阿里云
CDN

常见问题

文档版本：20190918

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
##	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 功能相关

1.1 阿里云CDN和国内其他CDN对比优势

介绍阿里云CDN和国内其他CDN对比的优势，有利于您更好的了解阿里云CDN。

阿里云CDN的优势如下：

- 阿里云CDN拥有全球超过1300个加速节点，是国内拥有最多节点的CDN服务商。
- 阿里云是国内领先的云计算厂商，多年的技术积累让阿里云CDN的调度系统非常高效和智能。
- 可用资源相对更充足，地域分布相对更广泛，在其他CDN通常只有大客户才能拥有比较多的节点资源。
- 命中率会相对更高，因为我们的节点采用的是一致性hash的方式，回源相对更少。
- 得益于阿里云在云计算领域的耕耘和先发优势，阿里云CDN的价格比其他CDN价格低，将云计算普惠进行到底。
- 标准化的配置响应更及时，我们是通过用户自助提交的方式实现自动化，而其它CDN是需要人工的交互，响应时间相对较长。阿里云CDN的控制台响应迅速，使用体验非常流畅。

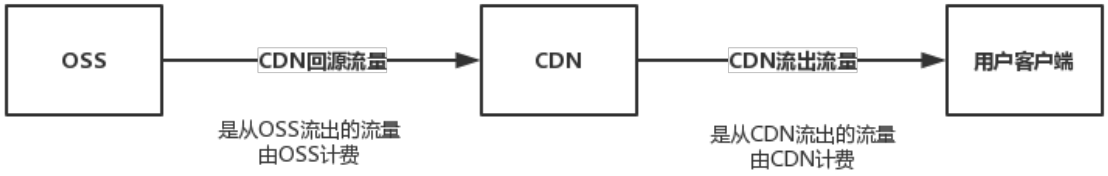
1.2 阿里云CDN与阿里云其他产品流量的关系

介绍阿里云CDN与阿里云其它产品流量的关系，有利于您更好的了解CDN产品流量计算方式。

阿里云CDN可与其他阿里云产品配合使用，如ECS、OSS等，由于CDN节点在全国多地均有分布，所以与其他云产品间流量通过公网传输。

CDN流量与其他云产品流量各自独立计费，之间并无关系。每个产品的收费请看每个产品的计费规则。

例如：某客户购买了CDN和OSS，来提供文件下载服务。当客户端访问CDN时，如果节点无对应的资源缓存，则需回源请求，就产生两次流量费用，分别是CDN的流出流量和OSS的流出流量，这两个流出流量由两个产品单独进行计费。



> **说明:**
> 阿里云各产品配套使用会有一定优惠和折扣。 例如，CDN回源OSS获取资源时，OSS的流出流量将有非常优惠的价格。

1.3 使用CDN加速的网站如何设置CORS访问

介绍使用CDN加速的网站如何设置CORS访问。

背景信息

网站使用CDN加速后，如果某个CDN节点下先发生了非跨域的访问，CDN会缓存一个没有CORS头部的文件内容，在过期之前发生的跨域访问，会因为没有CORS头部信息而导致访问报错。这种情况可以利用CDN的自定义Header的方式设置CORS的头部信息的方式来避免。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击缓存配置。
5. 单击HTTP头。
6. 在HTTP头设置页签，单击添加。

7. 根据需要设置Access-Control-Allow-Origin 、 Access-Control-Allow-Methods 和 Access-Control-Max-Age 的头部信息。

8. 查看设置的CORS头部信息。

```
[root@h ~]# curl -I http://video.youkouyang.com/1.png
HTTP/1.1 200 OK
Server: Tengine
Content-Type: image/png
Content-Length: 16300
Connection: keep-alive
Date: Fri, 11 Sep 2015 08:30:25 GMT
Accept-Ranges: bytes
Content-Disposition: attachment; filename="123321.jpg"
ETag: "CDA3B2549979B4AEB09DA21DCD2A500E"
Last-Modified: Mon, 03 Aug 2015 11:15:11 GMT
x-oss-object-type: Normal
x-oss-request-id: 55F29121257784D63A820895
Via: cache3.l2et2-1[124,200-0,M], cache43.l2et2-1[125,0], bcache1.cn24[140,200-0,M], bcache3.cn24[143,0]
X-Cache: MISS TCP_MISS dirn:-2:-2
X-Swift-SaveTime: Fri, 11 Sep 2015 08:30:25 GMT
X-Swift-CacheTime: 3600
Access-Control-Max-Age: 3600
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, HEAD
Access-Control-Allow-Origin: *
```

说明:

CDN控制台上设置的CORS等头部信息对整个加速域名生效，会覆盖掉源站设置的头部信息。

1.4 自定义404功能介绍

介绍自定义404错误码的原因、功能和注意事项。

背景信息

Web服务器返回HTTP 404状态码时，会自动跳转到404 Not Found页面。由于网页URL生成规则改变、网页文件更名或移动位置、导入链接拼写错误等，导致原来的URL地址无法访问；当Web服务器接收到类似请求时，会返回一个404状态码，告诉浏览器需要请求的资源并不存在。

导致这个错误的原因如下：

- 无法在所请求的端口上访问Web站点。
- Web服务扩展锁定策略阻止本请求。
- MIME映射策略阻止本请求。

说明:

访问单个资源时，若出现资源无法找到返回404状态码，将会跳转到404页面；若访问URL链接中包含多个资源，只有部分资源不能正常访问，则该页面不会发生404页面跳转。

404注意事项如下：

- 默认不开启自定义404服务，返回服务器默认的404 Not Found页面。
- 选择默认404，当http返回404时，会跳转到服务器默认的404 Not Found页面。
- 选择公益404，当http返回404时，将会跳转到富含公益主题的404页面。

- 选择自定义404，则需要自己设计和编辑符合网站整体风格的404页面，只需要将该页面资源如其他静态文件一样存储到源站域名下，并通过加速域名访问，只需填写完整的加速域名URL（包含http://）。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击缓存配置。
5. 单击自定义页面。
6. 在自定义页面页签，单击添加。

7. 选择自定义404页面，可以根据自身业务情况选择合适的404返回页面。
8. 单击确认。

   您也可以单击修改或删除，对当前配置进行相应操作。

1.5 CDN支持的调用方式

介绍CDN支持的调用方式。

除CONNECT调用方式之外，其他调用方式CDN均可支持，会透传至您的源站响应。

说明:

- CDN只对GET请求进行缓存，对于非GET请求的资源建议进行域名分离。
- 仅支持POST和 PUT方式发送带有请求体（BODY）的HTTP请求。

请求方式	描述	是否支持
GET	从指定的资源请求数据。	支持
POST	向指定的资源提交要被处理的数据。	支持
HEAD	与 GET 相同，但只返回HTTP 报头，不返回文档主体。	支持
PUT	上传指定的URI。	支持
DELETE	删除指定资源。	支持
OPTIONS	返回服务器支持的HTTP方法。	支持
CONNECT	把请求连接转换到透明的TCP/IP通道。	不支持

1.6 阿里云CDN健康检查机制

介绍阿里云CDN健康检查机制。

CDN智能调度系统会对所有CDN节点做健康检查，主要是针对各个节点做80端口检查，如果健康检查失败，则访问该节点的请求会被重新调度到附近的节点，保证节点可用性。

阿里云CDN对用户配置的源站地址有健康检查机制的。健康检查采用4层检查机制，测试源站的80端口。目前的检查策略为，每5秒检查一次，连续3次失败标记为不可用。 当源站不可用时，如果有一次成功，则标记为可用（恢复）。如果问题还未能解决，请提交工单。

1.7 CDN对源站健康检查机制

通过本文您可以了解阿里云CDN对源站的健康检查机制。

阿里云CDN对源站的健康检查采用四层检查机制，测试源站的80端口。检查策略如下：

- 每5秒检查一次，连续3次失败标记为不可用。
- 不可用时，有一次成功，即标记为可用（恢复）。

1.8 CDN与镜像站点的区别

介绍阿里云CDN与镜像站点的区别。

阿里云CDN用于文件加速，实现方式：由用户触发，CDN节点被动回源获取内容，缓存该资源的同时返回该资源给用户，是一个被动拉取数据的过程。后续对该资源的访问，CDN返回缓存资源给用户。

镜像站点是将数据全部都放在本地，用户请求时，直接推送给用户，不需要再额外回源取数据。

1.9 切换加速区域后的影响

介绍切换加速域名的加速区域后的影响。

为什么切换加速区域会导致回源流量增加和命中率下降?

加速区域由中国大陆修改为全球加速，增加了中国大陆以外的节点，这部分新节点没有缓存源站的资源。所以当请求访问该新节点时，新节点只能从源站获取资源，于是导致了短期内的回源流量增加。同时，这部分新节点的回源，短期内也会拉低整体节点的命中率。

回源流量增加可能会带来什么问题?

回源流量增加，您需要实时关注源站服务器是否能承受增加的回源流量。一般来说，阿里云CDN的二级节点会使回源的流量大大减少，但是为了防止可能的风险，建议您在切换加速区域后，关注源站服务器压力情况。如有问题，请提交工单。

2 域名接入相关

2.1 什么是CNAME记录

本文档通过介绍域名解析、A记录和CNAME记录的基本概念，帮助您更好地使用CDN加速。

什么是域名解析

了解CNAME之前，您需要了解域名解析。

为什么要解析域名?

因为，只有域名解析完成后，外部用户才可以通过域名访问网站。在您自助建站过程中，域名解析是必须的一步操作。当您购买完云服务器、部署完网站、购买完域名并备案完成后，就需要进行域名解析。

什么是域名解析?

当您购买了云服务器后，系统会默认给您这台服务器分配一个已经绑定的IP地址。由于IP地址是数字组成，不便于记忆，所以这时候就需要使用域名来代替，这就是。例如`www.aliyun.com`就是一个域名，它的背后就是一个IP地址。所以，域名解析就是把域名指向网站IP地址，让用户通过该域名即可方便地访问到您网站的一种服务。

阿里云通过云解析DNS（Alibaba Cloud DNS），提供域名解析服务。DNS是一种安全、快速、稳定、可扩展的权威DNS服务，云解析DNS为企业和开发者将易于管理识别的域名转换为计算机用于互连通信的数字IP地址，从而将用户的访问路由到相应的网站或应用服务器。了解更多，请参考云解析DNS。

如何进行域名解析?

