

CDN

# 产品介绍

文档版本 18  
发布日期 2026-04-27



版权所有 © 华为技术有限公司 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

---

|                           |           |
|---------------------------|-----------|
| <b>1 什么是华为云 CDN</b> ..... | <b>1</b>  |
| <b>2 工作原理</b> .....       | <b>3</b>  |
| <b>3 节点分布</b> .....       | <b>5</b>  |
| <b>4 产品优势</b> .....       | <b>7</b>  |
| <b>5 应用场景</b> .....       | <b>8</b>  |
| <b>6 产品功能</b> .....       | <b>12</b> |
| <b>7 性能指标</b> .....       | <b>17</b> |
| <b>8 基本概念</b> .....       | <b>20</b> |
| <b>9 约束与限制</b> .....      | <b>23</b> |
| <b>10 安全</b> .....        | <b>29</b> |
| 10.1 数据保护技术.....          | 29        |
| 10.2 审计与日志.....           | 29        |
| <b>11 权限管理</b> .....      | <b>31</b> |
| <b>12 与其他云服务的关系</b> ..... | <b>39</b> |

# 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, 通过在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                      |
|---------------------------|-----------------------------|
| <a href="#">CDN 基本概念</a>  | 快速了解 CDN 的常用概念, 帮助理解和使用 CDN |
| <a href="#">CDN API</a>   | 快速了解通过调用 API 来实现对应的控制台操作    |
| <a href="#">入门概述</a>      | 快速了解如何接入 CDN 加速             |
| <a href="#">域名管理</a>      | 快速了解 CDN 的域名管理功能            |
| <a href="#">域名配置</a>      | 快速了解 CDN 的相关配置              |
| <a href="#">缓存刷新和缓存预热</a> | 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。

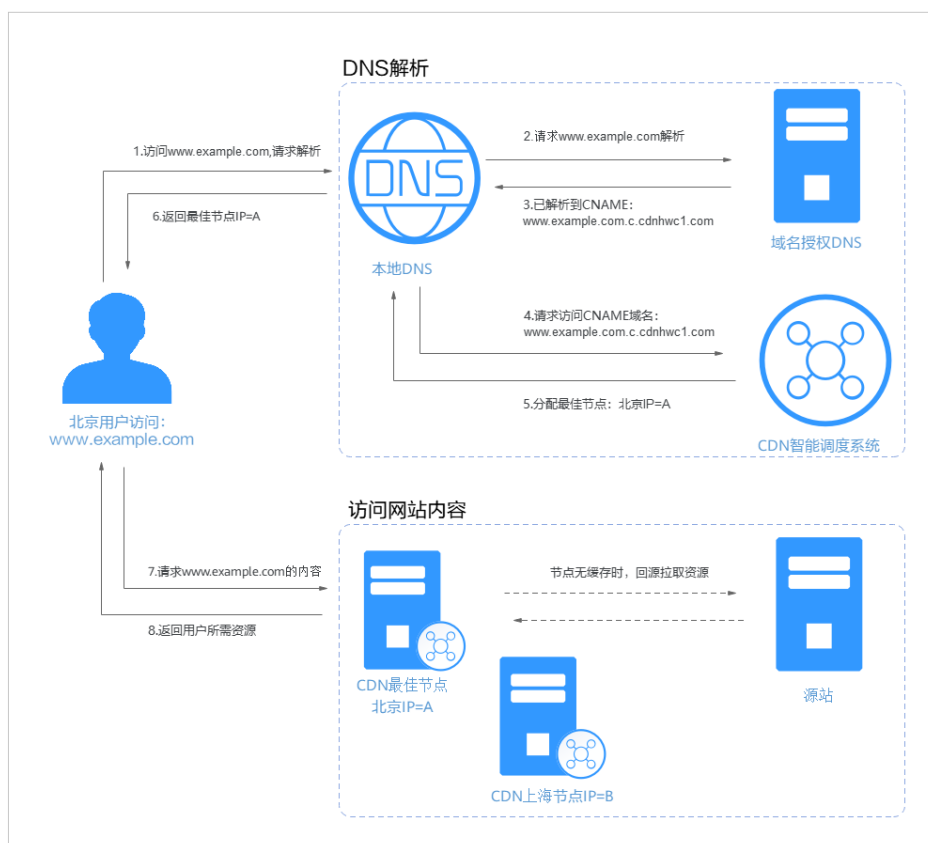
#### 说明

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\$15,000 USD 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。此时由最佳节点返回资源给用户，达到加速目的。
  - 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。用户再次请求该资源时，将由节点返回已缓存的资源给用户，无需回源，达到加速目的。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中国大陆2000+加速节点，中国大陆境外800+加速节点，全网带宽输出能力高达180Tbps。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，提供了有效且稳定的加速效果。

表 3-1 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                   |

表 3-2 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 |

| 大区    | 节点分布（以华为内部业务划分区域）  |
|-------|--|
| 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   | 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AICache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。

