

CDN

产品介绍

文档版本 19
发布日期 2024-12-23



版权所有 © 华为技术有限公司 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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

目录

1 什么是华为云 CDN	1
2 工作原理	3
3 节点分布	5
4 产品优势	7
5 应用场景	8
6 性能指标	12
7 基本概念	15
8 约束与限制	17
9 安全	22
9.1 责任共担.....	22
9.2 数据保护技术.....	23
9.3 审计与日志.....	23
9.4 监控安全风险.....	24
10 CDN 权限管理	25
11 与其他云服务的关系	30

1 什么是华为云 CDN

CDN (Content Delivery Network, 内容分发网络) 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。CDN 服务缩短了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。

华为云 CDN 将源站资源缓存到遍布全球的加速节点上, 当终端用户访问资源时, 无需回源, CDN 通过一组预先定义好的策略 (如内容类型、地理区域、网络负载状况等), 将当时能够最快响应用户的 CDN 节点 IP 地址提供给用户, 使用户可以以最快的速度获得网站内容。接入华为云 CDN 的方法, 请参考[快速入门](#)。

华为云 CDN 加速节点资源丰富, 有 2000+ 中国大陆加速节点, 800+ 中国大陆境外加速节点。有充足的带宽资源, 全网带宽输出能力高达 180Tbps。涵盖了电信、联通、移动、教育网等主流运营商, 以及多家中小型运营商。覆盖 130 多个国家/地区, 支持运营商网络超过 1,600 家。保证将用户请求精准调度至最优边缘节点, 提供有效且稳定的加速效果。

CDN 使用

快速了解 CDN 产品, 帮您更好的使用 CDN 产品提供的功能。

参考文档	CDN 使用
CDN 基本概念	快速了解 CDN 的常用概念, 帮助理解和使用 CDN
CDN 成长地图	快速了解和使用 CDN
CDN API	快速了解通过调用 API 来实现对应的控制台操作
入门概述	快速了解如何接入 CDN 加速
域名管理	快速了解 CDN 的域名管理功能
域名配置	快速了解 CDN 的相关配置
缓存刷新和缓存预热	快速了解 CDN 的刷新预热功能

CDN 定价

当您开通CDN时，可以选择基础计费方式：流量计费或者带宽计费，具体计费标准请参见[价格计算器](#)。

流量计费

- 您可以选择通过按量计费，即按照每小时实际使用的流量进行计费。
- 您也可以购买价格更优惠的CDN流量包进行抵扣，购买流量包成功后，系统会一次性按照购买价格对账户余额进行扣费。

带宽计费

峰值带宽计费采用按量计费方式，即按照每日峰值带宽进行计费，带宽计费包含峰值带宽计费、月结95带宽峰值计费、日峰值月平均计费。

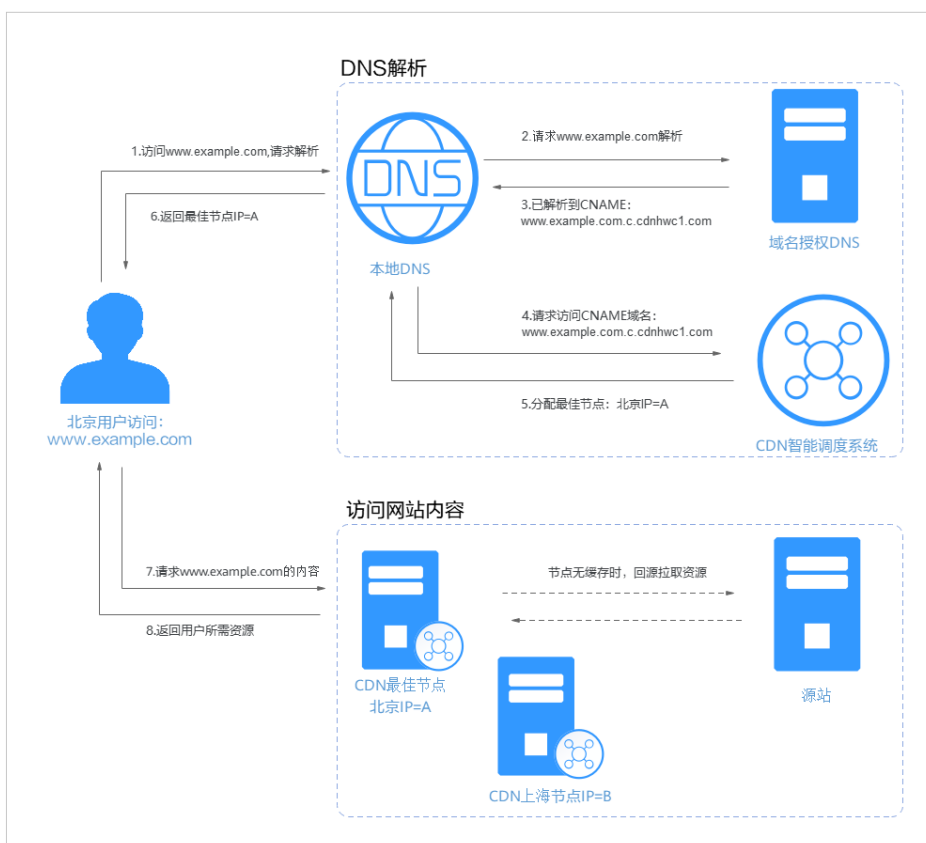
说明

月结95带宽峰值、日峰值月平均计费方式仅支持CDN月消费金额大于10万或预期超过10万的用户，并且需要[提交工单](#)或拨打客服电话进行申请。

有关CDN计费的详细描述，请参考[计费项](#)。

2 工作原理

当用户访问使用CDN服务的网站时，本地DNS服务器通过CNAME方式将最终域名请求重定向到CDN服务。CDN通过一组预先定义好的策略（如内容类型、地理区域、网络负载状况等），将当时能够最快响应用户的CDN节点IP地址提供给用户，使用户可以以最快的速度获得网站内容。使用CDN后的HTTP请求处理流程如下。



HTTP请求流程说明:

1. 用户在浏览器输入要访问的网站域名www.example.com，向本地DNS发起域名解析请求。
2. 本地DNS检查缓存中是否有www.example.com的IP地址记录。如果有，则直接返回给终端用户；如果没有，则向网站授权DNS查询。

