

CDN

CDN 最佳实践

文档版本 08
发布日期 2026-04-23



版权所有 © 华为云计算技术有限公司 2026。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

1 最佳实践汇总	1
2 CDN 加速访问 OBS 桶文件	2
2.1 方案概述.....	2
2.2 CDN 加速访问 OBS 桶文件.....	4
2.3 自定义 OBS 私有桶策略配置.....	7
2.4 多云存储数据同步方案.....	8
2.5 CDN 加速 OBS 常见问题.....	10
3 CDN 加速访问基于 ECS 搭建的网站	12
4 CDN 加速访问 WAF 防护资源	15
5 如何设置缓存过期时间	20
6 如何提高缓存命中率	31
7 源站是 OBS 桶时如何配置自定义首页内容	34
8 通过日志分析恶意访问地址	36
9 防范恶意流量盗刷	39
10 CDN 联动 GA 实现跨境访问加速	43
11 使用规则引擎功能限制客户端恶意请求	54

1 最佳实践汇总

本文汇总了内容分发网络（CDN）服务的常见应用场景，并为每个场景提供详细的方案描述和操作指南，以帮助您使用CDN加速网站。

表 1-1 CDN 最佳实践

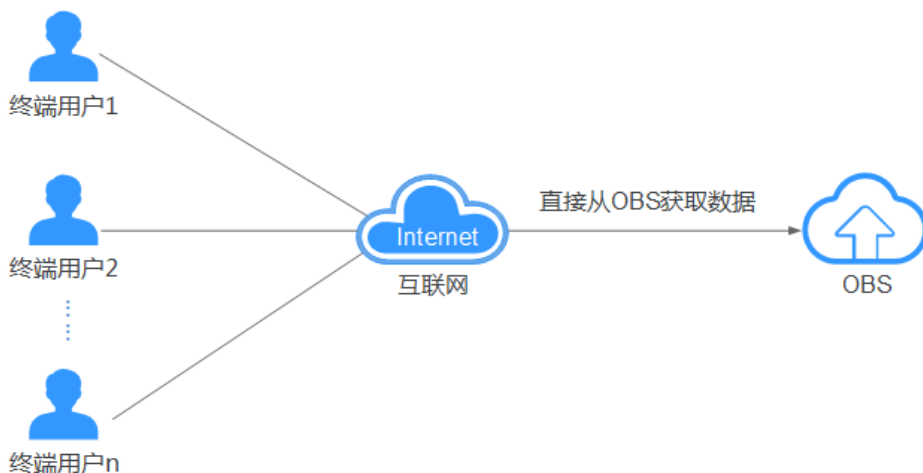
分类	相关文档
网站接入CDN加速	CDN加速访问OBS桶文件
	CDN加速访问基于ECS搭建的网站
	CDN加速访问WAF防护资源
	CDN联动GA实现跨境访问加速
	源站是OBS桶时如何配置自定义首页内容
提高缓存命中率	如何设置缓存过期时间
	如何提高缓存命中率
日志分析	通过日志分析恶意访问地址
安全相关	防范恶意流量盗刷
	使用规则引擎功能限制客户端恶意请求

2 CDN 加速访问 OBS 桶文件

2.1 方案概述

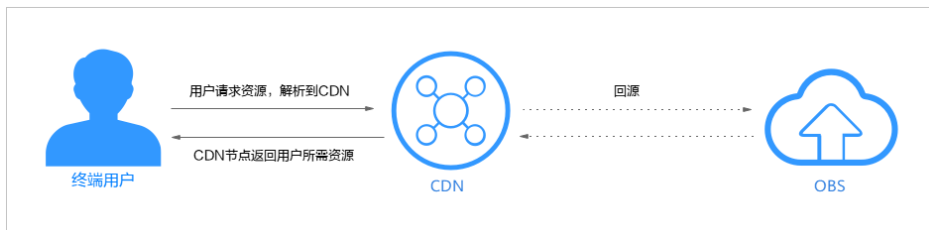
背景介绍

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桶能够很好地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。



资源与成本规划

本实践所需资源请见下表。

资源	资源说明	每月费用
内容分发网络 CDN	流量/带宽 ：用户访问CDN节点产生的流量/带宽，“计费方式”“流量计费”时可购买流量包抵扣。	具体的计费方式及标准请参考 计费说明 。
对象存储服务 OBS	流量 ：CDN回源OBS时会产生公网流出费用，按需计费，版本为3.0以上的桶且以“OBS桶域名”形式接入CDN可购买回源流量包抵扣。	具体的计费方式及标准请参考OBS 计费说明 。

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。
- 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。

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**查看KMS密钥**和**加密数据密钥**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](#)。

2.2 CDN 加速访问 OBS 桶文件

场景介绍

某游戏网站主要服务在中国大陆范围，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。如果您的服务范围为“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 工信部备案并在有效期内 才可以 使用CDN加速 。 <ul style="list-style-type: none">• 域名在华为云备案请参考备案。	download.game-apk1.com（已备案）
OBS桶	版本号为3.0以上的OBS存储桶，桶策略为公共读，未开通静态网站托管。	obs-doc-test

实施步骤

1. 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，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](#)。
2. 在CDN控制台添加加速域名
 - a. 登录[CDN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：中国大陆。
 - 加速域名：download.game-apk1.com，首次接入CDN加速需要验证域名归属权。
 - 业务类型：文件下载加速。
 - 源站配置：
 - 回源方式：协议跟随。
 - 源站类型：选择“OBS桶域名”。
 - 源站地址：选择本账号桶“obs-doc-test”的桶域名。
 - 静态网站托管：不勾选。
 - 回源鉴权：关闭。
 - 优先级：70。
 - 回源HOST：默认为桶域名。
 - e. 根据业务需求设置**突发带宽告警**和**用量封顶**功能，勾选**数据跨境合规承诺**。
 - f. 单击“确定”，完成域名添加。

📖 说明

- 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](#)。

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”页面。
- e. 根据表2-1示例列填写相关参数值，表中未提到的参数可保持默认值。

表 2-1 解析配置

参数	说明	示例
主机记录	主机记录指域名前缀。	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
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。	5分钟
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。