国内的域名注册商大多有自己的DNS服务器。以阿里云云解析DNS为例，您可以查看文档完成操作，详情请参见云解析新手引导。

什么是A记录

配置域名解析中，您需要选择记录类型，这就需要了解什么是A记录。

A记录又被称为IP指向，用来记录域名对应的IP地址。下图中，主机记录是域名前缀（常用的域名前缀一般是 www、mail 等），记录值是您网站服务器的 IP 地址。

如果您在购买了多个域名，希望将多个域名都指向同一个网站服务器上时，这就需要对这些子域名（即顶级域名下面的二级域名、三级域名都称之为子域名）进行设置，并指向自己的网站服务器上。

但是，当您需要更换云服务器时，这些原本指向这台服务器的域名就需要重新设置，并指向新的服务器，这样就会产生比较大的工作量。这时，如果使用CNAME记录就会比较方便。

什么是CNAME记录

CNAME记录又叫别名记录，用来把域名解析到其他域名上，通常用于mail邮箱解析和CDN加速解析。

如果您想为您的网站实现CDN加速，配置CNAME是最关键的一步。开通CDN服务、添加域名成功后，阿里云CDN会分配对应的CNAME地址。您需要将域名指向CNAME地址，访问加速域名的请求才能转发到CDN节点上，达到加速效果。您可以查看文档完成操作，详情请参见#unique_15。

CNAME指向的域名，最终也要指向A记录。

CNAME记录与A记录

区别

A记录就是把一个域名解析到一个IP地址，而CNAME记录则是把域名解析到另外一个域名。

选择

如果您的目的是长期建站，建议您使用CNAME记录。因为CNAME可以用于CDN加速，在加速的同时，又能够隐藏网站的真实IP地址，减少被攻击的几率。

CNAME在CDN加速中的原理

CDN的主要功能，是将您源站的内容，缓存到距离您网站访问用户最近的节点（缓存服务器）上，以此实现用户对您网站资源的。CNAME的参与必不可少。详情请参见#unique_16

2.2 CDN支持泛域名加速吗?

泛域名是指利用 （通配符）来做加速域名以实现所有的次级域名加速效果，例如您添加了.test.com 作为加速域名，将 `*.test.com` 解析至 CDN 生成的 CNAME域名后，则所有test.com的次级域名（如`a.test.com`）均支持 CDN 加速。注意：泛域名（`*.test.com`）的三级域名（如`b.a.test.com`）不提供加速服务。

阿里云CDN 支持泛域名加速。目前支持泛域名加速的加速业务类型如下：

- 图片小文件加速
- 大文件下载加速

- 视音频点播加速

泛域名添加规则

- 加速域名总长度小于100字节
- 最多支持4级泛域名（3个点，比如: `*.b.c.com`）
- 计费方面，泛域名所有次级域名的流量都会和普通域名一样产生费用，资源监控中会将泛域名产生的流量做汇总，单个泛域名加速将按照一个加速域名做计费处理，即不提供单个准确次级域名的计费数据。

注意事项

日志方面，单个泛域名每个时段提供一份日志文件，日志中将包含该泛域名的所有次级域名加速日志信息。

刷新或预热缓存时不支持泛域名 URL 或者泛域名文件夹，支持刷新准确域名的 URL 和目录。

2.3 如何处理CDN域名审核失败问题?

现象描述

在CDN控制台上，添加新域名审核失败。

原因分析

如果您源站不在阿里云，则接入时需要进行审核，审核失败的原因如下:

- 无法正常访问或内容不含有任何实质信息
- 游戏私服类
- 传奇类游戏和纸牌类游戏
- 盗版软件等无版权下载网站
- P2P类金融网站
- 彩票类网站
- 违规医院和药品类网站
- 涉黄、涉毒、涉赌等

处理方法

1. 登录阿里云CDN平台
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，选择审核失败域名对应的更多 > 删除。
4. 审核失败后点击域名列表中审核失败域名右侧的删除，先将域名进行删除。

5. **处理域名审核失败问题，重新添加域名。**

   重新添加域名的操作方法，请参见#unique_19。

3 刷新预热相关

3.1 CDN使用JAVA SDK刷新缓存示例代码

本文为您介绍了CDN使用JAVA SDK刷新缓存。

阿里云CDN为您提供了JAVA、Python、PHP、.Net等多种语言的SDK，详情请参见阿里云SDK中心。

使用JAVA SDK刷新缓存的示例代码如下所示。

1. 引入SDK。

   请在pom.xml文件中添加以下依赖，准确的SDK版本号，详情请参见阿里云SDK中心。

```
<!--添加阿里云core依赖和cdn依赖-->
<dependency>
   <groupId>com.aliyun</groupId>
   <artifactId>aliyun-java-sdk-cdn</artifactId>
   <version>3.0.10</version>
</dependency>
<dependency>
   <groupId>com.aliyun</groupId>
   <artifactId>aliyun-java-sdk-core</artifactId>
   <version>4.1.0</version>
</dependency>
```

2. 初始化Client。

   发起调用前，请先初始化IAcsClient实例。示例代码如下：

```
DefaultProfile profile = DefaultProfile.getProfile("cn-hangzhou", "<
accessKeyId>", "<accessSecret>");
IAcsClient client = new DefaultAcsClient(profile);
```

3. 构造刷新请求。

   完整的示例代码如下：

```
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.google.gson.Gson;
import java.util.*;
import com.aliyuncs.cdn.model.v20180510.*;

public class RefreshObjectCaches {
    public static void main(String[] args) {
        DefaultProfile profile = DefaultProfile.getProfile("cn-
hangzhou", "<accessKeyId>", "<accessSecret>");
        IAcsClient client = new DefaultAcsClient(profile);
```

```
        RefreshObjectCachesRequest request = new RefreshObj
ectCachesRequest();
        request.setObjectPath("www.abc.com/abc/1.png");
        request.setObjectType("File");
        try {
            RefreshObjectCachesResponse response = client.getAcsResp
onse(request);
            System.out.println(new Gson().toJson(response));
        } catch (ServerException e) {
            e.printStackTrace();
        } catch (ClientException e) {
            System.out.println("ErrCode:" + e.getErrCode());
            System.out.println("ErrMsg:" + e.getErrMsg());
            System.out.println("RequestId:" + e.getRequestId());
        }
    }
}
```

如果问题还未解决，请联系售后技术支持。

4 计费相关

4.1 CDN按月95计费说明

- 仅支持部分用户： 为月消费金额大于10万的用户提供了更为灵活的月度95带宽峰值计费方式，有需求的用户可以联系阿里云商务洽谈接入
- 计费项：95峰值带宽

> 说明:
>
> - 95带宽峰值计费按自然月结算，在一个自然月内，按账户取每5分钟有效带宽值进行降序排列，然后把带宽数值最高的5%的点去掉，剩下的最高带宽就是95带宽峰值计费值。以一月30天为例，默认均为有效取值点：每5分钟1个带宽取值点，每小时12个取值点，每月取值点数为 12 x 24 x 30 = 8640个；将所有的点按带宽数值降序排列，去掉前5%的点 8640 x 5 % = 432 个点，即第433个点为计费点。
> - 国内和国外的 95 带宽将分开统计。即国内和国外的带宽分别排序，取各自的 95 峰值和对应的峰值时刻用于计费值。

- 计费规则

  计费项：95峰值带宽/月

  - 付费方式：后付费
  - 计费规则：以账户为维度，按95%峰值带宽阶梯价格计费，当月国内费用和国外费用分别超额累进（以自然月为一个累计周期）。
  - 计费周期：按自然月计费。
  - 有效天数：对在计费周期内变配至 95 计费的用户来说，有效天数为 95 计费生效那天开始到月末的天数（如 2016-04-05 为 95 计费生效时间，则 2016-04 期账单的有效使用天数为 26 天）。
  - 有效因子：以一个自然月的天数为分母，该自然月内用户的有效使用天数为分子计算得到的小数（假设 2016-04 账期有效天数为 26 天，则有效因子为 26 / 30 = 0.86666667）。
  - 最终费用：按上述计费规则得到的费用 x 有效因子。

  > 说明:
  >
  > ■ 账单出账时间：计费周期结束的下个自然月1日凌晨的出账并进行结算。举例：3月1日会产生2月的月95带宽峰值计费账单（2017-02-01 00:00:00 至 2017-02-28 23:59:59）。

- 结算时间：每个自然月1日账单生成后会自动从您的账户余额中扣除费用以结算账单。请确保账单出账和结算时刻账户的余额充足，以免出现欠费问题（了解CDN欠费说明）。您可以在CDN控制台-用量查询查看当月95带宽峰值，预估本月95带宽消费金额。
- 计费方式切换生效时间说明：
  - 从“流量”或“带宽”变更成为“月结95带宽”计费类型，第二日零点生效；
  - 从“月结95带宽”变更成为“流量”或“带宽”计费类型，下个自然月1日零点生效，月中不允许变更。相关链接：CDN价格总览。

4.2 停用CDN服务后，为什么仍会有一部分费用产生

造成这种情况主要有以下两个原因：

- 由于一些用户的LocalDNS服务器有缓存，在停用CDN服务后，若客户LocalDNS服务器中缓存未过期，LocalDNS还会把访问已停用CDN域名的请求解析到CDN节点，造成少量CDN流量计费。
- 一些下载类软件也存在LocalDNS缓存，在这部分缓存过期前，下载类软件也会把访问已停用CDN域名的请求解析到CDN节点上，造成少量CDN流量计费。

5 安全相关

5.1 沙箱说明

什么是沙箱?

阿里云CDN是公共的加速服务，承载着成千上万的域名加速，所以当您的域名遭受攻击时，CDN系统会自动将您的域名切入沙箱，防止影响其他正常用户的加速服务。攻击较严重的，同账户下的其他域名也被切入沙箱。域名切入沙箱后依旧保有CDN加速服务，但不再保证服务质量。

如何查询域名是否处于沙箱中?