3. 网站DNS服务器解析发现域名已经解析到了CNAME：
www.example.com.cdnhwc1.com。
4. 请求被指向CDN服务。
5. CDN对域名进行智能解析，将响应速度最快的CDN节点IP地址返回给本地DNS。
6. 用户获取响应速度最快的CDN节点IP地址。
7. 浏览器在得到最佳节点的IP地址以后，向CDN节点发出访问请求。
 - 如果该IP地址对应的节点已缓存该资源，节点将数据直接返回给用户，如图中步骤7和8，请求结束。
 - 如果该IP地址对应的节点未缓存该资源，节点回源请求资源。获取资源后，结合用户自定义配置的缓存策略，将资源缓存至节点，如图中的北京节点，并返回给用户，请求结束。配置缓存策略的操作方法，请参见[缓存配置](#)。

3 节点分布

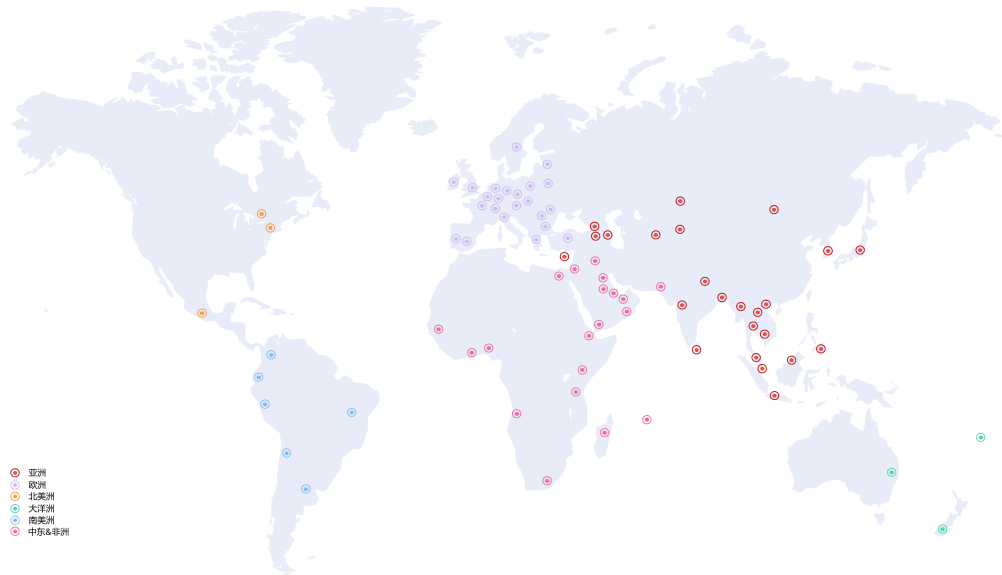
华为云CDN在中国大陆境内有2000+加速节点，覆盖所有省份、自治区、直辖市，在中国大陆境外有800+加速节点，全网带宽输出能力高达180Tbps。涵盖了电信、联通、移动、教育网等主流运营商，以及多家中小型运营商。保证将用户请求精准调度至最优边缘节点，提供了有效且稳定的加速效果。

中国大陆节点分布



大区	节点分布
华北	北京, 天津, 山西, 河北, 内蒙古自治区
华东	上海, 江苏, 浙江, 安徽, 江西, 山东, 福建
华中	河南, 湖北, 湖南
华南	广东, 海南, 广西壮族自治区
西北	陕西, 甘肃, 青海, 宁夏回族自治区, 新疆维吾尔自治区
西南	重庆, 四川, 贵州, 云南, 西藏自治区
东北	黑龙江, 吉林, 辽宁

中国大陆外节点分布



大区	节点分布（以华为内部业务划分区域）
亚洲	中国香港、中国澳门、中国台湾、日本、韩国、越南、印度、印尼、泰国、菲律宾、新加坡、马来西亚、柬埔寨、老挝、吉尔吉斯斯坦、文莱、缅甸、尼泊尔、孟加拉、蒙古、斯里兰卡、哈萨克斯坦、格鲁吉亚、亚美尼亚、乌兹别克斯坦、塞浦路斯、阿塞拜疆
欧洲	英国、德国、法国、荷兰、西班牙、意大利、爱尔兰、瑞典、比利时、奥地利、波兰、罗马尼亚、白俄罗斯、葡萄牙、土耳其、摩尔多瓦、保加利亚、拉脱维亚、瑞士、捷克、匈牙利、卢森堡、希腊、克罗地亚、塞尔维亚、芬兰
中东&非洲	阿联酋、沙特、巴基斯坦、卡塔尔、阿曼、科威特、巴林、伊拉克、南非、埃及、肯尼亚、坦桑尼亚、马达加斯加、吉布提、毛里求斯、加纳、安哥拉、尼日利亚、约旦、也门、以色列、塞内加尔
北美洲	美国、加拿大、墨西哥
大洋洲	澳大利亚、新西兰、斐济
南美洲	巴西、智利、阿根廷、秘鲁、哥伦比亚、厄瓜多尔