4. 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。

5. 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
```

6. 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。

2.3 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. 登录[华为云控制台](#)，在控制台首页中选择“存储 > 对象存储服务 OBS”“，进入OBS控制台。
2. 在左侧导航栏选择“对象存储”。
3. 在桶列表单击待操作的桶名称，进入“对象”页面。
4. 在左侧导航栏，选择“权限控制 > 桶策略”。
5. 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”和“GetObject”。

图 2-1 创建桶策略

创建桶策略 [如何配置?](#)

1 【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 所有账号
 当前账号
 其他账号

*“账号ID”表示授权给账号下的所有IAM用户。[如何查看“账号ID”和“IAM用户ID”?](#)

委托账号 [删除](#)

* 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

[选择动作](#)

授权条件 (可选) [增加条件](#) 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 如果存在 限定词 条件运算符 值 操作

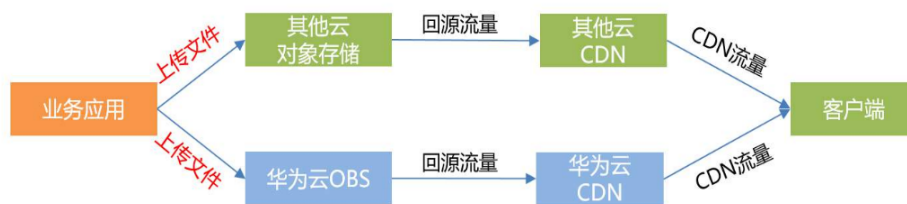
[取消](#) [创建](#)

6. 单击“创建”，完成桶策略创建。

2.4 多云存储数据同步方案

应用双写

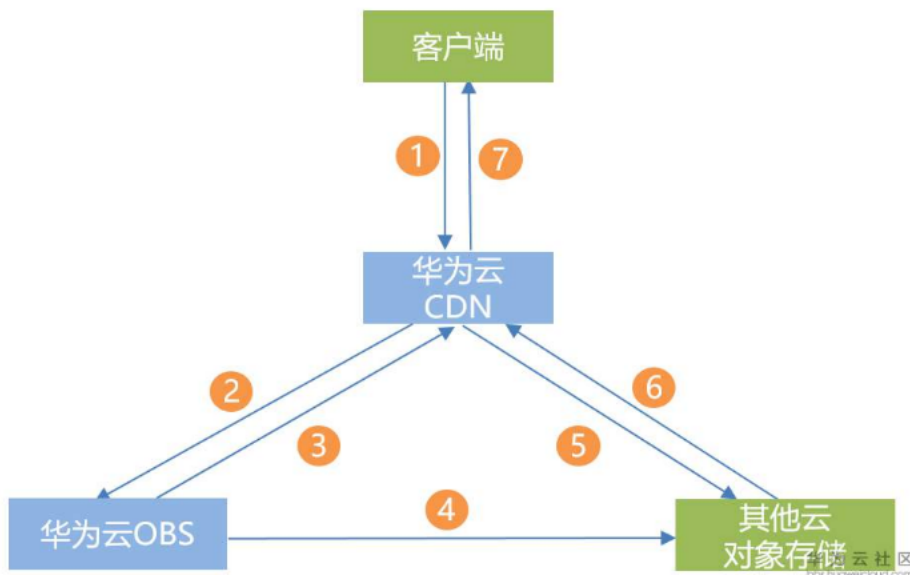
如果数据是在应用服务侧产生，或者数据在客户端产生但通过服务端将数据写入对象存储，则建议使用双写方案，架构如下：



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。

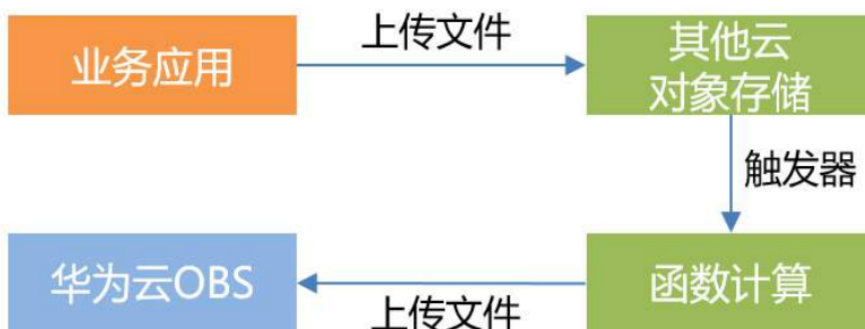
📖 说明

“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 2-2 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。

2.5 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和流量包优惠，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**，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 2-2 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”。

3 CDN 加速访问基于 ECS 搭建的网站

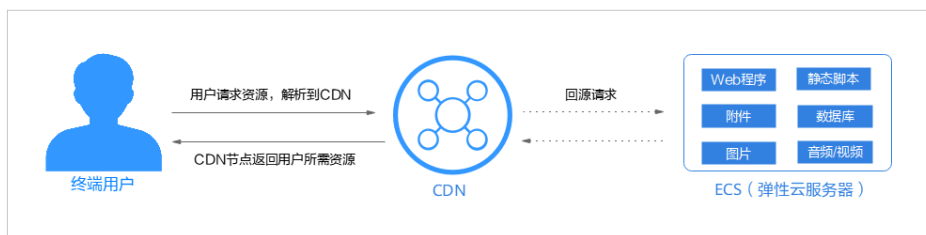
场景介绍

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。某客户将一论坛网站部署在华为云ECS上，并通过域名访问该论坛。初期业务量较小，用户访问流畅，随着业务越做越大，访问量骤增，陆续有用户反馈访问速度慢等问题。客户决定使用华为云CDN提高终端用户访问速度、提升用户体验。

方案概述

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加速搭建在ECS服务器上的网站，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。

业务流程：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。
- 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。

实施步骤

1. 在ECS服务器上搭建论坛网站，实施步骤请参考[搭建Discuz论坛网站](#)。
 - 服务器IP地址为：192.168.1.1。
 - 网站域名为：discuztest.com。
2. 开通CDN服务
 - a. 登录[华为云控制台](#)，在控制台首页左上角选择“服务列表 > CDN与智能边缘 > 内容分发网络 CDN”。
 - b. 单击“前往开通”，进入服务开通界面。
 - c. 选择计费方式，勾选服务协议，单击“立即开通”。
3. 在CDN控制台添加加速域名
 - a. 登录[CDN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”，配置加速域名及源站信息。
 - 加速域名：discuztest.com。
 - 服务范围：中国大陆。
 - 业务类型：网站加速。
 - 源站配置：
 - 回源方式：HTTP。
 - 源站类型：源站IP。
 - 源站地址：192.168.1.1。
 - 优先级：70。
 - 回源HOST：默认为加速域名。
 - d. 根据业务需求设置[突发带宽告警](#)和[用量封顶](#)功能，勾选[数据跨境合规承诺](#)。
 - e. 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

4. **本地测试加速域名**：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](#)。
5. **配置CNAME解析**：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“discuztest.com.cdnhwc1.com”。

- 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“discuztest.com”。
- d. 单击“discuztest.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”页面。

- e. 根据表3-1示例列填写相关参数值，表中未提到的参数可保持默认值。

表 3-1 解析配置

参数	说明	示例
主机记录	主机记录指域名前缀。	www
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
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。	5分钟
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。	discuztest.com.cdnhw1.com

- f. 单击“确定”，完成添加。

6. 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“discuztest.com”。如果回显CDN分配的CNAME域名，则表示CNAME配置已经生效。

7. 验证操作是否成功

登录论坛网站，浏览网页，如果可以正常访问网站，则表示加速配置成功。

4 CDN 加速访问 WAF 防护资源

应用场景

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，全面提升网站防护能力。

📖 说明

- 本实践建立在用户已经[开通CDN服务](#)、准备好域名（www.example.com），且解析在华为云。
- 待加速的域名已在华为云完成[备案](#)。

方案概述

CDN+WAF可以对华为云、非华为云或云下的域名进行联动防护，同时提升网站的响应速度和网站防护能力，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。



方案优势

CDN和WAF同时部署，缩短用户查看内容的访问延迟，提高了用户访问网站的响应速度与网站的可用性，解决了网络带宽小、用户访问量大、网点分布不均等问题，同时可以防御Web应用攻击（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），确保业务持续可靠运行。

资源与成本规划

实践所需资源请见下表。

资源	资源说明	每月费用
CDN	<ul style="list-style-type: none"> 计费模式：按需计费 支持使用资源包 	具体的计费方式及标准请参考 计费说明 。
Web应用防火墙	云模式-标准版： <ul style="list-style-type: none"> 计费模式：包年/包月 域名数量：10个防护域名 QPS配额：2,000QPS业务请求 支持带宽峰值： <ul style="list-style-type: none"> 源站服务器部署在华为云内：100Mbps 源站服务器部署在华为云外：30Mbps 	具体的计费方式及标准请参考 计费说明 。

实施步骤

1. 购买WAF云模式标准版

- a. 登录[华为云控制台](#)。
- b. 在控制台页面中选择“安全与合规 > Web应用防火墙 WAF”，进入Web应用防火墙控制台。
- c. 在总览页面，单击“购买WAF实例”，进入购买页面，“WAF模式”选择“云模式”。
 - “区域”：根据防护业务的所在区域就近选择购买的WAF区域。
 - “计费模式”：包年/包月。
 - “版本规格”：选择“标准版”。
 - “高阶功能”、“扩展包”及“购买时长”：根据具体情况进行选择。
- d. 确认参数配置无误后，在页面右下角单击“立即购买”。
- e. 确认订单详情无误后，阅读并勾选《Web应用防火墙免责声明》，单击“去支付”，完成购买操作。
- f. 进入“付款”页面，选择付款方式进行付款。

2. 将网站信息添加到WAF


- a. 在左侧导航树中，选择“网站设置”，进入网站设置列表。
- b. 在网站列表的左上角，单击“添加防护网站”。
- c. 选择“云模式-CNAME接入”并单击“开始配置”。
 - 云模式-ELB接入方式请参见[将网站接入WAF防护（云模式-ELB接入）](#)。

- d. 根据界面提示，配置网站信息，如表4-1取值样例列所示，表中未给出的配置请根据实际情况选择配置。

表 4-1 重点参数说明

参数	参数说明	取值样例
防护域名	需要添加到WAF中防护的域名。 <ul style="list-style-type: none"> 域名已完成备案 支持单域名（例如，一级域名example.com，二级域名www.example.com等）和泛域名（例如，*.example.com）。 	www.example.com
防护端口	需要防护的域名对应的业务端口。	标准端口
服务器配置	网站服务器地址的配置。包括对外协议、源站协议、源站地址、源站端口和权重。 <ul style="list-style-type: none"> 对外协议：客户端请求访问服务器的协议类型。包括“HTTP”、“HTTPS”两种协议类型。 源站协议：Web应用防火墙转发客户端请求的协议类型。包括“HTTP”、“HTTPS”两种协议类型。 源站地址：客户端访问的网站服务器的公网IP地址（一般对应该域名在DNS服务商处配置的A记录）或者域名（一般对应该域名在DNS服务商处配置的CNAME）。 源站端口：WAF转发客户端请求到服务器的业务端口。 权重：负载均衡算法将按权重将请求分配给源站。 	对外协议：HTTP 源站协议：HTTP 源站地址：IPv4 XXX.XXX.1.1 源站端口：80
代理情况	在WAF前使用了其他代理产品。 此处选择“七层代理”。	七层代理

📖 说明

- 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。
- e. 单击“下一步”，根据界面提示，完成[放行回源IP](#)、[本地验证](#)的操作。
3. **复制WAF的CNAME：**在域名基本信息页面，单击CNAME所在行的，复制“CNAME”。
4. **在CDN侧添加加速域名（WAF的防护域名）**
- a. 登录[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。
 - **服务范围：**包含WAF的防护区域，例如WAF的“区域”为“华北-北京四”，“服务范围”可根据业务情况选择“中国大陆”或“全球”。
 - **加速域名：**www.example.com。
 - **业务类型：**网站加速。
 - **源站配置：**
 - **回源方式：**HTTP。
 - **源站类型：**源站域名。
 - **源站地址：**WAF的CNAME域名。
 - **回源HOST：**默认为加速域名。
 - d. 根据业务需求设置[突发带宽告警](#)和[用量封顶](#)功能，勾选[数据跨境合规承诺](#)。
 - e. 单击“确定”完成域名的添加，CDN会为加速域名生成专属CNAME。
5. （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](#)。
6. **配置CNAME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。配置以下信息：
 - “主机记录”：www。
 - “类型”：CNAME-将域名指向另外一个域名。
 - “别名”：选择“否”。
 - “线路类型”：全网默认。
 - “TTL(秒)”：一般建议设置为5分钟，TTL值越大，则DNS记录的同步和更新越慢。

- “值”：步骤4产生的CNAME。
 - 其他的设置保持不变。
- d. 单击“确定”，完成CNAME解析配置。

7. 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.huawei.com
Address:
非权威应答:
www.example.com canonical name = www.example.com.cdnhwcl.com
```