## 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

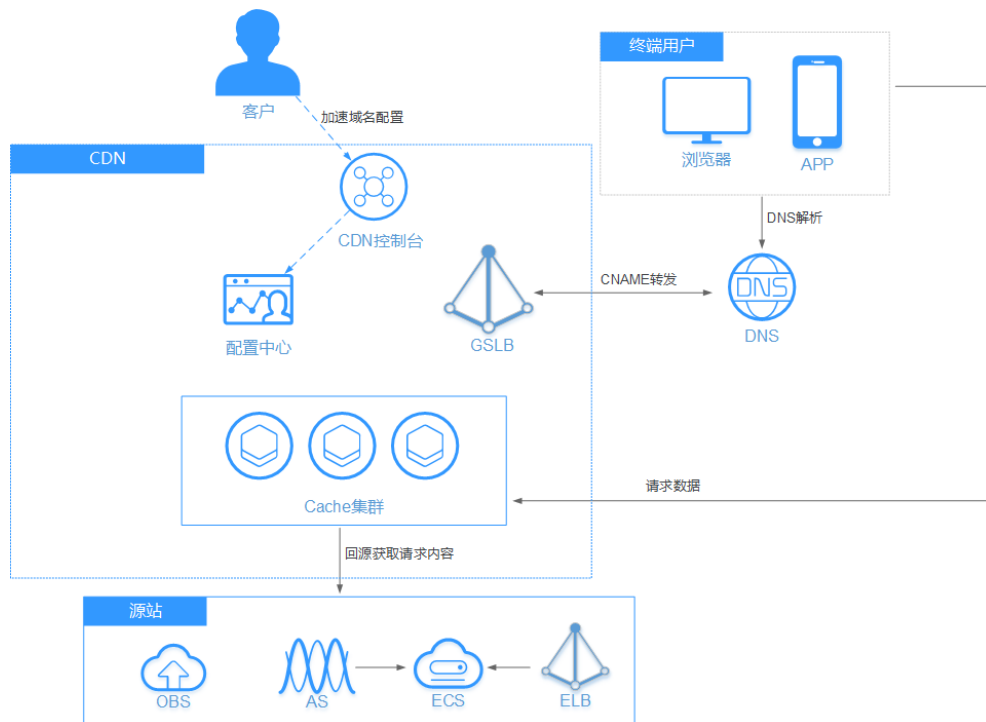
## 场景概述

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  |
|---------------|---|
| <b>网站加速</b>   | 适用于有加速需求的网站，对网站中图片、小文件等 <b>静态资源</b> 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。 |
| <b>文件下载加速</b> | 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。   |
| <b>点播加速</b>   | 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。   |
| <b>全站加速</b>   | 适用于各行业动静态内容混合，含较多 <b>动态资源</b> 请求（如asp、jsp、php等格式的文件）的网站。  |