当您的域名被切入沙箱中后，您会收到一条短信提示。同时您可以在CDN控制台的域名状态中，看到域名处于沙箱中，如下图所示。

域名进入沙箱后能否恢复?

为防止影响其他正常用户的加速服务，您受攻击的域名进入沙箱后无法恢复。

如何解决?

阿里云CDN是加速服务，默认不提供抗攻击能力。您的域名进入沙箱后，服务质量不再保证且无法恢复。您可以根据自身是否有防攻击的需求选择使用 安全加速SCDN或阿里云高防产品

注意:

- 对于多次被攻击或违反产品限制导致被攻击的用户，阿里云CDN保留不再接入加速服务的权利。违反产品限制接入的域名，若您的域名遭受攻击，您需要自行承担因攻击而产生的全额费用。
- 如果您使用纯海外加速区域的未备案域名，则该域名切入沙箱后将无法访问。

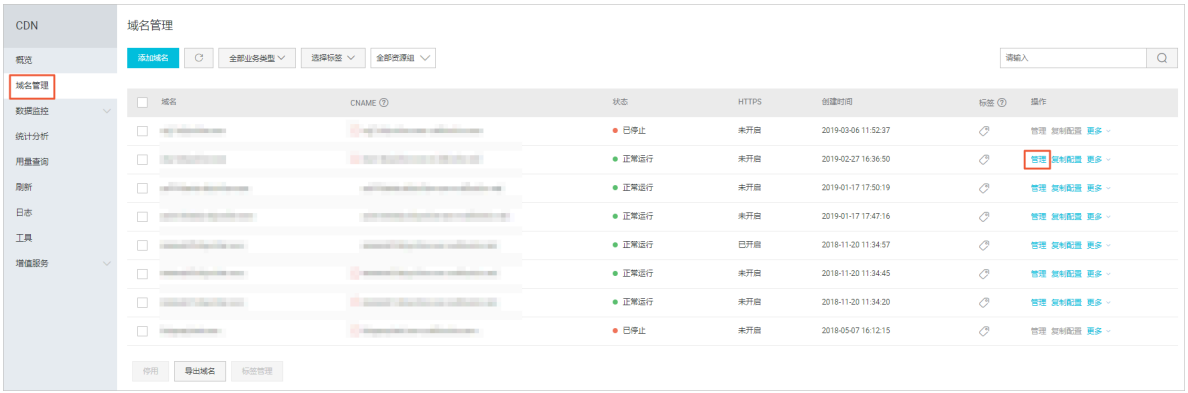
6 加速内容

6.1 CDN支持cors（跨域）配置的步骤与注意事项

目前，CDN已开放支持cors跨域访问的白名单配置功能。本文档为您介绍在使用CDN产品时如何进行cors功能配置及注意事项。

操作步骤

1. 登录CDN控制台，单击域名管理。
2. 选择需要配置cors功能的域名，单击管理。



3. 单击缓存配置 > HTTP头，单击添加。

4. 配置参数，选择Access-Control-Allow-Origin参数。

说明:

参数Access-Control-Allow-Origin的取值不支持多个域名。

5. 配置参数，选择Access-Control-Allow-Methods参数。

注意事项

- 目前不支持泛域名添加，如*.12345.com，仅支持域名精确匹配。
- 目前仅支持配置一条白名单域名。
- 若使用OSS产品作为源站，OSS与CDN平台同时配置Cors，CDN的配置将覆盖OSS。
- 若源站为自己的服务器或ECS产品，建议先进行动静分离，静态文件使用CDN加速，CDN控制台配置的Cors功能，仅对静态文件生效。

6.2 如何处理未备案域名?

问题

依据中国大陆相关法律法规，阿里云CDN不能为中国大陆未备案的域名提供加速服务。因此当您域名的备案信息失效时，阿里云CDN将依法停止其加速服务。如何处理未备案或备案信息失效域名?

方法一:

建议您暂时将域名的加速区域修改为全球（不包含中国大陆）。该加速区域不使用中国大陆内的节点，域名无需备案。

域名采用海外加速收费较高，具体请参见CDN 详细价格信息。

说明:

海外指中国香港、中国澳门、中国台湾和海外。

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在基础信息区域，单击修改配置。
5. 在加速区域对话框，将加速区域修改为全球（不包含中国大陆）。
6. 单击确定。

方法二:

建议您暂时将业务迁出阿里云CDN，使用友商CDN服务，待备案补充完成后再重新接入阿里云CDN。

7 故障检测

7.1 CDN某个地域节点访问异常

问题症状

- 问题1：某地区客户ping不通CDN的加速域名。

  原因：用户本地网络异常；节点网络异常或者被攻击；用户本地到运营商中间链路某路由节点故障。
- 问题2：源站更改文件之后，某个地区的用户从CDN节点上拿到的还是更改之前的文件。

  原因：刷新未生效；读取的是本地浏览器缓存；被本地运营商劫持。
- 问题3：某个地区用户访问CDN加速域名上拿到的非其站点文件内容。

  原因：访问的非CDN节点；被劫持。

解决方案

问题1：某地区用户ping不通CDN的加速域名

1. 排查用户的加速域名是否在沙箱节点中（目前可以在CDN控制台得知其加速域名是否在CDN沙箱节点）。以ycc.pier39.cn为例，域名在沙箱中，则控制台域名状态提示会如下图所示：

   沙箱中的域名无法保证服务稳定性，所以会存在ping不通的情况，此时可能沙箱正在受到攻击。

2. 根据提交的Ping截图，拿到所访问的节点IP，核实该IP是否是CDN节点IP，以IP：1.2.3.4，域名zihu-live.pier39.cn为例，请按照 这里的方法核查是否该IP为CDN节点。

   如果用户的访问节点不是CDN节点IP，需要用户核实几个情况：

   - 用户本地是否有开启代理软件（有些代理软件会强制更改访问域名的解析情况）。
   - 用户是否有绑定Host文件，将加速域名强制解析到了某个IP。
   - 用户本地存在DNS劫持，这种情况，让用户本地开启杀毒安全软件，并且固定本地所使用的DNS为阿里的223或者电信的114或者其他知名的DNS，如果劫持情况比较严重，并且无法解决，则需要向你的网络服务提供商投诉要求解决劫持。

3. 自己本地实际ping该节点IP，以及使用站长工具（比如17ce.com或者听云平台）在全国探测该节点IP，是否存在问题（问题现象：各个地区访问该节点均延迟均较大或者不通，自己本地也Ping该节点不通），这种情况该节点存在问题的可能性较大（结合步骤1确认好域名确实没有在沙箱中）。
4. 让用户本地使用tracert（win主机）或者traceroute（linux主机）到该IP进行探测并提供完整探测截图，根据得到的截图确定整个网络链路的问题点。MTR信息判断方法：目的节点丢包率为100%，并且从目的节点往前一直找到第一个开始丢包的节点（中间不能有丢包率为0%的路由节点），则第一个开始丢包的路由节点是问题路由的可能性较大。详细排查步骤可以参考 这篇文章。

   也可以给阿里云技术同学进行排查。在此期间缓解用户问题的方法：让用户更改本地所使用的localDNS为其他DNS（比如电信的114或者阿里的223）并且刷新本地的DNS缓存，使其调度到其他正常的节点，走另外一条线路，则该问题可能得到缓解。

问题2：源站更改文件之后，某个地区的用户从CDN节点上拿到的还是更改之前的文件。

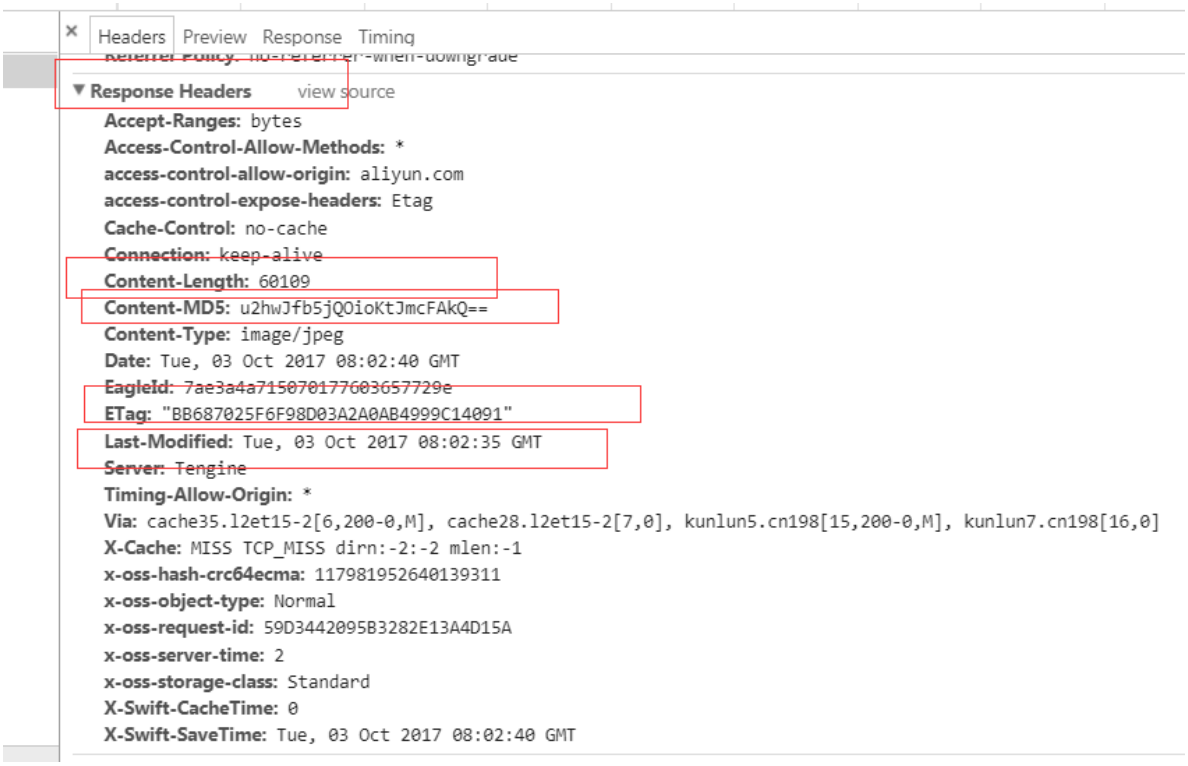
1. 让客户提交ping CDN加速域名的截图，拿到客户访问的节点IP。
2. 判断该节点是否是CDN的节点，判断方法请看问题*1*的步骤*2*。
3. 根据CDN的配置，绑定客户提供的CDN节点，以及CDN的源站（绑定用户源站测试的时候#注意一下用户*CDN*的回源*Host*配置#举例#如果用户*CDN*加速域名为*A*#源站域名为*B*#回源*Host*配置的为*A*#那么测试源站的时候#以*curl*来说#命令应该为*curl -H “Host: A” “B”*#如果是绑定*Host*文件#那么应该将用户的*CDN*加速域名绑定*Host*到源站域名所解析出来的*IP*上），绑定源站测试