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。

5 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。

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桶域名”，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。

3. 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：
 - a. 对php、aspx、asp、jsp、do、dwr、cgi、fcgi、action、ashx、axd、json等动态文件不缓存。
 - b. 对以shtml、html、htm、js结尾的文件，建议缓存7天。
 - c. 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：
 - a. 对php、aspx、asp、jsp、do等动态文件不缓存。
 - b. 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：
 - a. 对php、aspx、asp、jsp、do等动态文件不缓存。
 - b. 对mww、html、htm、shtml、hml、gif、swf、png、bmp、js等缓存7天。
 - c. 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

1. 登录[CDN控制台](#)。
2. 在左侧菜单栏中，选择“域名管理”。
3. 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。
4. 选择“缓存配置”页签。
5. 在缓存规则模块，单击“编辑”，系统弹出“配置缓存策略”对话框。
6. 单击“添加”，根据业务需求配置缓存策略。

图 5-1 配置缓存策略

添加规则

- 1. 新规则仅对后续资源缓存生效，如希望对节点已缓存资源立即生效，请在修改缓存规则后对该部分资源执行刷新操作。[查看缓存配置策略](#)
- 2. 自定义CDN节点指定缓存资源的缓存过期时间规则。支持按照“首页”、“所有文件”、“目录路径”、“文件名后缀”、“全路径”方式指定资源范围。[了解更多](#)

基本配置

匹配类型

文件名后缀 目录路径 全路径 首页

匹配内容

如: .jpg;.zip;.exe

缓存过期时间来源 [?]

CDN

缓存过期时间 [?]

30

天

优先级 [?]