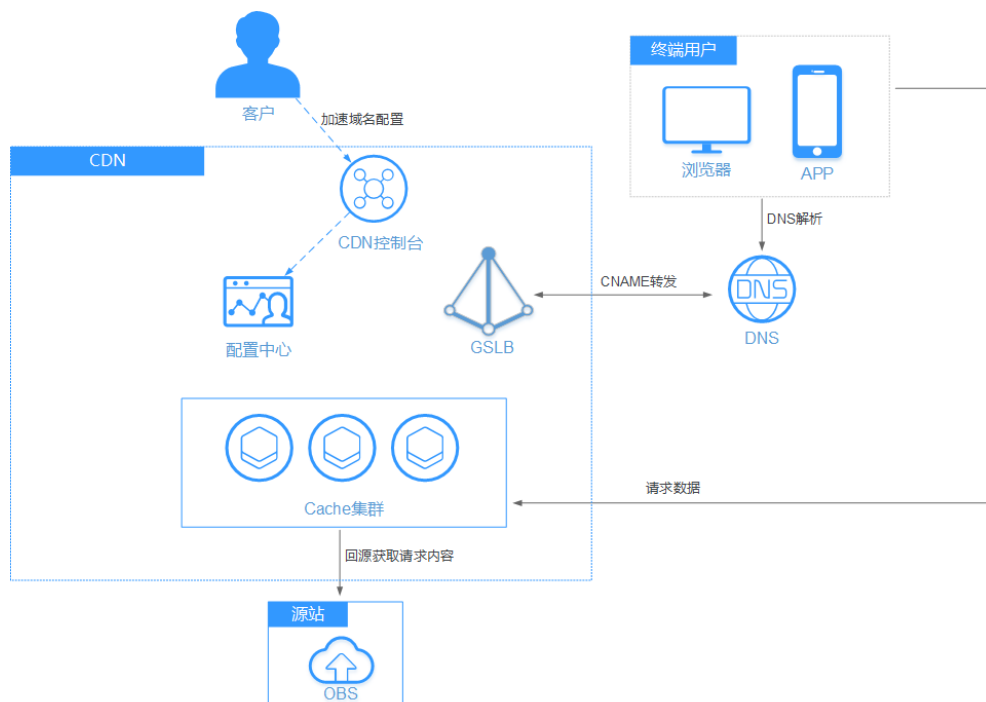
## 网站加速

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。



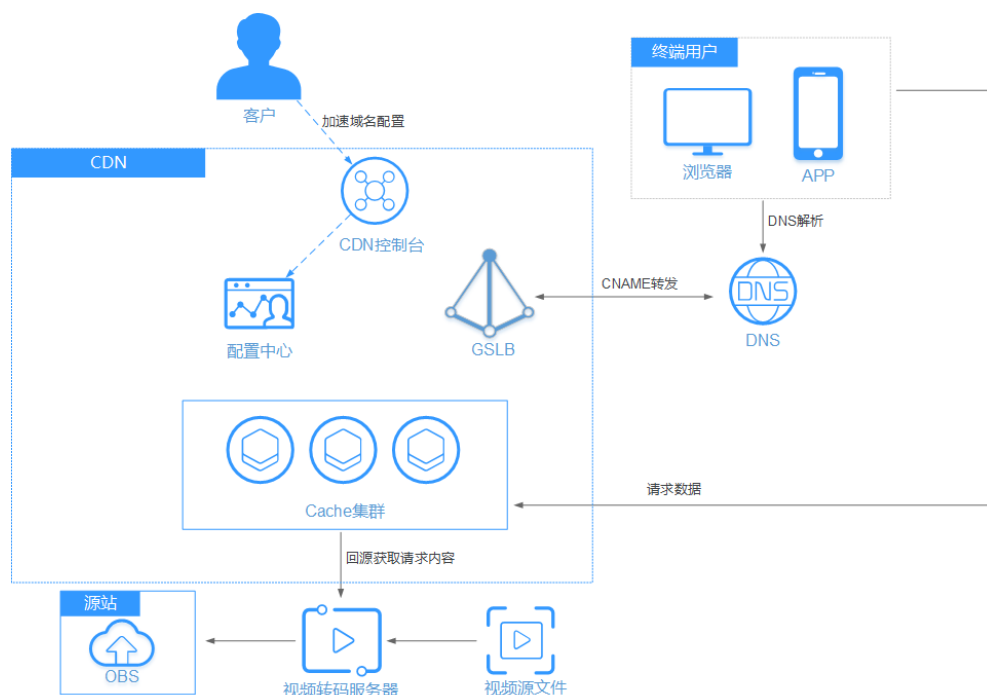
## 文件下载加速

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。



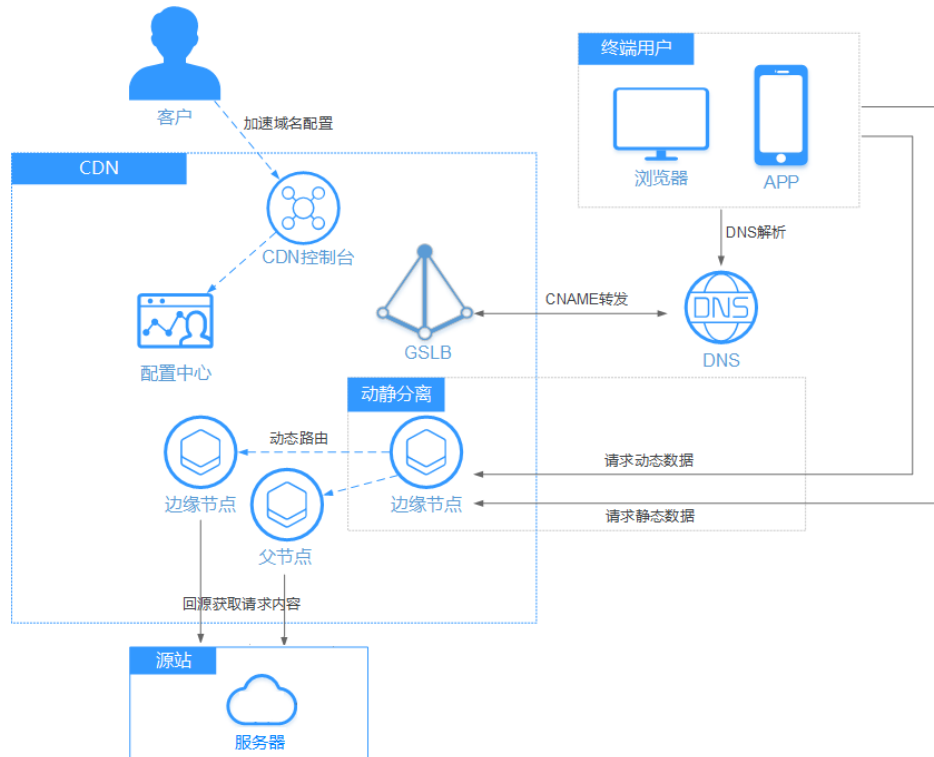
## 点播加速

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。



# 6 产品功能

本页面介绍了CDN服务支持的主要功能。

## 管理加速域名

域名添加完成后，您可以在CDN控制台对接入CDN的加速域名进行启用、停用、移除、重新审核加速域名的操作。

- **添加CDN加速域名**：如果您想通过CDN加速指定网站的业务，那么您要将需要加速的网站作为源站，并为其创建加速域名。CDN通过加速域名将源站上需要加速的内容缓存到CDN节点，达到加速访问资源的效果。
- **启用/停用加速域名**：适用于暂时停用或者重新启用已停用的域名。
- **删除加速域名**：适用于域名不再需要CDN加速的场景，支持删除处于“已停用”、“配置失败”或“审核不通过”状态下的加速域名。
- **重新审核加速域名**：对于因域名备案过期而被禁用的加速域名，您在工信部恢复域名备案后，CDN支持通过控制台进行重新审核，重新审核通过后CDN会为您解禁域名。
- **域名配额管理**：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。

## 模板管理

CDN支持**自定义模板配置**，您可以将多个功能集成在一个模板里，并将模板应用到多个域名，快速完成自定义域名配置。

## 复制配置到其他域名

适用于将某个存量域名的配置复制到其他域名的场景。

- **复制配置到存量域名**：如果您想要复制某个加速域名的配置到其它加速域名，可以使用CDN的复制到存量域名功能，以达到快速、批量配置加速域名的目的。
- **复制配置到新添加域名**：如果您有一个新的域名想要添加到CDN加速，并且新域名的配置与某个存量域名一致，可以使用复制配置到新添加域名功能。

## 修改域名基本配置

当您在使用CDN加速的过程中，源站、终端用户的所在地区有变化，需要调整CDN配置，您可以通过域名基本配置完成。

- **修改域名业务类型**：如果您的业务有变，当前CDN加速域名的业务类型已经无法匹配您的需求时，您可以修改业务类型。
- **修改域名服务范围**：如果您的用户所在地域发生改变，您可以修改加速域名的服务范围，更好地匹配当前业务。
- **修改域名源站配置**：当您的源站IP、域名发生变化，源站信息配置错误，或需要添加多个源站时，可以在此项配置中配置相关源站信息。
- **修改域名回源HOST**：如果CDN回源时访问的站点域名不是您的加速域名（CDN默认回源HOST为加速域名），您需要设置回源HOST。
- **配置客户端用IPv6协议访问CDN节点**：如果您需要以IPv6协议访问CDN，您需要开启此项配置。

## 修改域名回源配置

当终端用户访问资源时，如果CDN节点没有缓存该资源，就会向源站请求资源返回给用户并缓存到CDN节点。您可以根据业务需求对回源的各个参数进行设置，提升资源访问效率。

- **修改回源协议**：您可以通过配置回源方式来指定CDN回源时的请求协议。
- **配置回源SNI**：如果源站IP绑定了多个域名，当CDN节点以HTTPS协议访问源站时，您可以设置回源SNI，指定CDN节点在回源时访问的域名。
- **回源URL改写**：当回源请求URL与源站URL不匹配时，会导致回源失败。您可以在CDN控制台改写回源URL，提高回源请求URL与源站的匹配度，提升回源命中率。
- **配置高级回源**：如果您需要根据不同的资源类型或路径回源到不同源站，可以通过高级回源配置实现。
- **配置Range实现资源分段回源**：如果您的资源内容较大，希望CDN回源时分片返回内容，以便缩短大文件的分发时间，提升回源效率，减少回源消耗，可以通过开启Range回源实现。
- **回源跟随**：如果您的源站地址因业务需求做了301/302重定向，您需要开启回源跟随功能才可以将重定向的资源缓存到CDN节点，达到加速分发的效果。
- **配置回源是否校验ETag**：CDN节点缓存的资源过期后，如果您希望CDN通过ETag的值判断资源是否改变，需要开启回源是否校验ETag。
- **修改回源超时时间**：如果您需要根据源站特性和业务场景调整回源超时时间（默认30s），您需要配置此项。
- **配置回源请求头**：如果您想在回源时加入或删除指定的HTTP消息头部，改写终端用户请求URL中的头部信息，您需要设置回源请求头。
- **配置动态加速回源模式**：如果您想动态内容回源请求时根据权重（默认是择优回源）回源，您需要设置动态加速回源模式。

## HTTPS 证书相关配置

HTTPS是以安全为目标的HTTP通道，在HTTP的基础上通过传输加密和身份认证保证了传输过程的安全性。CDN支持SSL证书及相关配置，提升域名的安全性。

- **配置域名HTTPS证书**：CDN支持HTTPS安全加速，您可以通过在CDN控制台配置加速域名的HTTPS证书，启用HTTPS加速服务，证书配置成功后，客户端可以使用HTTPS协议请求CDN节点。
- **批量配置域名证书**：CDN支持为多个域名批量配置证书、批量更新多个域名证书，以达到快速配置的目的。