的时候，还要注意一下源站回源端口的设置，不同的回源端口得到的访问结果也可能是不一样的；分别测试得到response header相关信息，判断是否如客户所说访问的文件会是不一致。

这里判断是否一致，着重看几点：

- ***content-length***大小是否一致
- ***last-modified***(如果有)：修改时间是否一致
- ***Etag/Content-Md5***（如果有）是否一致

上述三点只要有任何一个是不一致的，那么均可认为源站和节点上文件的确是不一致的，上述三点中，条件允许（意思是几个信息都有的情况下）其中第三点是最具备判断依据的点。



4. 上述步骤确认都OK，并且最终还是拿到节点上文件的确和源站文件不一致的情况下，那么建议用户刷新该URL，等待约10分钟之后再去测试（刷新生效时间约为5~10分钟），如果多次刷新之后问题仍未解决，请提交工单。

某个地区用户访问CDN加速域名上拿到的非其站点文件内容。

1. 判断用户访问的IP是否CDN的节点IP，方法看*问题1*的*步骤2*。
2. 排查是否CDN节点本身缓存了非用户站点上的文件，思路可以按照*问题2*系列步骤进行，下面针对用户客户端到CDN L1这一段链路进行方法排查用户在能够复现问题的情况下，使其使用浏览器开发者工具，切到network标签下，浏览器地址栏键入访问URL然后回车访问，network标签下，点击用户访问的那个URL，截图general /request header，看看用户实际的访问情

况，报错request URl、remote ip、requestUrl主要看访问形式是否如`http://x.x.x.x/cache/CDN`的访问URL或者remote IP非CDN节点IP，如下图这种则是劫持：

需要联系其本地运营商投诉处理，解除劫持。

相关文档

如何判断问题出现在节点还是本地

CDN节点IP核实方法

8 故障处理

8.1 如何解决CDN控制台无法删除域名的问题?

问题场景:

登陆CDN控制台想要删除加速域名，但是控制台删除按钮是灰色的，无法进行删除操作。

解决方法:

正常运行状态下的域名无法直接删除，您需要登录CDN控制台，停用目标加速域名，然后才能删除该域名。

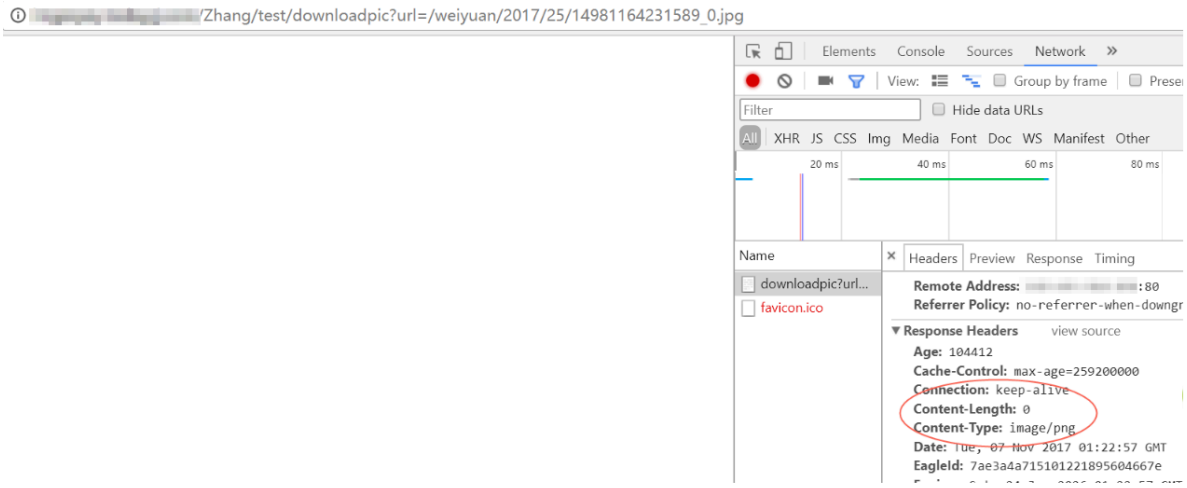
8.2 如何解决设置CDN时，报错“检测到没有启用状态的AccessKey，暂不提供CNAME绑定服务”的问题?

您可以通过创建accesskeys解决该报错问题。如何创建，请参见#unique_38。

8.3 如何解决使用CDN加速后，页面出现空白页面的问题?

如果您使用CDN加速访问URL时，出现空白页面的情况，可以通过如下操作解决该问题。

1. **访问源站，通过开发者工具查看Content-Length是否为0，如下图所示。**



2. **如果Content-Length为0，您可以请求源站，看源站是否返回头信息Transfer-Encoding: chunked。由于CDN不支持该头信息，您只需删除它即可。**

8.4 如何排查微信小程序访问CDN证书校验失败的情况?

Android端微信小程序访问CDN的HTTPS请求，出现证书校验失败时，您可以按如下步骤进行排查：

1. 在Android端微信小程序端访问CDN的证书出现校验失败的情况，而在其他的浏览器中测试均是正常的，排查中间证书是否存在问题。
2. 查看其证书链是否完整，如果完整，说明不是证书链问题。
3. 排查是否是SNI问题导致的该问题，抓取Android微信端访问具体异常。
4. 分析该客户端发起请求到服务器端，与服务器端交换证书报Certificate Unknown后抛出Reset，并且查看客户端发出的SSL请求也带有SNI信息。测试结果如下图：

图 8-1: 客户端与服务器端交换证书后报错并发送RST包

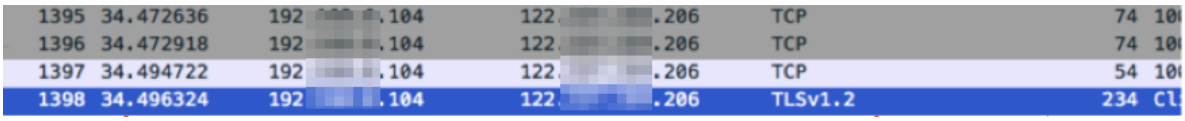
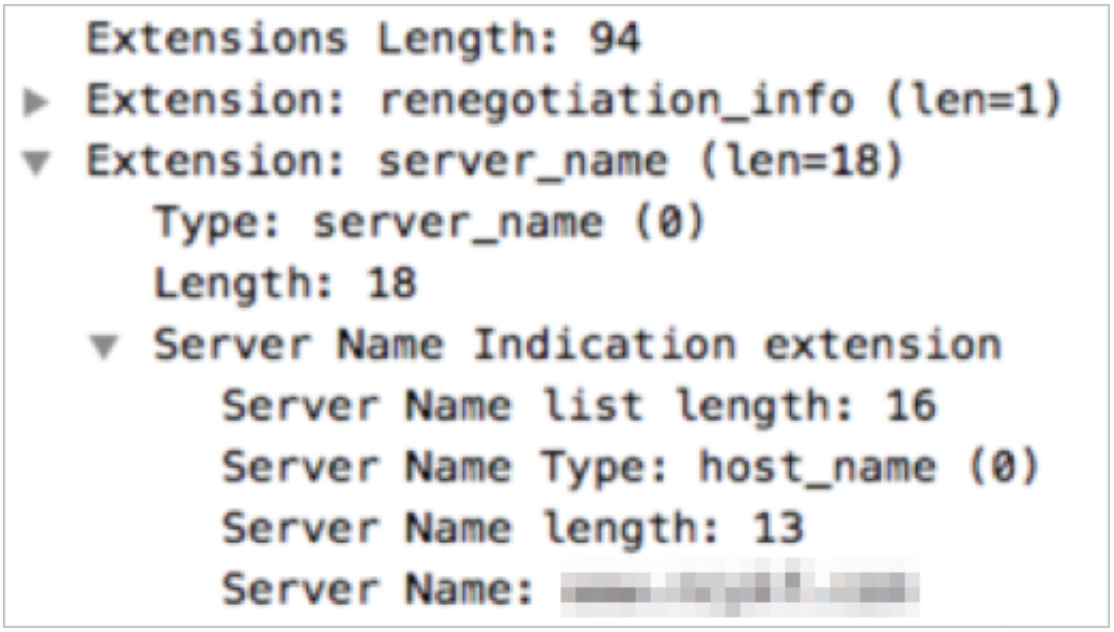
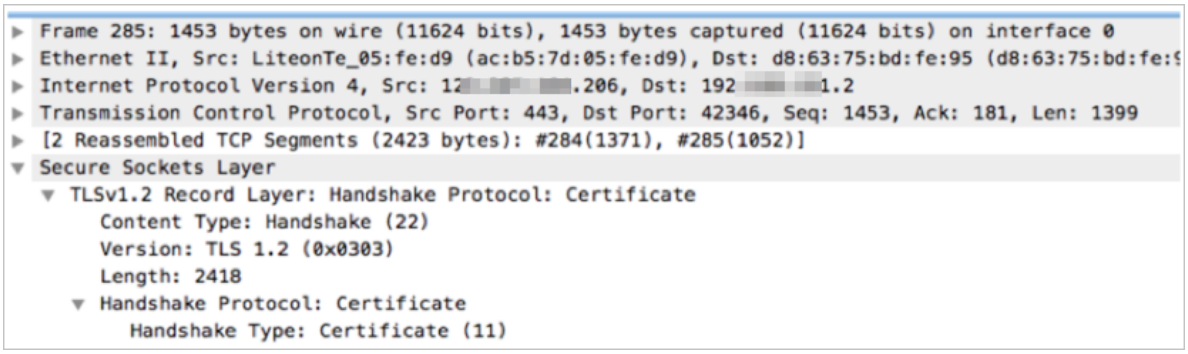