1-1,000整数, 1是最低优先级, 1

高级配置

取消

确定

表 5-1 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（全站加速默认缓存时间为0），此默认规则允许修改，不允许删除。
文件名后缀	<p>设置指定文件类型的缓存资源的缓存规则。</p> <p>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“源站IP”或“源站域名”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。</p>	<ul style="list-style-type: none"> 支持所有格式的文件类型。 输入首字符为“.”，以“;”进行分隔。 输入的文件后缀名总数不能超过100个。 字符总数不能超过1000。 文件名后缀英文字符支持大写和小写。 <p>示例： .JPG;.zip;.exe。</p> <p>说明 如果您的域名在后台有特殊配置，支持的文件后缀总数不能超过20，总字符数不能超过255。</p>

参数	说明	配置规则
目录路径	设置某一指定路径下的缓存资源的缓存规则。	<p>前缀匹配，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。示例： /test/folder01;/test/folder02。</p> <ul style="list-style-type: none"> 支持通配符匹配，使用通配符时要注意以下规则： <ul style="list-style-type: none"> 使用通配符匹配时每条规则只能配置一个*，且只能输入一个目录路径如： /test/*。 前缀匹配，如果配置路径为 /test/*，则/test/abc、 /test/abc/001都会遵循该条缓存规则。 后台有特殊配置的域名，不支持配置通配符*。 通配符*不能匹配“/”，如 /test*/abc不能匹配到 /test/folder01/folder02/abc。 通配符只能匹配一个或多个字符，例： /test*不能匹配到 /test。 不可配置/*。 支持配置连续多个“/”，且默认为不同路径，即：“/test”与“//test”代表不同路径。
全路径	设置完整路径下 某一文件 的缓存规则。	<p>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。示例： 如/test/index.html或/test/*.jpg。</p> <ul style="list-style-type: none"> 支持配置连续多个“/”，且默认为不同路径，即：“/test”与“//test”代表不同路径。
首页	设置根目录缓存规则	<p>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。</p> <ul style="list-style-type: none"> 只能配置一条“类型”为“首页”的缓存规则。

参数	说明	配置规则
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1~1000之间的整数，数值越大优先级越高。
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"> 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。 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。 对于动态文件（如php、jsp、asp、动态接口等），建议设置成0秒，回源获取。
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>配置原则：</p> <ul style="list-style-type: none"> URL参数变化，资源不变，可以配置忽略参数。 URL参数变化，资源变化，不可配置忽略参数。 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”。 	<ul style="list-style-type: none"> 不忽略参数：不忽略“？”之后的参数。 忽略参数：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。 忽略指定参数：CDN缓存时将忽略您在控制台配置的参数，保留其它参数。 保留指定参数：CDN缓存时将保留您在控制台配置的参数，忽略其它参数。
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"> 最多可填写30个参数名，多个参数之间用“;”分隔。 支持数字0-9、字符a-z、A-Z，及特殊符“.”、“_”、“~”。

参数	说明	配置规则
<p>缓存过期时间来源，即原缓存遵循源站配置。</p>	<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，或者取缓存规则配置的过期时间与源站的最小值，可以通过配置缓存过期时间来源实现。默认缓存过期时间来源为CDN，支持配置的取值如下：</p> <ul style="list-style-type: none"> ● 源站：CDN节点的缓存过期时间遵循源站的设置。 ● CDN：CDN节点的缓存过期时间遵循“缓存规则”中的“缓存过期时间”。 ● 源站和CDN的最小值：CDN节点的缓存过期时间取缓存规则和源站二者的最小值。 <p>说明</p> <ul style="list-style-type: none"> ● 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。 ● 如果“缓存过期时间来源”为“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。 	<p>缓存过期时间来源默认为CDN。</p>

参数	说明	配置规则
强制缓存	<p>强制缓存决定CDN节点缓存过期时间是否忽略源站响应头Cache-Control中的no-cache、private、no-store字段，开启代表忽略，关闭代表不忽略。强制缓存与缓存过期时间来源功能配合使用，配合使用规则如下：</p> <ol style="list-style-type: none"> 缓存过期时间来源配置为“源站”，强制缓存功能关闭。 <ul style="list-style-type: none"> 此时如果源站响应头Cache-Control设置了no-cache、private、no-store，CDN节点将不缓存资源。 如果源站设置了其他响应头，缓存优先级为s-maxage->max-age->expires。例如源站同时设置了Cache-Control: max-age=500, s-maxage=400，此时CDN节点的缓存过期时间遵循s-maxage的值400s。 如果源站没有设置以上响应头，执行CDN控制台配置的缓存过期时间。 缓存过期时间来源配置为“源站”，强制缓存功能开启。 <ul style="list-style-type: none"> 如果源站响应头设置了缓存过期时间，缓存优先级为s-maxage->max-age->expires。例如源站同时设置了Cache-Control: max-age=500, s-maxage=400，此时CDN节点的缓存过期时间遵循s-maxage的值400s。 如果源站没有设置以上响应头，执行CDN控制 	默认开启强制缓存功能。

参数	说明	配置规则
	<p>台配置的缓存过期时间。</p> <p>3. 缓存过期时间来源配置为“CDN”，强制缓存功能开启。</p> <ul style="list-style-type: none"> • 此时忽略源站响应头，执行CDN控制台配置的缓存过期时间。 <p>4. 缓存过期时间来源配置为“CDN”，强制缓存功能关闭。</p> <ol style="list-style-type: none"> a. 如果源站响应头Cache-Control设置了no-cache、private、no-store，CDN节点将不缓存资源。 b. 如果源站响应头Cache-Control未设置no-cache、private、no-store，执行CDN控制台配置的缓存过期时间。 <p>5. 缓存过期时间来源配置为“源站和CDN的最小值”，强制缓存功能关闭。</p> <ul style="list-style-type: none"> • 如果最小值为CDN节点设置的缓存过期时间，则与6.d规则一致。 • 如果最小值为源站设置的缓存时间，则与6.a一致。 <p>6. 缓存过期时间来源配置为“源站和CDN的最小值”，强制缓存功能开启。</p> <ul style="list-style-type: none"> • 如果最小值为CDN节点设置的缓存过期时间，则与6.c规则一致。 • 如果最小值为源站设置的缓存时间，则与6.b一致。 	

参数	说明	配置规则
SWR开关	如果您的源站的Cache-Control头部设置了stale-while-revalidate=***（***为时间），可以在CDN侧开启SWR开关，当CDN节点缓存的资源过期后，如果客户端请求该资源时过期时间没有超过stale-while-revalidate设置的时间，浏览器仍然返回已缓存的资源，同时cdn节点会回源请求最新的资源并缓存，用户再次请求时就会得到最新的资源。	-

- （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：某客户的域名“www.example.com”配置了CDN加速，缓存规则配置见下图。

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

配置结果：网站首页不缓存，所有页面均不会忽略URL参数。

配置场景2：设置某个类型的文件不缓存

- 某客户的域名“www.example.com”配置了CDN加速，由于业务需求，需要对“.do”格式的文件不缓存，同时所有文件都忽略URL参数。

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。

6 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

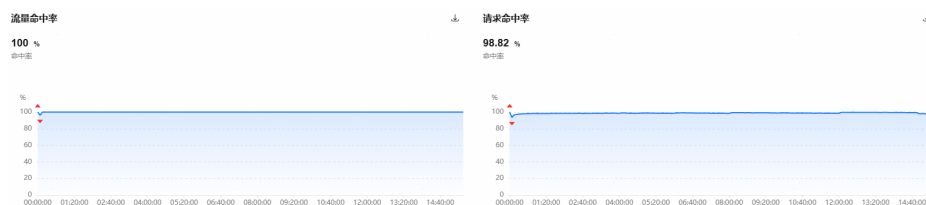
流量命中率越低，回源流量越大，源站的流出流量越大，源站带宽资源占用越大，其代表了源站服务器收到的负载压力，请重点关注流量命中率。

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[CDN控制台](#)。
2. 在左侧菜单栏中，选择“业务监控 > 命中率统计”。
3. 在命中率统计页面即可查看“流量命中率”和“请求命中率”。

图 6-1 命中率统计



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，“缓存过期时间来源”设置为“源站”、“强制缓存”功能关闭，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[配置资源在CDN节点的缓存规则](#)。

