

**云点播**  
**解决方案**  
**产品文档**



**腾讯云**

**【版权声明】**

©2013-2019 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。

## 文档目录

### 解决方案

- 行业领域

  - 短视频

  - 视频网站

### 推荐实践

- 如何对视频进行内容审核

- 视频床问题与防范

- 防盗链的测试

# 解决方案

## 行业领域

### 短视频

最近更新时间：2019-06-26 20:09:29

针对短视频应用的特点，云点播提供了适用于该类型应用的方案，帮助您快速高效地实现一款短视频应用。

## 视频制作

短视频 App 制作视频时，常用的功能有拍摄、裁剪、混音、特效、字幕和贴纸等。

云点播提供了 [短视频 SDK](#)，帮助您在客户端快速集成丰富的视频制作能力（完整功能列表及下载地址请参见 [腾讯云短视频 SDK 各版本下载](#)。

### ⚠ 注意：

使用短视频 SDK 需付费，但您购买云点播的资源包之后将免费获得 SDK 的使用权，详情请参见 [购买说明](#)。

## 视频上传

App 客户端完成视频制作后，需要将视频上传到云点播。

[短视频 SDK](#) 集成了客户端视频上传的功能，推荐使用该 SDK 实现客户端视频上传。如果您不希望使用短视频 SDK，我们也提供了独立的 [客户端上传 SDK](#)。

## 视频播放

视频上传后，在 App 客户端播放云点播中的视频。

[短视频 SDK](#) 集成了客户端视频播放的功能，推荐使用该 SDK 实现客户端视频播放。如果您不希望使用短视频 SDK，也可以使用第三方播放器。

## 内容审核

App 用户上传的视频可能存在涉黄、涉暴和涉政问题。

云点播提供了 [视频内容审核](#) 功能，使用腾讯云强大的 AI 对视频进行快速准确的智能审核。内容审核的具体集成方案，请参见 [如何对视频进行内容审核](#)。

## 视频床防范

恶意用户上传自有内容视频并分发给第三方用户，这是一种侵占您带宽和存储资源的行为，即 [视频床问题](#)。

云点播提供了一种 [视频床防范](#) 方案，通过限制 URL 的获取和播放次数防止您的资源成为“视频床”。

# 视频网站

最近更新时间：2019-05-29 10:49:17

视频网站是互联网视频中的传统行业，主要提供电影剧集、综艺赛事和教育课程等高质量长视频内容（例如腾讯视频、CNTV 及企鹅辅导等）。云点播针对视频网站场景提供了相应的解决方案，帮助您实现一款视频网站应用。

## 防盗链

视频盗链是指未经许可的情况下，将您的视频 URL 转载到第三方视频平台的侵权行为。视频被盗链后，不仅视频版权收到侵害，而且还会造成巨额的 CDN 带宽流量损失。

云点播提供了完备的 [视频防盗链](#) 功能，帮助您全方位保护视频防止盗链。另外，点播还提供了一套 [防盗链测试](#) 方案，指导您如何安全地开启和变更防盗链配置。

## 自适应码流

App 终端的网络环境复杂，当网络环境较差时播放高码率视频将产生卡顿。HLS 和 Dash 是两种通用的自适应码流视频格式，包含多种分辨率和码率的视频流，播放器可以根据当前网络带宽动态切换合适的视频流。

