

腾讯云 CDN 产品白皮书

[2017 年 03 月 22 日]

[版本 2.0]



【版权声明】

©2015-2016 腾讯云 版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】



及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。

本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

目录

1	网络现状与 CDN 产品	7
1.1	互联网现状	7
1.2	CDN 产品简介	7
1.2.1	什么是 CDN	7
1.2.2	CDN 的基本原理	8
1.2.3	CDN 的通用功能	9
1.3	腾讯云 CDN 产品	10
1.3.1	腾讯云 CDN 简介	10
1.3.2	腾讯云 CDN 部署	11
1.3.3	腾讯云 CDN 优势	12
2	腾讯云 CDN 方案架构	14
2.1	方案概览	14
2.2	内容系统	15
2.2.1	DiskTank3 存储引擎	15
2.2.2	双层缓存架构	17
2.2.3	NWS 节点架构	18
2.2.4	TGW 负载均衡	18
2.2.5	大禹安全拦截系统	19
2.3	监控系统	21
2.3.1	立体化监控系统	21
2.3.2	海外专属监控系统	22
2.4	管理系统	23
2.4.1	GSLB	23

2.4.2	配置管理系统.....	24
3	腾讯云 CDN 平台方案.....	26
3.1	平台共有特性.....	26
3.1.1	HTTPS 优化.....	26
3.1.2	防盗链.....	31
3.2	网页加速平台.....	35
3.2.1	平台适用场景.....	35
3.2.2	平台架构.....	36
3.2.3	平台功能.....	37
3.3	下载加速平台.....	43
3.3.1	平台适用场景.....	43
3.3.2	平台架构.....	44
3.3.3	平台功能.....	45
3.4	点播加速平台.....	49
3.4.1	平台适用场景.....	50
3.4.2	平台架构.....	51
3.4.3	平台功能.....	52
3.5	直播加速平台.....	58
3.5.1	平台适用场景.....	59
3.5.2	平台架构.....	59
3.5.3	平台功能.....	61
4	接入指南.....	64
5	结语.....	67

图表目录

图 1 CDN 基础流程示意图.....	8
图 2 腾讯云发展历程.....	11
图 3 腾讯云国内节点分布图 (2017/03/10)	12
图 4 腾讯云平台架构.....	14
图 5 DiskTank3 绕过文件系统	16
图 6 TGW 工作示意图.....	19
图 7 大禹安全系统架构图.....	20
图 8 腾讯云 CDN 海外节点分布 (2017/03/10)	22
图 9 GLSB 工作架构图	24
图 10 某网站 SSL 安全测试结果	27
图 11 腾讯云 SSL 安全测试结果图	27
图 12 AES-NI 效果对比.....	29
图 13 Flase Start 流程图.....	30
图 14 URL 防盗链流程图	34
图 15 网页加速平台架构图.....	36
图 16 动态请求影响加载示意图.....	38
图 17 静态内容回源流程.....	39
图 18 动态加速请求流程图.....	40
图 19 传统 TCP 拥塞控制示意图.....	41
图 20 图片鉴黄系统示意图.....	42

图 21 下载平台架构图.....	44
图 22 下载直通车架构图.....	46
图 23 内容分发动态识别流程图.....	48
图 24 点播加速平台架构.....	51
图 25 服务端上传步骤图.....	54
图 26 UGC 视频上传流程图	56
图 27 直播平台流程图.....	59
图 28 多路备份.....	61
图 29 柔性系统分级策略.....	62
图 30 直播关键帧.....	63
图 31 CDN 开通认证步骤 1	64
图 32 CDN 开通认证步骤 2	64
图 33 选择 CDN 计费方式	65
图 34 CDN 接入方式.....	65
图 35 CDN 控制台概览.....	66
表 1 下载平台适用场景表.....	43
表 2 下载直通车对比优势.....	47
表 3 上传视频格式支持.....	52
表 4 部分预设封装格式.....	53

1 网络现状与 CDN 产品

1.1 互联网现状

随着中国互联网的高速发展，互联网早已成为社会生活必不可少的部分。据 CNNIC 在 2017 年 1 月发布的第 39 次《中国互联网统计报告》的统计，截至 2016 年 12 月，我国网民规模达 7.31 亿人，相当于欧洲总人口互联网普及率为 53.2%。手机上网使用率为 95.1%，移动互联网的全面普及改变了包括 CDN 在内的互联网相关服务。而移动互联网的复杂度在让加速和用户体验成为刚需的同时，为互联网相关企业提出了许多难题。

截至 2016 年 12 月，我国手机网上支付用户达到 4.69 亿，线下手机支付成为了一种习惯，移动网络越来越多的涉及支付、出行等对可靠性有一定要求的领域。对 CDN 产品的动态内容加速提出新的考验，不仅需要速度上的提升，还需要对请求的成功率、稳定性提出了新的要求。

截至 2016 年 12 月，中国国际网络出口带宽超过 6640Gbps，年增长率为 23.1%。不仅越来越多的企业走进中国，国内的互联网企业也在飞快的走向世界。海外 CDN 加速成为重要的能力。各大 CDN 厂商都在加快海外布局，为跨国企业提供缓存以及加速服务。腾讯云 CDN 在以上领域走在了业界的前列，不仅在依旧快速发展的视频直播、点播领域保持高速增长，腾讯云 CDN 海外的业务仅 2016 年增长 120%以上。

1.2 CDN 产品简介

1.2.1 什么是 CDN

为了解决互联网上越来越多内容的传输、存储、分发等问题，提供给终端用户更好的访

问和使用体验，CDN 便是一个高性价比，操作便捷，快速实现的解决方案。CDN (Content Delivery Network)，是在现有 Internet 中增加一层新的网络架构，由遍布全国的高性能加速节点构成。这些高性能的服务节点都会按照一定的缓存策略存储您的业务内容，当您的用户向您的某一业务内容发起请求时，请求会被调度至最接近用户的节点，直接由服务节点直接快速响应，有效降低用户访问延迟，提升可用性。

1.2.2 CDN 的基本原理

假设您的业务源站域名为 `www.test.com`，当域名接入 CDN 开始使用加速服务后，您的用户发起 HTTP 请求，实际的处理流程如图 1 CDN 基础流程示意图所示：

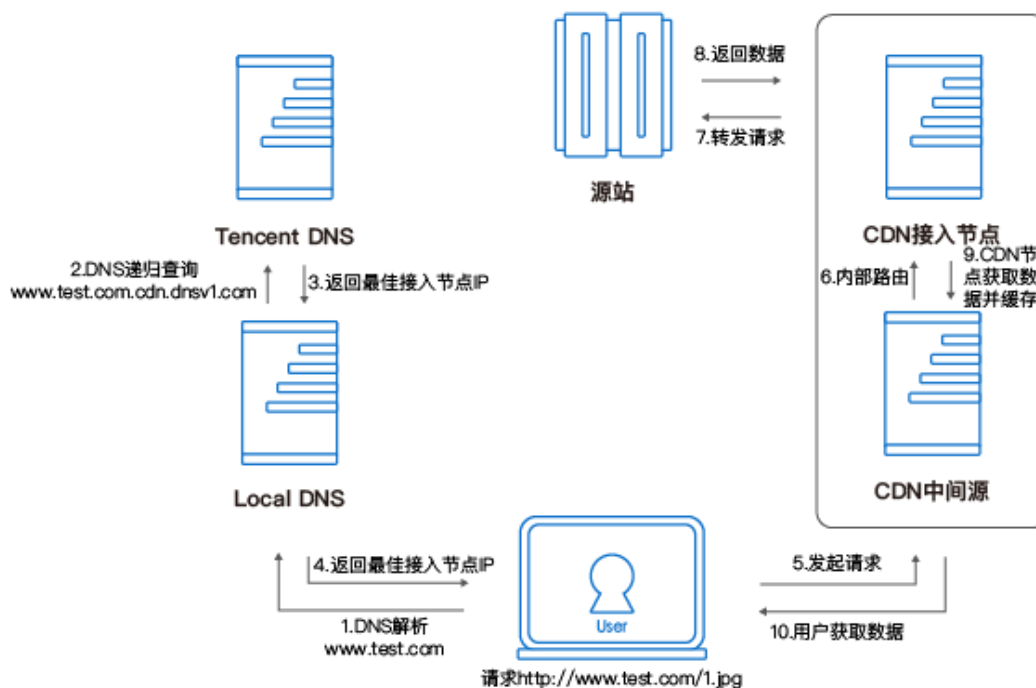


图 1 CDN 基础流程示意图

详细说明如下：

- 用户向 `www.test.com` 下的某图片资源，如 `1.jpg` 发起请求，先要向 Local DNS 发起域名解析请求；
- 当 Local DNS 解析 `www.test.com` 时，会发现已经配置了 CNAME `www.test.com.cdn.dnsv1.com`，解析请求会发送至 Tencent DNS (GSLB)，GSLB 为腾讯云自主研发的调度体系，会为请求分配最佳节点 IP；
- Local DNS 获取 Tencent DNS 返回的解析 IP；
- 用户测获取解析 IP；
- 用户向获取的 IP 发起对资源 `1.jpg` 的访问请求；
- 若该 IP 对应的节点缓存有 `1.jpg`，则会将数据直接返回给用户 (10)，此时请求结束。若该节点未缓存 `1.jpg`，则节点会向业务源站发起对 `1.jpg` 的请求 (6、7、8)，获取资源后，结合用户自定义配置的缓存策略 (可参考用户指南中缓存时间设置章节内容)，将资源存储 (9)，并返回给用户 (10)，此时请求结束。

1.2.3 CDN 的通用功能

1.2.3.1 提升客户体验

随着互联网的快速发展，网站内容已由传统的图文为主发展到以大量高清图片、流媒体内容为主，网站整体的资源消耗越来越大，对网络质量的要求也日益增高。另外，网民一方面希望网站内容越来越丰富，另一方面希望内容的访问的速度越来越快。对于网站而言，这是一个不得不面对的矛盾。

1.2.3.2 减少源站成本

目前视频行业格局趋于稳定，同质化现象严重，为增加用户粘性，一些网站花费重金购买优质的文案或视频内容，甚至与内容提供商合作自制内容，用户成本非常高。然而，随着上网带宽的提升，以及智能终端的普及，用户对网站和视频的展示以及播放质量的要求也越来越苛刻，如果网站服务质量差，可能导致用户流失，前期的投入打了水漂。越来越多的内容让源站的承载能力受到极大的挑战，如果斥巨资对源站进行扩容或者考虑用户访问进行分布式部署，成本的压力极大，而 CDN 是公认的最具性价比的解决方案。

1.2.3.3 网络安全防护

大部分网站在安全方面隐患严重，而目前网络上各类攻击愈演愈烈，历史上共出现 10 起超过 300 Gbps 的 DDoS 攻击，其中有七起发生在 2016 年。DDoS 攻击数量同比增长了 1 倍以上，原因主要是重复攻击和对同一目标的攻击次数增多。每个目标平均受到 29 次攻击。攻击方式复杂多样，攻击者利用多种协议进行攻击，防御困难。

除了攻击以外，内容的安全问题同样严峻。为了吸引用户，有财力支持的网站和公司大量购买影视剧的版权，用以吸引客户。2016 年以来，IP 的价值愈加被炒作。与此同时，无力购买版权的网站，往往通过盗链等方式窃取内容。即使以正版维权行动进行打击，依旧屡禁不止。安全问题也是腾讯云 CDN 希望协助内容提供商一起解决的问题。

1.3 腾讯云 CDN 产品

1.3.1 腾讯云 CDN 简介

基于腾讯自建的 CDN 平台，腾讯云打造了开放的 CDN 云产品，为互联网业务提供全面

稳定的 CDN 服务，将腾讯多年在 CDN 加速上积累的经验开放给广大互联网业务厂商。

腾讯自建 CDN 于 2007 年启动建设，历经 8 年时间，逐步打造了静态内容平台、游戏下载平台、UGC 加速平台、流媒体平台、动态加速平台等一系列创新而有价值的海量业务加速平台，服务于 Qzone、微信、QQ、腾讯视频、QQ 音乐、腾讯游、手机应用、腾讯云、、QTalk 等腾讯公司自营业务。腾讯 CDN 于 2013 年开始在腾讯云（QCloud）上逐步开放给外部用户使用，经过几年的发展形成了腾讯云 CDN 的产品和品牌。未来腾讯云 CDN 将开放更多的海量服务能力，为云上的用户提供更满足互联网业务需求的 CDN 加速服务。

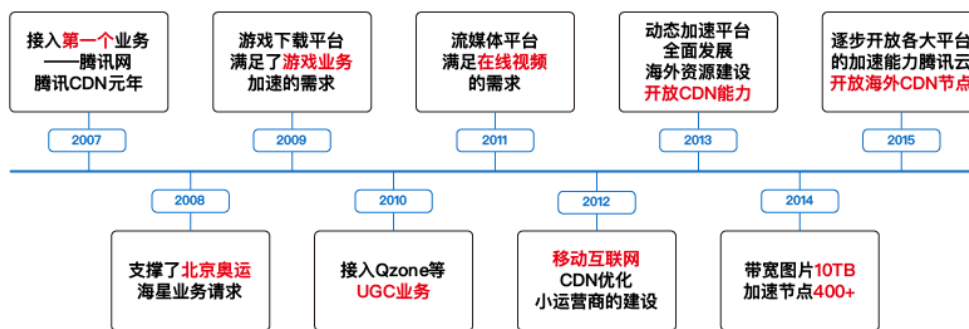


图 2 腾讯云发展历程

1.3.2 腾讯云 CDN 部署

截止 2017 年 3 月，腾讯云 CDN 在全国各省份部署 500+ 加速节点，覆盖移动、联通、电信及十几家中小型运营商，总 40T+ 资源储备。同时快速扩大海外布局，海外部署 50+ 加速节点，覆盖全球 30+ 国家地区。丰富的节点资源是提供稳定高质量服务的最佳保障。

CDN 的节点通常分为两类：合作类代理节点以及自部署网络节点。为了保障 CDN 网络的运维质量，做到从硬件开始的第一层保障，腾讯云 CDN 所有的节点均为自部署网络节点，甚至重金打造了高可用性，高负载的数据中转中心。腾讯云 CDN 的节点数目和质量的综合能力

目前在国内同行业 CDN 产品中名列第一。



图 3 腾讯云国内节点分布图（2017/03/10）

1.3.3 腾讯云 CDN 优势

- 稳定可信赖的自建 CDN

500+个节点、40T 带宽，每天都有超过 6 亿用户使用

与 QQ、微信、QQ 空间、腾讯视频享受同样的加速服务

- 追求极致的加速效果

海量用户实时收集访问时延，动态调整调度策略；

掌握全网链路质量，帮助用户获得最佳访问路径；

- 互联网业务的丰富经验

腾讯和外部业务的多年积累；

支持宽突发型、高 IO 型、大流量型等多种业务模型；

拥有突发事件、热点运营等解决方案；

- 计费灵活，项目管理

按需付费，可根据业务情况灵活修改计费方式，为您精打细算；

提供项目支持，方便进行企业内项目化管理。

- 灵活配置，丰富报表

提供缓存策略等配置项，灵活控制 CDN

实时监控告警，及时反馈问题

丰富的统计分析报表和日志信息，为您的业务决策助力

2 腾讯云 CDN 方案架构

2.1 方案概览

腾讯云 CDN 产品为了解决复杂多变网络环境下页面、动态、流媒体等内容访问速度慢、访问可用性不高的普遍问题，通过腾讯部署在全国各地的边缘、中间节点辅以涵盖全局的监控系统组成了 CDN 缓存网络，配备完善的运营管理系统，建成了涵盖“管理——内容——监控”的 QCloud CDN 架构平台。平台架构如图 4 所示：