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。

7 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 7-1 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：**首页回源。
 - a. 请登录CDN控制台，在左侧菜单栏中，选择“域名管理”。
 - b. 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。
 - c. 选择“缓存配置”页签。
 - d. 在缓存规则模块，单击“编辑”，系统弹出“配置缓存策略”对话框。
 - e. 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。

- f. 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。
- g. 单击“确定”，完成回源URL改写配置。
- h. 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。

8 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" x.x.x.x
```

各字段从左到右含义如表8-1所示。

表 8-1 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"> • bytes=x-y: 表示请求第x个字节到第y个字节的数据内容。 • bytes=-y: 表示请求最后y个字节的数据内容。 • bytes=x-: 表示请求第x字节到最后一个字节的数据内容。 	bytes=-256
14	服务端IP: CDN服务端响应IP。	x.x.x.x

操作步骤

1. 登录[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，将日志解压。如果想要分析多个日志文件，可以在Windows系统下合并多个日志文件。

```
copy *.com-cn hebing.txt
```
6. 将日志上传至本地Linux系统服务器。
 - **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。
统计访问排名前100的URL

```
awk '{print $9}' hebing.txt | sort -n | uniq -c | sort -nr | head -n 100
```
 - **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。
列出访问前100的IP地址

```
awk '{print $3}' hebing.txt | sort -n | uniq -c | sort -nr | head -n 100
```

📖 说明

`awk '{print $3}'`: 提取日志文件的第三列（列之间使用空格隔开），即访问IP地址。
`hebing.txt`: 合并后的日志文件名称，如果使用单个日志文件，使用日志名称替换即可。

`sort -n`: IP地址排序。

`sort -nr`: 按降序排列。

`uniq -c`: 统计每个IP地址出现的次数。

`head -n 100`: 提取排名在前100的访问IP。

- **分析User-Agent信息**: 通过UA请求头看是否存在不常见和空的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。

提取日志中的访问量排名前10位的User-Agent信息

```
grep -o 'Mozilla[^\"]*' hebing.txt | sort -n | uniq -c | sort -nr | head -n 10
```

排除常见的User-Agent的User-Agent信息

```
grep -o 'Mozilla[^\"]*' hebing.txt|grep -v -E "Firefox|Chrome|Safari|Edge"
```

统计空User-Agent的行数，即访问次数

```
awk '!/Mozilla/' hebing.txt | wc -l
```

📖 说明

`grep -o`: 只输出匹配的内容。

`grep -v -E`: 排除符合条件的字符。

`wc -l`: 统计数量。

- **状态码分析**: 可以通过分析日志中异常状态码来识别恶意访问。如果某IP有大量异常访问状态码（4xx或5xx），说明可能在进行攻击。

筛选排名前10的状态码