云点播提供了为视频提供了 [转自适应码流](#) 功能，可以将视频转码并打包成 HLS 和 Dash 两种自适应码流格式。

## 缩略图预览

视频播放进度条上展示缩略图，可以帮助用户快速预览指定时间点的内容，提升视频播放体验。

云点播提供了 [截取雪碧图](#) 功能，结合生成的雪碧图大图和 VTT 文件，即可实现缩略图预览功能。

## 多功能播放

App 客户端播放视频时，常用的功能有设置播放器尺寸、视频画面打 logo、设置贴片广告和展示进度条标记等。

针对视频网站播放器的常见功能，云点播提供了 [超级播放器](#)，帮助您在客户端快速集成丰富的视频播放能力。

## 推荐实践

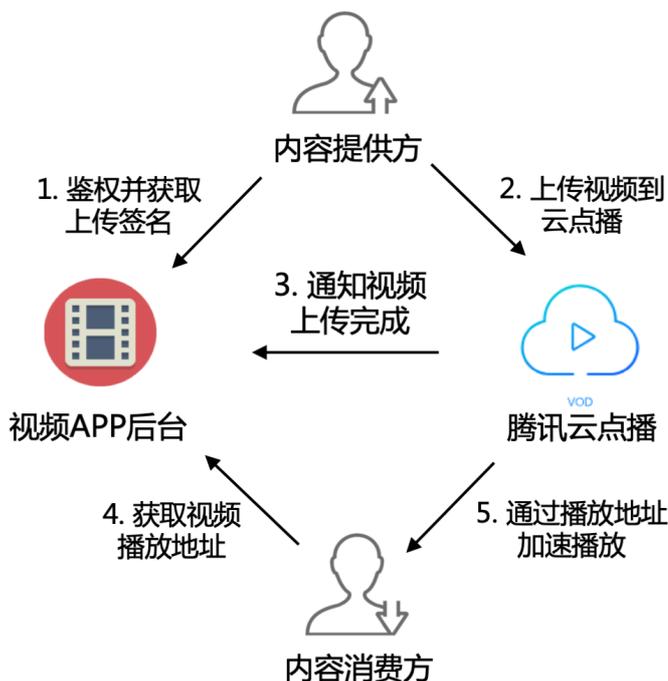
# 如何对视频进行内容审核

最近更新时间：2019-05-07 17:23:31

UGC（用户生产内容）和 PGC（专业生产内容）是视频行业中常见的两类场景，可以由视频分享者自由上传和分享视频内容。然而视频分享者上传的内容五花八门，其中可能就包含了大量“涉黄”、“涉暴”及“涉政”的视频，如果视频平台不对这些违规内容进行管控，则会带来重大的法律风险和品牌伤害。

## 违规视频问题的产生

UGC 或 PGC 的视频平台，与内容提供方、内容消费方及云点播的交互方式如下（第1 - 3步，可参考 [客户端上传](#)）：



1. 视频 App 后台对内容提供方进行鉴权，鉴权通过后派发 [客户端上传签名](#)。
2. 内容提供方执行上传，把分享的内容上传到腾讯云点播。
3. 云点播通知 App 后台成功上传的视频 FileId 和播放 URL 等 [相关信息](#)。
4. 内容消费方向视频 App 后台请求视频的播放 URL。
5. 内容消费方通过播放 URL，从云点播加速播放视频。

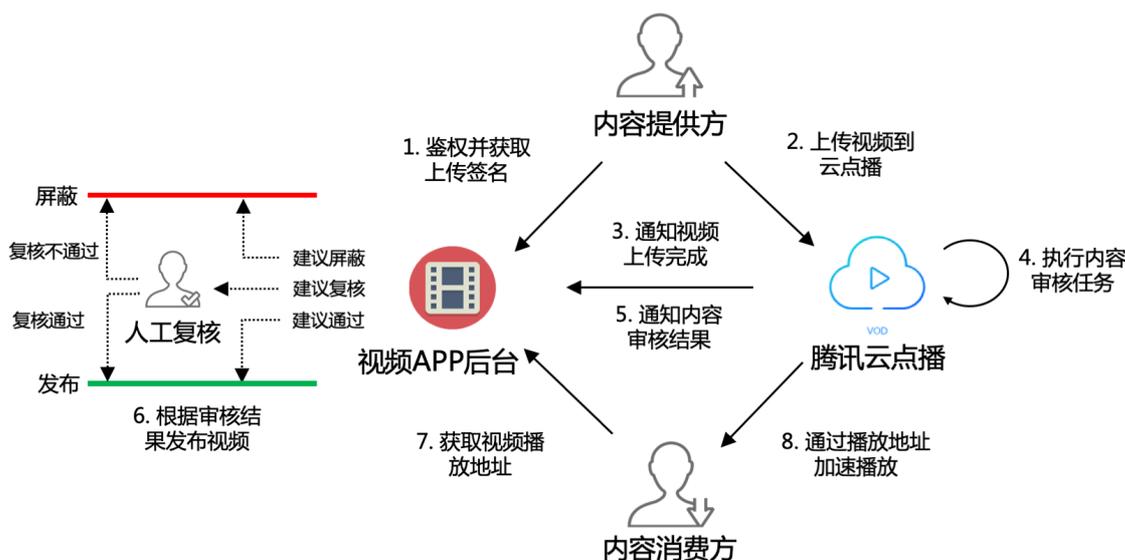
App 平台在第3步获取到视频的上传信息后，即在平台中发布该视频，允许第4步用户获取到视频的播放 URL 并播放视频。如果这个视频是违规视频，那么这些视频就会直接暴露给内容消费方。

## 引入视频内容审核

云点播提供了 [视频内容审核](#) 功能，可以对视频发起内容审核，并在审核结果中给出建议（建议屏蔽、建议复核和建议通过）。App 后台获取审核结果后，可以根据建议来决定是否发布视频：