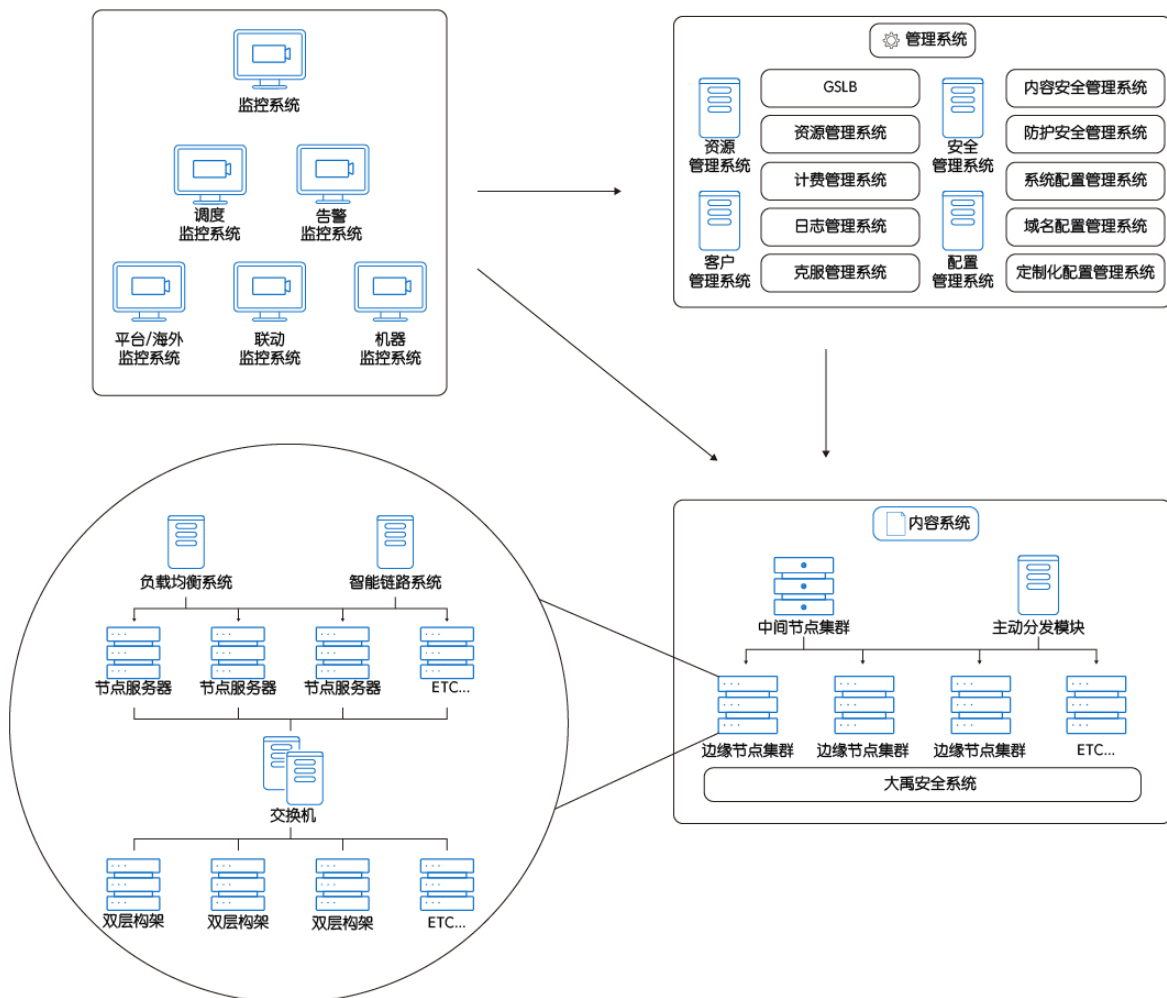


图 4 腾讯云平台架构

2.2 内容系统

2.2.1 DiskTank3 存储引擎

针对不同的大小文件，腾讯云 CDN 节点配备了 SSD 和 SATA 不同的硬盘机型。在提供足够的加速性能的同时，保证 CDN 边缘节点的命中率。但是目前 CDN 常用的缓存组件例如 SQUID 等无法在 SSD 和 SATA 盘上同时提供理想的效果，无法兼顾 IO 性能和加速效果，这限制 CDN 节点的服务能力。

DiskTank3 是腾讯云自研的第三代存储引擎，目前部署于线上所有机器中。

2.2.1.1 系统层优化

通用的缓存管理系统中，发现在内存吃紧时，即使 Page Cache 中还有空闲内存时，内核会使用 Swap 的内存，或者是回收内存带来额外的 CPU 开销等问题。同时，文件系统的元数据也会有 IO 的开销。而 CDN 的存储引擎可以自行进行缓存数据的管理，节省文件系统的开销。如下图所示，DiskTank3 支持越过文件系统直接使用裸盘读写，来完全解放磁盘 IO 性能。读写裸盘同时可以使用内核提供的异步 IO 功能，得以解放 CPU，进一步提高服务器的处理能力。

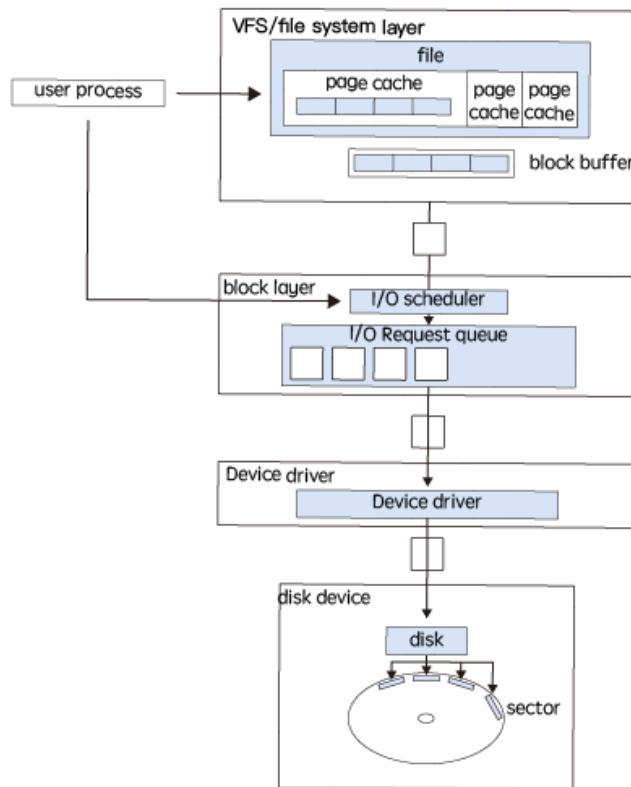


图 5 DiskTank3 绕过文件系统

2.2.1.2 文件分片存储

常用的文件系统使用连续的存储空间，当文件系统达到阈值，接收新文件的同时需要删除老文件，此时往往需要将整个老文件从缓存中删除。如果老文件较小，并不会造成影响。但是同时也存在为了存储一个 4KB 的小文件而将一个旧的 1GB 的文件删除的问题，如果大文件短时间内被请求，则需要再次回源或者到中间源节点获取。因此，在 DiskTank3 中，所有大文件都会被分成一个个小的数据分片进行存储。这样在淘汰时也只需要淘汰一个数据分片，在大文件被请求的时候，也只需要重新获取被删除的分片部分即可。这解决了缓存文件系统在淘汰大文件时引起大量回源流量的问题。

另外，使用分片存储的 CDN 缓存系统可以支持变长文件。这在源站只支持 HTTP Chunked

传输编码的情况下十分有用。传统文件系统由于在存储之前需要知道文件的确切大小，常用在内存中接受并缓存数据，等到接受完毕确定文件大小后，再存储到缓存中。DiskTank3 可以将数据直接写到缓存中，降低了内存和 CPU 开销。

2.2.1.3 元数据隔离

腾讯云 CDN 发现在许多场景下，元数据频繁的被读写。导致元数据的读写 IO 开销变得十分明显。而元数据与正常文件数据是存放在同一块磁盘中，这影响了正常文件数据的存取。因此，在 DiskTank3 中可以将元数据与文件数据分开存储。元数据可以存储在 IO 能力较强的 SSD 盘中，而文件数据则单独存储在数据盘中，规避元数据的 IO 开销。

2.2.1.4 单盘容灾

运营海量服务器的场景下，坏盘时有发生。如果等待服务器告警，再进行人工介入处理就需要比较长的响应时间，甚至影响服务器上业务的运行。新版本的 DiskTank3 支持将坏盘自动从缓存中剔除坏盘，坏盘问题不会中断业务的正常运行。坏盘在被剔除之后，缓存会在剩余的其他磁盘上重新 Hash 分布，不影响正常文件存取。该功能配合文件的分片存储，能将坏盘造成的影响减到最低。

2.2.2 双层缓存架构

通常的 CDN 边缘节点架构为单层架构，集群内的单机为了兼顾 CPU 的效率、成本，以及挂载硬盘的成本（SSD/机械硬盘），采用单层配置，如果在边缘节点无法缓存，便会直接回源或是到中间节点请求资源。此方案节点的命中率以及缓存的使用效率较低。

为了解决这个问题，腾讯云 CDN 在边缘节点和中间节点集群上采用双层缓存架构，即集

群内的缓存机器分为两层：

- 第一层的缓存机器挂载全 SSD 硬盘，兼顾速度以及处理的准确性；
- 第二层的缓存节点挂载海量机械硬盘，能够做到存储大量信息。在第一层缓存未命中的情况下，会优先向第二层缓存请求数据；
- 在两层缓存均未命中的情况下，才会向中间节点请求数据。

此方案能将边缘节点的命中率大大提升，实现了小而海量文件的处理以及读取速度的同时，顾及了大文件的存储以及达到一般 CDN 架构中中间节点前置的效果。达到存储和效率的最佳平衡。

2.2.3 NWS 节点架构

腾讯云 CDN 边缘节点均采用 NWS (Next Generation Webserver) 服务器为客户提供最优的服务性能，作为腾讯自研的高性能 HTTP 服务器，比常用的 nginx 等服务器，功能和性能上均有明显提升：

NWS 不使用多进程的机制，而是采用单进程多线程事件驱动模型。每个链接由独立线程处理，减少上下文切换带来的开销，进程间的调度更节省时间和性能。

2.2.4 TGW 负载均衡

TGW , 全称 Tencent Gateway , 是一套实现多网统一接入 , 支持自动负载均衡的系统。TGW 具有可靠性高 , 扩展性强 , 性能高 , 抗攻击能力强等特点。在用户新建连接时 , TGW 根据 server 的权重选择一个 server , 并建立用户端到 server 的会话信息 ; 对于已经建立连接的用户数据 , 根据会话信息 , 请求会转发到对应的 server 上 , 这样就达到了负载均衡的目的。

除了常用的负载均衡以外 TGW 通过多通接入来解决跨运营商访问延时大的问题。多通接入基本原理是：TGW 把外网不同运营商的请求，通过内网隧道转发给 server，server 返回数据时，再把数据通过内网隧道返回给 TGW，再由 TGW 发送给不同的运营商。这样通过 TGW，腾讯云 CDN 节点同时解决了多线节点的跨网互通问题。



图 6 TGW 工作示意图

2.2.5 大禹安全拦截系统

大禹网络安全平台（Dayu Distributed Defense）是腾讯云部署了超 100+节点遍布全国，4T 带宽互为备份的综合防攻击安全平台，能够为多种业务场景的开发商提供专业 DDoS 防护服务。其能提供的安全防护能力同时覆盖 CC 攻击防护、Web 入侵防护等，通过高效动态调度，有效组织起腾讯云全网各点冗余带宽和防护能力，保证服务在被大流量攻击情况下保持业务平滑。在防海量攻击安全之余避免黑客入侵篡改保护网站信息，同时为最易受到攻击行业网站制定专属策略，针对特殊类型攻击实时抓包并制定特殊策略。同时针对不同行业 and 情况配置两个子产品：

- 大禹 BGP（BGPAntiDDoS）高防是腾讯云针对游戏、金融、网站等用户遭受大流量 DDoS 攻击时服务不可用的情况推出的增值服务。高达 300G 的防护服务和多达 21 线

的 BGP 线路，让您的业务不再畏惧 DDoS 攻击的挑战，同时拥有极速的访问体验。

- 大禹网站高防（WebsiteAntiDDoS）是针对网站用户在遭受大流量 DDoS 攻击时导致服务不可用的情况推出的增值服务。您可通过配置网站高防，将流量引流至大禹网站高防系统，对攻击流量进行清洗，确保源站能稳定可靠地提供服务。

腾讯云 CDN 包含自动切换防御平台的功能，当检测到客户域名在遭受攻击时，会自动客户的域名切换至大禹平台，保障客户服务的持续性以及安全性。在攻击后再自动切换回加速平台。这种策略能在保障客户加速质量的前提下，尽可能的将客户可能遇到的突发攻击对平台以及客户服务造成的影响降至最少。

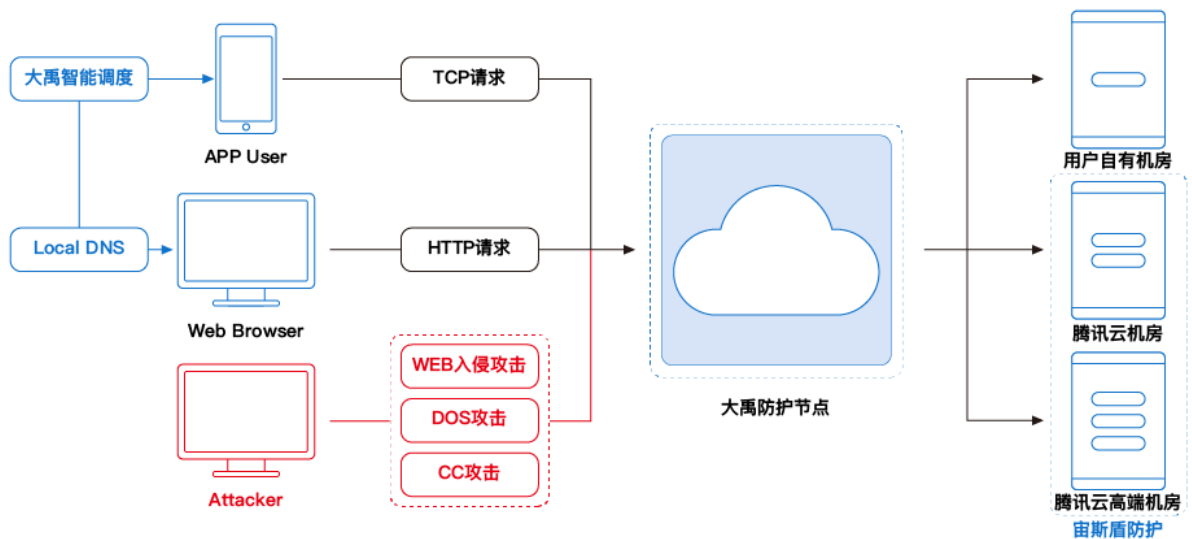


图 7 大禹安全系统架构图

在大禹安全拦截系统中，利用了 SynX 抗 DDOS 攻击安全模块，这是腾讯云自研的针对 DDOS 攻击包特征进行针对性识别分析的模块，能够高效快速的过滤恶意攻击数据包，清洗出正常流量。SynX 直接在网卡中断钩子上加入过滤器筛选数据包，这样可以显著提高系统的

包处理能力。经过 SynX 优化后的单集群节点可以很轻易的抵御 10Mpps, 5Gbps 的 Synflood 攻击以及超过 1300Mpps, 8Gbps 的 UDP 攻击