图 8-2: 客户端携带的SNI信息



5. 查看CDN节点服务器端返回的证书也是该域名的证书，并没有查看到异常。CDN服务器端返回证书情况如下图：

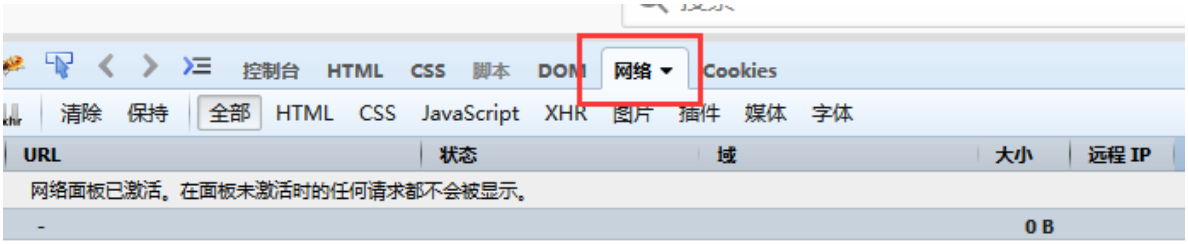


6. 发现提交的中间证书错误导致该问题。而导出中间证书可以使用浏览器的导出证书功能。导出中间证书方式如下图所示。

8.5 如何排查某个URL是否命中CDN缓存的情况?

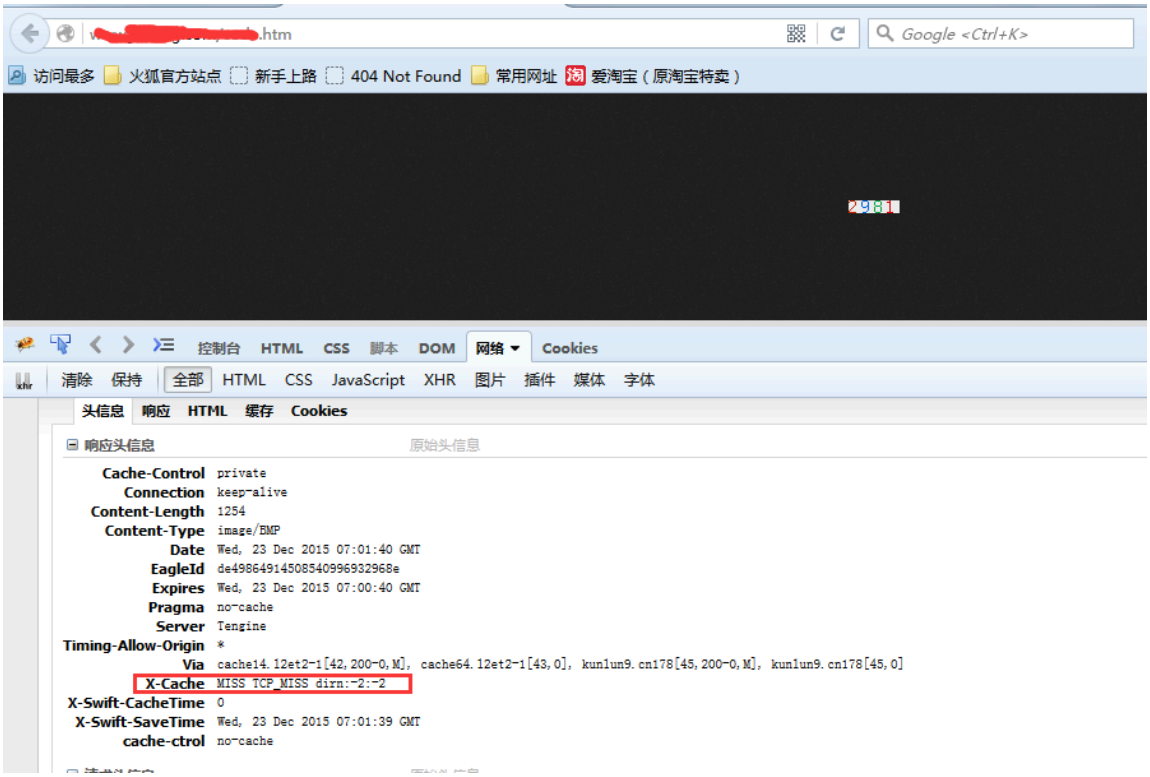
使用CDN后，您可以通过浏览器进行简单的访问测试，查看访问网站是否命中CDN缓存。具体方法如下：

1. 使用Chrome或者火狐浏览器，在浏览器界面，按F12打开浏览器调试界面，然后选择网络或Network。

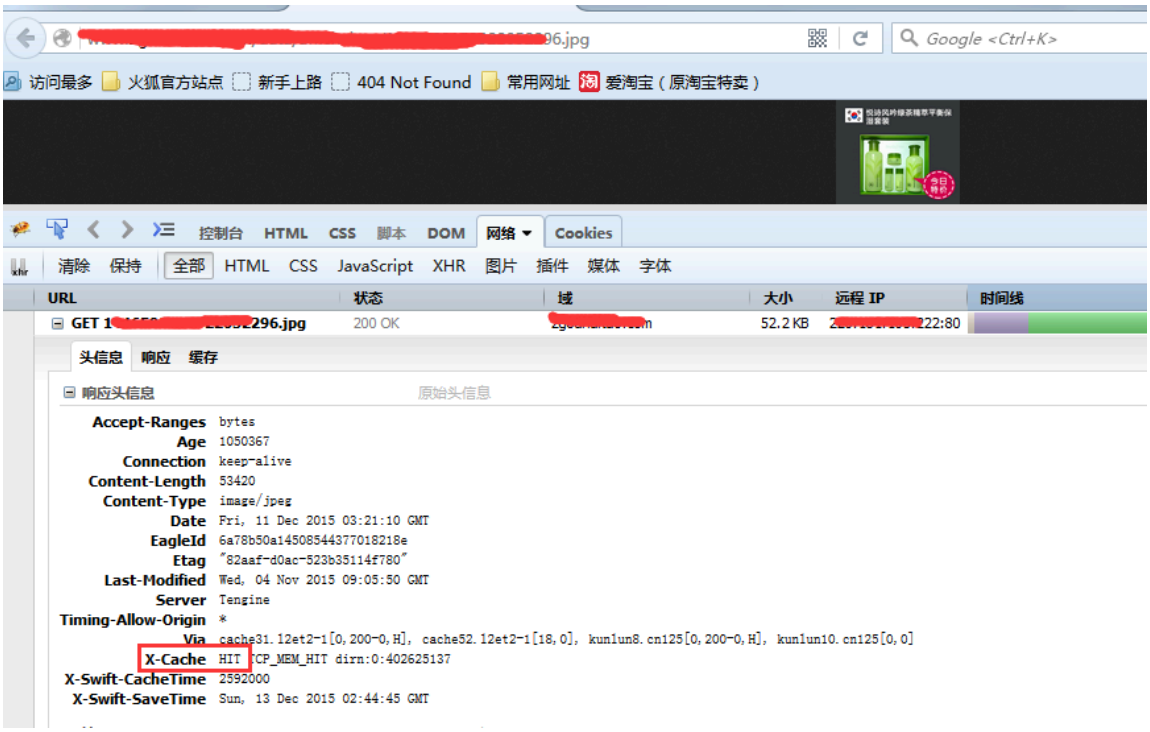


2. 访问一个网站链接，查看响应头信息中的X-Cache字段。

- 显示MISS，说明没有命中CDN缓存，是回源的。



- 显示HIT，说明命中了CDN缓存。



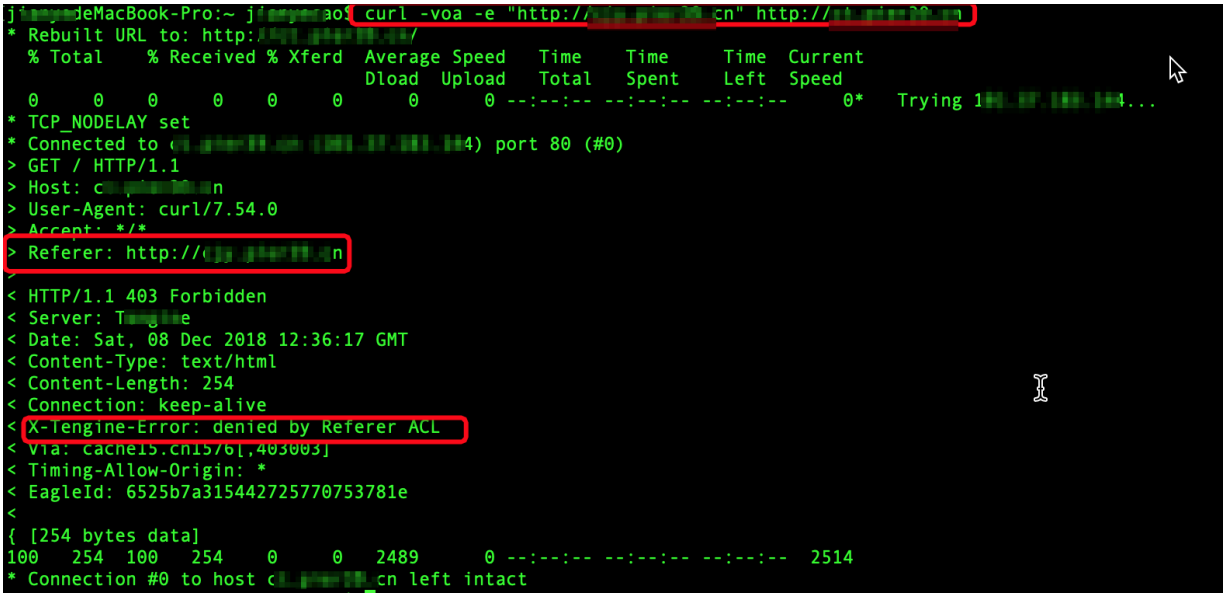
如问题还未解决，请提交工单。

8.6 如何处理CDN由于防盗链异常导致的403问题?