- 审核结果为“block（建议屏蔽）”时，App 后台屏蔽该视频。
- 审核结果为“pass（建议通过）”时，App 后台直接发布该视频。
- 审核结果为“review（建议复核）”时，App 后台进行人工复核，选择是否发布视频。

启用云点播的视频内容审核，视频 App 后台可以高效识别并过滤违规视频，推荐使用的流程如下：



1. 视频 App 后台对内容提供方进行鉴权，鉴权通过后派发视频 [客户端上传签名](#)。
2. 内容提供方执行上传，把分享的内容上传到腾讯云点播。
3. 云点播通知视频 App 后台成功上传的视频 FileId 以及播放 URL 等 [相关信息](#)。
4. 云点播执行上传签名时对 `procedure` 参数进行配置的视频内容审核任务。
5. 云点播通过 [任务流状态变更](#) 通知视频 App 后台审核结果。
6. 视频 App 后台发布“建议通过”的视频，以及“建议复核”且经人工复核通过的视频。
7. 内容消费方向视频 App 后台请求已发布视频的播放 URL。

8. 内容消费方通过播放 URL，从云点播加速播放视频。

加入了第4 - 6步之后，以上的流程可以保证内容消费方在第7步获取到的视频是经审核验证的合规视频。

**⚠ 注意：**

此处介绍的流程属于“先审后发”模式（仅发布审核通过的视频）。如有需要，也可采用“先发后审”模式（视频上传完成后即发布，审核发现违规后再撤下视频）。

# 视频床问题与防范

最近更新时间：2019-05-07 17:19:41

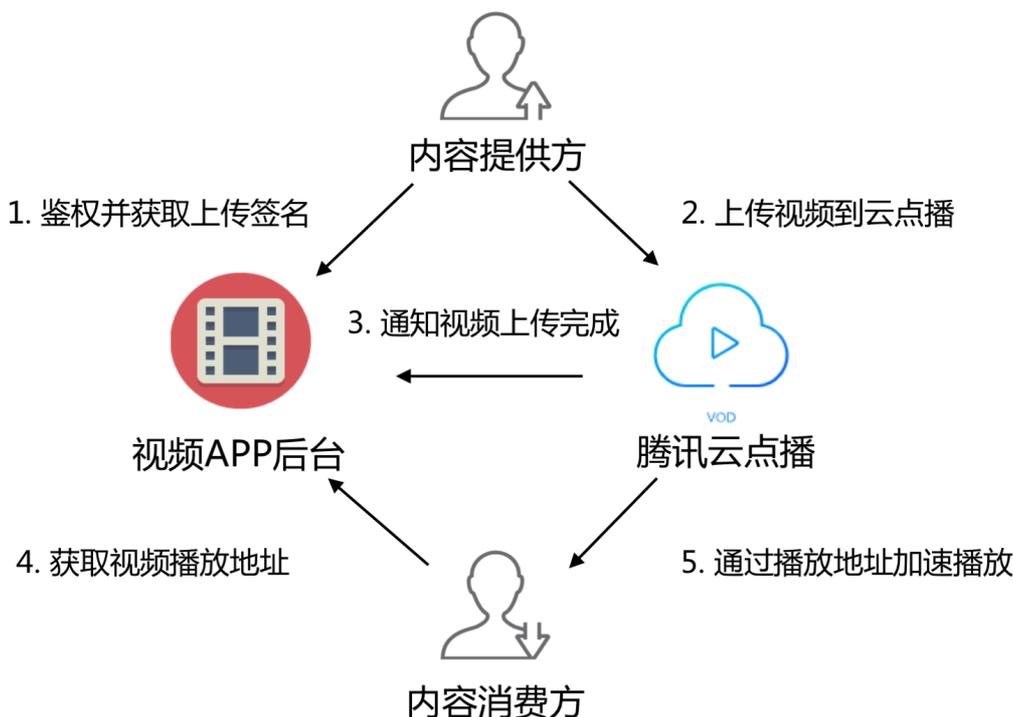
UGC（用户生产内容）和 PGC（专业生产内容）是视频行业中常见的两类场景，可以由视频分享者自由上传和分享视频内容。

然而，第三方的视频平台，可能会冒充 App 的普通用户，上传自有视频，然后将视频的播放 URL 放在自己的平台上播放。这样，他们就能“寄生”于开发者的平台，享受“免费”的视频存储和加速播放。因为开发者的视频平台被当做了他人视频的温床，我们称之为“视频床”。