4 产品优势

全球稳定加速

2800+ 全球节点，180Tbps+带宽能力，覆盖六大洲，支持主流运营商，为各类型业务保驾护航，提供高速、稳定的业务访问体验。

精准调度

全球精准IP库，并具备自我进化能力，全网链路质量大数据实时分析、预测，为用户精准调度最优节点，保障访问质量。

简单易用

接入方式简捷，控制台自助配置丰富且易操作，API接口开放，便于企业应用集成、跨云平台管理。

高性能缓存

独创AI-Cache技术+多级缓存调度，实时跟踪全局热度，超高速、大容量SSD存储，有效提升缓存命中率、减少用户访问等待时间。

合规认证

华为云具备AAA级CDN企业信用评估、IPv6认证、可信云等认证，为加速提供保障。

安全防护

华为云CDN为客户提供安全、可靠的内容分发服务，支持全网HTTPS安全传输、防盗链、URL鉴权、IP黑白名单等高级安全功能。

精细化用量管理

多维度监控告警能力，包括访问情况统计、使用量统计、套餐剩余量预警、离线日志等功能，方便您精细化了解业务运行情况。

5 应用场景

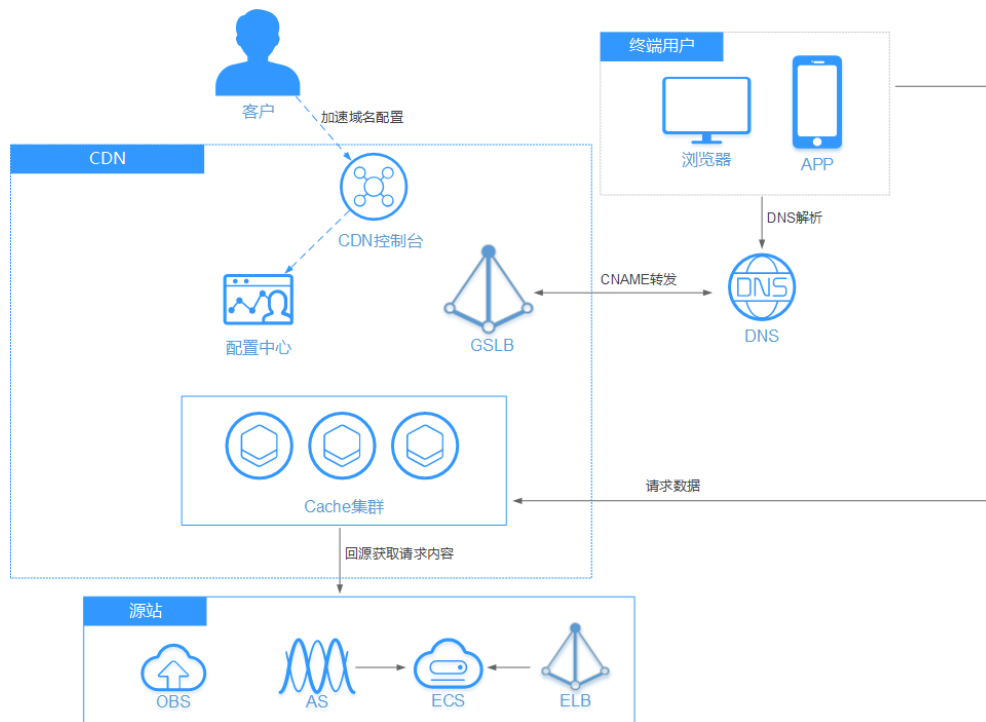
场景概述

华为云CDN为您提供4种业务类型，分别对应不同的应用场景：

业务类型	应用场景
网站加速	适用于有加速需求的网站，对网站中图片、小文件等 静态资源 提供加速服务，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。
文件下载加速	适用于使用HTTP/HTTPS文件下载业务的网站、下载工具、游戏客户端、APP商店等。
点播加速	适用于提供音视频点播服务的客户，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。
全站加速	适用于各行业动静态内容混合，含较多 动态资源 请求（如asp、jsp、php等格式的文件）的网站。

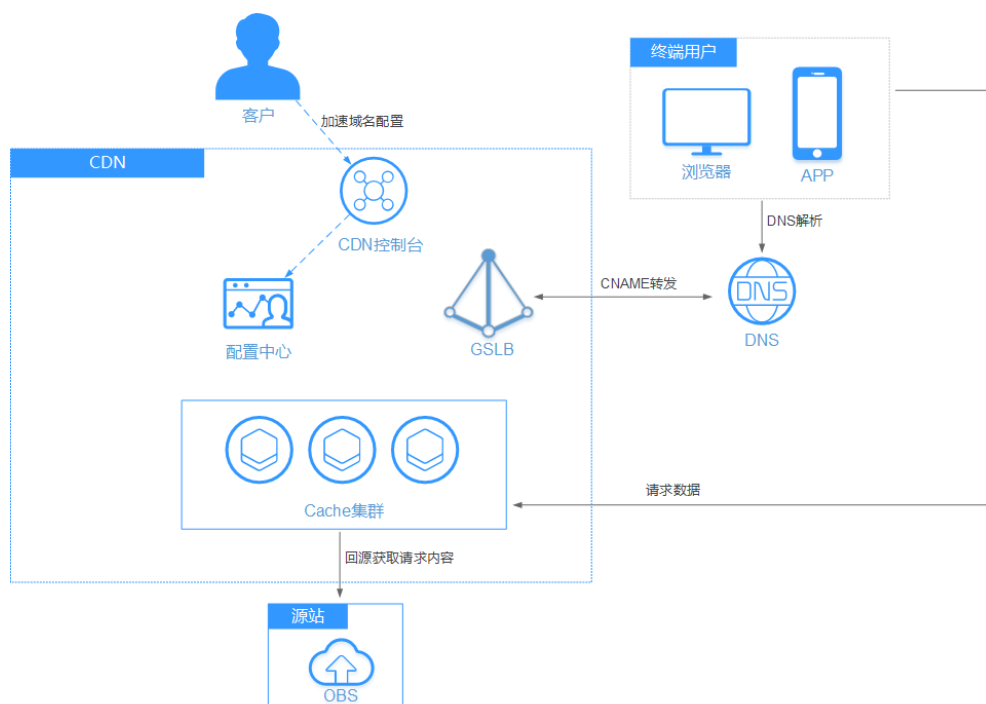
网站加速

适用于有加速需求的网站，对网站中图片、小文件等静态资源提供加速服务，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。CDN网络能够对加速域名下的**静态资源**提供良好的加速服务，支持通过自定义缓存规则控制文件在CDN节点的缓存过期时间，缓存格式包括但不限于zip、exe、wmv、gif、png、bmp、wma、rar、jpeg、jpg等。