```
awk '{print $10}' hebing.txt | sort -n | uniq -c | sort -nr | head -n 10
```

- 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。

9 防范恶意流量盗刷

域名被恶意攻击或盗刷流量时，会产生高于日常消费金额的账单，并且该账单无法免除或退款，本文为您介绍如何配置相关防护和提醒功能，以减少突发高带宽带来的风险。

发生盗刷后及时止损

如果您的域名已经被恶意攻击或盗刷流量，您可以配置用量封顶和请求限速，防止损失进一步扩大，然后分析攻击行为，配置相关防护策略。

1. **配置用量封顶**：配置域名最大使用带宽/流量，当用量达到配置的阈值时，CDN将停用域名，有效预防流量盗刷或恶意攻击带来的高额账单。详细配置请参考[用量封顶](#)。

图 9-1 添加用量封顶

添加用量封顶

① 1. 由于统计数据存在一定的时延，当实际用量达到阈值后10分钟左右才会停用域名，域名停用前产生的流量、带宽、请求数等资源消耗将正常计费。 ×

2. 瞬时用量采用5分钟粒度，统计域名5分钟内的用量。

3. 累积用量（小时）按照整点（如00:00:00~00:59:59）、累积用量（天）按照UTC+8时间的整天（00:00:00~23:59:59）统计域名所用的流量，每个统计周期开始时数据清零，重新统计用量。

统计类型

瞬时用量(五分钟粒度) 累积用量(小时) 累积用量(天)

封顶配置

带宽封顶 Mbit/s

您当前账号的带宽进制为：1,000，流量进制为：1,024

告警阈值

开启

当 访问带宽/带宽阈值 的比值达到配置的告警阈值时（10% - 90%），CDN将发出告警消息

解封周期

2. **配置请求限速**：配置用户请求限速，对用户访问到CDN节点的请求进行下行速率限速，控制总请求带宽，一定程度上减少突发高带宽风险。详细配置请参考[请求限速](#)。

图 9-2 请求限速配置



分析攻击行为

域名被攻击后，可以通过以下步骤分析攻击时间和攻击者的信息，以便加固安全防护配置。

1. **确定攻击时间范围**：通过查看账单分析攻击的具体时间，根据需要选择统计周期和维度，分析高额账单发生时段，账单导出方式详见[费用账单](#)。
2. **分析离线日志**：通过查看对应时段的离线访问日志，分析HTTP请求信息，识别异常IP地址、防盗链等信息，以便针对性设置防护规则。详细信息请参考[通过日志分析恶意访问地址](#)。
3. **查看运营报表**：CDN支持定制热门URL、热门Referer、热门UA和热门客户端IP等报表，如果在发生攻击前被攻击的域名已经定制了运营报表，可以下载攻击时段的报表分析相关信息，详见[运营报表](#)。

⚠ 注意

运营报表需要提前配置，如果因攻击产生高额账单时未配置这项功能，只能通过离线日志分析历史数据。

解决问题

1. 通过对攻击行为的分析，可提取相应的攻击IP/Referer/UA，CDN提供的基础访问控制功能可以实现相应的防护。
 - 配置[防盗链](#)拒绝带有恶意Referer请求：攻击者会伪造请求头中的Referer字段，试图假冒合法引用来源。可以配置Referer黑白名单，允许合法的Referer请求，拒绝未经授权的第三方网站链接到资源。

编辑防盗链

状态

* 类型 referer黑名单 referer白名单

包含空referer

* 规则

请输入域名或IP地址，以“;”进行分割，域名、IP地址可混合输入，支持添加泛域名和带端口的域名。输入的域名、IP地址总数不能超过500个，端口最大值为65535。如：www.example.com:443;*.test.com;192.168.0.0

取消

确定

- 配置**IP黑名单**限制恶意IP访问：筛选出恶意IP地址，将这些IP地址列入黑名单。

编辑IP黑白名单

- 1. 支持配置IP地址和IP&掩码格式的网段，最多支持配置500个，一行一个。
- 2. 网段“IP/掩码”中的IP必须是该网段IP区间首个主机IP地址。
- 3. 多个完全重复的IP/IP段将合并为一个。
- 4. 不支持带通配符的地址，如192.168.0.*。
- 5. 支持IPv6。

状态

* 类型 IP黑名单 IP白名单

* 规则

192.168.0.1
192.168.0.11

取消

确定

- 配置**UA黑名单**过滤可疑User-Agent：攻击者会伪造User-Agent字段发送大量请求，试图绕过安全检查，可能包含空值或随机字段。可以通过配置相关UA黑白名单，限制空UA访问。

编辑User-Agent黑白名单

状态

* 类型 黑名单 白名单

User-Agent黑名单与白名单二选一，不可同时配置。

包含空User-Agent ?

* 规则

仅支持通配符*实现正则匹配，无*时均为完全匹配；最多配置200条规则，每行一条规则。

取消

确定

2. 开通**边缘安全防护**：开通**边缘安全服务**，边缘安全（Edge Security, EdgeSec）是华为云基于CDN边缘节点提供的安全防护服务，包括：边缘DDoS防护、CC防护、WAF防护、BOT行为分析等功能，可根据业务情况配置相关安全规则，实现加速域名的全方位防护。

后续防护

配置CES监控：开启CES监控上报功能，将重要指标上报并设置告警，监控指标数据超过告警阈值时，会发出告警，方便您实时了解业务情况，及时规避风险。详细配置流程请参考[CES监控上报](#)。

📖 说明

CES监控功能CDN侧不收费，如果您在CES侧设置了告警，发送告警通知时消息通知服务（SMN）会收取相应的费用，SMN服务的价格详见[这里](#)。

配置IP访问限频：配置**IP访问限频**功能，通过限制单IP的单URL每秒访问单个节点的次数（QPS），实现CC攻击防御及恶意盗刷防护，降低高额账单风险。

配置突发带宽告警：配置**突发带宽告警**，当客户端请求带宽达到配置的阈值时发出告警信息，方便及时发现异常攻击，有效预防流量盗刷或恶意攻击带来的高额账单。

10 CDN 联动 GA 实现跨境访问加速

前提条件

- 已经按照[使用限制](#)准备好需要接入的域名。
- 已[开通CDN服务](#)。

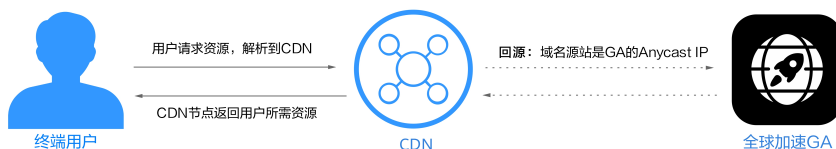
应用场景

使用CDN加速域名访问时，如果选择的服务范围与源站的位置在不同的国家，客户端访问节点无缓存的资源时，CDN节点回源受跨境网络影响，加速效果不太明显，甚至回源失败。例如：域名的服务范围为中国大陆境外，源站在中国大陆，此时所有客户端请求均会调度到中国大陆境外的节点，节点回源时就可能会受到跨境网络影响，导致加速效果不明显或访问失败。

因此，当您的跨国业务需要CDN加速时，可以联动华为云全球加速（Global Accelerator，GA）服务，依托GA服务的跨境访问能力，解决CDN跨境回源的相关痛点，实现动静态内容全面加速。

方案概述

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（GA）请求资源，由GA服务实现跨境访问并返回资源给CDN节点，CDN节点将资源返回给用户并缓存。



资源成本与规划

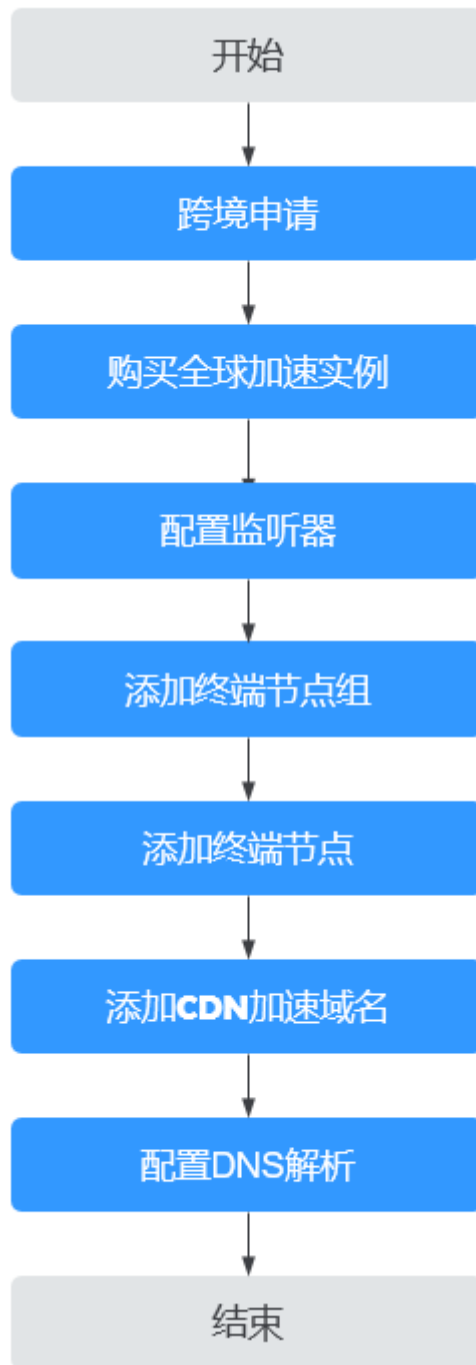
本实践以加速域名为www.example.com，源站在中国大陆（IP地址：192.168.1.1），CDN加速域名的“服务范围”为“中国大陆境外”为前提。

本节介绍最佳实践中资源规划情况，包含以下内容：

表 10-1 CDN 联动 GA 实现跨境访问加速的资源成本与规划

资源	资源说明	数量	费用
GA加速实例	按照每个全球加速实例的创建时长收费。 <ul style="list-style-type: none"> 按小时计费，创建时长不满1小时按1小时收费。 实例费=实例单价*创建时长 	1	请参见 全球加速价格详情 。
GA数据传输	通过全球加速服务转发的流量费用，按GB收费。 <ul style="list-style-type: none"> 从一个全球加速接入点到一个应用部署区域之间的流量，定义流量大的方向为主方向，按照每条流量的主方向收费。 数据传输费=流量单价*使用量 	根据实际转发的流量	
公网解析记录	线路类型选择“全网默认”，解析记录值配置为CDN服务的CNAME地址。	1	免费
CDN加速域名	服务范围： 中国大陆境外 源站类型： 源站IP 源站地址： 全球加速实例分配的加速IP地址，即Anycast IP。	1	请参见 内容分发网络价格详情 。

流程简介



步骤一：跨境申请

根据中华人民共和国工业和信息化部（简称工信部）相关法律、行政法规规定，中国大陆只有三大运营商具备跨境业务运营资质。所以涉及跨中国大陆访问的业务场景，都需要通过跨境资质审核。