寄生者产生的所有存储和播放带宽流量上的费用，全部需要 App 开发者来承担，是一项严重的经济损失。

## 视频床问题产生的原因

### UGC 和 PGC 平台的一般交互方式

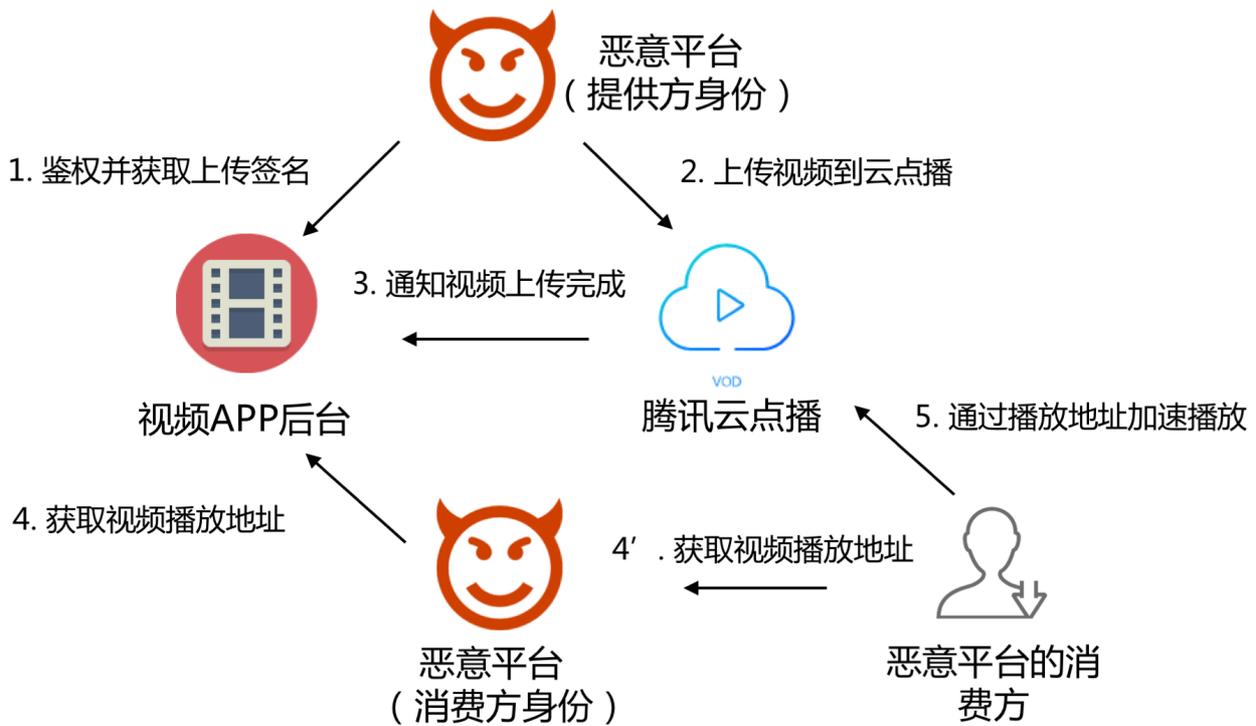


UGC（或 PGC）的视频平台，与内容提供方、内容消费方和云点播的交互方式如下（第 1-3 步，可参考 [客户端上传](#)）：

1. 视频 App 后台对内容提供方进行鉴权，鉴权通过后派发视频上传签名。
2. 内容提供方执行上传，把分享的内容上传到腾讯云点播。

3. 云点播通知视频 App 后台成功上传的视频 fileId，以及播放 URL 等相关信息。
4. 内容消费方向视频 App 后台请求视频的播放 URL。
5. 内容消费方通过播放 URL，从腾讯点播加速播放视频。

### 恶意用户如何实现视频床



恶意的第三方视频平台，会冒充开发者 App 平台的普通用户。首先，以视频提供方的身份，将自有视频上传到云点播中（第 1，2 步），然后再以消费者的身份，从 App 平台获取视频的播放地址（第 4 步）。最后，恶意平台自己的用户，可以获取到这些播放地址（第 4 步），并通过云点播加速播放这些视频（第 5 步）。

### 导致问题的核心原因

恶意用户寻找猎物作为视频床的根本目的，是盗用他人的 CDN 带宽资源（附带也占用了存储资源）。恶意用户有机可乘的核心原因在于：

- 第 4 步，恶意平台能无限制地从 App 快速获取视频的播放 URL，存储并分发给自己的消费用户。
- 第 5 步，恶意平台的消费用户获取视频的播放 URL 后，能够无限制地加速播放视频。