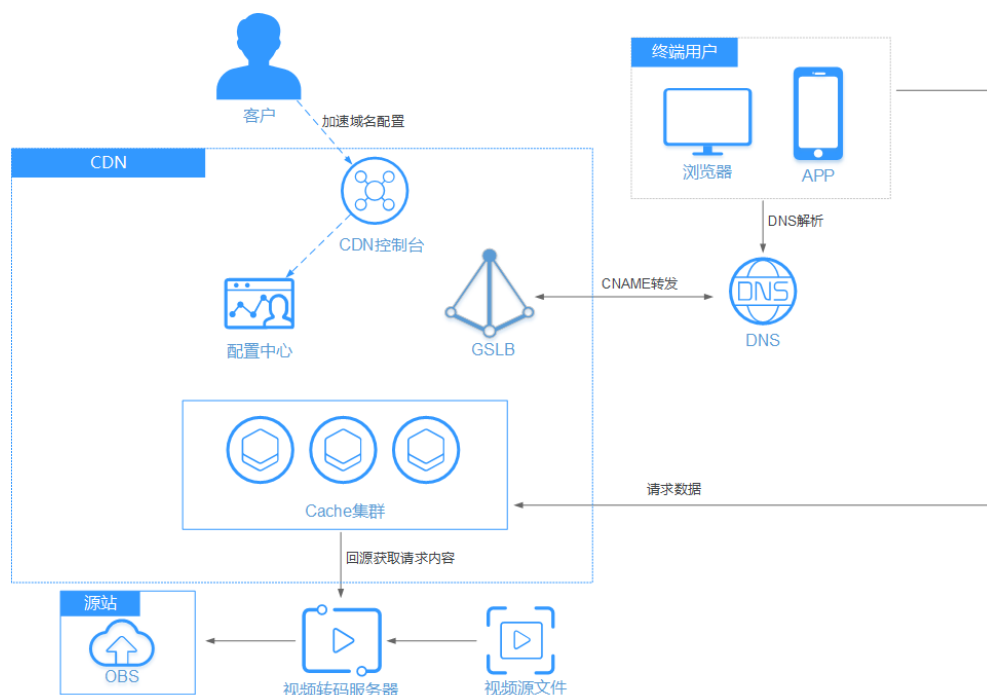
文件下载加速

适用于使用HTTP/HTTPS文件下载业务的网站、下载工具、游戏客户端、APP商店等。现在越来越多的新业务需要通过网络对客户端软件进行实时更新，包括APP更新，手游更新等，传统的下载类业务也需要支持更多的文件数量和更大的文件，如果所有的请求都通过源站服务器来处理，服务器和网络会成为很大的瓶颈，导致下载体验变差。使用CDN下载加速可以将下载量大的内容分发到各地的CDN节点，有效减轻源站的压力，同时保证了客户端高速下载的需求。



点播加速

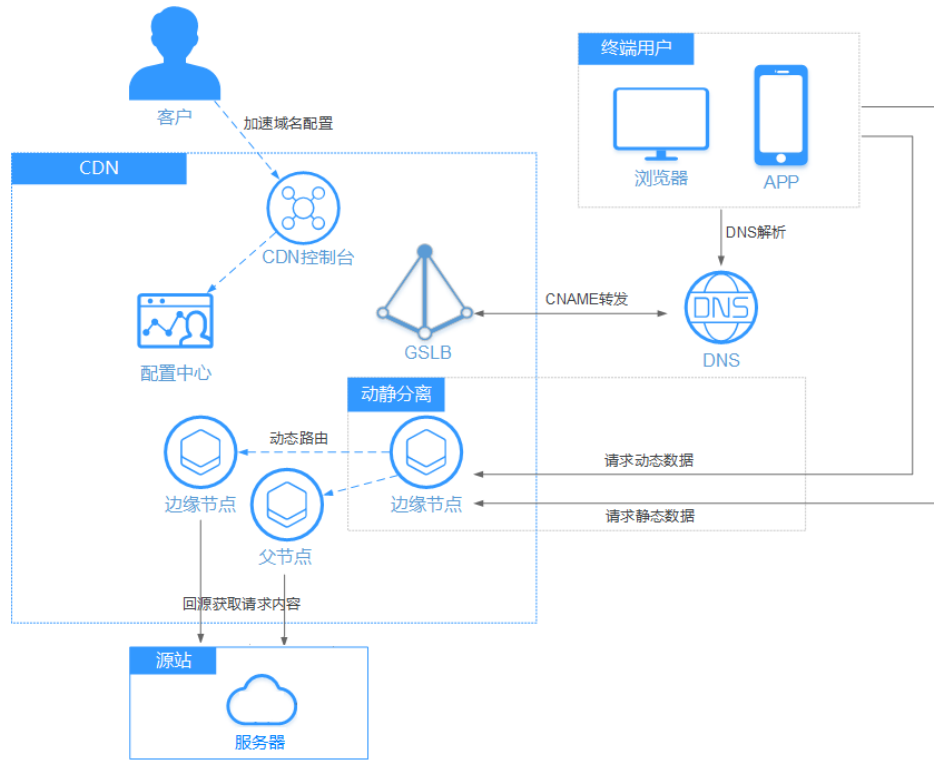
适用于提供音视频点播服务的客户。例如：在线教育类网站、在线视频分享网站、互联网电视点播平台、音乐视频点播APP等。传统的点播服务会加大服务器的负载，并消耗巨大的带宽资源，同时又无法保证终端用户访问时需要的高速体验，CDN点播加速可以提供快速、稳定和安全的点播加速服务，通过分布在各个区域的CDN节点，将音视频内容扩展到距离用户较远的地方，随时随地为用户提供高品质的访问体验。



全站加速

适用于各行业动静态内容混合，含较多动态资源请求（如asp、jsp、php等格式的文件）的网站。全站加速融合了动态和静态加速，用户请求资源时，静态内容从边缘节点就近获取，动态内容通过动态加速技术智能选择较优路由回源获取。CDN全站加速有效提升动态页面的加载速度，避开网络拥堵路由，提高访问成功率，实现网站整体加速与实时优化。

全站加速目前作为华为云的新服务，更多资讯请移步到[全站加速](#)产品页面进行咨询。



6 性能指标

CDN为您提供稳定的加速效果，有效缓解源站压力，您可以通过性能指标衡量使用CDN前后的加速效果。

通用指标

CDN通用指标（非全量指标）如下表所示：

参数	描述
时延	指完成整个文件的上传或下载所需的总时长。
丢包率	指在网络传输中所丢失数据包数量占所发送数据组的比率。
回源率	回源率分为回源请求数比例及回源流量比例两种。 <ul style="list-style-type: none">● 回源请求数比：指CDN节点对于没有缓存、缓存过期（可缓存）和不可缓存的请求占全部请求记录的比例。● 回源流量比：回源流量是CDN节点回源请求资源时产生流量。回源流量比=回源流量/（回源流量+用户请求访问的流量），比值越低，性能越好。
缓存命中率	缓存命中率为请求命中率和流量命中率，缓存命中率越高，性能越好。 <ul style="list-style-type: none">● 请求命中率 = 命中缓存的请求数 / 请求总数。● 流量命中率 = 命中缓存产生的流量 / 请求总流量 请求总流量：指命中缓存产生的流量和请求回源产生的流量之和。 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。