- **配置TLS版本与加密套件**：华为云CDN为您提供了TLS版本与加密套件配置的功能，您可以根据自己的业务需求配置合适的TLS版本与加密套件配置。
- **配置强制跳转**：您可以通过配置强制跳转功能，将客户端到CDN节点的请求跳转为HTTP或HTTPS。
- **配置HSTS安全访问**：HSTS（HTTP Strict Transport Security）即严格传输安全，是国际互联网工程组织IETF推行的Web安全协议。配置HSTS后，将强制客户端（如浏览器）使用HTTPS协议访问服务器，提升访问安全性。
- **启用HTTP/2协议**：介绍了HTTP/2的背景信息和优势，有助于您决定是否开启此项配置。
- **配置OCSP Stapling**：开启OCSP Stapling功能，CDN可以预先查询并缓存在线证书验证结果，在与浏览器进行TLS连接时返回给浏览器，浏览器无需再次前往CA站点查询，从而减少用户验证时间。
- **启用QUIC协议**：启用QUIC协议，提高了传输的安全性，减少传输和连接时的延时，避免网络拥塞。
- **配置客户端证书**：CDN支持双向证书认证，通过配置客户端证书，实现客户端与CDN节点的双向证书认证，提高网站通信安全性。

## 缓存配置

CDN加速的原理就是将源站资源缓存到遍布全球的各个边缘节点，终端用户就近获取资源，从而达到加速效果。您可以通过修改资源的缓存规则，控制资源在CDN节点的缓存时间，提高缓存命中率、减轻源站压力。

- **配置资源在CDN节点的缓存规则**：CDN支持配置不同资源在边缘节点的缓存过期时间，合理设置缓存过期时间能有效提升缓存命中率，降低回源率。
- **配置浏览器缓存过期时间**：CDN支持配置浏览器缓存过期时间，当终端用户请求资源时，如果浏览器有缓存，直接返回给用户，降低回源率。
- **配置源站响应状态码在CDN节点的缓存时间**：CDN节点回源站请求资源时，源站会返回响应的状态码，您可以在CDN控制台设置状态码的缓存时间，当客户端再次请求相同资源时，不会触发回源，减小回源概率，减轻源站压力。
- **配置客户端访问URL重写**：当用户请求URL与CDN节点缓存资源的URL不一致时，可以通过访问URL重写功能重定向或重写到目标URL。
- **配置域名共享缓存组**：如果不同域名对应相同的资源，您可以配置共享缓存组，将一个域名设置为主域名，组内其他域名共享该域名的缓存，以提高缓存命中率。

## 访问控制

如果您想对访问者身份进行识别和过滤，限制部分用户访问，提高CDN的安全性，您可以通过设置防盗链、IP黑白名单、UA黑白名单、URL鉴权来实现。

- **配置防盗链规则拦截/放行指定Referer**：通过设置HTTP Request Header中referer字段值的过滤策略，对访问者身份进行识别和过滤，实现限制访问来源的目的。
- **配置IP黑白名单规则拦截/放行指定IP**：通过设置过滤策略，对用户请求IP地址进行过滤，从而限制访问来源，阻拦恶意IP盗刷、攻击等问题。
- **配置User-Agent黑白名单规则拦截/放行指定User-Agent**：通过配置User-Agent黑名单和白名单实现对访客身份的识别和过滤，从而限制访问CDN资源的用户，提升CDN的安全性。

- **配置区域访问控制规则拦截/放行指定区域请求**：如果您因为业务需求，需要限制某些地理位置的用户访问，可以通过区域访问控制功能实现。
- **配置URL鉴权防止资源被恶意盗用**：CDN分发的内容默认为公开资源，URL鉴权功能主要用于保护用户站点资源，防止资源被用户恶意下载盗用。
- **配置远程鉴权防止资源被恶意盗用**：配置远程鉴权功能，当用户向CDN节点请求资源时，CDN将用户请求转发到您指定的鉴权服务器，CDN根据鉴权服务器返回的结果判断是否给用户返回资源。
- **配置IP访问限频防御CC攻击**：配置IP访问限频，通过限制单IP的单URL每秒访问单个节点的次数，实现CC攻击防御及恶意盗刷防护。

## 高级配置

进一步配置相关参数，提升用户体验和产品易用性。

- **配置节点响应给客户端的HTTP header（跨域请求）**：当您的网站需要自定义HTTP响应头取值时，可以在此项中进行配置。
- **配置自定义错误页面**：用户访问报错时，会给客户端返回错误页面，而此时的页面一般不美观。您可以在CDN控制台设置自定义错误页面，当访问页面出错时，会给客户端返回指定的页面，优化用户体验。
- **配置智能压缩**：开启智能压缩功能时，CDN会自动压缩您的静态文件。智能压缩能够有效缩小传输文件的大小，提升传输效率，减少带宽消耗。
- **配置WebSocket协议**：如果在CDN添加了全站加速的域名，此类域名有弹幕聊天、协同会话、行情播报、体育实况更新、在线教育和物联网等场景，需要实现长时间双向传输数据，可以通过配置WebSocket协议来实现。
- **配置客户端请求限速规则**：配置请求限速，将用户请求速度限制在指定范围内，一定程度上减少突发高带宽风险，节省成本。
- **配置流量/带宽封顶**：如果您想给域名配置流量或带宽上限，当用量达到阈值时暂停CDN加速，以减少因流量盗刷或攻击带来的高额账单，可以配置用量封顶功能。
- **配置突发带宽告警**：CDN支持配置突发带宽告警，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。

## 视频拖拽

用户观看视频时可以随意拖拽播放进度，不会影响观看效果，配置详细步骤请参见[视频拖拽](#)。

## 规则引擎

**规则引擎**功能通过图形化的方式实现各种规则配置，实现更加灵活、细粒度的规则配置。通过限制触发条件，控制当前配置生效的资源范围，满足多种场景的配置需求。

## 刷新预热

**缓存刷新**：提交缓存刷新请求后，CDN节点的缓存内容将会被强制过期，当用户向CDN节点请求资源时，CDN会直接回源站请求对应的资源。

**缓存预热**：提交缓存预热请求后，源站将会主动将对应的资源缓存到CDN节点，用户就能直接从CDN节点获取到最新的资源。

## 统计分析

CDN为您提供的相关[统计报表](#)，您可以查看并分析相关数据，及时发现异常、调整业务。

## 资源包管理

如果您的计费方式为流量计费，您可以在[资源包管理](#)页面通过购买流量包来获取更多流量抵扣优惠。您也可以在资源包管理页面查看资源包的基本信息，还可以进行相关设置。

## 日志管理

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，您可以前往[日志管理](#)页面下载最近30天内指定时间段的日志，对您的业务资源被访问情况进行详细分析。