### 视频床防范方案

面对视频床问题以上的核心原因，关键在于：

- 防止第 4 步中的 **无限制获取视频播放 URL**。
- 防止第 5 步中的 **无限制加速播放视频**。

下面，将分别介绍如何限制视频 URL 的 **播放** 和 **获取**。

### 限制视频 URL 的播放

云点播的 [KEY 防盗链](#) 提供了限制 URL 允许播放终端数的能力，防止一个视频 URL 被传播给任意多个客户终端播放。

为了实现对视频播放 URL 的控制，开发者需要在控制台开启防盗链，并且第 4 步中 App 后台需要按照 KEY 防盗链生成规则（参考“[视频播放地址最多可播放 IP 数](#)”的 [示例](#)）生成防盗链，限制 URL 的有效时间和允许播放的 IP 数。

### 限制视频 URL 的获取

若仅限制视频的加速播放，视频床的防范是不完整的：第 4 步中，恶意平台能对同一视频请求大量不同的防盗链 URL，然后为自己平台的用户分发各不相同的 URL，避开 IP 播放数量的限制。

因此，App 后台需要识别第 4 步中的用户身份，对同一用户在给定时间内获取某一视频播放 URL 的次数进行频控，防止恶意用户短时间内获取视频的大量播放地址。

# 防盗链的测试

最近更新时间：2019-05-07 16:45:14

## 防盗链测试简介

云点播提供了 [防盗链](#) 功能，开发者可以根据实际需要，对视频播放 URL 使用的域名合理设置防盗链，实现对用户视频播放行为的控制。

然而，不经测试就对使用中的域名设置防盗链有以下风险：

- 可能导致现网用户播放失败。
- 可能未达到播放控制的效果。

例如，开发者希望对视频播放 URL 的有效期进行控制，就需要启用 [KEY 防盗链](#)：

- 如果生成的防盗链中签名参数 `sign` 计算错误，**启用防盗链可能导致现网所有视频播放失败。**
- 如果生成的防盗链中过期时间参数 `t` 过大，**启用防盗链后视频播放 URL 不会在预期的时间失效。**