如果您的防盗链设置异常，则可以使用curl命令模拟场景。

非空refer场景模拟

非空refer场景模拟，如下图。



排查步骤如下：

1. 查询错误信息。从上图看出request请求的http头带有`refer example1.cn`，出现403错误，具体错误信息为denied by Referer ACL。
2. 判断`refer example1.cn`与加速域名`example2.cn`设置的防盗链是否匹配。
3. 查看您的防盗链配置。

   查看防盗链的操作方法，请参考#unique_43。

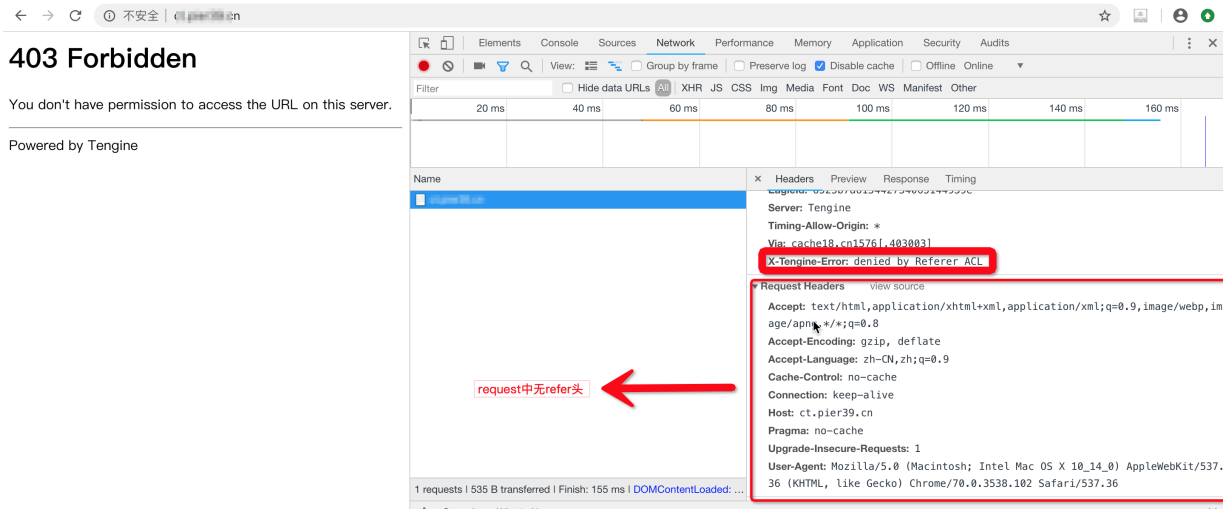
结论：由于防盗链设置和请求referer不匹配导致403错误。

解决方法：在防盗链配置的白名单中，增加`example2.cn`即可。操作方法请参见#unique_43。

空refer场景模拟

空refer场景模拟，如下图。

```
MacBook-Pro:~ j          o$ curl -voa  http:/          n
* Rebuilt URL to: http://c          n/
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0*   Trying          ...
* TCP_NODELAY set
* Connected to c          n (1          8) port 80 (#0)
> GET / HTTP/1.1
> Host:
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 403 Forbidden
< Server: Tengine
< Date: Sat, 08 Dec 2018 12:48:50 GMT
< Content-Type: text/html
< Content-Length: 254
< Connection: keep-alive
< X-Tengine-Error: denied by Referer ACL
< Via: cache5.cn1576[,403003]
< Timing-Allow-Origin: *
< EagleId: 6525b79915442733301371586e
<
{ [254 bytes data]
100   254  100   254    0     0    992      0 --:--:-- --:--:-- --:--:--   996
* Connection #0 to host c          n left intact
```



排查步骤如下：

1. **查询错误信息。从上图看出request请求的http头没有refer信息，出现403错误，具体错误信息为denied by Referer ACL。**

2. 查看加速域名`example2.cn`设置的防盗链是否勾选允许通过浏览器地址栏直接访问资源URL。

结论：由于防盗链设置不允许空referer访问导致403错误。

解决方法：在防盗链配置的白名单中，勾选允许通过浏览器地址栏直接访问资源URL。详细说明，请参见#unique_44。

说明:
此设置存在被盗链的风险。

8.7 如何排查CDN访问异常是CDN节点还是网络问题?

如何排查CDN访问异常是CDN节点还是网络问题?

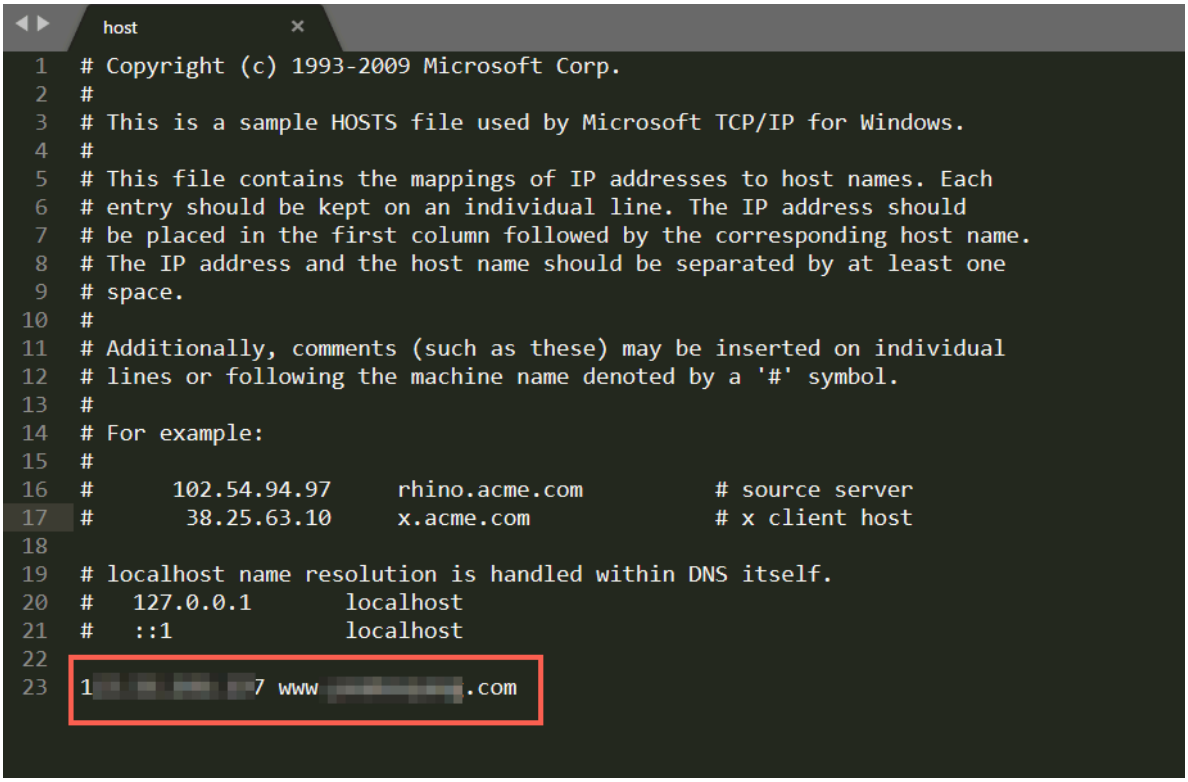
如果您使用了阿里云CDN后，出现访问慢、访问异常等问题，可参照如下方法排查：

- 查看Local DNS是否正常。

  访问`http://tool.alikunlun.com/doc.html`并查看LDNS和本地的IP地址是否正常。

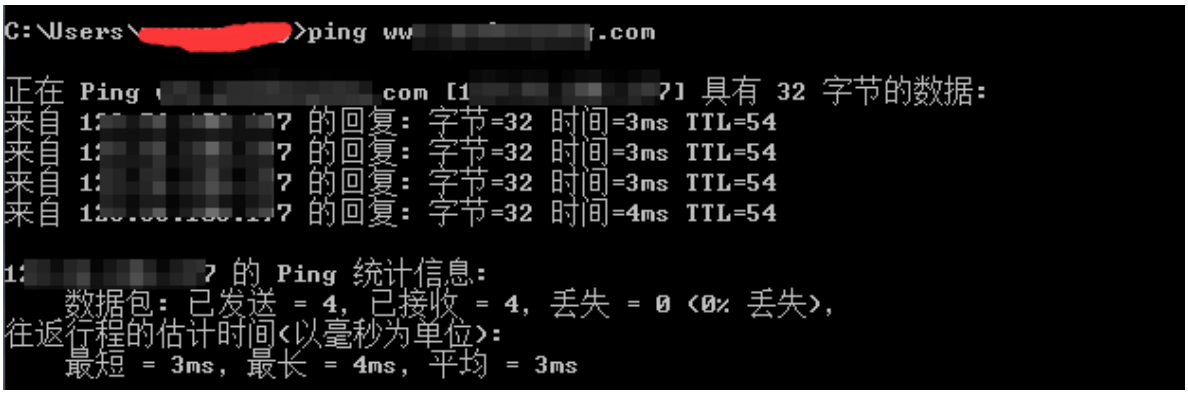
- 查看您的服务器源站是否正常。

  您将本地的hosts文件绑定您的源站和加速域名，这样您就能用加速域名直接访问到您的源站，而不经过阿里云CDN。如果这样直接访问您的服务器源站也有问题，说明是您的服务器源站出了问题。



- 查看CDN是否正常。

  通过输入`ping`您所添加的加速域名来验证，如果ping通，说明CDN节点正常。



如问题还未解决，请提交工单。

8.8 如何排查CDN解析CNAME后无法正常访问的问题?