## 节点 IP 归属查询

如果您的加速域名被访问时页面内容显示异常，您可以通过[节点IP归属查询](#)工具来查询指定的IP地址是否为华为云CDN节点IP地址，从而判断是否为运营商网络问题等原因造成的页面异常显示。

# 7 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   | 指在网络传输中丢失的数据包数量占发送数据包总数的比率。  |
| 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"><li>● <b>回源请求数比</b>：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。</li><li>● <b>回源流量比</b>：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。</li></ul>   |
| 缓存命中率 | 缓存命中率分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"><li>● <b>请求命中率</b> = 命中缓存的请求数 / 请求总数。</li><li>● <b>流量命中率</b> = 命中缓存产生的流量 / 请求总流量</li></ul> 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。<br><b>说明</b><br>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

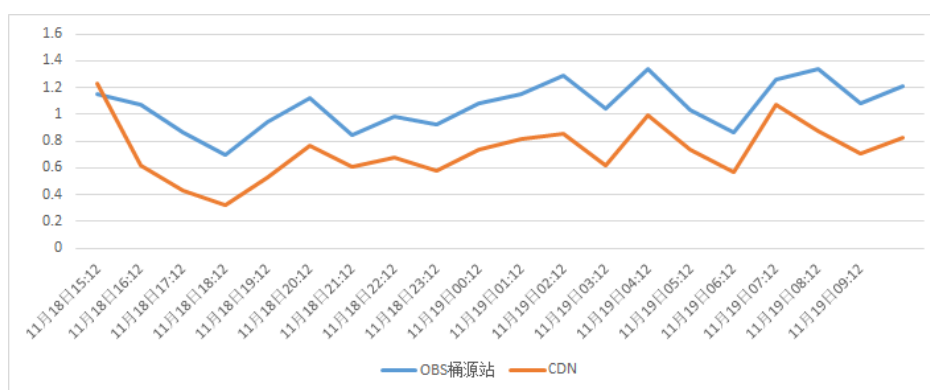
- 使用CDN后，时延、丢包率、回源率通常会降低，缓存命中率则会提高。但是由于业务场景和业务类型不同，即使您选择了相同配置的CDN服务，实际产生的加速效果也不相同，因此本文仅提供了定性的指标以供观测。
- 回源率、缓存命中率是指使用CDN后的衡量指标，如果您没有使用CDN，回源请求数为100%，缓存命中率为0。

## 加速案例

本次测试采用业内通用的**基线测速**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。

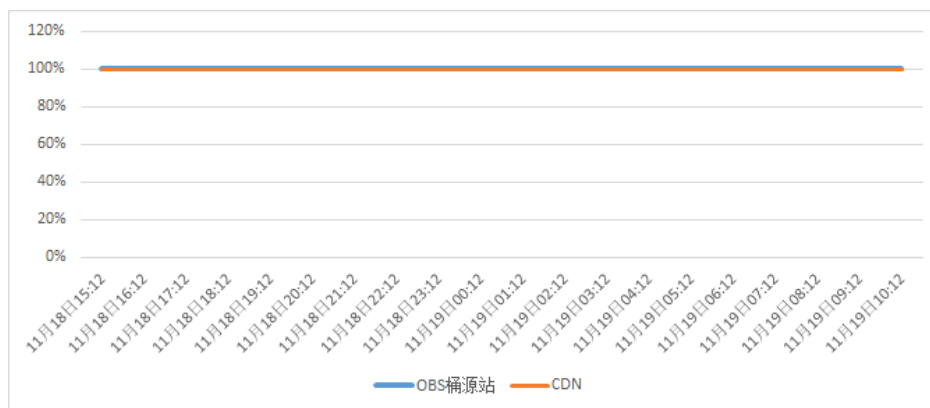
### 时延性能

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 |

# 8 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。例如，客户将example.com接入华为云CDN，那么example.com即为加速域名。用户访问加速域名时，解析到距用户最近的CDN节点，就近访问资源，达到加速目的。

## 源站

源站指用户的业务服务器，即被加速分发数据的来源。当客户端请求的资源在CDN节点无缓存时，节点会向源站发出请求，获取资源后返回给客户端并缓存在节点。源站可以是域名、IP地址、华为云对象存储OBS。

## 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。

## 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：

1. 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。

2. 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。
3. 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。

## 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。

## 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。

## SWR

SWR ( stale-while-revalidate ) 是HTTP响应头Cache-Control的一个字段，配置SWR字段值后，允许客户端在SWR有效期内请求已过期资源时，先返回过期资源给客户端，同时后台发起异步请求获取最新资源并缓存。

## 回源协议

指CDN节点回源获取资源时使用的协议，可选HTTP或者HTTPS。

## 回源失败率

CDN节点回源获取资源失败的概率，回源失败率 = 回源请求失败数 / 回源请求总数。

## 请求命中率

客户端请求命中CDN节点缓存的概率，请求命中率 = 命中缓存的请求数 / 请求总数。

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

| 限制项  | 说明   |
|------|--|
| 加速域名 | <p><b>域名基础规范：</b></p> <ul style="list-style-type: none"> <li>• 域名长度不能超过200个字符，支持大小写字母、数字、“-”、“.”“*”，“*”必须是首字符，首字符不能是“-”或“.”。</li> <li>• 域名单节点长度不超过63个字符，即：***.***.com中，***的字符数最多63个。</li> <li>• 每个账号最多支持加速100个域名。</li> <li>• 加速域名不允许重复添加。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul> <p><b>欠费及攻击处理规则：</b></p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul> <p><b>泛域名接入规范：</b>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"> <li>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。</li> <li>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。</li> </ol> <p><b>说明</b><br/>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：<br/>泛域名：*.a.com，子域名：1.a.com、2.a.com、3.a.com。<br/>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> |