因此，开发者为域名设置防盗链前应当先测试，确认符合预期后再执行变更操作。并且，开发者终端测试防盗链的同时，不能影响现网用户（即保证防盗链测试对现网安全）。

## 实现安全的防盗链测试

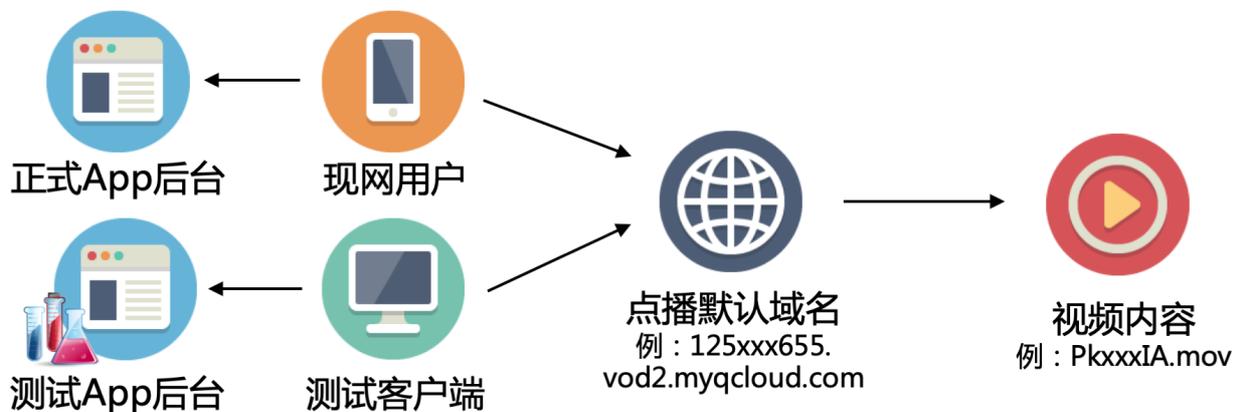
点播为开发者提供了安全测试防盗链的解决方案。

### 术语说明

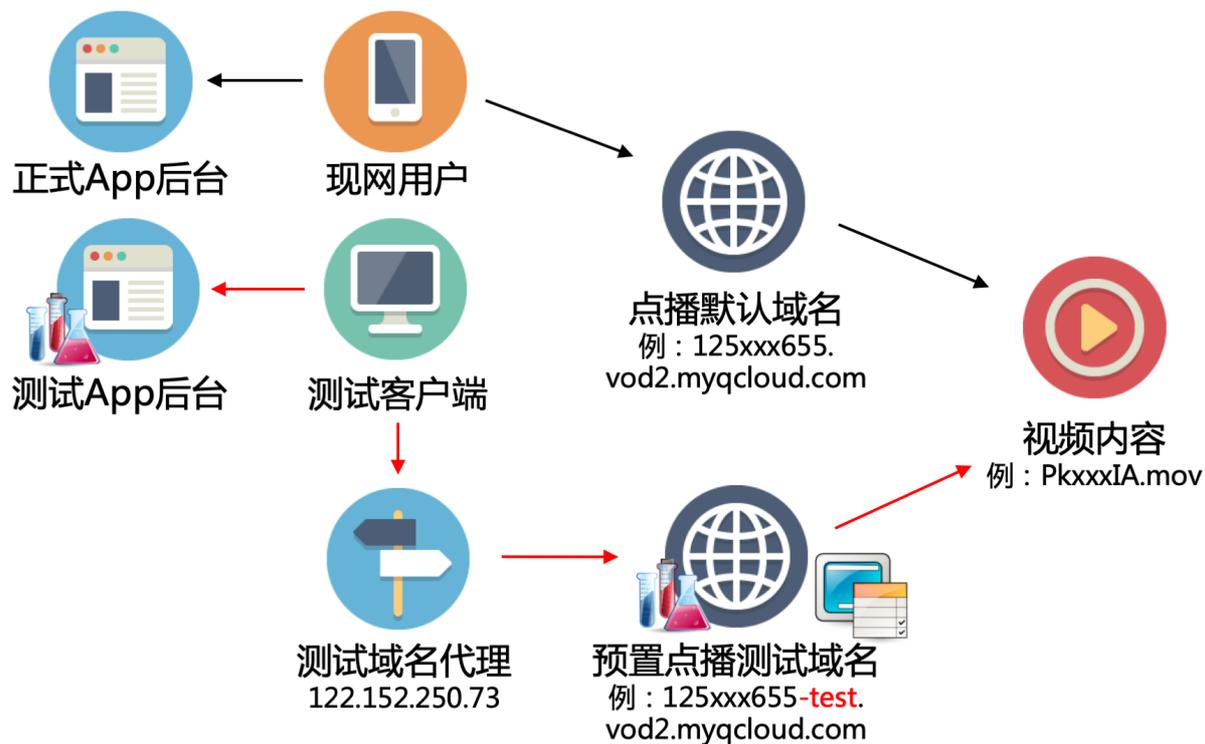
为了便于说明方案，下面介绍一些会涉及的术语：

- **点播默认域名**：现网环境中，用户播放点播视频使用的正式域名。“预置点播域名”和“自定义域名”都能被设置成“点播默认域名”（设置方法参见 [自定义域名](#) 文档）。
- **预置点播测试域名**：一个用于开发者调试的测试域名（通常为 `xxx-test.vod2.myqcloud.com`），不得用于现网环境，不能被设为默认域名。
- **正式 App 后台**：业务的 App 后台服务，现网用户从这里获取视频的播放 URL。
- **测试 App 后台**：业务测试环境中的 App 后台服务，测试客户端从这里获取视频的播放 URL。

### 方案细节



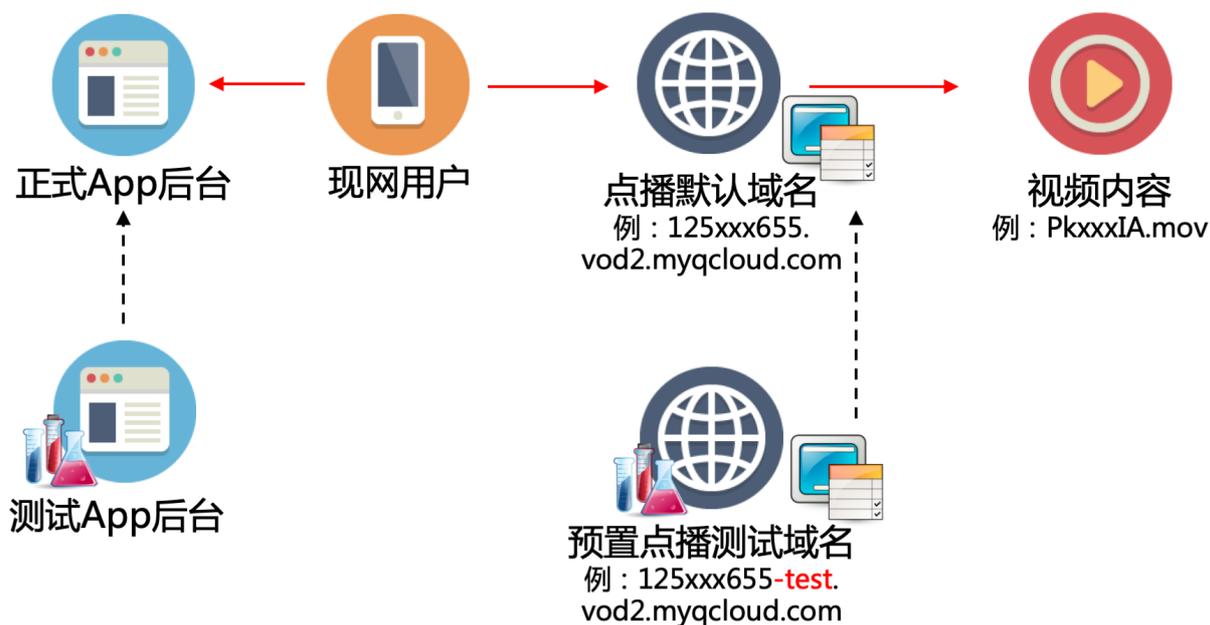
一般的，现网用户从业务的正式 App 后台获取视频的播放 URL，测试客户端从业务的测试 App 后台获取视频播放 URL，两处获得的 URL 中的域名相同（都是点播默认域名）。当对防盗链测试时，不能直接变更点播默认域名，否则现网用户将受到影响。