2.3 监控系统

2.3.1 立体化监控系统

立体化监控是一种多维度、全方位的监控方式，旨在从各个层面对 CDN 节点的服务器状况做出监控和评估，进而调整全网的流量分布状况，保证用户业务服务处于最优状态。从底层开始，依托腾讯云内部的操作系统发行版本 TLinux，系统能够对硬件基础数据做全面监控；依托腾讯云自研的高性能 Web 服务器 NWS，系统能够实时采集当前的应用层访问数据和访问质量；依托外部系统的测试（专用拨测点、QQ 客户端），能够采集精准采集全国网络访问质量。综合这些数据，腾讯云 CDN 能够实时调整服务质量，为用户提供最优质的 CDN 服务。

立体化监控手段：

- 单机节点健康监控：从网络层面和硬件层面收集 CPU/IO/Network 状态，监控节点到用户的最后一公里体验指标监控
- CDN 平台多维度监控：实时监控 NWS 架构的日志，把握 CDN 的运营质量，做到主动的告警处理而不是被动的响应。
- 联动测试运营系统：腾讯云有许多可参考测试的终端和方式。腾讯自营最大的业务 QQ、微信等使用的是同一个平台，海量的网络数据形成了一张覆盖全地区无死角的“网络交通地图”，作为 CDN 和云厂商中用户最多覆盖最广的公司，腾讯云 CDN 能

在第一时间采集到真实的网络质量，进一步去调整线上节点的覆盖情况。

2.3.2 海外专属监控系统

腾讯云的海外节点横跨五大洲，提供超过 50 个海外加速集群，合计超过 2T 的带宽。目前海外加速的市场愈加成为腾讯云 CDN 拓展的重点。

但是海外 CDN 在监控以及运维上完全不同于国内的 CDN 节点，

- 硬件服务上海外 CDN 节点的运维更加依托于精确快速的监控系统，海外专用监控系统的严格限制保证第一时间会将节点集群可能发生的问题自动过滤或通知到运维人员处；
- 跨国间的网络质量通常比国内的网络连通质量差，腾讯云 CDN 通过调整 BBR 拥塞算法等手段很好的解决了跨国传输的瓶颈。但是依旧需要完备的监控系统，保证尤其是动态加速等服务的顺利运营，当监控体系检测跨国链路的延迟时，会自动重新计算并切换链路，保障国际网络的健康运行。



图 8 腾讯云 CDN 海外节点分布（2017/03/10）

2.4 管理系统

腾讯云的管理系统主要由四大系统构成：资源管理系统、安全管理系统、配置管理系统以及客户管理系统组成。主要以业务划分。从单机情况的管理到每个域名和平台的配置管理，到以客户为维度的综合管理，均配置完善的管理体系。另外安全作为最重要的体系之一独立进行管理配置。以下为各系统重要技术分析：

2.4.1 GSLB

资源管理系统包括 GSLB (全局负载均衡系统) 负责资源的调度方案，以及资源管理系统负责资源的统筹和管理。目前主要的 CDN 调度方式依旧是依赖 DNS 地址进行就近分配节点，但是由于中国的复杂网络情况以及运营商 IP 库以及出口的不规范，经常存在调度失误的现象。

GSLB (全局负载均衡) 可以对腾讯云 CDN 节点服务器状态及用户方位时延情况进行实时监控，并将监控数据实施同步到调度决策模块，调度决策模块根据亮相结果进行分析计算，将高可用的节点信息同步到域名解析系统中，域名解析系统给出高可用的节点信息。如图 9：

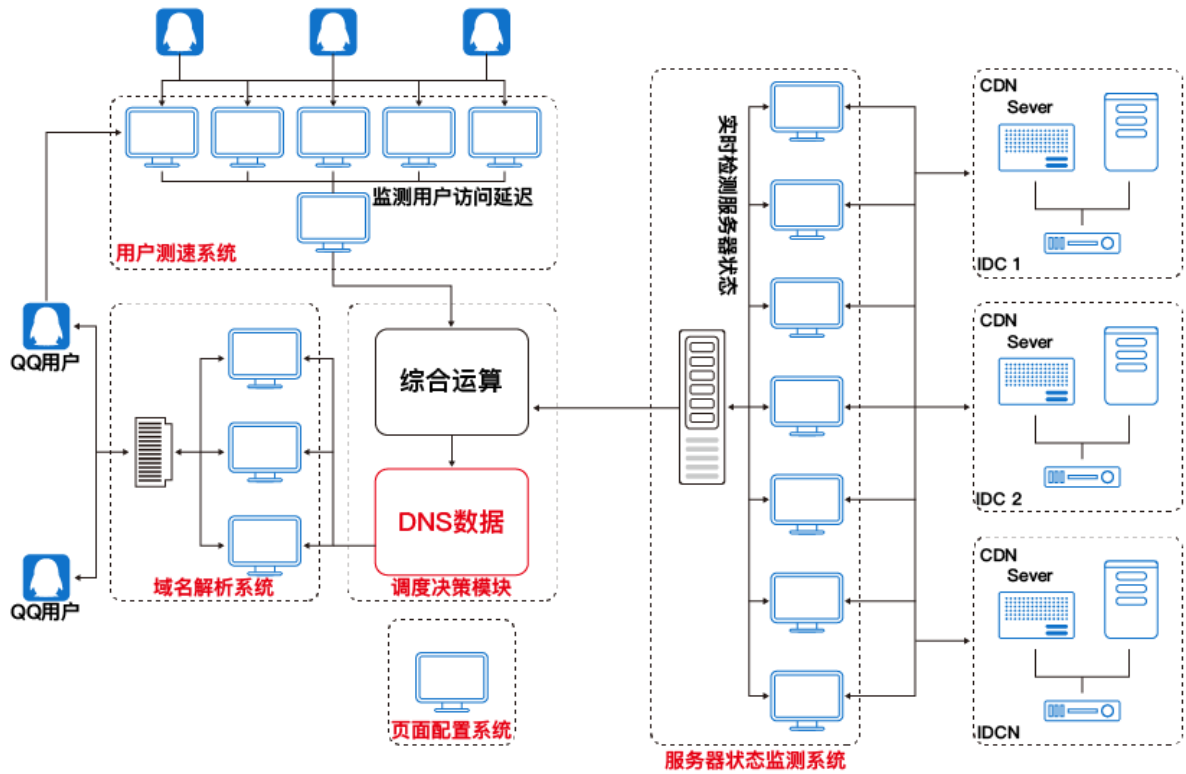


图 9 GLSB 工作架构图

该方案不仅支持标准的 DNS 协议接入，同时提供 HttpDNS 的接入方案，在保证调度质量的情况下，HttpDNS 也能起到防止流量被 DNS 劫持的问题，兼顾了调度的准确性和安全性。

2.4.2 配置管理系统

配置管理系统包括系统配置管理系统、域名配置管理系统以及定制化配置管理系统。

- 系统管理配置：用于下发 CDN 系统管理项，维护系统的运营以及全局的部分策略；
- 域名管理系统：CDN 系统通常需要 20 分钟~30 分钟做到配置下发。而腾讯云 CDN 依托分布式的域名配置管理服务器，以 CDN 的思维逐级快速传递配置，能做到 5 分钟内域名配置下发，全网部署生效。极高效的部署效率能保证域名的配置能在第一时间生效成功。

- 定制化配置管理系统：腾讯云 CDN 承接许多客户定制化需求，但是客户的定制化需求和标准功能配置区分管理，防止了可能产生的功能影响，保障线上客户的通用功能正常运营且迎合定制化需求方案。

3 腾讯云 CDN 平台方案

腾讯云 CDN 平台根据加速内容的不同，分为网页加速平台、下载加速平台、点播加速平台和直播加速平台。各平台虽然有所不同，但是具有一些相同的功能特性。

3.1 平台共有特性

3.1.1 HTTPS 优化

从 2015 年初开始，为了提升网站安全性以及防止流量劫持，广告植入等问题，各大网站纷纷启用 HTTPS，其中百度，阿里更是先后实现了全站的 HTTPS 方案。但是根据 Google 的性能数据，针对 1024 位的证书，CPU 单核性能大约为 1500 CPS (Connection Per Second)。由于 SSL 加密中的非对称加密消耗大量 CPU 资源，对源站改造造成的成本和压力较大。如果是针对 2048 位证书，CPU 的 CPS 更是下降到 300~800 CPS，对比 HTTP 请求，性能下降 6~8 倍，下降了一个数量级。如果需要在性能相当的情况下进行改造，需要付出一定的硬件成本和人力成本。

SSL 证书意味着使用 HTTPS 协议，但是并不意味着有着相同的安全性。即使购买的证书和使用的服务符合苹果推荐的 ATS 协议：

- 服务端必须支持 TLS 1.2 或以上版本；
- 必须使用支持前向保密的密码；
- 证书必须使用 SHA-256 或者更好的签名 hash 算法来签名等

但是还有许多因素制约着实际使用 HTTPS 的安全，著名的网站 SSLLABS.COM 提供了针对 HTTPS 安全的评估方案。

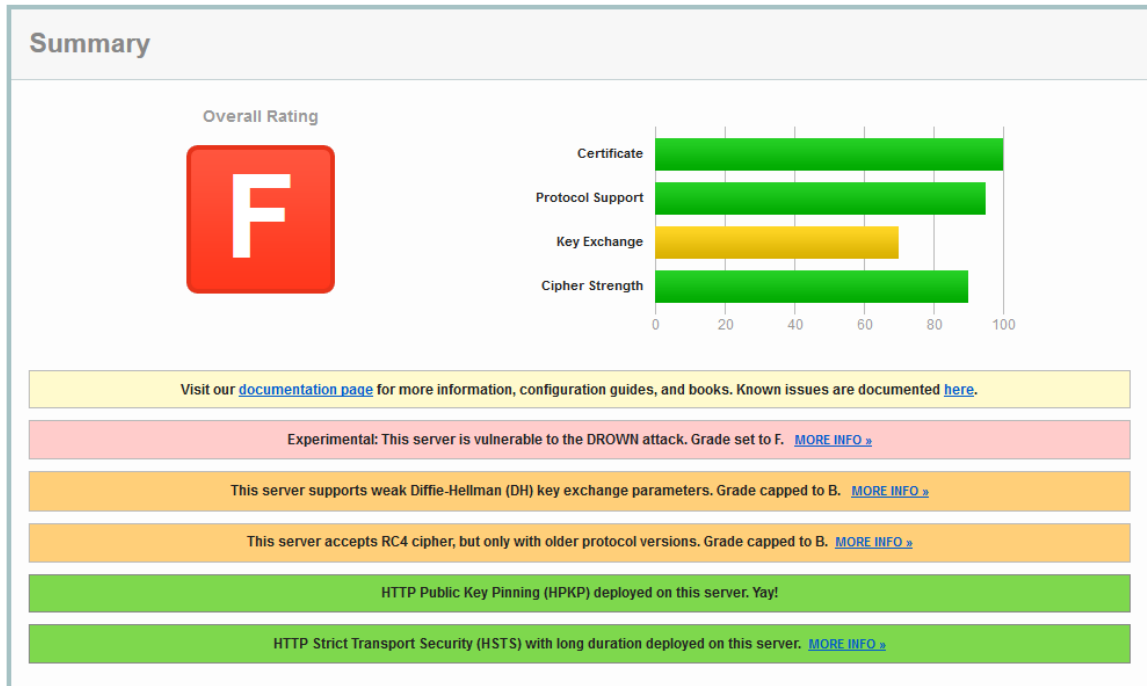


图 10 某网站 SSL 安全测试结果

如图 10 所示，即时在证书购买合规的情况下，CDN 平台的整体安全策略和措施决定了最后的 SSL 安全等级评定。

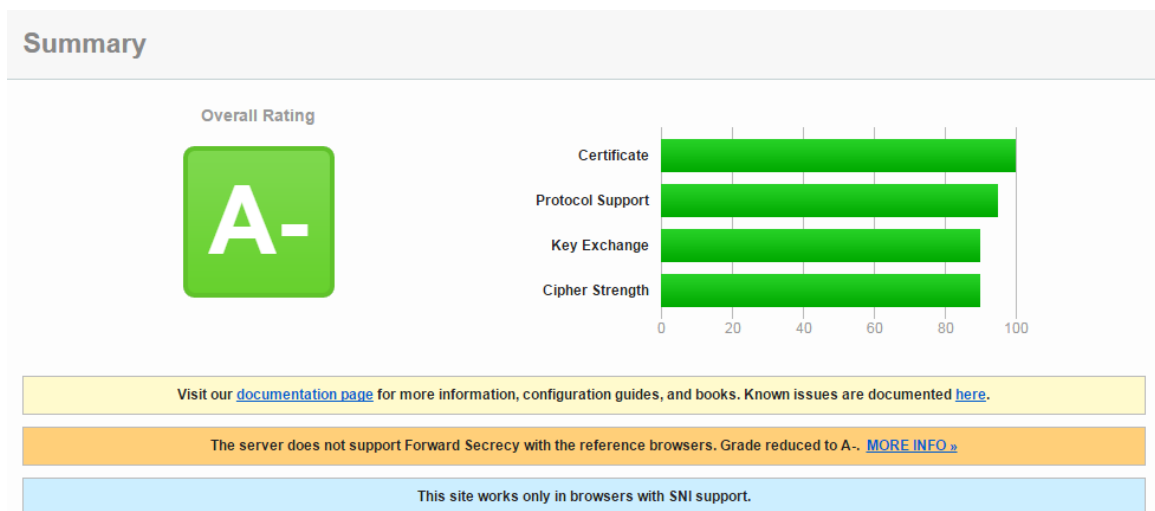


图 11 腾讯云 SSL 安全测试结果图

如图 11，腾讯云 CDN 全平台达到了 A 的保护等级。

3.1.1.1 证书方案

腾讯云 CDN 的 HTTPS 证书方案可以分为三种，分别是

- 针对源站便捷快速改造的半程 HTTPS 方案，由终端至腾讯云 CDN 实现腾讯云 CDN 证书加密，HTTPS 传输，由腾讯云 CDN 系统回源实现 HTTP 回源，源站不需要任何修改；
- 针对源站部署客户证书，但是不便于对外提供的客户，由终端至腾讯云 CDN 实现腾讯云 CDN 证书加密，HTTPS 传输，由腾讯云 CDN 回源实现客户证书回源，源站不需要提供证书；
- 针对源站部署客户证书，同时可以对外提供的客户，可以实现从终端至源站全程的客户证书加速。

客户可随意在三个证书方案中选择适合自身情况的证书部署方案。

3.1.1.2 加速技术

3.1.1.2.1 SNI 快速部署

在旧的 CDN 系统部署方式中(目前许多 CDN 平台依旧在沿用旧式设计)，由于在 SSL 握手的过程中不会传递域名这条信息，所以服务器端通常返回的是配置中的第一个可用证书；如果要使用多个证书呢，就只能配置不同的 SSL 端口或增加 IP 地址，或者可以花重金使用一个“多域名 SSL 证书”或一个“通配型证书”来达到相同效果。所以 CDN 希望在节点上部署证书，需要以绑定 IP 的方式绑定证书。导致流程漫长，修改和调整覆盖均非常繁琐。

SNI (Server Name Indication) 是一项用于改善 SSL/TLS 的技术，在 SSLv3/TLSv1 中被启

用。它允许客户端在发起 SSL 握手请求时，就提交请求的 Host 信息，使得服务器能够切换到正确的域并返回相应的证书。这样对于 CDN 系统而言意义重大，证书部署和调整的流程大大缩短，调整资源覆盖以及问题反馈的时间大大缩短。

3.1.1.2.2 AES-NI

AES-GCM 也是目前最为流行的对称加密算法。虽然 AES-GCM 解决了对称加密存在的安全问题，但带来了性能问题。为此，Intel 官方推出 AES-NI (Advanced Encryption Standard New Instruction)。AES-NI 是 Intel 和 AMD 微处理器上 x86 架构的一个扩展，可以从硬件上加速 AES 的性能，目前在服务器和 PC 端，CPU 对 AES-NI 的支持率已经非常普及。