1. 进入[全球加速跨境申请管理](#)界面。
2. 在跨境申请管理页面，单击“跨境申请”。
进入中国联通跨境云服务在线申请页面。

图 10-1 跨境申请



3. 在跨境云服务在线申请页面，根据提示配置相关参数，并上传相关材料。
4. 单击“立即申请”。

步骤二：购买全球加速实例

跨境资质申请完成后，购买全球加速实例。

1. 登录[全球加速控制台](#)。
2. 在全球加速页面，单击“购买全球加速服务”。

图 10-2 购买全球加速实例



3. 根据界面提示配置相关参数，“加速区域”选择“中国大陆以外”，详细请参见[表10-2](#)。

图 10-3 创建全球实例

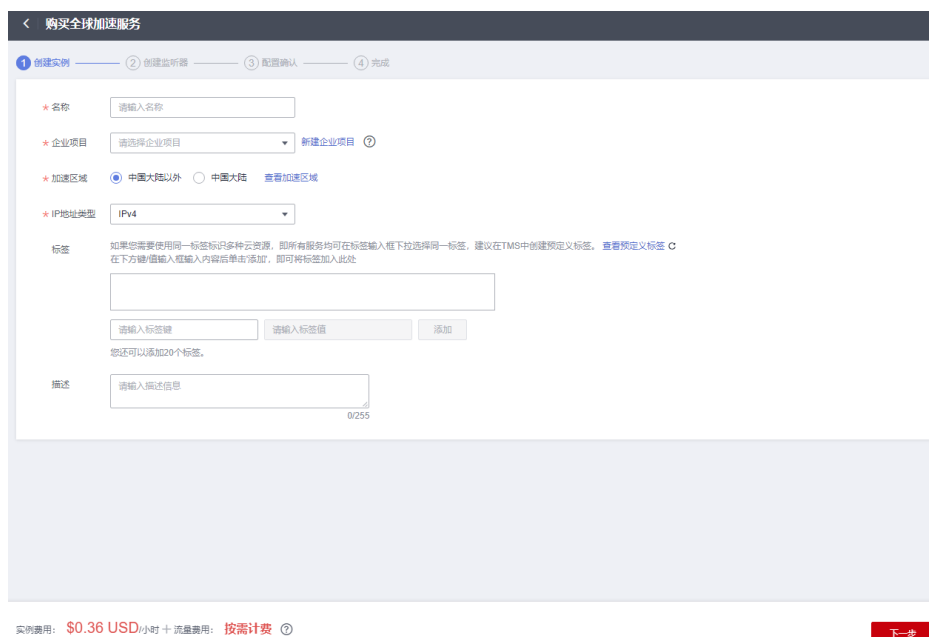


表 10-2 创建全球加速实例

参数	说明
名称	用户将要创建的全球加速实例的名称。 只能由中文、英文字母、数字、中划线组成。 长度范围：1-64个字符。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 您可以使用已有企业项目，也可以新建企业项目。
加速区域	加速区域指需要进行访问加速的区域。 支持选择“中国大陆以外”或“中国大陆”，默认选择“中国大陆以外”。 本实践中请选择“中国大陆以外”。
IP地址类型	全球加速实例的地址类型。 “加速区域”选择“中国大陆”时，支持选择“IPv4”或“IPv4+IPv6”。 默认：IPv4。
标签	全球加速的标识，包括键和值。可以为全球加速实例创建20个标签。 说明 如果已经通过TMS的预定义标签功能预先创建了标签，则可以直接选择对应的标签键和值。 预定义标签的详细内容，请参见 预定义标签简介 。 如您的组织已经设定全球加速服务的相关标签策略，则需按照标签策略规则为加速实例添加标签。标签如果不符合标签策略的规则，则可能会导致加速实例创建失败，请联系组织管理员了解标签策略详情。
描述	全球加速实例描述。 长度范围：不超过255个字符。

4. 单击“下一步”，进入监听器配置页面。

步骤三：配置监听器

创建全球加速实例后，您需要为全球加速实例配置监听器。监听器负责监听连接请求，并根据流量转发策略将请求流量分发至终端节点。

根据界面提示配置监听器的相关参数，详细请参见[表10-3](#)。

图 10-4 添加监听器



表 10-3 添加监听器

参数	说明
名称	监听器名称。 只能由中文、英文字母、数字、中划线组成。 长度范围：1-64个字符。
前端协议	客户端与监听器建立流量分发连接的协议。 取值范围：TCP、UDP。
前端端口	客户端与监听器建立流量分发连接的端口。 端口取值在1-65535之间，端口范围用“-”连接， 多个端口或端口范围以逗号隔开。 例如：1-10, 11-50, 51, 52-200
客户端亲和性	会话保持。 支持选择“关闭”或“按源IP保持会话”。 TCP和UDP协议仅支持“按源IP保持会话”。 按源IP保持会话：基于源IP地址的简单会话保持， 将请求的源IP地址作为散列键（HashKey），从静态分配的散列表中找出对应的服务器。即来自同一IP地址的访问请求会被转发到同一台后端服务器上进行处理。

参数	说明
标签	<p>监听器的标识，包括键和值。可以为监听器创建20个标签。</p> <p>说明 如果已经通过TMS的预定义标签功能预先创建了标签，则可以直接选择对应的标签键和值。 预定义标签的详细内容，请参见预定义标签简介。 如果您的组织已经设定全球加速服务的相关标签策略，则需按照标签策略规则为监听器添加标签。标签不符合标签策略的规则，则可能会导致监听器创建失败，请联系组织管理员了解标签策略详情。</p>
描述	<p>监听器描述。 长度范围：不超过255个字符。</p>

步骤四：配置终端节点组和终端节点

根据界面提示配置终端节点组和终端节点的相关参数，**终端节点组区域选择“上海一”**，详细请参见[表10-4](#)。

表 10-4 添加终端节点组和终端节点

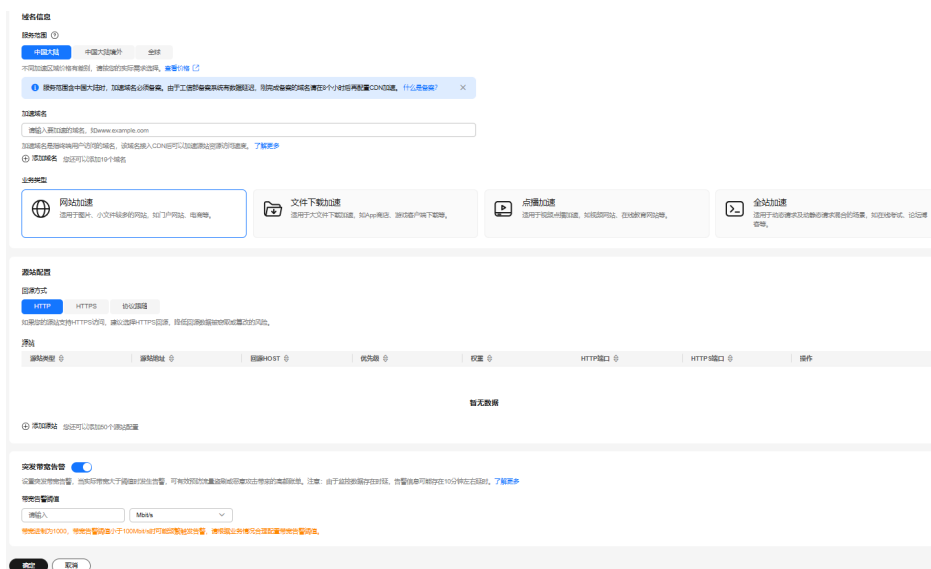
类型	参数	说明
终端节点组	名称	<p>终端节点组名称。</p> <ul style="list-style-type: none"> 每个监听器下每个区域只允许关联一个终端节点组。 只能由中文、英文字母、数字、中划线组成。 长度范围：1-64个字符。
	区域	终端节点组所属区域。 本实践选择“上海一”
	描述	<p>终端节点组描述。 长度范围：不超过255个字符。</p>
	流量调度	<p>配置到不同终端节点组的流量比例。 如果增加流量调度比例，将有更多的请求分发到此终端节点组。 如果将流量调度比例设置为0，则不会将任何请求分发到此终端节点组。 取值范围为：[0-100]。</p> <p>说明 如果监听器中有多个终端节点组，分配流量时优先选择时延最低的终端节点组，并按照该终端节点组的流量调度值分配流量，然后再向其他终端节点组分配其余流量。</p>

类型	参数	说明
	终端节点	终端节点充当客户端的接触点，加速实例跨正常运行的终端节点分发传入流量。 本实践填入实际的源站地址（192.168.1.1）。
健康检查配置	是否开启	开启或者关闭健康检查。 关闭健康检查可能会导致业务请求转发至异常的后端服务器。
	前端协议	健康检查目前支持选择TCP协议或UDP协议。 默认：TCP协议。
	前端端口	健康检查端口号。 取值范围：[1, 65535]。
	高级配置	
	检查间隔 (秒)	每次健康检查响应的最大间隔时间。 取值范围：[1-60]。
	超时时间 (秒)	每次健康检查响应的最大超时时间。 取值范围：[1-60]。
	最大重复次数	健康检查最大的重试次数。 取值范围：[1-10]。

步骤五：添加 CDN 加速域名

1. 登录[CDN控制台](#)。
2. 在左侧导航栏选择“域名管理”，进入域名管理页面。
3. 在域名管理界面，单击“添加域名”，配置相关参数。
 - 加速域名：www.example.com。
 - 服务范围：中国大陆境外。
 - 业务类型：网站加速。
 - 源站配置：
 - 回源方式：HTTP。
 - 源站类型：源站IP。
 - 源站地址：全球加速Anycast IP。
 - 回源端口：与[步骤三：配置监听器](#)中的前端端口保持一致。
 - 回源HOST：默认为加速域名。

图 10-5 添加域名



详细参数解释请参见[添加CDN加速域名](#)。

步骤六：配置 DNS 解析

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。

本文以配置华为云DNS解析为例，请按照以下步骤操作：

1. 进入[公网域名列表页面](#)。
2. 在“公网域名”页面的域名列表的“域名”列，单击域名的名称。进入“解析记录”页面。
3. 在页面右上角，单击“添加记录集”。
4. 在“添加记录集”页面，根据界面提示为域名添加CNAME记录，下表中未提到的参数可保持默认值。

表 10-5 记录集参数说明

参数	参数说明	本实践取值
主机记录	<p>解析域名的前缀。</p> <p>例如创建的域名为“example.com”，其“主机记录”设置包括：</p> <ul style="list-style-type: none"> • www：用于网站解析，表示解析的域名为“www.example.com”。 • 空：用于网站解析，表示解析的域名为“example.com”。主机记录置为空，还可用于为空头域名“@”添加解析。 • *：用于泛解析，表示解析的域名为“*.example.com”，匹配“example.com”的所有子域名。 	WWW
类型	记录集的类型。	CNAME-将域名指向另外一个域名
线路类型	解析的线路类型用于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。	全网默认
TTL(秒)	<p>解析记录在本地DNS服务器的缓存时间，以秒为单位。</p> <p>默认值：300秒</p> <p>取值范围为：1~2147483647</p> <p>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。</p> <p>本实践中该参数保持默认配置。</p>	5分钟，即300s
值	需指向的域名。	CDN分配的CNAME域名

5. 单击“确定”。

6. **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“www.example.com”。如果回显CDN分配的CNAME域名，则表示CNAME配置已经生效。

配置验证

在本实践中，在海外国家/地域使用windows电脑测试访问上海一加速效果，具体如下：

在加速地域电脑上执行curl命令查看数据丢包时延情况