## 安全限制

| 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"> <li>● 涉黄、涉赌、涉毒、涉诈、侵权内容的网站</li> <li>● 游戏私服类网站</li> <li>● 传奇类游戏和纸牌类游戏</li> <li>● 盗版游戏、盗版软件和盗版视频网站</li> <li>● P2P类金融网站</li> <li>● 彩票类网站</li> <li>● 违规医院和药品类网站</li> <li>● 网站无法正常访问或内容不含有任何实质信息</li> <li>● 虚拟货币，包括不限于挖矿、虚拟货币交易</li> <li>● 翻墙类应用：采用非正规渠道接连网络，包括不限于擅自建立、使用非法定信道进行国际联网；未经许可从事国际联网经营业务；未经批准擅自进行国际联网</li> </ul> <p>了解更多禁止的行为及禁止的内容，请参见<a href="#">可接受的使用政策</a>。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>● 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。</li> <li>● 如果发现加速域名有违规行为，CDN将封禁该域名，因违规而封禁的加速域名不可解禁。</li> <li>● 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。</li> </ul> |
| 突发带宽/QPS限流规则 | <p>根据您与华为云签订的《<a href="#">CDN服务协议</a>》，如果您在使用CDN服务过程中有突发带宽/QPS的需求（包括但不限于新功能发布、重大节假日、促销活动等），请至少提前3个工作日以工单的形式告知华为云CDN，以免业务受损。</p> <ul style="list-style-type: none"> <li>● 若申请不成功或未申请，则对于突发业务量，华为云有权采取限流等措施（华为云会根据实际情况综合评估）来保障全网用户的稳定性，由此导致的可用性问题的，华为云不承担责任。</li> <li>● 若申请不成功或未申请，QPS突增有可能会触发华为云CDN的防护规则，将域名切入沙箱。</li> </ul>   |

## 源站规范及限制

| 限制项 | 说明  |
|-----|---|
| 源站  | <ul style="list-style-type: none"> <li>● <b>源站数量：</b>每个加速域名最多可以添加50个源站。</li> <li>● <b>源站IP：</b> <ul style="list-style-type: none"> <li>- 使用IP作为源站地址时，CDN节点回源时直接访问该IP地址。</li> <li>- 支持配置IPv4，暂不支持IPv6。</li> </ul> </li> <li>● <b>源站域名：</b> <ul style="list-style-type: none"> <li>- 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。</li> <li>- 源站域名不能与加速域名相同。</li> <li>- 您也可以将“源站域名”设置为对象存储桶域名。</li> </ul> </li> </ul> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>● 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。</li> <li>● 不支持<b>私有桶</b>通过源站域名的形式接入CDN。</li> <li>● 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。</li> </ul> <ul style="list-style-type: none"> <li>● <b>OBS桶域名：</b>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<a href="#">CDN加速OBS计费规则</a>。 <ul style="list-style-type: none"> <li>- 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。</li> <li>- 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。</li> <li>- 如果OBS私有桶设置为源站，请开启<b>OBS委托授权</b>，同时勾选“私有桶”选项，否则将会导致回源失败。</li> <li>- 如果您使用<b>自定义OBS私有桶</b>作为源站，您需要为私有桶配置桶策略，配置详见<a href="#">自定义OBS私有桶策略配置</a>。</li> <li>- 如果您的OBS桶开启了<b>静态网站托管</b>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。</li> <li>- 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。</li> </ul> </li> </ul> |

## 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"><li>• 域名数量：100。</li><li>• 缓存刷新（文件）：2000条/日。</li><li>• 缓存刷新（目录）：100条/日。</li><li>• 缓存预热：1000条/日。</li></ul> <p>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，申请扩大配额的前提条件如下：</p> <ul style="list-style-type: none"><li>• 账号下域名的平均带宽日均峰值大于50Mbps，且无业务风险，可以提交工单申请扩大<b>域名数量</b>配额。</li><li>• 账号的日带宽峰值大于200Mbps，可以提交工单申请扩大<b>域名刷新/预热</b>配额，华为云CDN将根据您业务实际需求评估和配置。</li></ul> |

## 访问限制

| 限制项                                       | 说明  |
|---|---|
| 请求方式                                      | 常见的HTTP请求方式里面，CDN支持GET、HEAD、PUT、POST、DELETE、OPTIONS和PATCH这几种请求方式。   |
| HTTPS访问限制                                 | 如果客户端在发起与CDN节点的SSL握手时没有传递SNI信息，则CDN节点无法保证能够握手成功。  |
| URL长度限制、HTTP请求头长度限制、URL + 所有HTTP请求头的总长度限制 | <p><b>HTTP1.1场景下：</b>目前CDN的large_client_header_buffers值配置的是number=4、size=64 KB，即单个HTTP请求头和单个请求URL的长度，均不能超过64 KB，否则返回414错误码；并且所有HTTP请求头长度+URL的长度之和，不能超过256 KB，否则返回400错误码。</p> <p><b>HTTP2.0场景下：</b></p> <ul style="list-style-type: none"><li>• 默认Nginx参数http2_max_field_size=64 KB，即单个HTTP请求头和单个请求URL的长度，均不能超过64KB，否则将断开TCP连接。</li><li>• 默认Nginx参数http2_max_header_size=256 KB，表示所有HTTP请求头长度+URL的长度之和，不能超过256KB，否则将断开TCP连接。</li></ul> |

## 其他使用限制

| 限制项      | 说明  |
|----------|---|
| 回源       | <b>回源超时时间</b> ：CDN默认回源超时时间为30s。<br><b>源站HTTP响应头总大小限制</b> ：在源站返回CDN节点的信息里面，HTTP响应头的总大小不能超过16KB，否则会返回502错误状态码。                                      |
| 文件       | <b>文件上传</b> ：CDN支持上传文件，最大上传300M。  |
| 物联网卡访问限制 | 根据中华人民共和国工业和信息化部（简称：工信部）的相关规定（详见《关于印发〈物联网卡安全分类管理实施指引（试行）〉的通知》（工网安函[2020]1173号）），华为云CDN在中国大陆无法为使用物联网卡的终端提供加速服务，使用物联网卡的终端设备访问华为云CDN时，很可能会无法连接到节点IP。 |
| CNAME域名  | 华为云CDN产品的CNAME域名仅可以作为华为云CDN的调度解析使用，对于恶意使用CNAME域名的行为，华为云有权清退对应的域名和账号。  |

# 10 安全

## 10.1 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 10-1 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 <a href="#">HTTPS配置</a> 。 |
| 证书管理    | 华为云CDN支持批量配置SSL证书功能，详情请参见 <a href="#">证书管理</a> 。            |
| 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](#)。

## 10.2 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[云审计服务入门指引](#)。

- CDN支持审计的操作事件请参见[使用CTS审计CDN](#)。
- 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](#)。

# 11 权限管理

如果您需要对华为云上购买的CDN（Content Delivery Network，内容分发网络）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。如果华为账号已经能满足您的要求，不需要通过IAM对用户进行权限管理，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。

通过IAM，您可以通过授权控制他们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，您希望他们拥有CDN的使用权限，但是不希望他们拥有删除CDN等高危操作的权限，那么您可以使用IAM进行权限分配，通过授予用户仅能使用CDN，但是不允许删除CDN的权限，控制他们对CDN资源的使用范围。