如图 12，Intel 官方公布，服务器开启 AES-NI 后，性能提高了 5-8 倍左右。

AES-128-GCM在开启AES-NI和关闭AES-NI

AES-128-GCM	开启AES-NI	关闭AES-NI
16 Bytes	404141.90	72163.37
64 Bytes	994097.92	96301.44
256 Bytes	1421557.93	215897.60
1024 Bytes	1515602.94	231689.22
8192 Bytes	1529460.05	235077.63

图 12 AES-NI 效果对比

3.1.1.2.3 Flase start

TLS False Start 是指客户端在发送 Change Cipher Spec Finished 同时(SSL 握手第二阶段)发送应用数据(如 HTTP 请求)，服务端在 TLS 握手完成时直接返回应用数据(如 HTTP 响应)。这样，应用数据的发送实际上并未等到握手全部完成。这个过程如图 13 所示：

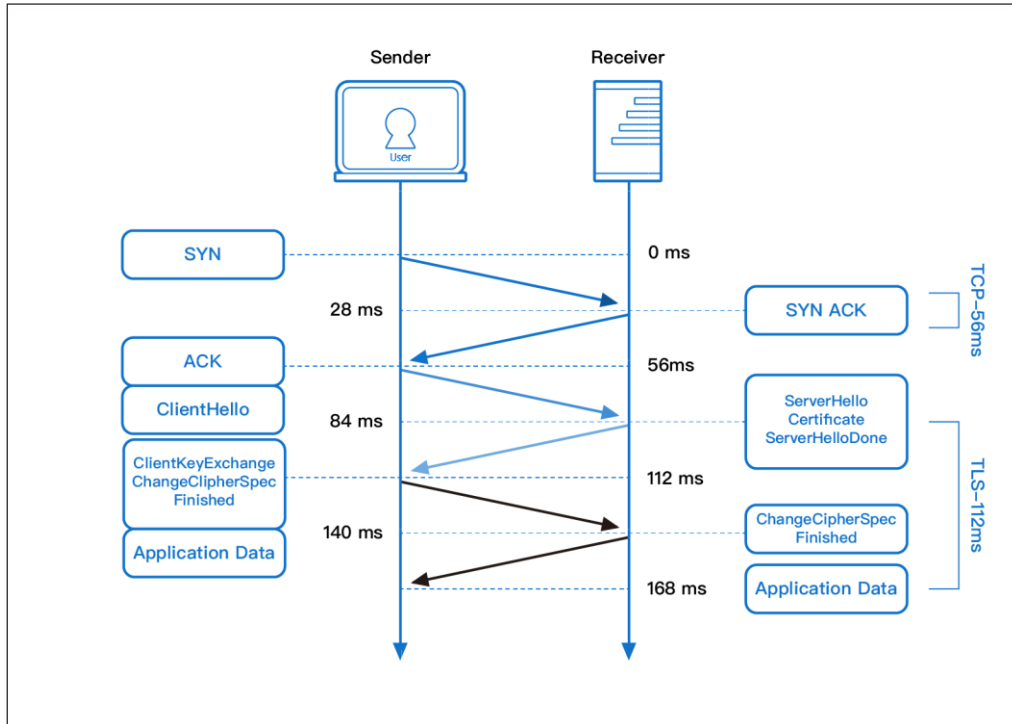


图 13 False Start 流程图

可以看到，启用 False Start 之后，TLS 阶段只需要一次 RTT 就可以开始传输应用数据。

False Start 相当于客户端提前发送加密后的应用数据，节省一次的 RTT 时间，而且不需要修改 TLS 协议，目前大部分浏览器默认都会启用。

3.1.1.2.4 OCSP STAPLING

出于某些原因，证书颁发者有时候需要作废某些证书。证书使用者通常有两种方式判定证书失效：CRL（Certificate Revocation List，证书撤销名单）和 OCSP（Online Certificate Status Protocol，在线证书状态协议）。

但是某些客户端会在 TLS 握手阶段进一步协商时，实时查询 OCSP 接口，并在获得结果前阻塞后续流程，这对性能影响很大。而 OCSP Stapling，是指服务端在证书链中包含颁发机构对证书的 OCSP 查询结果，从而让浏览器跳过自己去验证的过程。服务端有更快的网络，获取 OCSP 响应更容易，也可以将 OCSP 响应缓存起来。

OCSP 响应本身是加密过的，无法伪造，所以 OCSP Stapling 技术既提高了握手效率，也不会影响安全性。

3.1.1.2.5 HTTP/2 加速

历史悠久的超文本传输协议，即 HTTP 标准近期进行了升级。HTTP/2 在 2015 年 5 月被批准，目前已经在很多 Web 浏览器和服务器中得到实现（包括 NGINX Plus 和开源 NGINX）。大约有三分之二的浏览器已经支持 HTTP/2。

HTTP/2 的重要特性完全源自 SPDY，包括但不限于：

- HTTP/2 是二进制（而文本）协议，因此更简洁高效；
- 它针对每个域只使用一个多路复用的连接，而不是每个文件一个连接；
- 请求头部使用特制的 HPACK 协议（而非 SPDY 中使用的 gzip）压缩；
- 腾讯云 CDN 平台支持 HTTP/2 协议，对 HTTPS 而言，加速效果显著。

3.1.2 防盗链

盗链是指服务提供商自己不提供服务的内容，通过技术手段绕过其它有利益的最终用户界面（如广告），直接在自己的网站上向最终用户提供其它服务提供商的服务内容，骗取最终用户的浏览和点击率。受益者不提供资源或提供很少的资源，而真正的服务提供商却得不到任何的收益。

为了满足绝大多数客户的防盗链需求，腾讯云 CDN 对外提供 4 种防盗链的方式：

3.1.2.1 Referer 防盗链

3.1.2.1.1 实现原理

通过 http referer 过滤请求内容返回对应信息的配置。http referer 是 http 请求包包头的一部分，当浏览器向 web 服务器发送请求时，会带上 referer，告诉服务器此请求是从哪个链接而来，从而可进行信息的处理。

3.1.2.1.2 注意事项

- Referer 黑名单、白名单二者不兼容，同一时间只能生效一种类型；
- 当防盗链黑、白名单为空时，等同于关闭防盗链，防盗链规则不生效；
- 防盗链输入内容最多可输 200 条；
- 防盗链规则匹配的设定如下：
 - 支持域名/ip 规则，且为前缀匹配。
 - 支持域名前缀通配符。
 - Referer 为空（即指用户在浏览器中直接访问域名，则 Referer 为空），空 Referer 默认不匹配任何规则。
 - 包含空 Referer: 包含空 Referer 即指：选择 Referer 白名单时，白名单中包含空的 Referer（即：通过浏览器地址栏直接访问该资源 URL）时，CDN 将正常返回资源信息。

3.1.2.2 User-Agent 防盗链

User-Agent 头部包含了发起原始请求的客户端（通常是指浏览器）信息。不同的客户端通常具有不同的 User-Agent 信息。和 Referer 类似，腾讯云 CDN 支持针对 HTTP 请求头中的 User-Agent 信息，禁止或者允许符合特定 User-Agent 规则（支持正则匹配）的请求。但是由于 User-Agent 很容易伪造，因此 User-Agent 防盗链安全性较低。

适用场景举例：

1) 某个页面或者资源只希望被 IE 浏览器访问，不希望或者不支持被 Chrome 访问，这种情况下就可以配置 User-Agent 防盗链

2) 客户有自己专属的客户端下载工具进行内容下载，该下载工具在请求时 User-Agent 使用了自己定制的名称，希望只针对符合这种规则的请求开放下载，这种情况下也可以使用 User-Agent 防盗链。

3.1.2.3 URL 加密防盗链

URL 加密防盗链是一种保护用户视频内容安全的功能。通过使用此功能，用户可实时自行生成可用于播放器环境或 URL 访问的播放链接，该链接在用户指定时间内可用，从而有效保护视频内容。由于防盗链采用动态生成方式，该功能开启后，原有播放器代码和文件 URL 将不可用。

3.1.2.3.1 实现原理和步骤

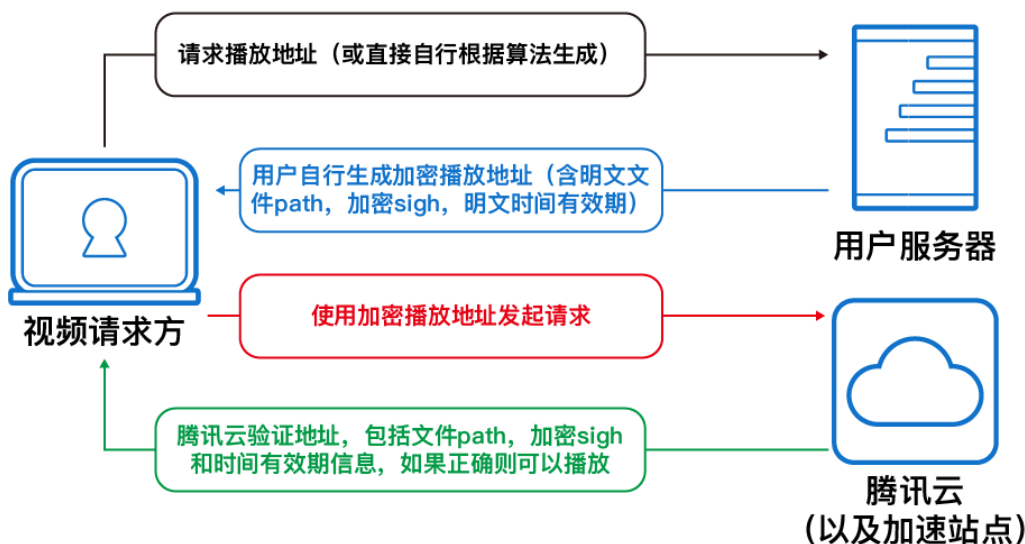


图 14 URL 防盗链流程图

1. 开启服务和获取密钥：客户申请开启此功能后，腾讯将为客户发送密钥 KEY，用户妥善保管该密钥。
2. 生成加密播放地址：文件或视频请求方在发起请求时，可以根据公开算法，自行生成或由用户服务器侧自行计算访问地址，最终生成的访问地址格式类似为：
 http://www.test.com/folder/vodfile.mp4?sign=abc123dsaadsasdads&t=55bb9b80 字段生成方法如下：sign=abc123dsaadsasdads（示例）：为校验串，算法为：
 $sign = MD5(KEY + path + t)$ ，字母小写。其中：
 - a) KEY：为 1 中腾讯云 CDN 为客户分配的密钥；
 - b) path：URL 中文件路径部分，不包括“?”之后的字符，示例中是/folder/vodfile.mp4；

- c) t :该链接有效的截止时间戳 ,示例是 4d024e80 ,为 UNIX 时间戳的 16 进制表示。
3. 文件或视频请求方根据以上计算结果 , 组成链接 , 发起请求至腾讯云以及其 CDN ;
 4. 腾讯云进行验证并判断是否播放 : 腾讯云首先会根据明文中有效的截止时间戳判断当前时间是否过期 , 如果未过期再验证校验串是否正确。有且仅有在两个条件均符合的情况下才会允许视频的播放或文件的请求。

3.2 网页加速平台

腾讯云 CDN 的网页加速平台是专门针对网页图片进行深度优化的加速方案。针对网页文件普遍为中小图片文件 , 更新频繁且数目巨大以及动态请求占比较高的特点进行了优化。同时 , 制定了动态加速、图片无损压缩优化等专门针对网页动静态内容加速的策略。做到快速分发内容 , 智能路由回源 , 解决了终端用户访问各种内容可能产生的访问延迟问题 , 大致具有以下效果 :

- 用户端 : 提升访问速度和访问质量 (可用性);
- 源站端 : 减少回源量 , 降低源站压力 , 减少源站投入 ;
- 业务端 : 应对可能的带宽突增 , 保证服务质量稳定 , 业务顺利运营 ;
- 运维端 : 保证源站安全运维 , 防止恶意入侵和海量攻击。同时提供内容完整 , 数据准确的用户日志和多维度数据统计分析系统 , 保证运维时刻掌握系统情况 ;

3.2.1 平台适用场景

网页加速平台主要用于解决当前复杂网络环境下 (尤其是移动互联网环境下) 各类 PC/ 手机网站以及移动 APP 访问速度慢、可用性偏低的问题。 主要适用于 HTTPS/HTTP 协议进行

传输的内容，尤其对含有大量图文内容的页面、应用有很好的加速效果。例如门户网站、电子商务平台、游戏、阅读资讯、社交、生活工具、政府网站、办公系统等。

3.2.2 平台架构

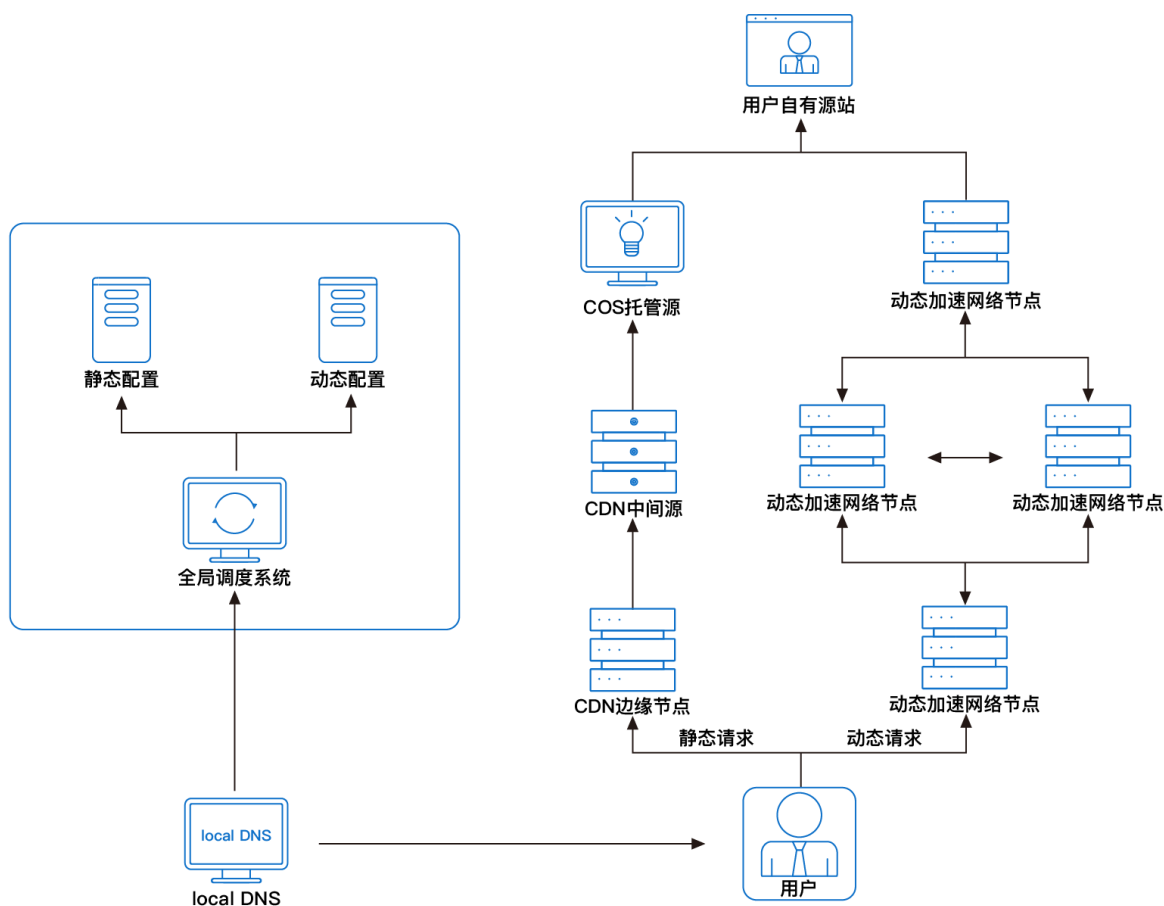


图 15 网页加速平台架构图

如图 15，网页加速平台的架构主要分为几个部分：

1. 节点的全局调动：如错误!未找到引用源。错误!未找到引用源。中所述，全局调度系统不仅根据 LocalDNS 的接入 IP 识别终端用户接入位置，同时也根据 GLSB 的决策模块计算全网接入的 QQ、微信服务质量以及目前的节点负载以及健康度来综合计算可以分配给用户的最佳节点。