```
curl -o /dev/null -s -w "time_connect: %{time_connect}\ntime_starttransfer: %{time_starttransfer}\ntime_total: %{time_total}\n" "http[s]://<应用服务域名>[:<端口>]"
```

说明

- 端口：应用对外发布服务的端口号。
- time_connect：连接时间。从开始建立TCP到连接完成所用的时间，单位为秒。
- time_starttransfer：开始传输时间。从客户端发出请求到后端服务器响应第一个字节所用的时间，单位为秒。
- time_total：连接总时间。从客户端发出请求到后端服务器响应会话所用的时间，单位为秒。

11 使用规则引擎功能限制客户端恶意请求

场景介绍

网站www.example.com遇到恶意用户上传伪装图片格式的html引流文件，导致请求被引流到非法网站。可以通过CDN服务的规则引擎功能，规避风险。

方案概述

客户源站为OBS桶，对象元数据中“Content-Type”头配置为“text/html”，允许用户请求html格式文件。

本方案使用CDN的规则引擎功能，当客户端请求图片格式的文件时，通过改写回源请求头和HTTP响应头，限制客户只能打开图片格式的文件，从而避免跳转到其他非法网站。

资源与成本规划

本实践所需资源请见下表。

资源	资源说明	每月费用
内容分发网络 CDN	流量 ：用户访问CDN节点产生的流量，可购买流量包抵扣。	具体的计费方式及标准请参考 计费说明 。
对象存储服务 OBS	流量 ：CDN回源OBS时会产生公网流出费用，按需计费，版本为3.0以上的桶且以“OBS桶域名”形式接入CDN可购买回源流量包抵扣。	具体的计费方式及标准请参考OBS 计费说明 。

实施步骤

1. 登录[CDN控制台](#)。
2. 在左侧菜单栏中，选择“域名管理”。
3. 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。
4. 选择“规则引擎”页签，单击“创建规则”，进入配置界面。

5. 根据业务场景，配置如下图参数即可。

图 11-1 规则引擎配置

The screenshot displays the configuration interface for a rule engine. It is divided into several sections:

- 规则名称 (Rule Name):** A text input field containing "规则01".
- 优先级 (Priority):** A text input field containing "1". Below it, a note states: "优先级取值范围为1-1,000, 数值越大优先级越高。" (Priority value range is 1-1,000, the larger the value, the higher the priority.)
- 触发条件 (Trigger Conditions):** A section for defining conditions. It includes a table with columns for "条件" (Condition), "运算符" (Operator), and "值" (Value).

条件	运算符	值
文件后缀	包含任意一个	jpg × png × .svg × .gif × jpeg ×

Below the table are options to "添加条件" (Add condition) and a "区分大小写" (Case sensitive) toggle switch.
- 执行操作 (Execution Actions):** A section for defining actions. It includes a "编辑操作" (Edit action) button and two sub-sections:
 - 回源请求头 (Origin Request Header):** A section for modifying the header of the user's request to the origin. It includes a "了解更多信息" (Learn more) link and a table with columns for "请求头操作" (Header operation), "请求头名称" (Header name), and "请求头取值" (Header value).

请求头操作	请求头名称	请求头取值
设置	Content-Type	image/jpg

A "+ 添加" (Add) button and a note "您还可以添加9条规则。" (You can also add 9 rules.) are present.
 - HTTP header响应头 (HTTP header Response Header):** A section for customizing the response header value. It includes a "了解更多信息" (Learn more) link and a table with columns for "响应头操作" (Header operation), "响应头名称" (Header name), and "响应头取值" (Header value).

响应头操作	响应头名称	响应头取值
设置	Content-Type	image/jpg