问题描述：

使用CDN后，将一级域名test.com和二级域名www.test.com解析后，发现一级域名test.com可以打开，二级域名www.test.com无法打开，而绑定源站后，发现均能访问。

问题分析：

通过解析发现，两个域名均解析到了同一个CNAME地址：test.com.w.alikunlun.com。每个CNAME对应一个域名，不能解析到其他的CNAME上。

解决方案：

将二级域名www.test.com的CNAME重新解析到www.test.com.w.alikunlun.com即可恢复。

如何解析，请参见#unique_47。

如问题还未解决，请提交工单。

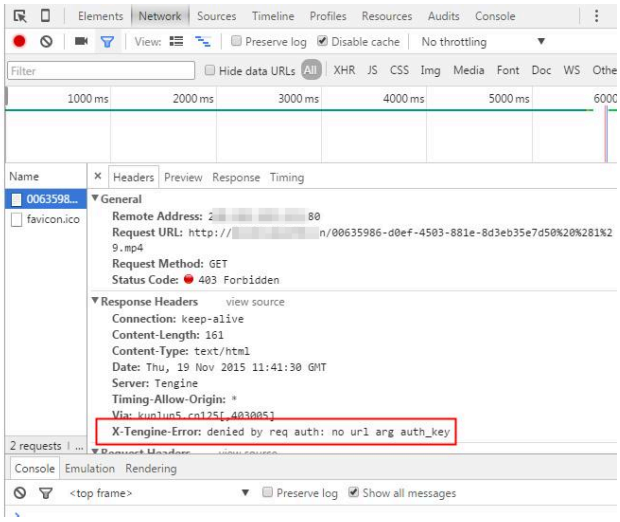
8.9 如何排查访问CDN加速资源返回状态码403的原因?

您可以通过以下方式排查访问CDN加速资源返回状态码403的具体原因：

1. 通过Chrome浏览器打开CDN加速的一个具体URL链接，打开开发者工具。

2. 排查是否开启鉴权，发现鉴权报错`X-Tengine-Error:denied by req auth: no url arg auth_key`。

```
403 Forbidden
```



这种情况下，您只需关闭鉴权。详细说明，请参见#unique_49。

3. 如果报如下错，请咨询是否开启了CC防护功能。

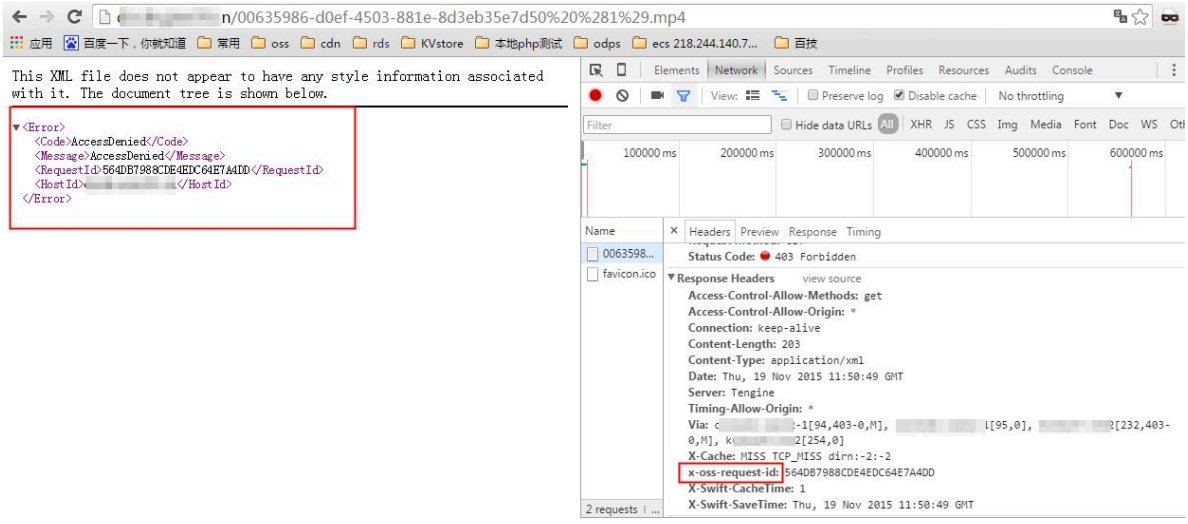
```
The website is under attack, You have requested too frequently
```

CC防护规则如下：

- 每分钟访问150次，URL非常集中，认为是攻击。
- 每分钟访问500次，不考虑URL，认为是攻击。
- 携带验证码Cookie，每分钟访问100次，认为是攻击。

这种情况下，您可以将自己的IP加入IP白名单。

4. 如果源站是OSS源站，报错AccessDenied。您可以在昆仑上查看源站，找到源bucket。

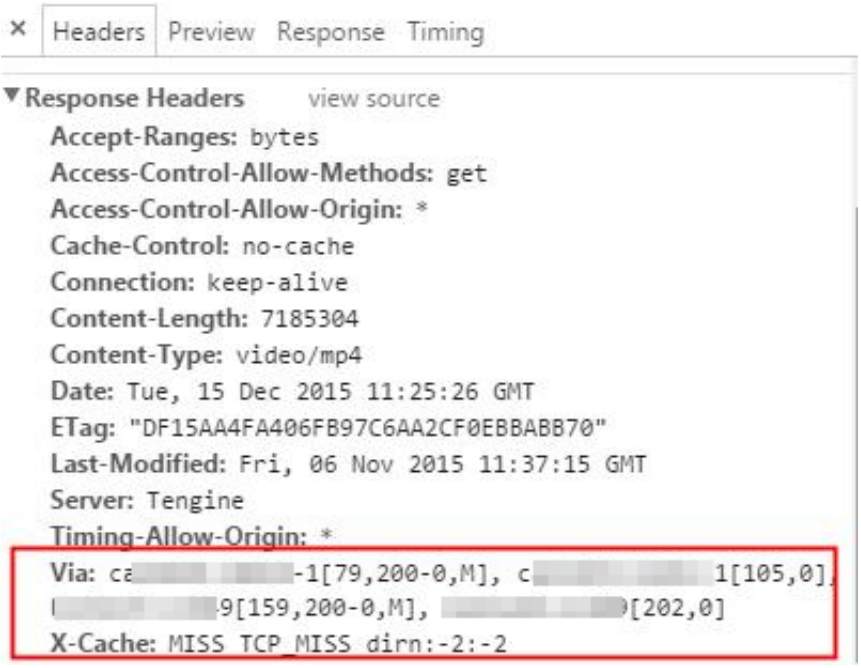


- 对于源bucket设置了私有这种情况，您需要提供签名URL，但不能开启CDN的过滤参数。
- 对于源bucket不允许refer为空这种情况，您需要将bucket的防盗链配置设置成允许为空。

5. 打开URL链接不是CDN域名，但应用了CDN的资源。排查是否是refer调用，如果Response头中有X-Tengine-Error:denied by Referer ACL，则说明refer规则设置不正确。

   这种情况下，您可以先取消CDN的refer配置，然后排查CDN日志，找到对应的访问日志，找到refer头并添加白名单。

6. 绑定源站，经测试仍返回403。http response头中，CDN的L1和L2缓存都不命中，说明是源站抛出的403。



   这种情况下，您可以排查源站是否有问题。绑定host后，测试是否返回403。

如问题还未解决，请提交工单。

8.10 如何解决CDN某个地域节点访问异常的问题?

问题症状：

- 问题1：ping不通CDN的加速域名。

  原因：您的本地网络异常；节点网络异常或者被攻击；您本地到运营商中间链路某路由节点故障。

- 问题2：源站更改文件之后，从CDN节点上获取的仍是更改之前的文件。

  刷新未生效；读取的是本地浏览器缓存；被本地运营商劫持。

- 问题3：访问CDN加速域名上拿到的非其站点文件内容。

  原因：访问的非CDN节点；被劫持。

解决方案：

- ping不通CDN的加速域名。

  1. 排查您的加速域名是否在沙箱节点中，由于沙箱中的域名无法保证服务稳定性，所以会存在ping不通的情况，此时沙箱可能正在受到攻击。
  2. 检测访问的IP是否为CDN的节点IP。如何检测，请参考#unique_51。

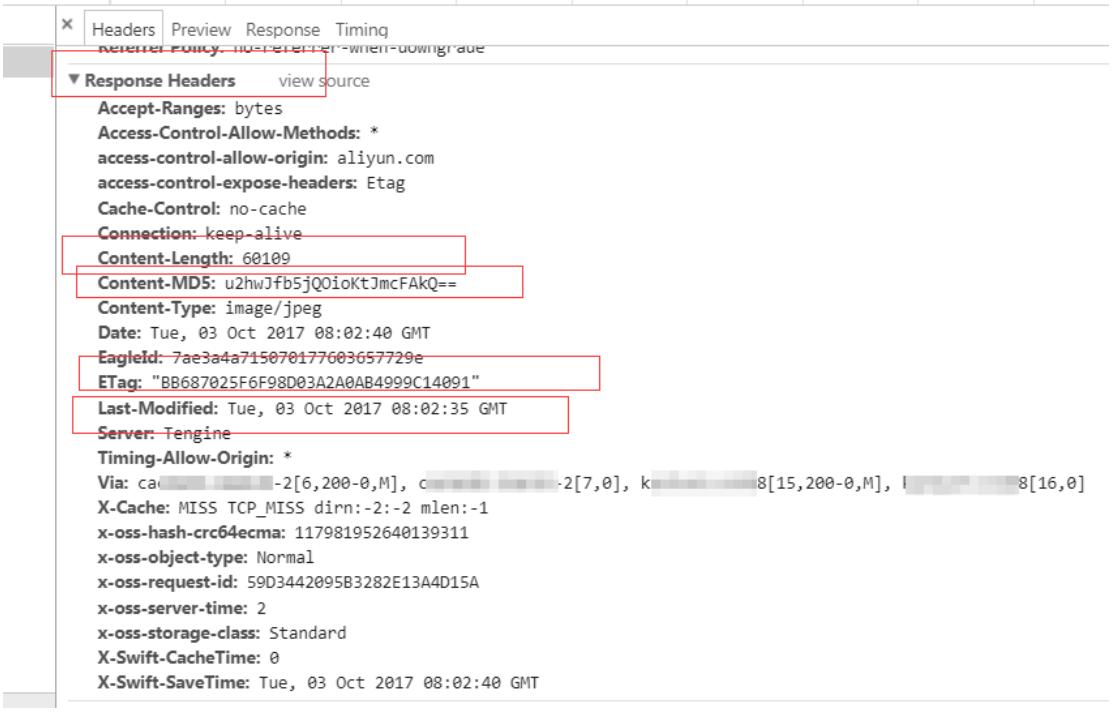
     如果您的访问节点不是CDN节点IP，请核实如下几种情况：

     - 您本地是否有开启代理软件（有些代理软件会强制更改访问域名的解析情况）。
     - 您是否绑定Host文件，将加速域名强制解析到了某个IP。
     - 您本地存在DNS劫持，这种情况下，您可以在本地开启杀毒安全软件，并且固定本地所使用的DNS为阿里的223或者电信的114或者其他知名的DNS，如果劫持情况比较严重，并且无法解决，则需要向您的网络服务提供商投诉要求解决劫持。
  3. 在本地ping该节点IP，以及使用站长工具（例如：`17ce.com`或者听云平台）在全国探测该节点IP是否存在问题（各个地区访问该节点均延迟均较大或者不通，本地也Ping不通该节点），这种情况该节点存在问题的可能性较大（前提是域名确实没有在沙箱中）。
  4. 在本地使用tracert（win主机）或者traceroute（linux主机）探测该IP并提供完整探测截图，根据得到的截图确定整个网络链路的问题点。MTR信息判断方法：目的节点丢包率为100%，并且从目的节点往前一直找到第一个开始丢包的节点（中间不能有丢包率为0%的路由节点），则第一个开始丢包的路由节点是问题路由的可能性较大。详细排查步骤，请参见ping丢包或不通时链路测试说明。