📖 说明

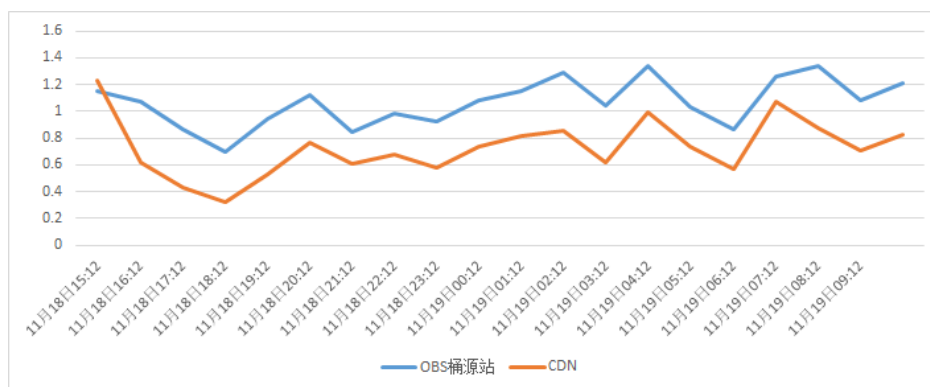
- 使用CDN后，时延、丢包率、回源率通常会降低，缓存命中率则会提高。但是由于业务场景和业务类型不同，即使您选择了相同配置的CDN服务，实际产生的加速效果也不相同，因此本文仅提供了定性的指标以供观测。
- 回源率、缓存命中率是指使用CDN后的衡量指标，如果您没有使用CDN，回源请求数为100%，缓存命中率为0。

加速案例

本次测试采用业内通用的基调测速方法，服务商为听云。测试对象为华为云OBS桶、华为云CDN。测试运营商为中国联通和中国电信。

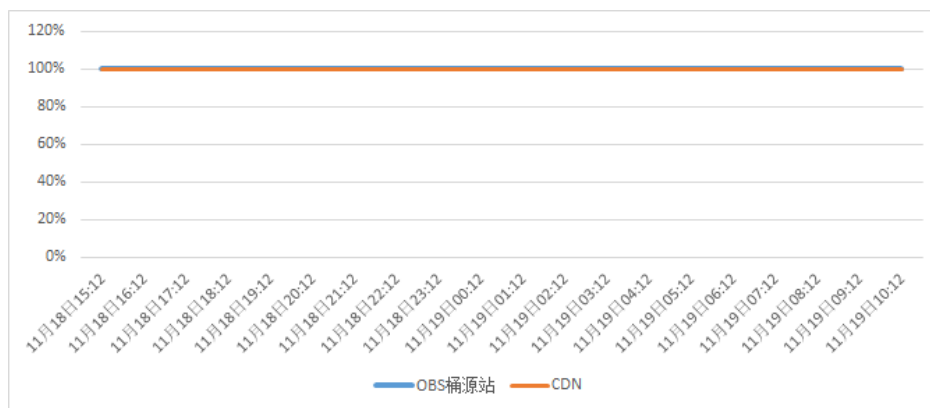
- 时延性能

单位：秒



- 可用性

经测试，OBS桶和CDN的可用性均为100%。



- 详细数据

时间	OBS桶源站			CDN		
	时延 (秒)	可用性 (%)	监测点数	时延 (秒)	可用性 (%)	监测点数
11月18日15:12	1.149	100	57	1.227	100	62
11月18日16:12	1.075	100	167	0.616	100	169
11月18日17:12	0.867	100	172	0.433	100	171

11月18日18:12	0.7	100	169	0.321	100	169
11月18日19:12	0.94	100	173	0.534	100	173
11月18日20:12	1.119	100	176	0.765	100	176
11月18日21:12	0.841	100	175	0.609	100	176
11月18日22:12	0.983	100	181	0.682	100	180
11月18日23:12	0.923	100	173	0.58	100	174
11月19日00:12	1.08	100	184	0.737	100	184
11月19日01:12	1.147	100	180	0.812	100	178
11月19日02:12	1.29	100	181	0.853	100	183
11月19日03:12	1.041	100	177	0.617	100	176
11月19日04:12	1.339	100	184	0.997	100	184
11月19日05:12	1.035	100	179	0.74	100	179
11月19日06:12	0.865	100	180	0.566	100	181
11月19日07:12	1.258	100	176	1.071	100	175
11月19日08:12	1.338	100	170	0.878	100	170
11月19日09:12	1.085	100	155	0.705	100	155
11月19日10:12	1.213	100	168	0.822	100	169

7 基本概念

- **静态资源**

每次访问得到的都是相同的文件，例如：图片、视频、网站中的文件（html、css、js）、软件安装包、apk文件、压缩包文件等。

- **动态资源**

每次访问得到的都是不同的文件，例如：网站中的文件（asp、jsp、php、perl、cgi）、API接口、数据库交互请求等。

- **加速域名**

加速域名是用户提供的需要使用CDN加速服务的域名，域名是便于记忆和沟通的一组服务器的地址，应用于网站，电子邮件，FTP等。

- **CNAME记录**

CNAME记录是指域名解析中的别名记录（Canonical Name），允许将多个域名映射到同一个域名。

例如：

- a. 您有一台服务器存放了一些文件，可以通过**file.example.com**访问该资源，但是希望通过另一个域名**data.example.com**也能访问。
- b. 那么您可以在DNS解析服务商处新增一条CNAME记录，将**data.example.com**指向**file.example.com**。
- c. 添加CNAME记录后，所有访问**data.example.com**的请求就会指向**file.example.com**，获得相同内容。

- **CNAME域名**

用户在管理控制台添加加速域名后，系统会为加速域名分配一个对应的“CNAME域名”（域名形式为：***.c.cdnhwc1.com**）。用户需要在域名服务商处，配置一条CNAME记录，将加速域名指向“CNAME域名”，记录生效后，域名解析的工作就正式转向CDN服务，该域名所有的请求都将转向CDN节点，达到加速效果。

- **源站**

源站指用户的业务服务器，即被加速分发数据的来源。

- **DNS**

TCP/IP网络中的功能实体，通过该服务器，用户只通过域名就可以访问对应的服务器。在TCP/IP网络中域名与IP地址一一对应，域名便于记忆，但网络中的服务器间只能通过IP地址相互识别，域名和IP地址之间的转换称为域名解析，域名解析需要通过专门的域名解析服务器来完成，DNS就是进行域名解析的服务器。