目前IAM支持两类授权，一类是角色与策略授权，另一类为身份策略授权。

两者有如下的区别和关系：

表 11-1 角色授权与策略授权的区别

| 名称      | 核心关系       | 涉及的权限   | 授权方式       | 适用场景  |
|---------|------------|---|------------|---|
| 角色与策略授权 | 用户-权限-授权范围 | <ul style="list-style-type: none"><li>● 系统角色</li><li>● 系统策略</li><li>● 自定义策略</li></ul> | 为主体授予角色或策略 | 核心关系为“用户-权限-授权范围”，每个用户根据所需权限和所需授权范围进行授权，无法直接给用户授权，需要维护更多的用户组，且支持的条件键较少，难以满足细粒度精确权限控制需求，更适用于对细粒度权限管控要求较低的中小企业用户。 |

| 名称     | 核心关系  | 涉及的权限   | 授权方式   | 适用场景  |
|--------|-------|---|--|---|
| 身份策略授权 | 用户-策略 | <ul style="list-style-type: none"> <li>系统身份策略</li> <li>自定义身份策略</li> </ul> | <ul style="list-style-type: none"> <li>为主体授予身份策略</li> <li>身份策略附加至主体</li> </ul> | 核心关系为“用户-策略”，管理员可根据业务需求定制不同的访问控制策略，能够做到更细粒度更灵活的权限控制，新增资源时，对比角色与策略授权，基于身份策略的授权模型可以更快地直接给用户授权，灵活性更强，更方便，但相对应的，整体权限管控模型构建更加复杂，对相关人员专业能力要求更高，因此更适用于中大型企业。 |

例如：如果需要对IAM用户授予可以创建华北-北京四区域的ECS和华南-广州区域的OBS的权限，基于角色与策略授权的场景中，管理员需要创建两个自定义策略，并且为IAM用户同时授予这两个自定义策略才可以实现权限控制。在基于身份策略授权的场景中，管理员仅需要创建一个自定义身份策略，在身份策略中通过条件键“g:RequestedRegion”的配置即可达到身份策略对于授权区域的控制。将身份策略附加主体或为主体授予该身份策略即可获得相应权限，权限配置方式更细粒度更灵活。

两种授权场景下的策略/身份策略、授权项等并不互通，推荐使用身份策略进行授权。[角色与策略权限管理](#)和[身份策略权限管理](#)分别介绍两种模型的系统权限。

关于IAM的详细介绍，请参见[IAM产品介绍](#)。

## 角色与策略权限管理

CDN服务支持角色与策略授权。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。

如表1所示，包括了CDN的所有系统权限。角色与策略授权场景的系统策略与身份策略授权场景的并不互通。

表 11-2 CDN 系统权限

| 系统角色/策略名称                    | 描述             | 类别   | 依赖关系 |
|------------------------------|----------------|------|------|
| CDN LogsReadOnlyAccess       | 具有CDN日志服务只读权限。 | 系统策略 | 无    |
| CDN RefreshAndPreheat Access | 具有CDN刷新预热权限。   | 系统策略 | 无    |

| 系统角色/策略名称                     | 描述                | 类别   | 依赖关系 |
|-------------------------------|-------------------|------|------|
| CDN Administrator             | 具有CDN的所有执行权限。     | 系统角色 | 无    |
| CDN ReadOnlyAccess            | 具有CDN所有服务读权限。     | 系统策略 | 无    |
| CDN FullAccess                | 具有CDN的所有权限        | 系统策略 | 无    |
| CDN StatisticsReadOnly Access | 具有CDN统计服务只读权限。    | 系统策略 | 无    |
| CDN DomainConfiguration       | 具有CDN加速域名的配置权限。   | 系统策略 | 无    |
| CDN DomainReadOnlyAccess      | 具有CDN加速域名信息的只读权限。 | 系统策略 | 无    |

**表11-3**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 11-3** 常用操作与系统权限的关系

| 操作        | CDN Administrator | CDN ReadOnly Access | CDN StatisticsReadOnly Access | CDN LogsReadOnly Access | CDN Domain Configuration | CDN RefreshAndPreheat Access | CDN Full Access | CDN DomainReadOnly Access |
|-----------|-------------------|---------------------|-------------------------------|-------------------------|--------------------------|------------------------------|-----------------|---------------------------|
| 查询计费模式    | √                 | √                   | √                             | √                       | √                        | √                            | √               | √                         |
| 创建或修改计费模式 | √                 | x                   | x                             | x                       | x                        | x                            | √               | x                         |
| 查询域名统计数据  | √                 | √                   | √                             | x                       | x                        | x                            | √               | x                         |
| 日志查询      | √                 | √                   | x                             | √                       | x                        | x                            | √               | x                         |

| 操作       | CDN Administrator | CDN Read Only Access | CDN StatisticsRead Only Access | CDN LogsRead Only Access | CDN Domain Configuration | CDN RefreshAndPreheatAccess | CDN Full Access | CDN DomainRead Only Access |
|----------|-------------------|----------------------|--------------------------------|--------------------------|--------------------------|-----------------------------|-----------------|----------------------------|
| 查询域名所有配置 | √                 | √                    | x                              | x                        | √                        | x                           | √               | √                          |
| 修改域名所有配置 | √                 | x                    | x                              | x                        | √                        | x                           | √               | x                          |
| 创建加速域名   | √                 | x                    | x                              | x                        | √                        | x                           | √               | x                          |
| 查询账户信息   | √                 | √                    | x                              | x                        | √                        | x                           | √               | √                          |
| 修改账户信息   | √                 | 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 控制台功能依赖的角色或策略