2. 边缘和中间源节点集群：如 [2.2.2 双层缓存架构](#) 中所述，对于静态文件当边缘节点的双层缓存集群都无法命中时，请求将会被引导到 CDN 中间源节点。如果在中间源节点上的缓存命中，缓存内容会被通过边缘节点返回给客户，同时边缘节点缓存住内容；如果中间源节点命中失败，会向源站请求内容，且中间源以及边缘节点都会收到并缓存内容。

对于动态请求，详见下文动态加速功能描述。

3. COS 托管源：对象存储（Cloud Object Storage）是面向企业和个人开发者提供的高可用，高稳定，强安全的云端存储服务。源站可以将任意数量和形式的非结构化数据放入 COS，并在其中实现数据的管理和处理。COS 托管源的内容可以以主动以及被动的两种方式被存储入 COS 托管源服务器，引入 COS 托管源可以显著的进一步减少源站的压力。（有关 COS 的相关产品介绍请参考 <https://www.qcloud.com/product/cos>）

3.2.3 平台功能

除了上述描述的网页加速平台说具有的 CDN 缓存通用功能以外，网页加速平台还具有一些特别的针对不同内容以及使用场景的功能：

3.2.3.1 DSA 动态加速

不论是手机 APP 内或是网站内容中，都有大量动态请求，在许多应用场景下（譬如证券交易等应用或网站），动态请求甚至是请求的主要部分。如图 16，在大多数网站和页面的加载过程中，通常需要优先加载动态资源列表请求后再逐一去请求静态资源，而动态请求的延迟可能会拖慢整个页面的加载，大大的影响用户体验。

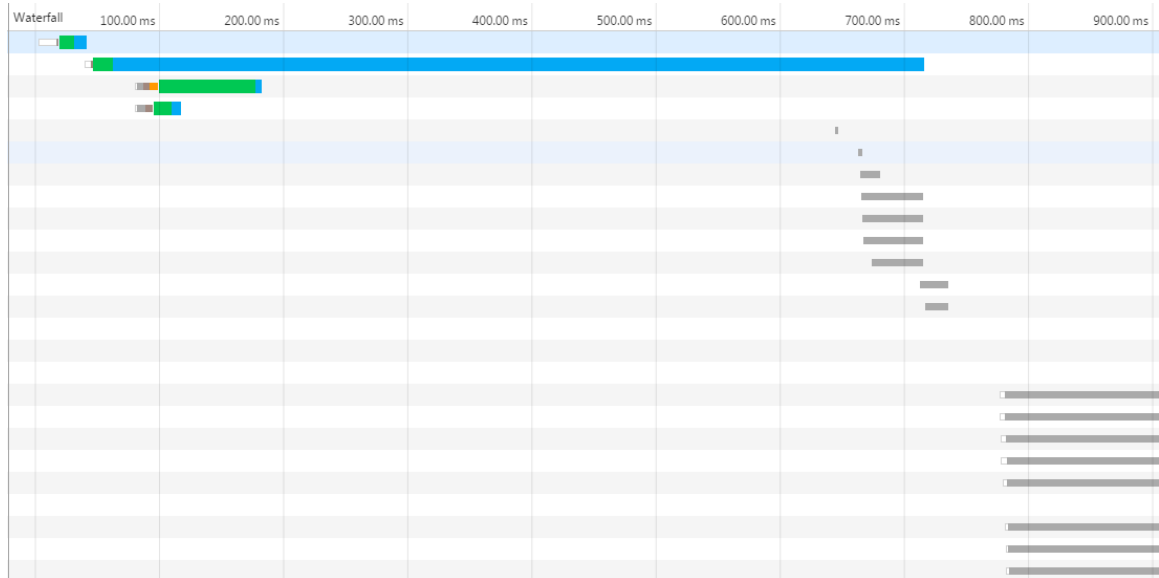


图 16 动态请求影响加载示意图

动态请求的加速需求刻不容缓，但是目前对于动态内容的加速一直有难以突破的瓶颈和亟待解决的问题：

1. 网民数量激增，网络中需要承载的流量暴增。智能手机以及 PC 终端快速的发展，让用户对高清图片和高清视频的需求逐步递增，进一步促进了网络流量的爆发。但是骨干网建设的速度难以匹配用户的需求，也受限于运营商的路由策略不佳和不同网络运营商间跨网带宽的限制，导致传输速度慢、网络拥堵。如何避开拥堵的网络，挑选最合适的回源路径成为动态请求加速的重要问题。
2. 传统的 TCP 协议是一个复杂但是在发展中的协议，虽然不停的有一些优化策略被提出并被实施（例如 RFC2581：《TCP 的拥塞控制》是一篇近年来关于 TCP 的很重要的 RFC），但是发表于 1981 年的 RFC793 中描述的 TCP 协议的基本操作还是未做改动，已经历经 36 年的 TCP 协议并不适应当前复杂的网络环境，给动态请求加速带来较大的影响。

3. CDN 很希望解决动态加速的问题,但是通用的 CDN 架构甚至可能适得其反,因为 CDN 严格的边缘节点——中间源节点的请求路径,可能会拉长回源路径,在一些情况下让回源路径更长,请求耗时更多。

所以腾讯云 CDN 推出了 DSA 动态加速产品,从网络架构、通讯技术、硬件架设等方面解决了动态请求加速的难题。

3.2.3.1.1 网络结构

通常来说静态资源的访问和存储遵循的是等级严格的链条结构,用户初步访问边缘节点,只有在边缘节点无缓存的时候才会去访问中间源节点,不存在用户直接访问中间源节点的情况。同样,边缘和中间源以及 COS 托管源之间也不准在越级访问的情况。

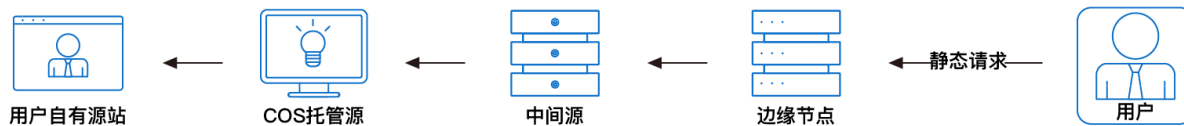


图 17 静态内容回源流程

但是 DSA 不同,用户的请求在根据 GSLB 调度系统的分配的节点接入动态加速网络后,动态加速网络中并没有严格的分等级节点制度。请求从用户接入到回源,会被选择在网络中最快的传输路由。每个 DSA 节点会保存和网络中其他节点的链接信息,包括连接的延迟和丢包率信息等,根据不同的请求情况会赋予不同的权重,计算出最好的回源路径。

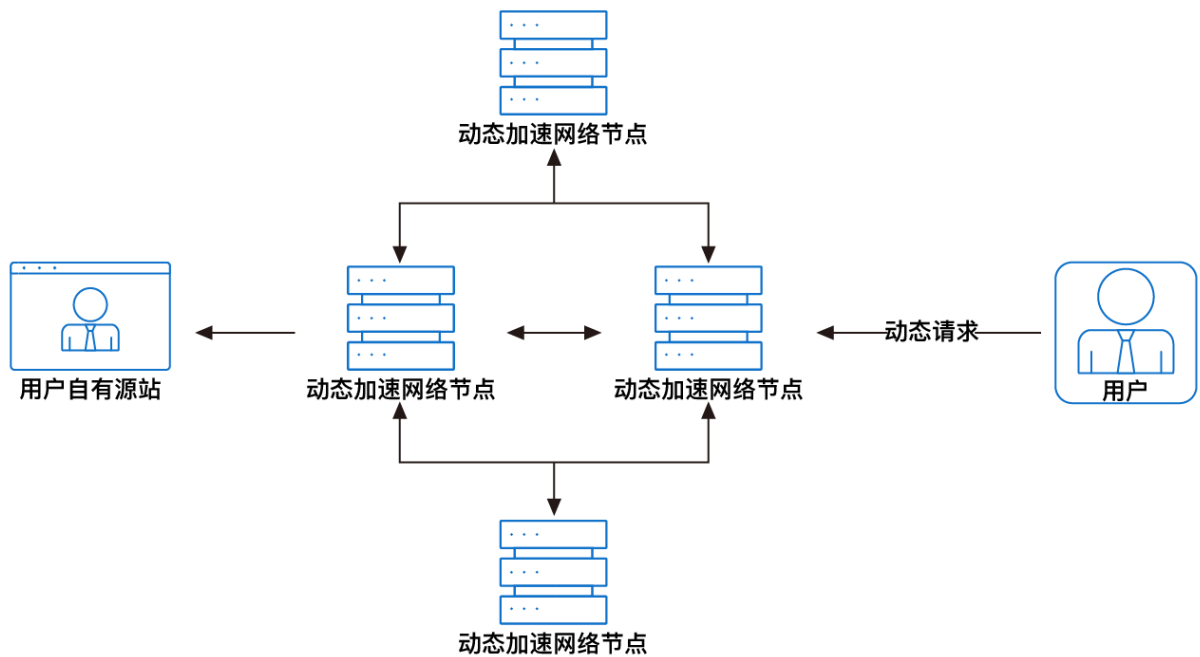


图 18 动态加速请求流程图

3.2.3.1.2 私有协议

TCP 协议在动态传输过程中还有极大的优化空间，因为 TCP 理论上是为流量设计的（每秒内可以传输多少 KB 的数据），其目的是充分利用现有带宽。但是针对动态请求而言，快速的传达比充分利用带宽更加重要。针对此特征，腾讯云 CDN 的研发团队结合 UDP 协议的高效和 TCP 协议的可靠的特征，设计了 QCTP 传输协议，以 UDP 的高效传输为基础，重新设计了可靠的逻辑方式，从重传机制、二次重传机制、ACK 发送机制等方面优化了协议的传输。

- **拥塞控制**：对于 tcp 来说，由于需要考虑拥塞控制和流量控制，拥塞窗口的初始值为 1，发送第一个报文，当收到接收端的 ACK 之后，拥塞窗口以指数形式增长，这就是 TCP 目前使用的慢启动算法。当拥塞窗口增长到限值时，拥塞窗口开始加法增加。这样就可以避免增长过快导致网络拥塞，慢慢的增加调整到网络的最佳值。但

是当丢包发生的时候，拥塞窗口立即大幅减小，重新进入指数增长阶段。具体阶段可参考图 19。

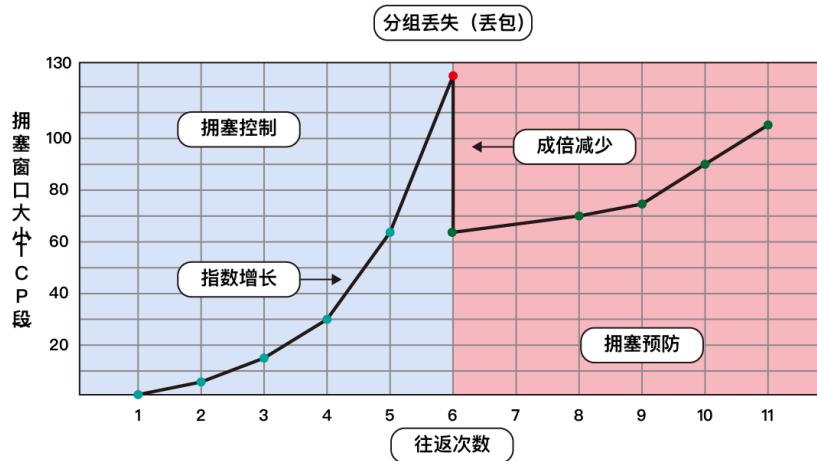


图 19 传统 TCP 拥塞控制示意图

该方式保守地避免了丢包造成的网络传输问题。但是同时传输效率不免被严重影响，并不适合于动态传输内容。QCTP 协议动态探测当前两个节点间的网路情况，综合发送数据大小、剩余内容大小等因素来动态调整了逻辑中的拥塞窗口大小，比 TCP 协议更加高效。

- 重传算法：TCP 丢包时会全部重传从丢的那个包开始以后的数据，QCTP 协议选择性地重传了真正丢失的数据包。另外改进了 TCP 算法中对超时的定义，提前预判可能发生的超时，激进地重新发包。用部分流量的重发可能造成的浪费来让传输更快更高效。DSA 以内部节点间的带宽消耗增加来换取相较 TCP 30%以上的传输效率。

3.2.3.2 图片鉴黄

图片鉴黄服务 (Pornfound) 基于腾讯优图的深度学习图片鉴黄技术，可以高效准确地鉴

别色情图片和性感图片，解决网站和 APP 开发者的鉴黄难题，告别大规模的人工鉴黄，节约成本的同时，大幅提高鉴黄效率，净化网络环境。

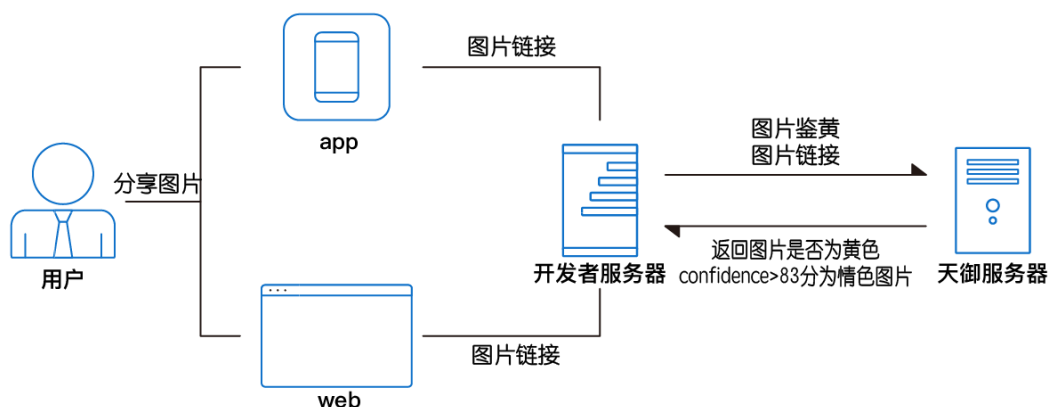


图 20 图片鉴黄系统示意图

提供色情识别，性感识别和自动鉴黄三大功能：

- 色情识别：图片鉴黄服务，通过开发者提供的图片地址，自动下载并进行鉴黄识别，通过置信分数的方式返回给客户，83 分以上判定为色情可疑图片，开发者可以对这部分图片的用户行为，进行跟踪分析。
- 性感识别：图片鉴黄服务针对开发者提供的图片，免费进行性感度识别，当性感度超过 83 分时，开发者可以对这部分图片的用户行为，进行跟踪分析。
- 图片鉴黄服务使用腾讯优图的 DeepEye 主动色情识别技术引擎，对图片进行色情置信度分析，依托腾讯社交的海量图片样本优势进行深度识别训练，算法识别准确率达到 99.9% 以上，远超人工识别水平，实际工作中可以取代 90% 人力，而且针对图片自动识别领域最难的色情与性感的界定问题，鉴黄引擎采用了分离图谱技术，精准识别性感和色情的差别。

3.3 下载加速平台

相比于 [3.2 网页加速平台](#)而言，针对较大文件的分发带来了完全不同的问题，下载场景的显著特点就是可以概括为：大文件、高带宽、波动大、下载工具广泛。针对以上特点，当前下载类的用户常见问题主要包含：下载质量不高，成功率低；软件发布不及时；带宽不稳定，客户下载体验差，盗链现象严重等。

