触发器 (TIMER)。
- 定时器名称：自定义的定时器名称，例如：Timer-0001。
- 触发规则：Cron表达式。
- Cron表达式：0 0 8 \* \* ? (每天早上8点执行一次日志转存储)。
- 是否开启：开启。

创建触发器

触发器类型 ? 定时触发器 (TIMER)

DDS、GAUSSMONGO、DIS、LTS、Kafka、TIMER触发器可创建数加起来最多10个，您已创建0个。

\* 定时器名称

支持字母、数字、下划线和中划线，必须以字母开头，且长度不能超过64个字符

\* 触发规则  固定频率  Cron表达式

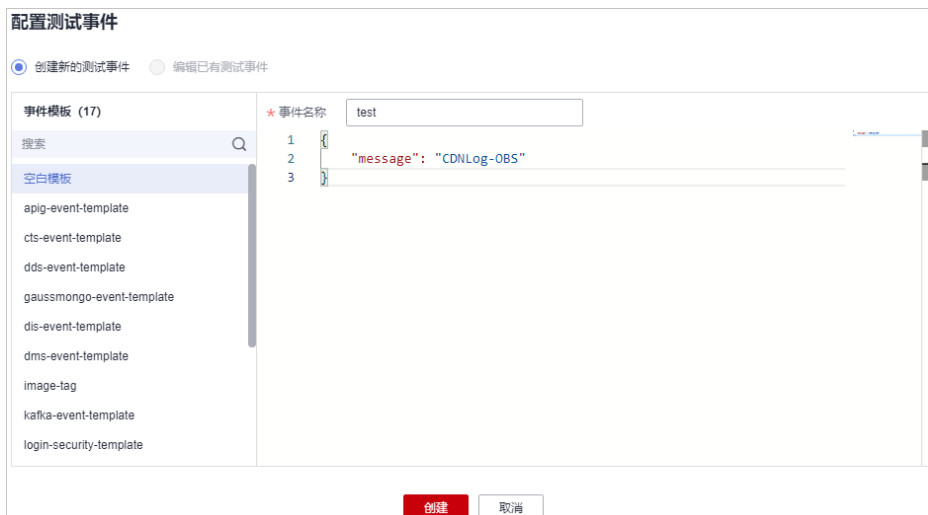
[了解Cron表达式](#)

\* 是否开启

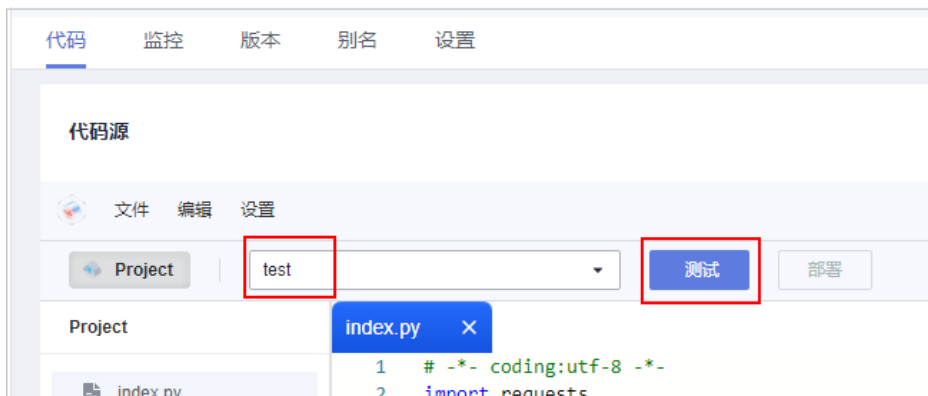
附加信息 ?

0/2,048

- i. 单击“确定”，完成定时触发器设置。
- h. 创建测试事件。返回“代码”界面，单击“测试”按钮。
  - 配置测试事件：创建新的测试事件。
  - 事件模板：空白模板。
  - 事件名称：test。
  - 测试事件：{"message": "CDNLog-OBS"}。



- i. 单击“保存”，完成测试事件创建。
- i. 测试函数。在函数详情页面，单击左侧下拉框，选择“test”，单击“测试”。



#### 4. 查看配置是否成功

- a. 登录[华为云控制台](#)，在左侧导航栏，选择“存储>对象存储服务 OBS”。
- b. 单击您存储日志的桶，在左侧导航栏选择“对象”。
- c. 访问路径：文件夹（桶名称）>文件夹（加速域名）>文件夹（日志日期）>日志内容。