为了避免防盗链测试影响现网用户，点播提供了一个“预置点播测试域名”，与现网中使用的点播默认域名隔离。开发者测试防盗链时，仅操作测试域名的防盗链配置。

点播还提供了一个“测试域名代理”（IP 为 `122.152.250.73`），开发者只需要修改测试客户端的 HOST 表，将点播默认域名解析到这个代理上。这样，测试客户端的视频播放请求，将经过代理转发到测试域名（上图中的红色路径），而现网用户的播放请求仍然通过正式域名获取视频内容（上图中的黑色路径）。

因此，开发者可以自由修改测试域名的防盗链配置，以及测试 App 后台派发的视频播放 URL，而不必担心影响到现网用户。



开发者使用测试客户端和测试 App 后台，充分验证防盗链并确认无误后，就可以依次执行以下步骤：

1. 将正式 App 后台派发视频播放 URL 的规则修改成与测试 App 后台一致。
2. 将点播默认域名的防盗链配置修改成和预置点播测试域名一致。

这样，点播默认域名的防盗链正式生效，经过测试验证的防盗链配置被应用到了现网。

## 操作实例

下面，以用户开启 KEY 防盗链为例，介绍防盗链测试的操作步骤：

1. 预置点播测试域名开启防盗链。
2. 获取一个原始播放 URL。
3. 测试客户端仍然能够播放视频原始 URL。
4. 测试客户端修改 HOST 表。
5. 测试客户端不能再播放视频原始 URL。
6. 测试客户端能够播放带防盗链参数的 URL。
7. 正式 App 后台生成带防盗链参数的 URL。
8. 点播默认域名开启防盗链。

## 背景

域名	CNAME	状态	证书到期时间	备注	操作
★  125____655.vod2.myqcloud.com		域名已启动		腾讯域名	<a href="#">设置</a> <a href="#">设为默认域名</a>
★  125____655-test.vod2.myqcloud.com		域名已启动		测试域名	<a href="#">停用</a> <a href="#">设置</a> <a href="#">设为默认域名</a>

用户（例中 appid 为 125xxx655）登录点播控制台的【域名管理】后，将看到以下两种域名：

- 预置点播域名（125xxx655.vod2.myqcloud.com）。
- 预置点播测试域名（125xxx655-test.vod2.myqcloud.com）。

初始状态下，预置点播域名 125xxx655.vod2.myqcloud.com 为点播默认域名，并且没有开启 KEY 防盗链。

## 1. 预置点播测试域名开启防盗链

**Key防盗链** [防盗链文档](#) 

预置点播测试域名 125xxx655-test.vod2.myqcloud.com

启用Key防盗链

防盗链KEY

---

选择预置点播测试域名（125xxx655-test.vod2.myqcloud.com），单击【设置】链接，进入【Key 防盗链】，打开【启用 Key 防盗链】按钮，并使用【生成 KEY】生成一个防盗链 KEY。单击【确定】保存，等待配置生效。

## 2. 获取一个原始播放 URL

名称	解码率	
原始	2213kbps	预览播放  隐藏源地址

```
https://125xxx655.vod2.myqcloud.com/ca754badvodgzp125xxx655/cfb5fd5152858 复制代码
```

视频的原始播放 URL，是指没有带 [防盗链参数](#) 的 URL 地址，可以从控制台 [云视频管理](#) 中获得（如上图所示）。例子中使用的 URL 为：`https://125xxx655.vod2.myqcloud.com/ca7xxx655/cfbxxx349/PkxxxIA.mov`。