3.3.1 平台适用场景

下载产品平台主要适用于：各类手机应用分发商店，应用和页面内影音文件的分发，游戏更新/程序/客户端，固件/硬件/软件更新程序的下载等，所以主要分为发行商、下载商以及视频供应商三类。为有大内容分发的内容提供商提供快速优质的服务。主要解决的客户问题如表 1：

目标客户	数据大小	全网同步速度	带宽要求	带宽波动	响应时间	成功率	是否需要防盗链
发行商	较小	高	大	大	高	高	否
下载商	大	一般	一般	一般	一般	一般	是
视频供应商	大	一般	大	一般	高	高	是

表 1 下载平台适用场景表

3.3.2 平台架构

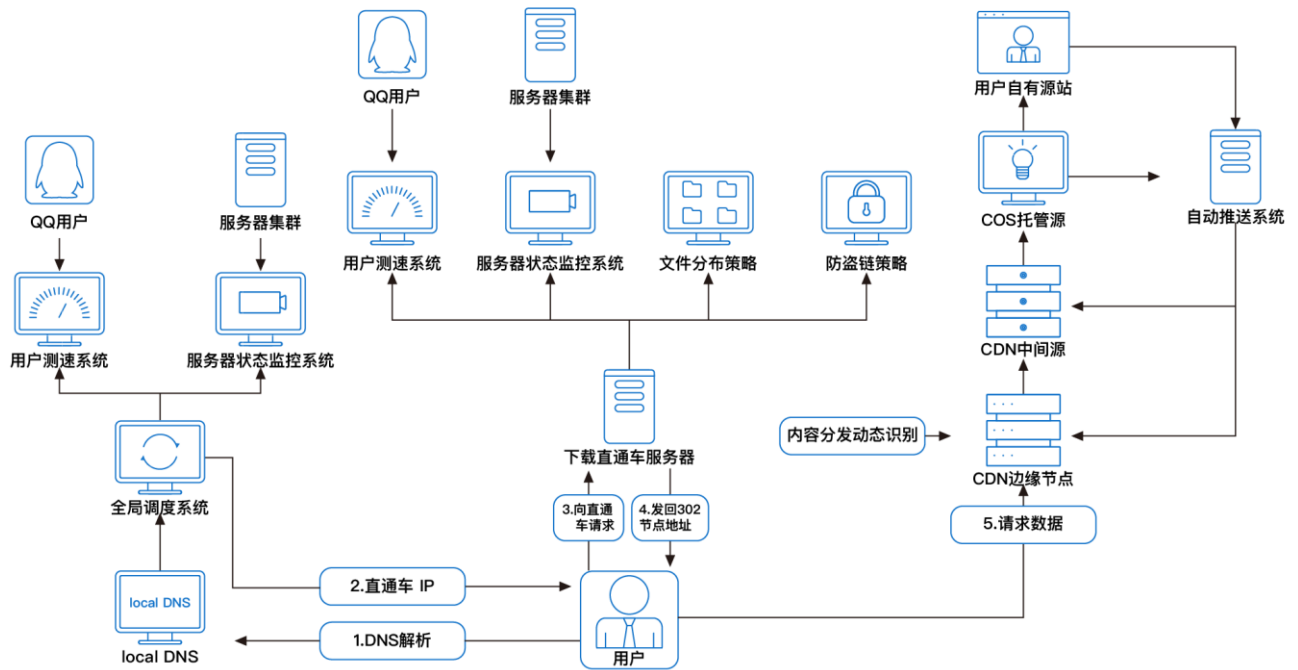


图 21 下载平台架构图

如图 21，平台架构类比 3.2.2 网页平台架构有很大的不同，下载平台的全局调度系统系统和用户之间可以采用下载直通车的方式连接。不再依赖 DNS 调度解析，“颠覆了” CDN 接入的流程根本，实时的决策最优的服务器资源，提升用户访问质量。和网页加速平台对静态文件的处理类似，当边缘节点的双层缓存集群都无法命中时，请求将会被引导到 CDN 中间源节点。如果在中间源节点上的缓存命中，缓存内容会被通过边缘节点返回给客户，同时边缘节点缓存住内容；如果中间源节点命中失败，会向源站请求内容，且中间源以及边缘节点都会收到并缓存内容。但是特殊的是，对于大内容（例如手机 ROM、大型游戏安装包等），被动回源时会导致源站带宽突然增大，源站压力较高。这种场景下，采用节点间的主动分发，能够有效控制节点构建缓存的进度，保障好源站带宽和服务压力。

3.3.3 平台功能

腾讯云 CDN 下载加速平台致力于帮助客户解决大小文件在下载过程中出现的问题。除了做到文件下载的加速以外，能结合腾讯云 CDN 独特的下载直通车功能，做到防止运营商的下载劫持，以及全局的负载均衡。另外，内容分发的动态识别功能，打破了传统 CDN 自上而下的分发机制，不同节点之间的文件更新传输让 CDN 文件预取效率达到分钟级，同时减小内部节点以及源站的压力。

3.3.3.1 下载直通车

因为中国网络较为复杂，依赖 DNS 就近解析的调度，仍然会存在部分请求调度失效、调度生效慢等问题。依据直通车方案，腾讯云 CDN 在全国部署的 302 重定向服务器集群，能够为每一个请求实时决策最优的服务器资源，精准解决小运营商的调度问题，提升用户访问质量。直通车调度生效时延为 0，能最快地把用户引导到最优的服务器节点上，避开性能差或者异常的节点。

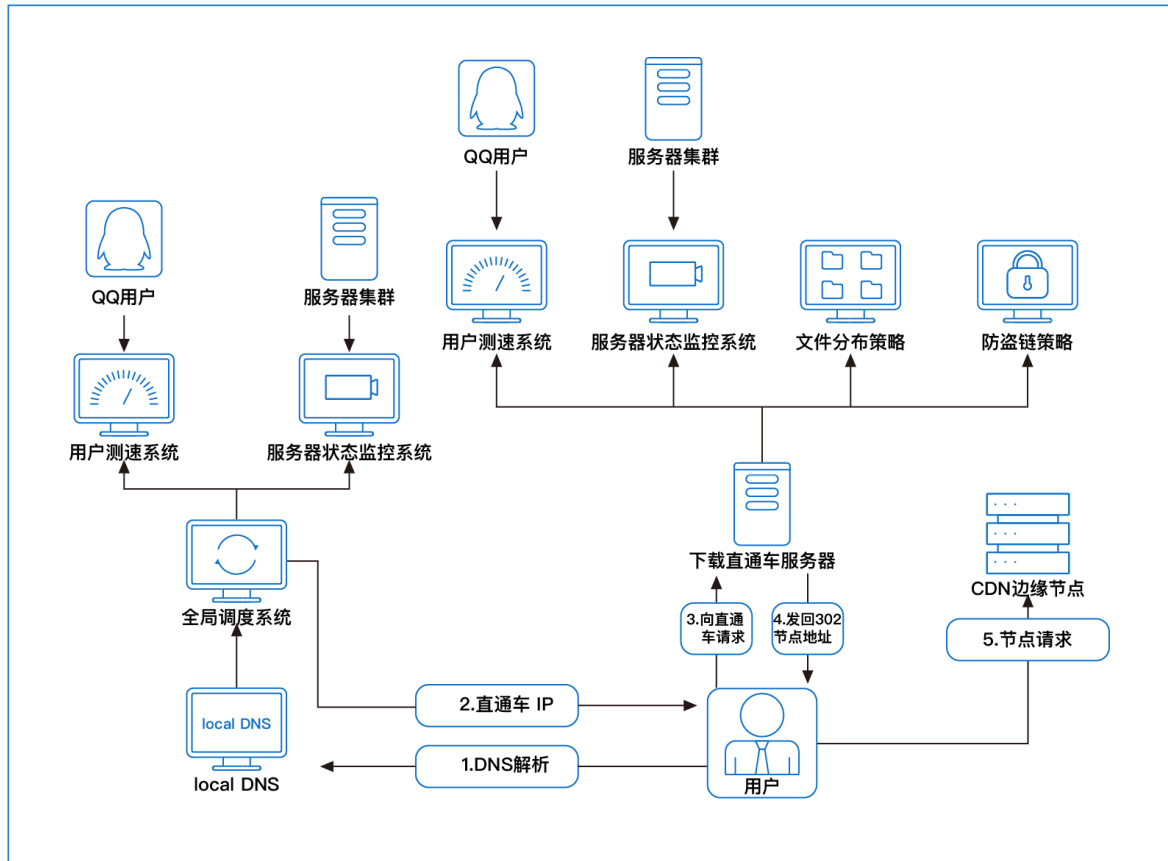


图 22 下载直通车架构图

下载直通车的使用步骤如下：

1. 用户请求某 URL，例如 <http://www.test.com/a.jpg>，由于 test.com 使用了腾讯云 CDN 加速，故域名会被解析至腾讯云 CDN 下载加速平台的全局调度系统。
2. 全局负载均衡系统根据用户测速系统以及直通车服务器的监控状态分配直通车服务器的 IP 返回给用户。
3. 用户继而向直通车服务器发起资源请求；
4. 直通车服务器的调度系统的服务器根据
 - a) 外调的用户测速系统（根据全网 QQ/微信的网络数据地图判断目前网络拥塞情况以及最佳链路）的网络全局地图；

- b) 监控系统的服务器以及节点机器状态；
- c) 配置系统的文件分布策略；
- d) 配置系统以及自定义配置系统的防盗链策略；

选定最佳的服务边缘节点，将 HTTP 请求以 302 跳转的方式发回给用户（返回的边缘节点直接以 IP 方式写在 URL 里），让用户向该节点发起请求；

5. 用户直接向边缘节点的机器请求资源，由于以 IP 方式请求，可以防止请求被流量劫持。

下载直通车对比 DNS 调度系统的优势如下表：

	DNS 调度	下载直通车
调度准确性	依赖 DNS 解析系统	调度系统自己维护 IP 库，可做到任何网段的精确识别，可解决 Local DNS 配置错误而导致的跨网访问，尤其是解决中小运营商调度不准确的问题
调度粒度	精确到域名层面	可以细化到域名、目录和的那个 URL
调度规则生效时间	取决于域名的 TTL	实时。应对突发类型业务，流量调度精确可控
适用场景	网页、图片等小静态资源	视频文件、应用安装文件等大文件下载，支持跟踪重定向

表 2 下载直通车对比优势

3.3.3.2 内容分发动态识别

服务器节点的缓存构建，主要有主动分发和被动回源两种方案。

对于普通小文件（例如图片、JS 文件、CSS 文件等），被动回源方案能够极大简化用户的操作：只需在源站上放置好内容，其他工作则交由 CDN 来完成。当用户访问 CDN 节点时，节点如果发现本地没有副本缓存，那么此时会选择最优网络路径，去源站获取该文件的副本存储在节点上。

但是对于大文件内容，例如程序的更新，在某一时刻发布后，往往会造成边缘/中间节点上并没有缓存数据，大量节点会在同时回源请求，造成源站压力陡然增大。若是利用预取功能，较为依赖程序员以及运维工程师的主观提前预判，需要客户的相关人员提前操作预取或是向客服提出预取。若是没有及时预取文件，也会造成流量问题，同时由于每个节点的被动回源拉取文件，如果采取纯被动回源方式，文件在 CDN 节点内部完全铺开需要大量时间。

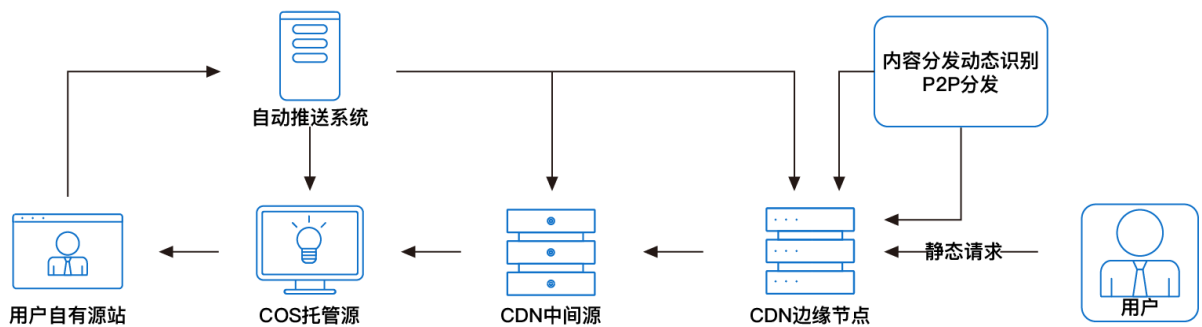


图 23 内容分发动态识别流程图

腾讯云 CDN 独特的内容分发动态识别功能能动态识别大流量的突增，分析其是否来自某些大文件的分发，继而采用主动推送的方式，将文件快速推送到各个节点。尤其借助腾讯 P2P 网络，能够加速整个分发进度，有效减少源站的带宽消耗。

3.4 点播加速平台

在过去的 2016 年，各大视频网站将自制内容提升到战略高度，内容向着精品化方向发展。而且在商业模式上，会员付费收入表现出非常强劲的增长趋势。而点播加速平台是腾讯云 CDN 视频解决方案的核心之一。通过提供完整的，囊括上传、转码、管理、发布、统计各个视频点播服务阶段的核心能力，腾讯云为客户提供一站式 VPaaS (Video Platform as a Service) 服务。借助灵活、快速、高质量的视频发布服务，用户可以快速具备稳定可靠的视频发布能力，聚焦于业务本身，敏捷响应市场变化。

方案的主要优势如下：

- 经验优势：基于腾讯长期在音视频领域的技术积累和能力，包括支撑腾讯视频亿级日均播放量、QQ 音视频聊天百万并发峰值的长期技术积淀等；
- 资源优势：覆盖全国的 CDN 节点网络，现有 500+全球节点，以及超过 40T 带宽。超过 10000 台分布式转码集群，2000 并发转码，保障转码质量效率；
- 渠道优势：同微信等产品的整合能力，提供腾讯云视频直接生成微信公众号发布链接功能，帮助用户发布视频内容至微信公众号；
- 生态能力：提供腾讯视频 V+频道对接资源，为用户提供多元化的视频发布平台和变现方式；
- 方案安全：支持对播放速度进行限制，可快速构建分级服务体验；支持基于时间戳等多种防盗链方案，保障视频内容的安全私密。

3.4.1 平台适用场景

腾讯云 CDN 点播平台将 CDN 的分布式部署的优势以及中心处理的高性能进行了结合,解决了流媒体点播在实际使用过程中的大流量、高延迟的问题。适用于所有基于 HTTP 以及 HTTPS 协议为主的流媒体点播站点。例如:各种视频网站(影视类、教育类等)、门户网站、音乐网站、网络电视台、网络音乐台、UGC 网站等。

目前在线点播目前常用的格式为 FLV 、 MP4 和 HLS :

- MP4: 比较经典的文件格式,在移动终端和 PC 浏览器上的支持度都很好,但是视频文件格式比较复杂,所以处理成本高,而且由于索引表复杂度高,导致时长大于 5 分钟的 MP4 文件在线播放时加载速度会很慢。
- HLS: 苹果公司力推的标准,在移动终端的浏览器上的支持度较好,但 IE 的支持情况依赖 FLASH 的二次开发工作。其精简的 m3u8 的索引结构可以规避 MP4 的索引慢问题,如果是用于点播,是非常不错的选择。
- FLV: Adobe 公司所推的标准,直播平台常用的封装格式,在 PC 端有 FLASH 的支持,但在移动终端只有 APP 实现播放器才有可能支持,大部分手机端浏览器均不支持。