#### 📖 说明

- 当前[代码示例](#)仅支持转存当前时间前一日的日志，如果您需要转存日志的加速域名前一日没有日志产生，则OBS桶侧不会产生相关文件。
- OBS桶将对转存到桶里的日志收费，具体收费规则请参考[计费说明](#)。

#### 5. 停止日志转存服务

- a. 登录[华为云控制台](#)，在左侧导航栏，选择“计算>函数 workflow”，region选择“北京四”。



- b. 在左侧导航栏选择“函数” > “函数列表”，选中2中创建的函数名。
- c. 在函数详情页选择“触发器”。



- d. 单击“停用”，完成配置。

## 代码示例

代码如下所示：

```
# -*- coding:utf-8 -*-
import requests
import datetime
import time
import os
import sys
import json

from com.obs.client.obs_client import ObsClient

from urllib.parse import urlparse

if sys.version_info.major == 2 or not sys.version > '3':
    import httplib
else:
    import http.client as httplib

current_file_path = os.path.dirname(os.path.realpath(__file__))
# Adds the current path to search paths to import third-party libraries.
sys.path.append(current_file_path)

TEMP_ROOT_PATH = "/tmp/" # Downloads a file from OBS to this directory.
region = 'china' # This parameter does not need to be changed and will be used when
FunctionGraph accesses OBS.
secure = True # This parameter does not need to be changed and will be used when
FunctionGraph accesses OBS.
signature = 'v4' # This parameter does not need to be changed and will be used when
FunctionGraph accesses OBS.
port = 443 # This parameter does not need to be changed and will be used when
FunctionGraph accesses OBS.
path_style = True # This parameter does not need to be changed and will be used when
FunctionGraph accesses OBS.

def handler(event, context):
    logger = context.getLogger()
    queryDate = context.getUserData('queryDate')
    if queryDate is None:
        yesterday = datetime.date.today() + datetime.timedelta(-1)
        queryDate = yesterday.strftime("%Y-%m-%d")
        timeStamp = int(time.mktime(yesterday.timetuple()) * 1000)
    else:
        date = datetime.datetime.strptime(queryDate, "%Y-%m-%d")
```

```
        timeStamp = int(time.mktime(date.timetuple()) * 1000)

        pageSize = 20
        pageNumber = 1

        requests.packages.urllib3.disable_warnings()
        start(context, queryDate, timeStamp, pageSize, pageNumber)

def start(context, queryDate, timeStamp, pageSize, pageNumber):
    logger = context.getLogger()
    logUrl = context.getUserData('url')
    domainName = context.getUserData('domain_name')

    params = {'query_date': timeStamp, 'domain_name': domainName, 'page_size': pageSize,
'page_number': pageNumber, 'enterprise_project_id': 'ALL'}
    headers = {'Content-Type': 'application/json;charset=UTF-8', 'X-Auth-Token':
context.getToken()}
    res = requests.get(logUrl, params=params, headers=headers, verify=False)
    if res.status_code != 200:
        logger.info("query log urls: " + res.url + ", error: " + res.text)
        return ("query log urls: " + res.url + ", error: " + res.text)

    resJson = json.loads(res.text)
    logger.info(res.text)
    total = resJson['total']
    i = 0
    for val in resJson['logs']:
        i += 1
        logger.info(val["link"])

        url = urlparse(val["link"])
        netlocs = url.netloc.split(":")
        conn = httplib.HTTPConnection(netlocs[0], int(netlocs[1]))
        conn.request('GET', url.path + "?" + url.query)
        objName = os.path.join(val["domain_name"], queryDate, val["name"])
        put_content_to_obs(context, objName, conn.getresponse())

    if pageSize * pageNumber < total:
        start(context, queryDate, timeStamp, pageSize, pageNumber + 1)

def put_content_to_obs(context, objName, content):
    ak = context.getAccessKey()
    sk = context.getSecretKey()
    obsAddress = context.getUserData('obsAddress')
    destBucket = context.getUserData('destBucket')
    TestObs = ObsClient(access_key_id=ak, secret_access_key=sk,
        is_secure=secure, server=obsAddress, signature=signature,
path_style=path_style, region=region,
        ssl_verify=False, port=port,
        max_retry_count=5, timeout=20)
    resp = TestObs.putContent(destBucket, objName, content=content)
    if resp.status < 300:
        print('requestId:', resp.requestId)
    else:
        print('errorCode:', resp.errorCode)
        print('errorMessage:', resp.errorMessage)
```