例如：您访问xxx.abc.com会通过DNS转换成xxx.xxx.1.1（IP地址）。您可以使用华为云解析，也可以使用其他的DNS服务商。

- **边缘节点**

边缘节点也称CDN节点、Cache节点等，指距离最终用户接入具有较少的中间环节的网络节点，对最终接入用户有较好的响应能力和连接速度。

- **回源**

CDN节点未缓存资源或者缓存资源已到期时，节点会回源站获取资源，返回给客户端。

例如：您访问某个URL，如果解析到CDN节点未缓存该资源，则您的访问请求会直接到源站获取资源，并根据URL请求返回。

- **回源HOST**

源站决定了回源时，请求到源站的IP地址。回源HOST决定回源请求访问到该IP地址的哪个站点。

例1：源站为域名时，源站为www.origin.com，回源HOST为www.abc.com，实际回源的是www.origin.com解析到的IP站点www.abc.com。

例2：源站为IP地址时，源站为192.168.1.1，回源HOST为www.abc.com，实际回源的是192.168.1.1对应主机上的站点www.abc.com。

- **SSL/TLS**

SSL（Secure Sockets Layer，安全通讯协议），是一个构架于TCP之上的安全套接层，是为网络通信提供安全及数据完整性的一种安全协议。标准化之后的SSL名称为TLS（Transport Layer Security，传输层安全协议）。

- **URL参数**

根据业务需要判断是否启用该项配置，对用户请求URL中“？”之后的参数进行过滤，提高缓存命中率。

8 约束与限制

域名接入华为云CDN前，您需要了解CDN对域名、源站的准入要求，以免因违规导致业务受损。

域名准入要求及规范

限制项	说明
域名准入条件	<ul style="list-style-type: none">● 中国大陆：<ul style="list-style-type: none">- 华为账号已完成实名认证。- 域名已在工信部备案，且当前备案信息正常可用。- 加速域名接入时需通过内容审核。● 中国大陆境外：<ul style="list-style-type: none">- 加速域名接入时需通过内容审核。● 全球：<ul style="list-style-type: none">- 已在华为云进行实名认证。- 域名已在工信部备案，且当前备案信息正常可用。- 加速域名接入时需通过内容审核。

限制项	说明
加速域名	<p>域名基础规范：</p> <ul style="list-style-type: none"> • 域名长度不能超过75个字符，支持大小写字母、数字、“-”、“.”。 • 每个账号最多支持加速100个域名。 • 加速域名不允许重复添加。 • CDN不支持非法网站接入，对于已接入CDN的域名，会进行定期复审，如发现存在违规行为，将立即中止该域名的CDN加速，同时中止该用户名下所有域名的CDN服务。 • 加速域名处于“停用”或“审核未通过”状态超过120天，CDN平台会启动删除域名流程，平台复核后会删除该域名相关记录。记录删除后如果想要再次使用该域名加速，需要重新添加域名。 • 如果域名超过180天没有任何访问流量，CDN平台会启动域名停用流程，平台复核后会停用该域名。 <p>欠费及攻击处理规则：</p> <ul style="list-style-type: none"> • 欠费进入保留期后，CDN将停用您的加速域名，删除加速域名的CNAME解析，此时将无法访问域名。 • 当域名受攻击时，CDN节点会承受攻击流量，不会造成源站被攻击瘫痪。如果攻击流量太大造成节点不能正常服务，CDN会封禁加速域名，最终域名状态调整为“停用”，停止CDN加速服务。因攻击时占用了CDN节点资源，所以会产生相关费用。 <p>泛域名接入规范：支持添加泛域名作为加速域名，如：您在CDN添加泛域名*.test.com作为加速域名，并将*.test.com解析至CDN生成的CNAME域名后，那么您所有*.test.com的次级域名（如a.test.com）都将默认支持CDN加速。泛域名（*.test.com）的三级域名（如b.a.test.com）不会被CDN加速。</p> <ol style="list-style-type: none"> 1. A账号添加泛域名后，其他账号不能再添加该泛域名的所有次级域名。 2. 泛域名的所有次级域名的加速都会产生费用，泛域名有多个次级域名时，CDN统计时将泛域名的产生的流量做汇总，不提供单个次级域名的计费数据。 <p>说明 刷新或预热泛域名缓存时，需要每个子域名单独预热或刷新，示例： 泛域名：*.a.com，子域名：1.a.com、2.a.com、3.a.com。 刷新时需要刷新具体子域名的URL，即输入：http://1.a.com/abc.jpg而不是http://*.a.com/abc.jpg。</p>

内容审核

限制项	说明
内容审核	<p>CDN不支持接入违反相关法律法规的域名，包括但不限于：</p> <ul style="list-style-type: none">● 涉黄、涉赌、涉毒、涉诈、侵权内容的网站● 游戏私服类网站● 盗版游戏 / 软件 / 盗版视频网站● P2P类金融网站● 彩票类网站● 违规医院和药品类网站● 网站无法正常访问或内容不含有任何实质信息 <p>说明</p> <ul style="list-style-type: none">● 如果您的加速域名含有以上违规的内容，您将自行承担相关风险。● 如果发现涉黄、涉赌、涉毒、涉诈等违规行为，CDN将执行域名封禁策略（删除相关加速域名且不允许再次接入，与违规域名使用相同源站的加速域名同样执行域名封禁策略），账号加速域名配额降为0。