3.4.2 平台架构

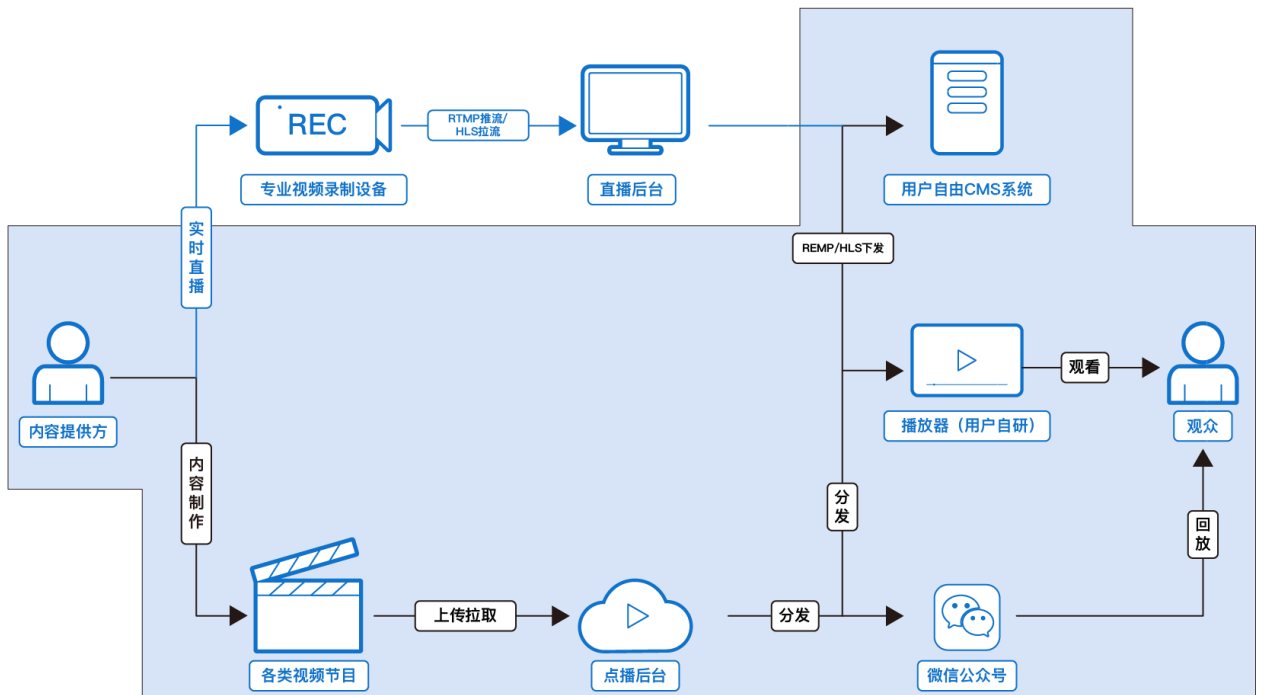


图 24 点播加速平台架构

如图 24，平台主要分为三大模块：

- 上传模块：用户通过 WEB 或 SDK 上传、拉取方式，将视频存放于点播后台，并根据需要进行自动转码；
- 管理模块：主要包括转码中心和控制管理中心。用户可通过 API、管理控制台方式，对文件进行管理（包括信息编辑、信息分类、信息导出、模糊搜索、在线预览等操作）和转码操作（包括转码和定义水印等）。；
- 分发模块：通过遍布全国的 CDN 系统，为点播用户提供快速灵活的播放方式；用户可使用自研或腾讯云提供的播放器 SDK 方便同自有业务集成，也可对视频生成专属微信公众号对应链接，使用微信公众号的相关内容发布。

3.4.3 平台功能

3.4.3.1 多途径上传

腾讯云 CDN 的点播平台视频上传功能可支持多个途径的视频上传，包括 API 形式的批量上传、WEB 页面提交上传以及针对 UGC 专属的 SDK 上传方案。包括支持 10G 大文件的上传以及断点续传。

上传视频格式支持：

标准格式	详细格式
微软格式	WMV , WM , ASF , ASX
REAL 格式	RM, RMVB , RA , RAM
MPEG 格式	MPG , MPEG , MPE , VOB , DAT
其他格式	MOV , 3GP , MP4 , MP4V , M4V , MKV , AVI , FLV , F4V

表 3 上传视频格式支持

为了便于用户调用 API，处理复杂的分片上传逻辑，用户可以选择使用辅助功能的 SDK。在 [3.4.3.3 各 SDK 服务](#) 中描述了腾讯云 CDN 提供的针对服务端上传 API 制作的上传 SDK，以及播放器 SDK 中自带整合的上传功能。

3.4.3.2 转码中心

腾讯云 CDN 对用户提供的音视频提供转码服务。匹配 240P~1080P 等不同清晰度，MP4 和 HLS 等不通过格式，同时支持自定义的水印添加。

对音视频文件进行转码，涉及很多复杂参数。为简化调用，腾讯云 CDN 点播预定义了一系列标准转码规格，每一个规格都对应一组转码参数，详细参数参见点播系统标准转码输出规格。除了标准转码规格之外，如果您存在定制化的转码规格，可以提需求工单，点播后台可以为您配置。表 4 展示了部分腾讯云 CDN 预设的封装格式。

规格名称	封装格式	视频参数							音频参数			
		编码器	帧率	宽边	色度空间	位深	码率模式	码率	编码器	码率	通道	采样频率
100	MP4	H.264	24	320	YUV420P	8	ABR	256kps	AC3	48kps	双	44100 Hz
200	MP4	H.264	24	640	YUV420P	8	ABR	512kps	AC3	48kps	双	44100 Hz
300	MP4	H.264	24	1280	YUV420P	8	ABR	1024k bps	AC3	48kps	双	44100 Hz
400	MP4	H.264	24	1920	YUV420P	8	ABR	2500k bps	AC3	48kps	双	44100 Hz

表 4 部分预设封装格式

3.4.3.3 各 SDK 服务

为了方便客户使用和上传视频，腾讯云 CDN 提供了点播的服务端上传 SDK 服务。同时为了便于客户快速实现点播方案，腾讯云 CDN 提供了点播播放器 SDK，实现了点播综合解决方案，让客户能便捷迅速的构建点播站点。针对 UGC(User Generated Content)业务，以及防止重要的 SecretID 和 SecretKey 对外暴露 腾讯云 CDN 提供了 UGC 专属解决方案以及配套 SDK。

3.4.3.3.1 服务端上传 SDK

服务端 API 的调用较为复杂。对于一般的 API ,需要对调用参数进行排序、计算鉴权签名。由于视频文件通常较大 ,故而一般需要采用分片上传的方式 ,整个上传过程涉及初始化上传、分片上传、结束上传三步 (如图 25)。

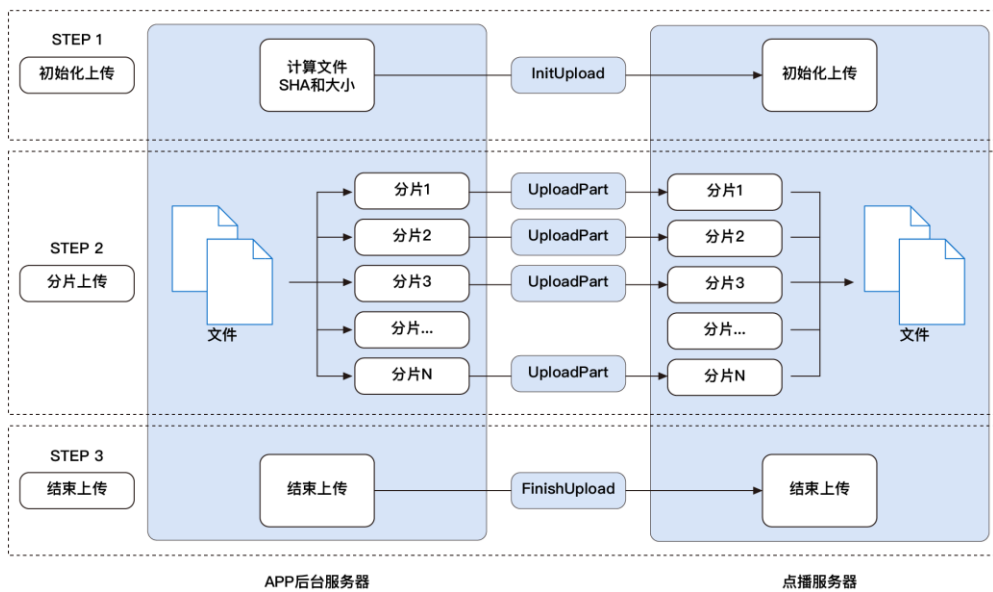


图 25 服务端上传步骤图

分片上传带来了较为复杂的逻辑和操作，为了方便开发者使用，点播提供了服务端 SDK 来简化开发。所有 API 均包含一般服务端 API 调用、服务端视频上传两大类功能。但是，为了防止重要的 `SecretID` 和 `SecretKey` 对外暴露，在客户端的请求或有报名需求的请求请使用 3.4.3.3.3 UGC 专属 SDK。

目前腾讯云 CDN 提供腾讯云点播 4.0 ServerSDK(For PHP)。可以让 PHP 开发者能够在自己的代码里更快捷方便地使用点播上传功能，支持开发者指定并发上传分片数目及每个分片可重传的次数、支持断点续传。可访问 <https://github.com/tencentyun/vod-php-server-sdk-v4> 获

取最新的 SDK 以及使用范例。针对 nodejs、Python、java、golang 以及 csharp 的 SDK 即将推出。

3.4.3.3.2 点播播放器 SDK

当视频文件已经存放在服务器上，用户即可在获取文件播放 URL 的情况下，使用腾讯云 CDN 提供的视频播放器 SDK 可以实现边下边播的功能。

同时，腾讯云 SDK 提供 WEB 和移动端（iOS / Android 不同版本）的全解决方案，通过灵活的接口，快速同自有 Web 以及 APP 应用集成。不需要内容提供商进行视频播放器的研发工作，直接使用腾讯云 CDN SDK 内附带的播放器对象，以实现桌面和移动端应用的点播视频播放功能。同时 SDK 还提供在 WEB 端和 APP 内上传视频的能力。

播放器提供功能：

- 视频控制：视频的播放、暂停、调整进度、停止续播等；
- 画面调整：调整将图像等比例铺满整个屏幕或是将图像等比例缩放等针对画面大小的调整功能；
- 视频弹幕：为当前视频添加视频弹幕（但是不附带视频弹幕的后台功能）；
- 视频加密：SDK 自动为加密视频显示输入密码，需要输入密码才可播放；
- 分享功能：可以简单的通过播放器自带的分享功能将内容分享到新浪微博和 QQ 空间等，同时可以通过播放器生成二维码方便传播；
- 清晰度自适应：可以根据当前网络情况自适应清晰度。如果在确认视频拥有该清晰度的情况下，可以使用参数指定播放视频的清晰度；

3.4.3.3.3 UGC 专属 SDK

随着终端用户个性化的需求愈加丰富，简单的文字交互和图片上传已经不能满足展示与分享信息的诉求，UGC 也就应运而生。对于 UGC 将客户端（iOS/Android/Web）视频上传到点播服务端的需求，因为 APP 不应当将自己的 SecretId 和 SecretKey 暴露到客户端，故而不适合使用上传 API 接口进行上传。用户可以选择使用 UGC 专属方案 API 或提供给 UGC 方案的专属 SDK（WEB/iOS/Android）实现。

UGC 功能的实现由 SDK，腾讯内部的 COS 服务器以及点播服务三部分组件配合完成。终端用户只需要点击视频上传操作即可。对于 app 而言，上传功能由 SDK 实现，所以只需要将 SDK 集成到应用中即可，其他部分由腾讯 CDN 来操作完成。

UGC 视频上传的整体业务流程共两个步骤：

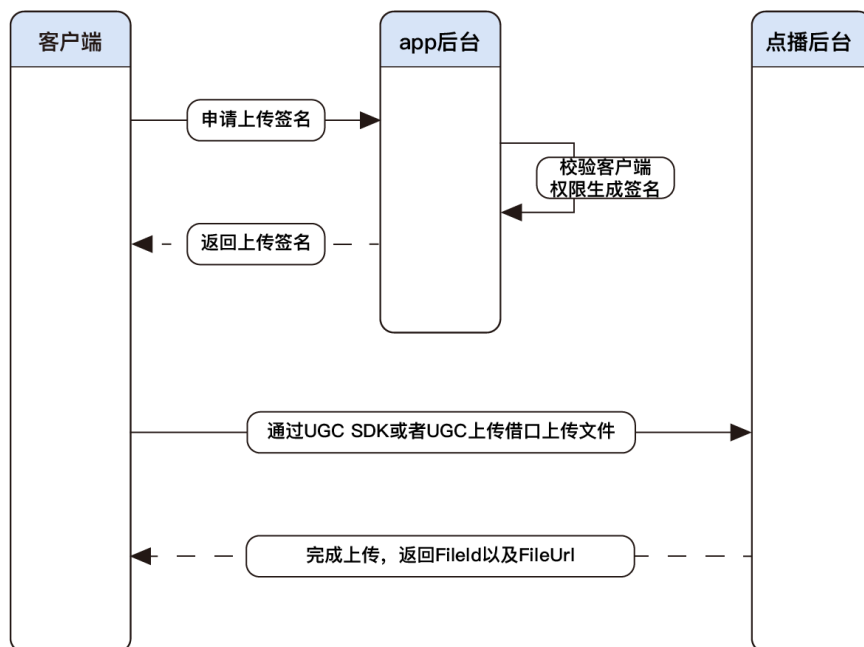


图 26 UGC 视频上传流程图

1. 生成上传签名：点播 UGC 视频上传签名是一段经过 Base64 编码的二进制串，其中包含的主要信息：
 - 1) 上传参数信息：包括但不限于 APP 的 SecretID，视频的基本信息（视频名称、标签）以及视频上传到点播之后的处理方式（是否进行转码、是否进行鉴黄等）
 - 2) 用 SecretKey 生成的 HMAC-SHA1 签名，点播后台据此来校验 UGC 上传签名的合法性；
2. 根据平台的不同，调用腾讯云点播的 UGC SDK（或者上传接口），进行视频上传。

3.4.3.4 微信公众号专用视频发布

微信公众号视频链接发布是腾讯云 CDN 点播服务的重要功能之一。当前为了确保微信公众号中消息发布的内容，微信平台当前仅允许特定视频链接可以作为公众号消息内容进行发布。

通过微信公众号视频链接发布功能，用户可方便的使用已经存放在腾讯云 CDN 中的视频，生成可在公众号消息发布中引用的专用链接，由此实现视频内容的公众号信息发布。使用该功能前需确保当前操作的腾讯云视频服务账号通过管理控制台-用户中心-账户信息完成个人或企业资质认证。

认证信息在审核成功后，用户当前可以在单个文件管理界面开启操作生成链接，系统将自动选择当前较高码率 mp4 文件进行转换并生成专用链接，该过程约在 4 个小时以内。链接生成后，用户可在“视频管理”界面下的对应文件页面查看链接，并通过二维码预览。用户可将链接复制至微信公众号的信息布界面发，实现视频内容的发布。

3.5 直播加速平台

视频直播应用，尤其是互联网的广泛应用和近几年的 OTT 的应用，对直播视频要求越来越大。根据 CNNIC 2017 发布的第 39 次《中国互联网络发展状况统计报告》，截止 2016 年 12 月，中国网络视频用户规模达到 5.45 亿，同比增长 8.1%，其中手机用户规模接近 5 亿，同比增长 23.4%。随着 4G 网络的进一步完善以及资费的下调，在手机上收看视频以及直播已经变得愈加普遍。