# 8 获取客户端真实 IP

本章节介绍了不同类型的Web应用服务器（包括Tomcat、Apache、Nginx、IIS 6和IIS 7）如何获取客户端的真实IP，如果有此方面需求，可以参考本文进行配置。

## 背景信息

网站接入CDN加速后，源站服务器端从IP头部获取的用户访问IP不是客户端的真实IP。当您因为业务需要获取客户端真实IP时，可以通过配置网站服务器获取客户端的真实IP。

代理服务器（CDN、WAF等）在把用户的HTTP、WebSocket、WSS请求转到下一环节的服务器时，会在头部中加入一条“X-Forwarded-For”记录，用来记录用户的真实IP，其形式为“X-Forwarded-For: 客户端的真实IP, 代理服务器1-IP, 代理服务器2-IP, 代理服务器3-IP, ……”。

因此，您可以通过获取“X-Forwarded-For”对应的第一个IP来得到客户端的真实IP。

## Nginx 如何在访问日志中获取客户端真实 IP

如果您的源站部署了Nginx反向代理，可通过在Nginx反向代理配置Location信息，后端Web服务器即可通过类似函数获取客户的真实IP地址。

1. 根据源站Nginx反向代理的配置，在Nginx反向代理的相应location位置配置如下内容，获取客户IP的信息。

```
Location ^ /<uri> {  
    proxy_pass ....;  
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;  
}
```

2. 后端Web服务器通过类似函数获取客户的真实IP。

```
request.getAttribute("X-Forwarded-For")
```

## Tomcat 如何在访问日志中获取客户端真实 IP

如果您的源站部署了Tomcat服务器，可通过启用Tomcat的X-Forwarded-For功能，获取客户端的真实IP地址。

1. 打开“server.xml”文件（“tomcat/conf/server.xml”），AccessLogValve日志记录功能部分内容如下：

```
<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"/>
```

- 在pattern中增加 “%{X-Forwarded-For}i” ，修改后的server.xml为：

```
<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>
```
- 查看 “localhost\_access\_log” 日志文件，可获取X-Forwarded-For对应的访问者真实IP。

## Apache 如何在访问日志中获取客户端真实 IP

如果您的源站部署了Apache服务器，可通过运行命令安装Apache的第三方模块 mod\_rpaf，并修改 “http.conf” 文件获取客户IP地址。

- 执行以下命令安装Apache的一个第三方模块mod\_rpaf。

```
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
```
- 打开 “httpd.conf” 配置文件，并将文件内容修改为如下内容：

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so ##加载mod_rpaf模块
<IfModule mod_rpaf.c>
  RPAFenable On
  RPAFsethostname On
  RPAFproxy_ips 127.0.0.1 <反向代理IPs>
  RPAFheader X-Forwarded-For
</IfModule>
```
- 定义日志格式。

```
LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"""
common
```
- 启用自定义格式日志。