源站规范及限制

限制项	说明
源站	<ul style="list-style-type: none"> ● 源站数量：每个加速域名最多可以添加50个源站。 ● 源站IP： <ul style="list-style-type: none"> - 使用IP作为源站地址时，CDN节点回源时直接访问该IP地址。 - 支持配置IPv4，暂不支持IPv6。 ● 源站域名： <ul style="list-style-type: none"> - 首字符为字母或数字，支持大小写字母、数字、“-”、“.”，长度不能超过255个字符。 - 源站域名不能与加速域名相同。 - 您也可以将“源站域名”设置为对象存储桶域名。 <p>说明</p> <ul style="list-style-type: none"> ● 如果您需要将非华为云服务商的对象存储桶作为您的源站，可以将对象存储桶访问域名作为“源站域名”接入CDN。 ● 不支持私有桶通过源站域名的形式接入CDN。 ● 如果您将对象存储桶作为您的源站，对象存储桶将根据它的收费规则收取回源流量费用。 <ul style="list-style-type: none"> ● OBS桶域名：可以选择当前账号下的OBS桶域名或自定义OBS桶域名。使用OBS桶域名作为源站接入CDN，OBS会收取CDN回源的流量费用，回源流量费用将按照公网流出费用进行结算。如果您使用了OBS 3.0及以上版本的桶作为华为云CDN的源站，可以购买OBS回源流量包抵扣回源流量，具体请见CDN加速OBS计费规则。 <ul style="list-style-type: none"> - 如果您的OBS私有桶内容不适合为加速域名提供回源数据，请勿将该私有桶设置为源站。 - 使用自定义OBS桶域名作为源站时，域名必须以myhuaweicloud.com或myhuaweicloud.cn结尾。 - 如果OBS私有桶设置为源站，请开启OBS委托授权，同时勾选“私有桶”选项，否则将会导致回源失败。 - 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。 - 如果您的OBS桶开启了静态网站托管业务，请在添加加速域名时勾选“静态网站托管”，这样用户访问的时候就不会显示桶中所有文件列表。 - 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。

配额

限制项	说明
域名配额	<p>为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如果当前域名配额限制无法满足使用需要，您可以提交工单申请扩大配额。</p> <ul style="list-style-type: none">• 域名数量：100。• 缓存刷新（文件）：2000条/日。• 缓存刷新（目录）：100条/日。• 缓存预热：1000条/日。

其他使用限制

限制项	说明
回源	<ul style="list-style-type: none">• 回源超时时间：CDN默认回源超时时间为30s。
文件	<ul style="list-style-type: none">• 文件上传：CDN支持上传文件，最大上传300M，文件上传会收取流量费用。
请求方式	常见的HTTP请求方式里面，CDN支持GET、PUT、POST和DELETE这几种请求方式。

9 安全

9.1 责任共担

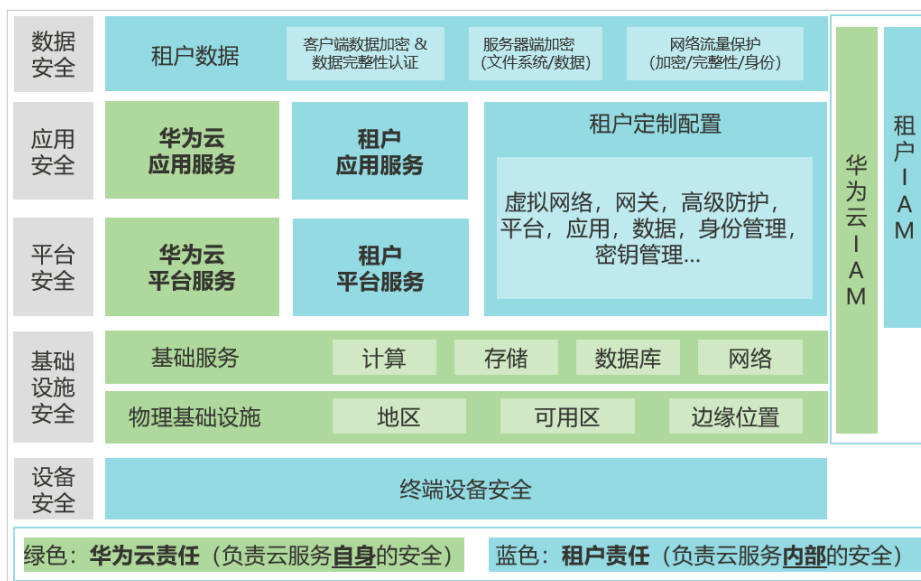
华为云秉承“将对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如[图9-1](#)所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《[华为云安全白皮书](#)》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 9-1 华为云安全责任共担模型



9.2 数据保护技术

华为云CDN通过多种数据保护手段和特性，保障客户数据在华为云CDN的安全性。

表 9-1 CDN 数据保护技术

数据保护技术	说明
传输加密	华为云CDN支持全网HTTPS、HTTP2.0安全协议，详情请参见 HTTPS配置 。
证书管理	华为云CDN支持批量配置SSL证书功能，详情请参见 证书管理 。
数据一致性保护	资源在CDN多节点内传输时，CDN支持对资源进行CRC校验，保证资源在CDN节点内传输过程中不会被劫持篡改。
数据一致性校验	CDN支持创建检查任务，检查CDN缓存的资源是否和源站一致。

同时，CDN服务充分尊重用户隐私，遵循法律法规。CDN仅为域名提供加速服务，不会采集和存储任何用户隐私数据。更多隐私数据使用和保护问题，请参考[隐私政策声明](#)。

9.3 审计与日志

- 审计

云审计服务（Cloud Trace Service, CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务后，CTS可记录CDN的操作事件用于审计。

- CTS的详细介绍和开通配置方法，请参见[CTS快速入门](#)。
- CDN支持审计的操作事件请参见[审计管理](#)。
- 开启了云审计服务后，系统开始记录CDN资源的操作。您可以在云审计服务控制台查看最近7天的操作记录，具体操作指导请参见[查看审计事件](#)。

- 日志

CDN记录了所有域名（包括已删除域名，如果客户开通了企业项目，则已删除域名不支持此功能）被网络用户访问的详细日志，客户可以下载最近30天内指定时间段的日志，对相关业务资源被访问情况进行详细分析。查看CDN日志请参考[日志管理](#)。

9.4 监控安全风险

CDN服务提供基于云监控服务的资源监控能力，帮助用户监控账号下的CDN加速资源，执行自动实时监控、告警和通知操作，帮助您更好地了解CDN加速的各项性能指标。

关于CDN服务支持的监控指标，以及如何创建监控告警规则等内容，请参见[实时监控](#)。

10 CDN 权限管理

如果您需要对华为云上购买的CDN资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制员工对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望这部分员工拥有CDN的使用权限，没有删除CDN等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用CDN，但是不允许删除CDN的权限，控制员工对CDN资源的使用范围。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用CDN服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见[IAM产品介绍](#)。

CDN 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

CDN部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，访问CDN时，不需要切换区域。

根据授权精细程度分为角色和策略。

- **角色：** IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- **策略：** IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对ECS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，CDN支持的API授权项请参见[权限及授权项说明](#)。

策略是以JSON格式描述权限集的语言。默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略，才能使得用户组中的用户获得策略定