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11-4](#)增加依赖服务的权限。

表 11-4 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  |
|--|--------------|---|
| <ul style="list-style-type: none"> <li>• OBS委托授权</li> <li>• SCM委托授权</li> </ul> | 统一身份认证服务 IAM | <ul style="list-style-type: none"> <li>• 创建委托：<br/>iam:agencies:createAgency</li> <li>• 查询指定条件下的委托列表：<br/>iam:agencies:listAgencies</li> <li>• 查询委托详情：<br/>iam:agencies:getAgency</li> <li>• 为委托授予项目服务权限：<br/>iam:permissions:grantRoleToAgencyOnProject</li> <li>• 查询委托是否拥有项目服务权限：<br/>iam:permissions:checkRoleForAgencyOnProject</li> <li>• 查询项目列表：<br/>iam:projects:listProjects</li> <li>• 查询权限列表：<br/>iam:roles:listRoles</li> <li>• 创建自定义策略：<br/>iam:roles:createRole</li> </ul> |
| 源站配置 <ul style="list-style-type: none"> <li>• 源站是OBS桶域名</li> </ul>             | 对象存储服务 OBS   | <ul style="list-style-type: none"> <li>• 列举全部桶：<br/>obs:bucket:ListAllMyBuckets</li> <li>• 列举桶内对象：<br/>obs:bucket:ListBucket</li> <li>• 判断桶是否存在并获取桶的元数据：<br/>obs:bucket:HeadBucket</li> </ul>   |
| SCM证书  | 云证书与管理服务 CCM | <ul style="list-style-type: none"> <li>• 查询证书列表：<br/>scm:cert:list</li> <li>• 导出证书：<br/>scm:cert:download</li> </ul>  |
| 按照标签筛选域名   | 标签管理服务 TMS   | 查询预定义标签：<br>tms:predefineTags:list  |
| 企业项目   | 企业管理         | <ul style="list-style-type: none"> <li>• 查询企业项目详情：<br/>eps:enterpriseProjects:get</li> <li>• 查询企业项目列表：<br/>eps:enterpriseProjects:list</li> </ul>   |

## 身份策略权限管理

CDN服务支持身份策略授权。如表11-5所示，包括了CDN身份策略中的所有系统身份策略。身份策略授权场景的系统身份策略与角色与策略授权场景的并不互通。

表 11-5 CDN 系统策略

| 系统策略名称                       | 描述                       | 策略类别   |
|------------------------------|--------------------------|--------|
| CDNAdministratorPolicy       | 对CDN的所有执行权限。             | 系统身份策略 |
| CDNReadOnlyPolicy            | 对CDN所有服务具有读权限。           | 系统身份策略 |
| CDNStatisticsReadOnlyPolicy  | 对CDN统计服务只读权限。            | 系统身份策略 |
| CDNLogsReadOnlyPolicy        | 对CDN日志服务只读权限。            | 系统身份策略 |
| CDNDomainConfigurationPolicy | 对CDN加速域名的配置权限。           | 系统身份策略 |
| CDNRefreshAndPreheatPolicy   | CDN刷新预热权限。               | 系统身份策略 |
| CDNFullPolicy                | 对CDN的所有执行权限。             | 系统身份策略 |
| CDNDomainReadOnlyPolicy      | 对CDN加速域名信息的只读权限。         | 系统身份策略 |
| CDNChargeConfigurationPolicy | 具有CDN计费服务开通、修改、查询计费模式权限。 | 系统身份策略 |

表11-6列出了CDN常用操作与系统身份策略的授权关系，您可以参照该表选择合适的系统身份策略。

表 11-6 常用操作与系统身份策略的关系

| 操作        | CDN Administrator Policy | CDN ReadOnlyPolicy | CDNStatisticsReadOnlyPolicy | CDNLogsReadOnlyPolicy | CDNDomainConfigurationPolicy | CDNRefreshAndPreheatPolicy | CDNFullPolicy | CDNDomainReadOnlyPolicy | CDNChargeConfigurationPolicy |
|-----------|--------------------------|--------------------|-----------------------------|-----------------------|------------------------------|----------------------------|---------------|-------------------------|------------------------------|
| 查询计费模式    | √                        | √                  | √                           | √                     | √                            | √                          | √             | √                       | √                            |
| 创建或修改计费模式 | √                        | x                  | x                           | x                     | x                            | x                          | √             | x                       | √                            |

| 操作       | CDN Administrator Policy | CDN ReadOnlyPolicy | CDN StatisticsReadOnlyPolicy | CDN LogsReadOnlyPolicy | CDN Domain Configuration Policy | CDN RefreshAndPreheat Policy | CDN Full Policy | CDN Domain Read Only Policy | CDN Change Configuration Policy |
|----------|--------------------------|--------------------|------------------------------|------------------------|---------------------------------|------------------------------|-----------------|-----------------------------|---------------------------------|
| 查询域名统计数据 | √                        | √                  | √                            | x                      | x                               | x                            | √               | x                           | x                               |
| 日志查询     | √                        | √                  | x                            | √                      | x                               | x                            | √               | x                           | x                               |
| 查询域名所有配置 | √                        | √                  | x                            | x                      | √                               | x                            | √               | √                           | √                               |
| 修改域名所有配置 | √                        | x                  | x                            | x                      | √                               | x                            | √               | x                           | x                               |
| 创建加速域名   | √                        | x                  | x                            | x                      | √                               | x                            | √               | x                           | x                               |
| 查询账户信息   | √                        | √                  | x                            | x                      | √                               | x                            | √               | √                           | x                               |
| 修改账户信息   | √                        | x                  | x                            | x                      | √                               | x                            | √               | √                           | x                               |

### 说明

不能单独配置CDN DomainConfigurationPolicy和CDN RefreshAndPreheatPolicy权限，如果想配置这两个权限，请同时配置CDN DomainReadOnlyPolicy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 控制台功能依赖的身份策略

CDN对其他云服务有诸多依赖关系，因此在您开启IAM系统身份策略授权后，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策略的集群权限，再按如下表11-7增加依赖服务的权限。

表 11-7 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"> <li>创建委托: iam:agencies:create</li> <li>查询委托详情: iam:agencies:list</li> <li>为委托授予项目服务权限: iam:agencies:grantRoleOnProject</li> <li>查询委托是否拥有项目服务权限: iam:agencies:checkRoleOnProject</li> <li>查询权限列表: iam:roles:list</li> <li>创建自定义策略: iam:roles:create</li> </ul> |
| 源站配置 <ul style="list-style-type: none"> <li>源站是OBS桶域名</li> </ul> | 对象存储服务 OBS   | <ul style="list-style-type: none"> <li>列举全部桶: obs:bucket:ListAllMyBuckets</li> <li>获取对象内容和对象元数据（源站是自定义OBS桶时需要此权限）: obs:object:GetObject</li> </ul>   |

相关链接

- [IAM产品介绍](#)
- [通过IAM进行授权](#)
- [权限和授权项说明](#)

# 12 与其他云服务的关系

表 12-1 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）           | <a href="#">CDN加速OBS桶文件方案概述</a>                 |
| 通过IAM服务实现以下功能： <ul style="list-style-type: none"><li>• 用户管理及权限设置：<ul style="list-style-type: none"><li>- 管理IAM用户和用户组</li><li>- 管理细粒度策略</li></ul></li><li>• 管理委托<br/>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。</li></ul> | 统一身份认证服务（Identity and Access Management, IAM） | <a href="#">用户权限</a><br><a href="#">OBS委托授权</a> |
| 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）               | <a href="#">审计</a>                              |
| 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）                 | <a href="#">企业项目</a>                            |