```
CustomLog "[apache目录]/logs/$access.log" common
```
- 重启Apache，使配置生效。

```
/[apached目录]/httpd/bin/apachectl restart
```
- 查看 “access.log” 日志文件，可获取X-Forwarded-For对应的客户端真实IP。

## IIS 6 如何在访问日志中获取客户端真实 IP

如果您的源站部署了IIS 6服务器，您可以通过安装 “F5XForwardedFor.dll” 插件，从IIS 6服务器记录的访问日志中获取客户端真实的IP地址。

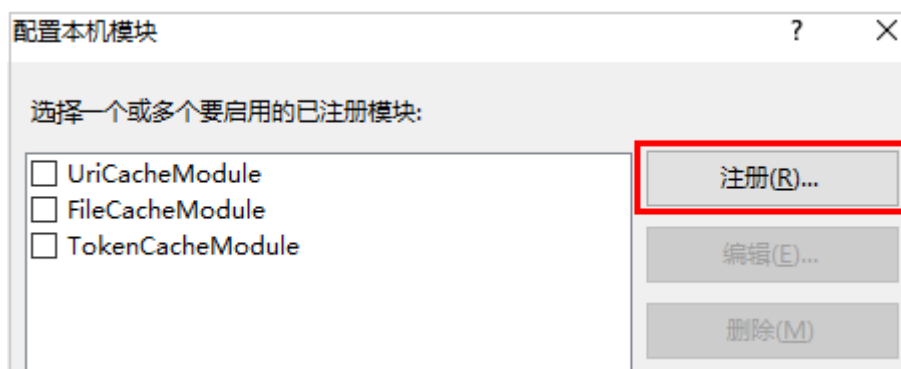
- 下载**F5XForwardedFor**模块。
- 根据您的服务器的操作系统版本将 “x86\Release” 或者 “x64\Release” 目录中的 “F5XForwardedFor.dll” 文件复制至指定目录（例如，“C:\ISAPIFilters”），同时确保IIS进程对该目录有读取权限。
- 打开IIS管理器，找到当前开启的网站，在该网站上右键选择 “属性”，打开 “属性” 页面。
- 在 “属性” 页面，切换至 “ISAPI筛选器”，单击 “添加”，在弹出的窗口中，配置如下信息：
  - “筛选器名称”：“F5XForwardedFor”；
  - “可执行文件”：“F5XForwardedFor.dll” 的完整路径，例如：“C:\ISAPIFilters\F5XForwardedFor.dll”
- 单击 “确定”，重启IIS 6服务器。

- 查看IIS 6服务器记录的访问日志（默认的日志路径为：“C:\WINDOWS\system32\LogFiles\”，IIS日志的文件名称以“.log”为后缀），可获取X-Forwarded-For对应的客户端真实IP。

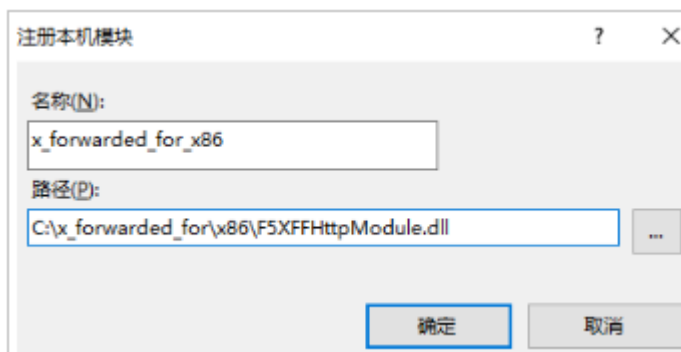
## IIS 7 如何在访问日志中获取客户端真实 IP

如果您的源站部署了IIS 7服务器，您可以通过安装“F5XForwardedFor”模块，从IIS 7服务器记录的访问日志中获取客户端真实的IP地址。

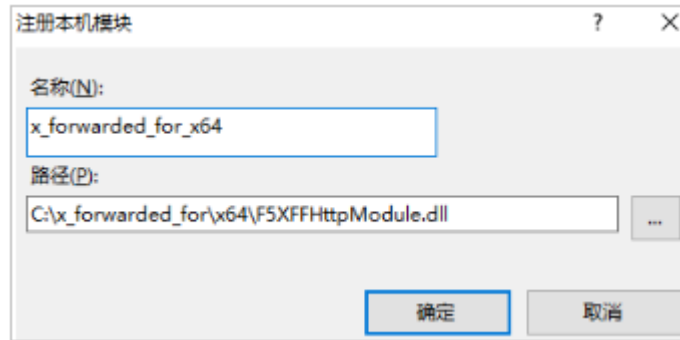
- 下载F5XForwardedFor模块。
- 根据服务器的操作系统版本将“x86\Release”或者“x64\Release”目录中的“F5XFFHttpModule.dll”和“F5XFFHttpModule.ini”文件复制到指定目录（例如，“C:\x\_forwarded\_for\x86”或“C:\x\_forwarded\_for\x64”），并确保IIS进程对该目录有读取权限。
- 在IIS服务器的选择项中，双击“模块”，进入“模块”界面。
- 单击“配置本机模块”，在弹出的对话框中，单击“注册”。



- 在弹出的对话框中，按操作系统注册已下载的DLL文件后，单击“确定”。
  - x86操作系统：注册模块“x\_forwarded\_for\_x86”
    - 名称：x\_forwarded\_for\_x86
    - 路径：“C:\x\_forwarded\_for\x86\F5XFFHttpModule.dll”



- x64操作系统：注册模块“x\_forwarded\_for\_x64”
  - 名称：x\_forwarded\_for\_x64
  - 路径：“C:\x\_forwarded\_for\x64\F5XFFHttpModule.dll”



6. 注册完成后，勾选新注册的模块（“x\_forwarded\_for\_x86”或“x\_forwarded\_for\_x64”）并单击“确定”。
7. 在“ISAPI和CGI限制”中，按操作系统添加已注册的DLL文件，并将其“限制”改为“允许”。
  - x86操作系统：
    - ISAPI或CGI路径：“C:\x\_forwarded\_for\x86\F5XFFHttpModule.dll”
    - 描述：x86
  - x64操作系统：
    - ISAPI或CGI路径：“C:\x\_forwarded\_for\x64\F5XFFHttpModule.dll”
    - 描述：x64
8. 重启IIS 7服务器，等待配置生效。
9. 查看IIS 7服务器记录的访问日志（默认的日志路径为：“C:\WINDOWS\system32\LogFiles\”，IIS日志的文件名称以“.log”为后缀），可获取X-Forwarded-For对应的客户端真实IP。

# 9 CDN 加速云速建站 CloudSite

## 应用场景

云速建站（CloudSite）可以帮助您快速搭建网站，您可以通过CDN加速您的站点，提高用户访问网站的响应速度与网站的可用性，解决网络带宽小和客户访问量大等问题。本文介绍如何在CDN控制台添加域名，加速站点。

目前企业版（多终端独立企业版）站点已支持通过CloudSite控制台配置CDN加速，详情请见[配置站点加速](#)。

## 前提条件

- 已购买[云速建站多终端独立版](#)的站点。
- 加速域名未绑定站点，如果已绑定，请先[解除绑定](#)。
- 待加速的域名已在华为云完成[备案](#)。

## 操作步骤

本文以加速域名www.example.com为例，为您展示配置过程。

1. 在CDN控制台添加加速域名
  - a. 登录[华为云控制台](#)，选择“所有服务 > CDN与智能边缘 > 内容分发网络CDN”，进入CDN管理控制台。
  - b. 单击左侧“域名管理”，进入域名管理页面。
  - c. 在域名管理页面单击“添加域名”。
  - d. 在“添加域名”弹框中配置域名及CDN加速等信息。
    - 加速域名：www.example.com。
    - 业务类型：实际业务结合[应用场景](#)选择合适的业务类型。
    - 服务范围：根据您的业务需要选择服务范围。
    - 源站配置：
      - 回源方式：根据需要选择合适的回源方式。
      - 源站类型：选择“源站域名”。
      - 源站地址：输入云速建站站点的CNAME。。

- 优先级：主源站或备源站。
- 回源HOST：默认为桶域名。

#### 说明

如果您使用多终端独立企业版站点，源站类型可以选择“源站IP”，绑定站点的独立IP。

e. 单击确定，完成域名添加。

## 2. 配置CNAME

添加加速域名后，CDN会自动生成一条CNAME域名。加速域名在CDN服务中获得的CNAME域名不能直接访问，必须在加速域名的域名服务商处配置CNAME记录，将加速域名指向CNAME域名，访问加速域名的请求才能转发到CDN节点上，达到加速效果。配置解析请参见[配置CNAME](#)。

## 3. 验证CNAME配置是否生效。

打开Windows操作系统中的cmd程序，输入如下指令：