传统的电信网络是可以直接提供组播的专有网络，网络内部可以通过采用组播协议来完成骨干网和接入网整个流程的组播支持，但在现有的 Internet 互联网应用下，OTT 运营商是采用公网来进行直播服务的，而且考虑到防火墙的问题，大多数都采用 Http 和 RTMP over HTTP 的协议来支持，但是这种情况下，就要求媒体直播服务器 Live Media Server 需要非常大的网络带宽来支持上百万的客户请求，而且运营商网络接入和用户网络接入的最后一公里就成为直播质量的关键，往往会产生许多的问题：

1. 延迟/清晰度：视频业务的核心竞争力是流畅和清晰度，这两个因素是受限于好的网络保障，但是运营商会经常遇到跨运营商的多网络连接，特别是接入网络和最后一共里网络经常不稳定，会大大影响用户的观看体验。
2. 流量的突发：在内容提供商进行市场推广或重大事件的现场直播活动，以及一些突发热点事件的发生时，经常会突发产生大量的网络直播请求，而原有的网络不一定能承受这种突发流量的要求。
3. 内容的不可控：直播的展现内容完全由主播自主生成，实时的向观众传递。在保证直播的流畅和实时性的基础上，平台策略和相关法律法规需要确保主播推送内容的

合法性。一旦主播推送的内容触及相关法规，不仅会在用户群中对平台产生严重的负面影响，更会让平台承担极大的政策压力。

3.5.1 平台适用场景

腾讯云 CDN 的直播加速平台能够帮客户解决直播方案中的：均衡延迟/清晰度，应对流量突发，监控直播内容等问题。一方面提升视频直播的质量，增加用户粘性；另一方面保障直播平台的安全以及内容的合规。

直播加速产品适用于各类流媒体直播 APP 以及页面：游戏直播、美女直播、新闻直播、体育比赛、网络课堂、视频会议等。

3.5.2 平台架构

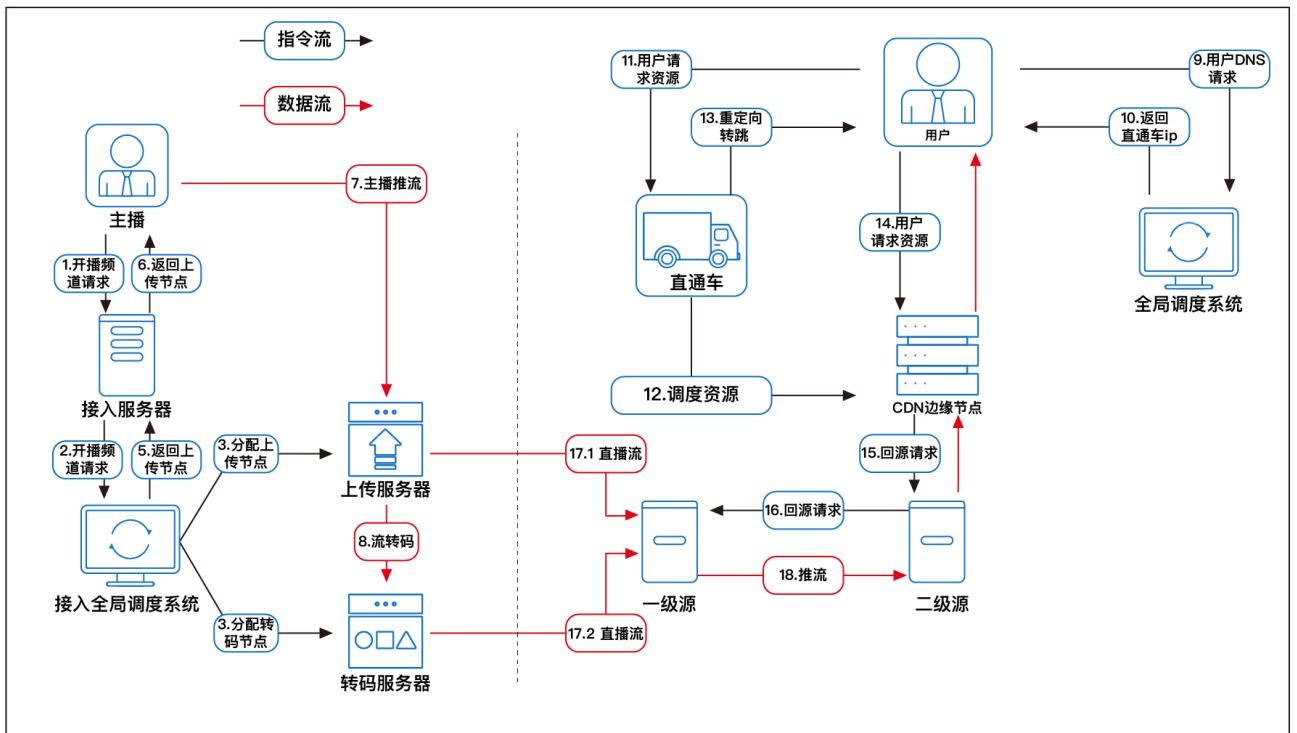


图 27 直播平台流程图

腾讯云的 CDN 直播平台加速，分为主播接入以及观众接入两个部分，图 27 详细说明了

两个部分流程，以下详细说明各个部分：

1~6：主播的接入请求并非直接传输到上传服务器中，主播需要首先接入“接入服务器”，由接入服务器以及接入全局调度系统为主播根据当前地理位置以及服务器负载/速度来选择合适的上传和转码服务器，并且将信息返回给主播；

7~8：主播客户端将主播视频推流给上传服务器，上传服务器会将直播流同时传输给转码服务器，根据直播协议的不同和业务要求不同，进行码流切片、转码为 HLS 协议的 TS 片段，或直接获取直播流输入的 HLS 的 M3U8 列表，并同时根据 M3U8 列表，去直接拉取 HLS TS 片段。直播流的码流码率可以进行转码系统后，可以进行单流输入多流输出，云转码系统，不仅仅支持直播流的转码，而且可以支持 VOD 视频的用户上载编码，用户可以选择自定义码率，根据自身业务情况和用户需求为客户提供高个性化的多码率服务。自定义包括码率、输出格式和分辨率等。

9~14：和 [3.3.3.1 下载直通车](#)类似，用户从 DNS 系统接入，在全局调度系统的协调下分配的并非边缘节点而是直通车节点，直通车将客户的请求重新引导至边缘节点，客户向边缘节点请求数据。

15~16：如果边缘节点没有数据的缓存，节点会逐层向上级节点请求；

17~18：从上传服务器和转码服务器输出的数据流，会逐级节点下发到用户处，并且在节点上留下缓存。

3.5.3 平台功能

3.5.3.1 多路备流

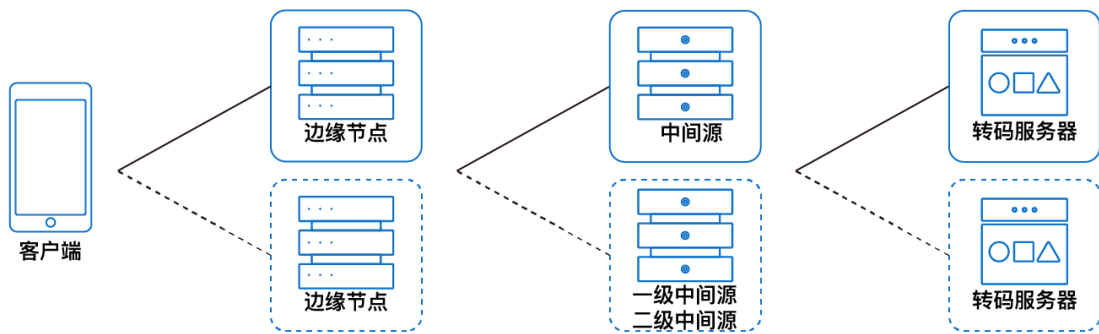


图 28 多路备份

腾讯云 CDN 为了保证直播的流畅性，逐级设计了备份系统：

1. 在边缘节点，如果遇到机器故障等特殊情况，或版本升级，定期运维等维护工作，客户端根据缺少的分片数据请求另一个备份边缘节点，将获取的数据进行拼接，保证视频流不间断；
2. 中间源节点故障则由其余的中间源节点来实现无缝切换，会根据私有协议块号或者 ts 分片块号来实现切换到其余的一级中间源/二级中间源；
3. 如果发生转码机器故障，中间源会切换到备转码机，做到直播转码主备机做到无缝切换。腾讯云 CDN 在转码模块上设置了主备转码机，主转码机持续编码出流，备机只拉源数据，但不编码。当主机故障时，上传服务器会切到备转码机并带上当前需要帧序号，则备机从这个帧开始转码（因原始数据已缓存），同时接管主转码机。

3.5.3.2 柔性系统

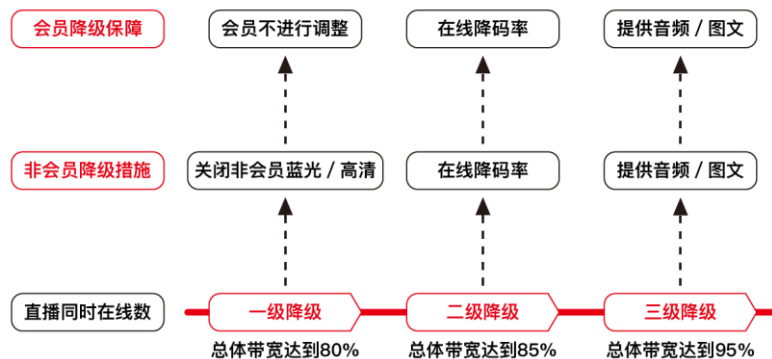


图 29 柔性系统分级策略

如上图，保证质量的同时，尽最大可能支撑更多用户数，腾讯云 CDN 的直播方案配置了备用的柔性系统，当发生流量突发，整体带宽比例剧烈上升后，资源池调整之前，柔性系统会发挥作用保证客户的观看，以下策略可以定制：

1. 当节目总体带宽达到 80% 时，需要进行清晰度降级策略来缓解带宽增长，区分非会员和会员用户。关闭非会员蓝光和高清选项，只提供标清观看，会员用户不调整。
2. 当节目总体带宽达到 85% 时，进行所有规格在线降码率柔性，按 20% 比例降码率，实施完成后，可以释放部分带宽来支撑新用户访问。
3. 当节目总体带宽达到 95% 时，只能新提供音频/图文选项，关闭视频选项。新用户虽然无法观看视频，但还可以通过音频/图文件来继续收看。

3.5.3.3 直播秒开

互动直播的首要要求就是要秒开，直播间需要做到在 1 秒内可以播放，在用户想浏览主播进行切换时才能快速切换。针对秒开腾讯云 CDN 的优化方式如下：

1. 边缘节点加速：调度到离用户最近的机房节点，TCP 协议加速，首次接入时加速推送数据到用户端。
2. 缓存关键帧：用户首次接入时提供已经缓存的最近的关键帧，如下图的 I 帧。当客户端获取到关键帧后，即可以开始播放。这当时也需要客户端配合一起优化，需要客户端减小缓存达到播放条件。

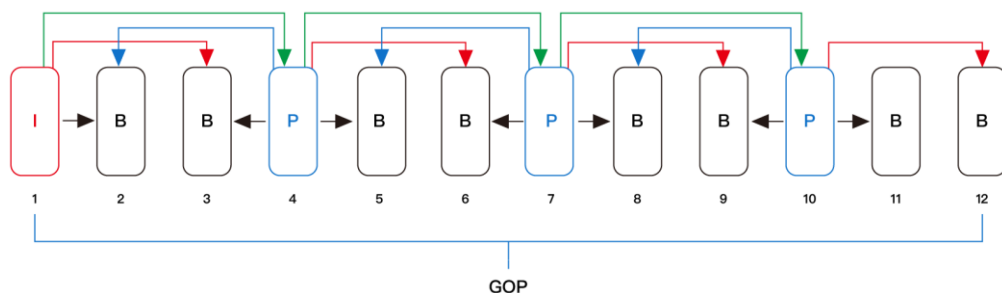


图 30 直播关键帧

3. HLS 首次接入返回 3 个 ts 分片：HLS 协议首次接入时的需要有 3 个 ts 分片播放器才能开始播放，这是 ios 播放器特性。如果首次接入时 m3u8 文件中只提供了一个 ts 分片，客户端会再次请求 m3u8 期望得到新的 ts 文件，如果这时 m3u8 文件没有更新，还是相同的 ts 分片，则会触发播放器等待一个超时时间再请求更新，导致开播慢。

4 接入指南

腾讯云 CDN 必须开通后才能够使用。新用户进入 CDN 控制台可以看到开通页面。

(<https://console.qcloud.com/cdn/overview>)

1. 开通 CDN 服务第一步，须在腾讯云用户中心完成“资质认证”或“银行卡认证”任意一种认证方式。



图 31 CDN 开通认证步骤 1

用户中心地址：<https://console.qcloud.com/>



图 32 CDN 开通认证步骤 2

2. 开通 CDN 服务第二步，完成资质认证后，用户需要选择计费方式，即成功开通 CDN 服务。详细计费价格可以参考 CDN 计费方式和价格。

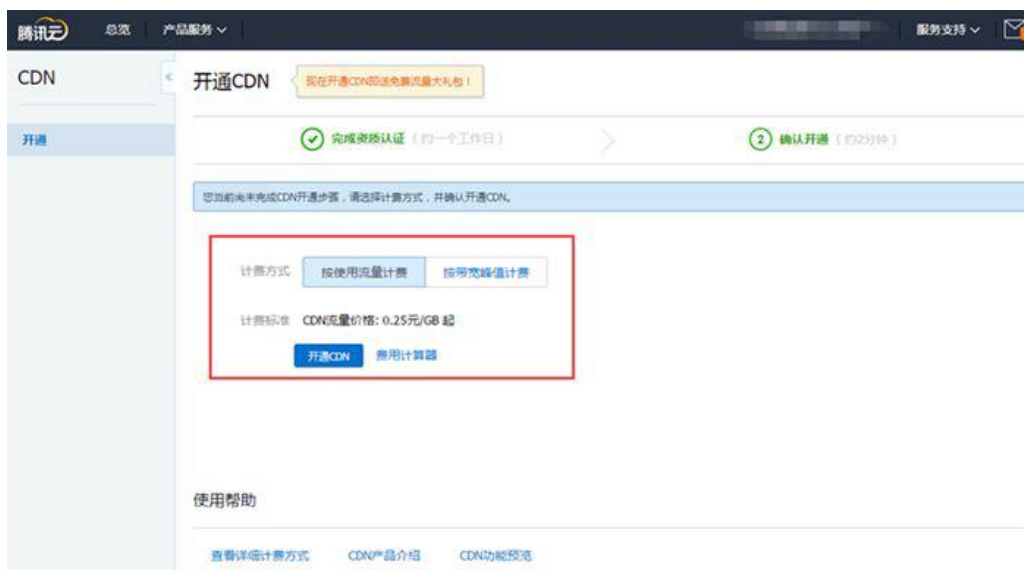


图 33 选择 CDN 计费方式

3. 完成开通后可以添加您的第一个域名，可在下方“CDN 接入方式选择”查看具体添加步骤。



图 34 CDN 接入方式

4. 开通后您的 CDN 首页为“概览”页，您可以通过“概览”页了解 CDN 整体情况，

在接入管理出进行接入配置等。



图 35 CDN 控制台概览

5 结语

互联网的进一步发展，人们对信息服务的要求也越来越高，人们希望得到更快的响应速度和更好的产品体验。

腾讯云 CDN 依托于多年来的自身互联网业务的发展，积累了丰富的经验和坚实的基础能力，实践也证明腾讯云是具备为海量用户提供高响应、高以体验、高安全的服务能力。腾讯云 CDN 服务能为客户提高网站的访问速度,缓解网站的服务器与带宽压力,增强网站的安全性选择，提高网站服务的不间断性。

为您的最终用户提供最佳体验的服务，提升用户满意度，腾讯云 CDN 服务是您最好的选择。