### 3. 测试客户端仍然能够播放视频原始 URL

```
MB0:~$ curl -I "https://125xxx655.vod2.myqcloud.com/ca7xxx655/cfbxxx349/PkxxxIA.mov"
HTTP/2 200
server: nws
date: Wed, 31 Oct 2018 03:16:24 GMT
content-type: application/octet-stream
content-length: 15733127
last-modified: Tue, 07 Aug 2018 15:02:41 GMT
```

此时，测试客户端仍然可以直接通过视频原始播放 URL 播放视频，执行 `curl` 返回的 HTTP 状态码为 200。

### 4. 测试客户端修改 HOST 表

```
##
# Host Database
#
# localhost is used to configure the loopback interface
# when the system is booting. Do not change this entry.
##
127.0.0.1      localhost
255.255.255.255 broadcasthost
::1          localhost
122.152.250.73 125xxx655.vod2.myqcloud.com
```

修改测试终端的 HOST 表（Windows 系统为 `C:\Windows\System32\drivers\etc\hosts`，Mac 系统为 `/private/etc/hosts`），添加一条记录 `122.152.250.73 125xxx655.vod2.myqcloud.com`，然后保存。

```
CHUXIONGYAN-MB0:~ chuxiongyan$ ping 125xxx655.vod2.myqcloud.com
PING 125xxx655.vod2.myqcloud.com (122.152.250.73): 56 data bytes
64 bytes from 122.152.250.73: icmp_seq=0 ttl=48 time=12.368 ms
64 bytes from 122.152.250.73: icmp_seq=1 ttl=48 time=12.354 ms
64 bytes from 122.152.250.73: icmp_seq=2 ttl=48 time=12.485 ms
64 bytes from 122.152.250.73: icmp_seq=3 ttl=48 time=12.553 ms
```

修改后，执行 `ping 125xxx655.vod2.myqcloud.com` 检查 HOST 修改是否生效。

## 5. 测试客户端不能再播放视频原始 URL

```
CHUXIONGYAN-MB0:~ chuxiongyan$ curl -I https://125xxx655.vod2.myqcloud.com/ca7xxx655/cfbxxx349/PkxxxxIA.mov
HTTP/1.1 403 Forbidden
Server: openresty
Date: Mon, 29 Oct 2018 01:54:08 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 128
Connection: close
```

修改 HOST 表后，测试客户端使用视频原始播放 URL 将无法播放，检查 HTTP 状态码为 403 Forbidden。因为修改了 HOST 表，测试客户端发起的视频播放请求，已经被映射到了预置点播测试域名，必须为视频播放 URL 带上正确的防盗链参数才能播放。

## 6. 测试客户端能够播放带防盗链参数的 URL

```
CHUXIONGYAN-MB0:~ chuxiongyan$ curl -I "https://1255566655.vod2.myqcloud.com/ca754bdvdvodzp1255566655/cfb5fd51285890780963510349/PkUeRlmlkIIA.mov?t=5bd6be00&sign=b3b98c71842aa4c486590a6d2c592941"
HTTP/2 200
server: nws
date: Wed, 31 Oct 2018 03:31:05 GMT
content-type: application/octet-stream
content-length: 15733127
last-modified: Tue, 07 Aug 2018 15:02:41 GMT
accept-ranges: bytes
```

按照 KEY 防盗链的 [生成规则](#) 生成带有防盗链参数的 URL，地址为 `https://125xxx655.vod2.myqcloud.com/ca7xxx655/cfbxxx349/PkxxxxIA.mov?t=5bd6be00&sign=18cxxx9deb`，就能成功播放视频了，执行 `curl` 返回的 HTTP 状态码为 200。

测试 App 后台按照防盗链生成规则，派发带有防盗链参数的 URL，并使用测试客户端进行验证。

## 7. 正式 App 后台生成带防盗链参数的 URL

测试环境验证后，业务正式 App 后台派发带防盗链参数的 URL，派发规则与测试 App 后台一致。

## 8. 点播默认域名开启防盗链

Key防盗链 [防盗链文档](#) 预置点播测试域名 125xxx655-test.vod2.myqcloud.com [编辑](#)

启用Key防盗链  已开启

防盗链KEY

先打开点播预置测试域名的【Key 防盗链】，复制测试域名的防盗链 KEY。

Key防盗链 [防盗链文档](#) 点播默认域名 125xxx655.vod2.myqcloud.com

启用Key防盗链

防盗链KEY

---

然后打开点播默认域名的【Key 防盗链】，把测试域名的 KEY 粘贴在【防盗链 KEY】文本框中，单击【确定】保存。

域名配置生效后，防盗链配置就会被应用到现网中使用的点播默认域名，并正式生效了。