```
nslookup -qt=cname 加速域名
```

如果回显CDN分配的CNAME域名，则表示CNAME配置已经生效。



# 10 源站是 OBS 桶时如何配置自定义首页内容

## 适用场景

当CDN的源站是OBS桶时，用户访问加速域名会展示桶内对象列表。如果您不想将桶内对象列表展示给用户，可以配置自定义首页内容。

## 操作步骤

- **源站是OBS公有桶**：开启静态网站托管并在CDN侧勾选静态网站托管。
  - a. 登录OBS控制台，在左侧菜单栏选择“桶列表”。
  - b. 单击您需要配置静态网站托管的桶名称。
  - c. 在左侧菜单栏选择“对象 > 基础配置 > 静态网站托管”进入静态网站托管配置页面。
  - d. 单击“配置静态网站托管”，打开“状态”开关，请参考[配置网站托管](#)配置相关参数。
  - e. 前往CDN控制台，添加域名或修改域名源站配置时，勾选“静态网站托管”选项。
  - f. 单击“确定”，源站地址将增加“-website”如下图所示。

图 10-1 源站信息

源站类型	源站地址	优先级
OBS桶域名	l.obs-website.la i-2.my...	主源站

- g. 刷新加速域名首页，刷新成功后再次访问该加速域名，即为静态网站托管配置的默认首页。
- **源站是OBS私有桶**：配置高级桶策略或首页回源。
    - a. 如果您选择配置高级桶策略，请参考[通过CDN加速OBS视频点播](#)中实施步骤的第6步完成配置。
    - b. 如果您选择配置首页回源，请登录CDN控制台，在左侧菜单栏中，选择“域名管理”。

- c. 在域名列表中，单击需要修改的域名或域名所在行的“设置”，进入域名配置页面。
- d. 选择“缓存配置”页签。
- e. 在缓存规则模块，单击“编辑”，系统弹出“配置缓存策略”对话框。
- f. 配置一条“类型”为“首页”，缓存过期时间为“0”的缓存规则，且优先级要高于其他规则。
- g. 前往“回源配置”页签，单击回源URL改写后的“编辑”，进入回源URL配置页面。
  - 匹配方式：通配符。
  - 待改写回源URI：/。
  - 目标回源URI：填写您希望用户访问时看到的首页路径。
  - 优先级：建议设置最高优先级。
- h. 单击“确定”，完成回源URL改写配置。
- i. 配置生效后（大约需要5-10分钟），刷新加速域名首页，再次访问首页即可显示改写后的页面。

# 11 通过日志分析恶意访问地址

## 适用场景

如果您的加速域名遭受攻击，想要加固安全防护配置，比如配置防盗链、IP黑白名单等，您可以通过分析攻击时段对应的日志实现。

CDN日志包含了终端用户访问的信息，日志内容示例如下：