义的权限，这一过程称为授权。授权后，用户就可以基于策略对云服务进行操作。IAM系统预置了各服务的常用权限，例如管理员权限、只读权限，您可以直接使用这些系统策略。

CDN部署时不区分物理区域，为全局级服务。授权时，在全局项目中设置策略，访问CDN时，不需要切换区域。

如表10-1所示，包括了CDN的所有系统策略。

表 10-1 系统策略

策略名称	描述	策略类别
CDN Administrator	操作权限：对CDN的所有执行权限。 作用范围：全局级服务。	系统角色
CDN DomainReadOnlyAccess	操作权限：对CDN加速域名信息的只读权限。 作用范围：全局级服务。	系统策略
CDN StatisticsReadOnlyAccess	操作权限：对CDN统计信息的只读权限。 作用范围：全局级服务。	系统策略
CDN LogsReadOnlyAccess	操作权限：对CDN日志的只读权限。 作用范围：全局级服务。	系统策略
CDN DomainConfiguration	操作权限：对CDN加速域名的配置权限。 作用范围：全局级服务。	系统策略
CDN RefreshAndPreheatAccess	操作权限：CDN刷新预热权限。 作用范围：全局级服务。	系统策略
CDN FullAccess	操作权限：对CDN的所有执行权限。 作用范围：全局级服务	系统策略
CDN ReadOnlyAccess	操作权限：对CDN的所有只读权限。 作用范围：全局级服务	系统策略

表10-2列出了CDN常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 10-2 常用操作与系统策略的关系

操作	CDN Administrator	CDN DomainReadOnlyAccess	CDN StatisticsReadOnlyAccess	CDN LogsReadOnlyAccess	CDN DomainConfiguration	CDN RefreshAndPreheatAccess	CDN FullAccess	CDN ReadOnlyAccess
查询加速域名	√	√	x	x	x	x	√	√
创建加速域名	√	x	x	x	√	x	√	x
删除加速域名	√	x	x	x	√	x	√	x
查询源站信息	√	√	x	x	x	x	√	√
查询HTTPS配置	√	√	x	x	x	x	√	√
查询缓存规则	√	√	x	x	x	x	√	√
查询IP黑名单	√	x	x	x	x	x	√	x
修改源站信息	√	x	x	x	√	x	√	x
配置HTTPS	√	x	x	x	√	x	√	x
设置缓存规则	√	x	x	x	x	x	√	x
开启刷新功能	√	x	x	x	x	√	√	x
开启预热功能	√	x	x	x	x	√	√	x
查询网络总流量	√	x	√	x	x	x	√	√
查询网络流量明细	√	x	√	x	x	x	√	√
查询网络带宽明细	√	x	√	x	x	x	√	√
查询消耗统计	√	x	√	x	x	x	√	√
查询运营商消耗统计	√	x	√	x	x	x	√	√
日志查询	√	x	x	√	x	x	√	√

 说明

不能单独配置CDN DomainConfiguration和CDN RefreshAndPreheatAccess权限，如果想配置这两个权限，请同时配置CDN DomainReadOnlyAccess权限，否则会造成所有域名不可见导致无法进行域名配置和刷新预热配置。

CDN 与其他服务间依赖关系

CDN对其他云服务有诸多依赖关系，因此在您开启IAM系统策略授权后，在CDN Console控制台的各项功能需要配置相应的服务权限后才能正常查看或使用，前提条件如下：

- 依赖服务的权限配置均基于您已设置了IAM系统策略授权的CDN FullAccess或CDN ReadOnlyAccess策略权限。

说明

如果IAM用户需要在CDN Console控制台拥有相应功能的查看或使用权限，请确认已经对该用户所在的用户组设置了CDN Administrator、CDN FullAccess或CDN ReadOnlyAccess策略的集群权限，再按如下[表10-3](#)增加依赖服务的权限。

表 10-3 CDN Console 中依赖服务的角色或策略

Console控制台功能	依赖服务	需配置角色/策略
OBS委托授权	统一身份认证服务 IAM	<ul style="list-style-type: none"> • 创建委托：iam:agencies:createAgency • 查询指定条件下的委托列表：iam:agencies:listAgencies • 查询委托详情：iam:agencies:getAgency • 为委托授予项目服务权限：iam:permissions:grantRoleToAgencyOnProject • 查询委托是否拥有项目服务权限：iam:permissions:checkRoleForAgencyOnProject • 查询项目列表：iam:projects:listProjects • 查询权限列表：iam:roles:listRoles
源站配置 <ul style="list-style-type: none"> • 源站是 OBS桶域名 	对象存储服务 OBS	<ul style="list-style-type: none"> • 列举全部桶：obs:bucket:ListAllMyBuckets • 列举桶内对象：obs:bucket:ListBucket • 判断桶是否存在并获取桶的元数据：obs:bucket:HeadBucket
SCM证书	云证书管理服务 CCM	<ul style="list-style-type: none"> • 查询证书列表：scm:cert:list • 导出证书：scm:cert:download
按照标签筛选域名	标签管理服务 TMS	查询预定义标签：tms:predefineTags:list
企业项目	企业管理	<ul style="list-style-type: none"> • 查询企业项目详情：eps:enterpriseProjects:get • 查询企业项目列表：eps:enterpriseProjects:list

相关链接

- [《IAM产品介绍》](#)
- [创建用户并授予使用CDN](#)
- [策略及授权项说明](#)

11 与其他云服务的关系

表 11-1 与其他云服务的关系

交互功能	相关服务	位置
将OBS桶作为CDN加速域名的源站。	对象存储服务（ Object Storage Service, OBS ）	CDN加速OBS桶文件方案概述
通过IAM服务实现以下功能： <ul style="list-style-type: none"> ● 用户管理及权限设置： <ul style="list-style-type: none"> - 管理IAM用户和用户组 - 管理细粒度策略 ● 管理委托 在IAM控制台进行委托授权，授权成功后CDN将有权限访问您账号下的OBS私有桶。 	统一身份认证服务（ Identity and Access Management, IAM ）	用户权限 OBS委托授权
通过CTS服务收集CDN资源操作记录，便于日后的查询、审计和回溯。	云审计服务（ Cloud Trace Service, CTS ）	审计
可在企业管理服务创建相关CDN的企业项目来集中管理CDN域名资源。	企业管理服务（ Enterprise Management ）	企业项目