```
[05/Feb/2018:07:54:52 +0800] x.x.x.x 1 "-" "HTTP/1.1" "GET" "www.test.com" "/test/1234.apk" 206 720 HIT  
"Mozilla/5.0 (Linux; U; Android 6.0; zh-cn; EVA-AL10 Build/HUAWEIEVA-AL10) AppleWebKit/533.1  
(KHTML, like Gecko) Mobile Safari/533.1" "bytes=-256"
```

各字段从左到右含义如表11-1所示。

表 11-1 CDN 日志字段说明

序号	字段含义	字段示例
1	日志生成时间	[05/Feb/2018:07:54:52 +0800]
2	访问IP地址	x.x.x.x
3	响应时间(单位ms)	1
4	Referer信息	-
5	HTTP协议标识	HTTP/1.1
6	HTTP请求方式	GET
7	CDN加速域名	www.test.com
8	请求路径	/test/1234.apk
9	HTTP状态码	206
10	返回字节数大小	720
11	缓存命中状态	HIT

序号	字段含义	字段示例
12	User-Agent信息，其作用是让服务器能够识别客户使用的操作系统及版本、CPU类型、浏览器及版本信息等。	Mozilla/5.0 (Linux; U; Android 6.0; zh-cn; EVA-AL10 Build/HUAWEIEVA-AL10) AppleWebKit/533.1 (KHTML, like Gecko) Mobile Safari/533.1
13	Range信息，其作用是在HTTP请求头中指定返回数据的范围，即第一个字节的位置和最后一个字节的位置。 bytes参数值表示方法一般分为如下三类： <ul style="list-style-type: none"><li>• bytes=x-y: 表示请求第x个字节到第y个字节的数据内容。</li><li>• bytes=-y: 表示请求最后y个字节的数据内容。</li><li>• bytes=x-: 表示请求第x字节到最后一个字节的数据内容。</li></ul>	bytes=-256

## 操作步骤

1. 登录[华为云控制台](#)，在控制台首页中选择“CDN与智能边缘 > 内容分发网络CDN”，进入CDN控制台。
2. 在左侧菜单栏中，选择“日志管理”。
3. 选择需要查询的加速域名和日期。
4. 在需要下载的日志行单击“下载”，即可将日志下载到本地。
5. 日志下载后，您可以用Excel打开，筛选您感兴趣的字段，然后进行以下分析：
  - **分析用户访问的资源**：如果访问的资源比较集中，访客IP较分散，可能是新增了资源。
  - **分析访客IP**：如果较集中在某些IP段且访问量很大，访问的URL具体资源比较集中，有可能这些访客IP是恶意访问，可将这些IP添加黑名单，请参考[IP黑名单](#)完成配置。
  - **分析User-Agent信息**：通过UA请求头看是否存在不常见的UA头，判断是否属于攻击行为，可参考[UA黑名单配置](#)配置访问控制。
  - 也可通过其他字段，如：referer、缓存命中状态或者多个字段进行结合过滤筛选，从而判断共性的部分，加固对应的防护配置。

# 12 客户端访问加速域名经过 Nginx 转发时，如何定期刷新 DNS 解析

## 适用场景

如果您配置了Nginx代理转发，即：终端用户访问加速域名时，首先解析到Nginx服务器，由Nginx服务器将该请求转发到CDN节点，而Nginx服务器在启动/重载的时候会去解析转发的域名，此时域名如果修改了DNS解析，Nginx服务器将无法感知，从而导致域名无法解析，域名访问失败。

## 解决方案

如果想要定期刷新域名DNS解析，不用重启Nginx服务器，可以通过在Nginx上配置Resolver实现。

- 示例一：
  - a. Nginx服务器原“nginx.conf”配置：

```
location /prod-url-test/ {  
    ...  
    proxy_pass http://$proxy_url;  
}
```
  - b. 添加resolver后的配置：\*\*\*为设备网络使用的公共DNS或本地DNS，可根据业务情况配置两个DNS，valid为解析结果有效期。

```
location /prod-url-test/ {  
    resolver **** valid=300s;  
    resolver_timeout 10s;  
    set $proxy_url "prod-url-test.example.com";  
    proxy_pass http://$proxy_url;  
}
```
- 示例二：
  - a. Nginx服务器原“nginx.conf”配置：

```
location = /test/example1.txt {  
    expires 30s;  
    rewrite ^/test/example2.txt break;  
    proxy_pass https://test.example.com;  
}
```
  - b. 添加resolver配置：\*\*\*为设备网络使用的公共DNS或本地DNS，可根据业务情况配置两个DNS，valid为解析结果有效期。

```
set $var_host "test.example.com";  
resolver **** valid=300s;  
resolver_timeout 10s;
```

```
location = /test/example1.txt{  
    expires 30s;  
    rewrite ^/test/example2.txtbreak;  
    proxy_pass https://$var_host;  
    proxy_set_header Host test.example.com;  
}
```

# A 修订记录

发布日期	修订记录
2024-03-20	第十九次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>新增“客户端访问加速域名经过Nginx转发时，如何定期刷新DNS解析”章节。</li></ul>
2023-12-07	第十九次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>更新“自定义OBS私有桶策略配置”章节。</li></ul>
2023-10-18	第十八次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>完善推送CDN日志到云日志服务（LTS）的配置流程指引。</li></ul>
2023-06-30	第十七次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>增加“源站是OBS桶时如何配置自定义首页内容”。</li><li>增加“通过日志分析恶意访问地址”。</li></ul>
2023-04-27	第十六次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>增加“推送CDN日志到云日志（LTS）服务”。</li></ul>
2022-02-23	第十五次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>从OBS控制台为桶绑定CDN加速域名后，支持自动刷新功能。</li></ul>

发布日期	修订记录
2022-09-06	第十四次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>● 增加“CDN加速匀速建站CloudSite”。</li></ul>
2022-08-10	第十三次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>● 增加“CDN加速OBS常见问题”章节。</li></ul>
2022-08-01	第十二次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>● 更新“CDN日志转存到OBS”章节，修改“创建委托”步骤。</li></ul>
2022-05-24	第十一次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>● 更新“CDN日志转存到OBS”章节，新增“创建自定义策略”。</li></ul>
2022-03-10	第十次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>● 新增“自定义OBS私有桶策略配置”章节</li></ul>
2021-12-28	第九次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>● 更新“如何提高缓存命中率”章节。</li></ul>
2021-09-08	第八次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>● 更新“CDN日志转存到OBS”代码示例。</li></ul>
2021-06-18	第七次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>● 新增“获取客户端真实IP”</li></ul>
2021-04-28	第六次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>● 新增“CDN日志转存到OBS”</li></ul>
2021-04-21	第五次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>● 新增“如何提高缓存命中率”</li></ul>



发布日期	修订记录
2021-04-02	第四次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>● 新增“CDN加速ECS资源”</li></ul>
2021-03-19	第三次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>● 更新“CDN加速OBS桶文件”</li><li>● 新增“如何设置缓存过期时间”</li></ul>
2020-04-15	第二次正式发布。 本次更新说明如下： <ul style="list-style-type: none"><li>● 更新操作步骤</li><li>● 优化相关描述</li></ul>
2019-06-27	第一次正式发布。