     您也可以给阿里云技术同学进行排查，在此期间缓解问题的方法：更改您的本地DNS为其他DNS（例如电信的114或者阿里的223），并刷新本地的DNS缓存，使其调度到其他正常的节点，走另外一条线路，则该问题可能得到缓解。

· 源站更改文件之后，从CDN节点上获取的仍是更改之前的文件。

1. 检测访问的IP是否为CDN的节点IP。
2. 根据CDN的配置，绑定CDN节点和源站。绑定源站测试时，请注意：
   - CDN的回源Host配置。例如CDN加速域名为A，源站域名为B，回源Host配置的为A，那么使用curl测试源站的命令应该为`curl -H "Host: A" "B"`。如果是绑定Host文件，那么应该将CDN加速域名绑定Host到源站域名所解析出来的IP上。
   - 不同的回源端口得到的访问结果也可能不一样，分别测试得到response header相关信息，判断访问的文件是否一致，主要判断以下几个方面：
     ■ content-length大小是否一致
     ■ last-modified的修改时间是否一致
     ■ Etag和Content-Md5是否一致



如果上述三点存在任何一项不一致的情况，那么可认为源站和节点上文件的确不一致。如果都存在的情况下，第三点最具备判断依据。

3. 如果上述步骤确认都OK，最终在节点上获取的文件仍和源站文件不一致，建议您刷新该URL，等待约10分钟后再去测试（刷新生效时间约为5~10分钟），如果多次刷新之后问题仍未解决，请提交工单。

- 访问CDN加速域名上拿到的非其站点文件内容。

  1. 检测访问的IP是否为CDN的节点IP。
  2. 排查CDN节点本身是否缓存了非用户站点上的文件，方法同上。
  3. 排查客户端到CDN L1这段链路。

     a. 打开Chrome浏览器的开发者工具，切换到Network并在地址栏输入访问的URL。

     b. 单击访问的URL，查看实际的访问情况。报错request URl、remote ip、requestUrl主要看访问形式是否如`http://x.x.x.x/cache/CDN`或者remote IP非CDN节点IP，如下图这种则是劫持：

那么，您需要联系其本地运营商投诉处理，解除劫持。

8.11 如何解决域名使用CDN访问后，提示504 Gateway Time-out的问题?

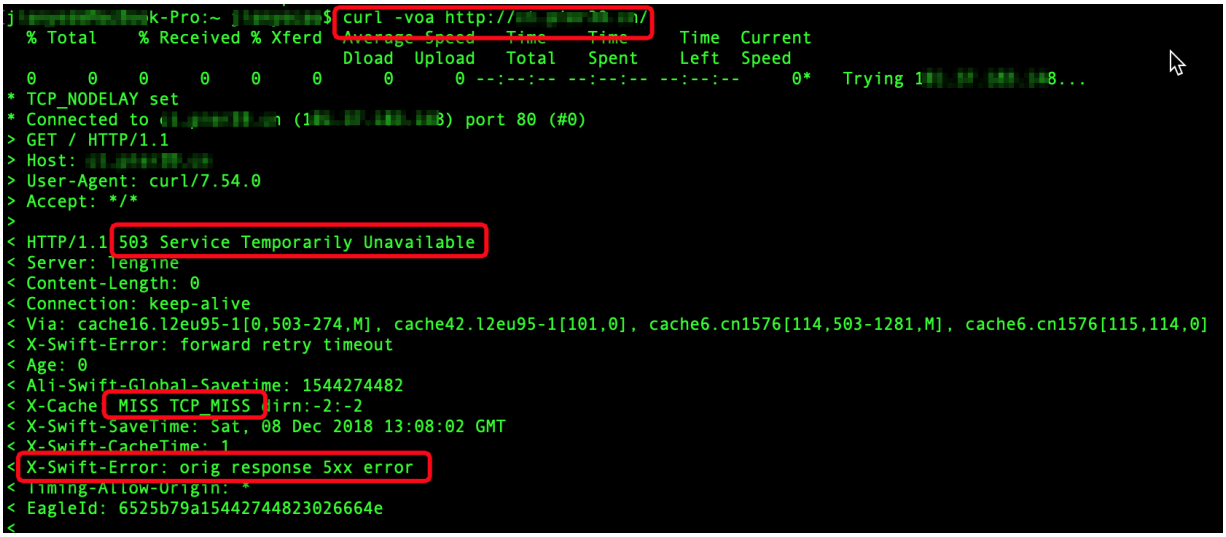
原因：出现此类情况一般都是由于源站异常导致，由于CDN回源取数据的时候，如果源站在30s内没有响应，CDN会提示504 Gateway Time-out的报错。

如问题还未解决，请提交工单。

8.12 如何排查源站存在安全防护导致503错误的原因?

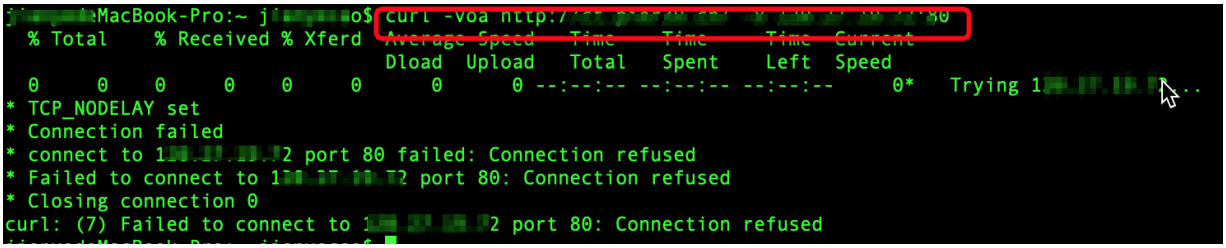
问题分析：

如果您的源站为一台ECS，上面部署了nginx，将nginx kill掉后，使用curl命令进行场景模拟：



从上图可以看到503服务不可用错误，同时可以看到x-cache为miss回源请求，swift报错5xx。

绑定源站IP 80回源访问。如果看到访问被拒绝，则没有web服务器程序进程占用80端口。那么，您的web服务器程序异常。



从以上分析得出结论，CDN 503报错原因为源站服务器程序异常。（或者因为服务器超载、服务器配置了单IP访问次数限制等）

解决方案：

您可以检查源站是否因为服务器程序异常或者超载导致的503错误。

8.13 如何解决使用CDN加速后，网站无法访问的问题？

假设加速域名为`www.a.com`，您可以通过以下步骤进行排查：

- 检查域名是否已经过CDN加速。

  通过ping域名测试，查看是否有`kunlun*.com`字样后缀的CNAME，若存在，则表示该域名已经成功解析到CDN节点；若ping的结果IP仍然是该域名的源站服务器IP，说明源站访问异常，请直接排查源站服务。

- 确定回源是否正常。

  如果步骤1中已确定解析到CDN，只需将该域名下的某URL在浏览器进行访问，则可知道经过CDN加速后的访问效果。此时修改hosts文件，添加`12.12.12.12 www.a.com`并保存

后，清除浏览器缓存并重新打开，再次访问则是回源访问效果，若依然访问异常，说明源站访问异常，请直接排查源站服务。

如何配置Hosts文件，请参见域名绑定host操作步骤。

- 检查CDN配置是否正确。

  检查域名`www.a.com`的配置，查看CNAME是否匹配正确。

  > 说明:
  > CDN控制台上的源站是对应源站的IP，无论您设置的是IP或域名，都会解析成对应的域名进行回源。而源站对应站点由回源host决定，因此回源host需要与源站对外服务的站点对应。

- 检查源站配置。

  检查源站的配置是否为该域名的源站服务器，若不是，请修改成对应的服务器IP。

- 检查源站安全策略。

  若如上均配置无误，说明CDN已正常配置，请确认源站是否配置了一些安全策略（如防火墙或安全狗等），若有，请排查是否有140.205.127.0/25、140.205.253.128/25、139.196.128.128/25、101.200.101.0/25四个IP段的IP拦截记录。若有，请添加白名单。

如问题还未解决，请提交工单。

8.14 如何解决CDN流量异常问题?

现象描述

CDN流量异常现象如下:

- 收到CDN流量异常报警。
- 在CDN控制台的用量查询菜单中，查看CDN的流量带宽和流量包，发现流量异常。

原因分析

CDN流量异常，可能是有恶意IP地址、Refer和URL刷流量引起。您可以通过以下方法处理流量异常问题。

- 通过日志下载功能，您可以识别出恶意IP地址和Refer，并加入黑名单。如果您没有开通实时日志功能，普通日志延迟约4-8小时，分析滞后，会给您带来损失。
- 通过统计分析功能，您可以分析热门Refer和URL的访问情况，识别出恶意Refer和URL，并将恶意Refer加入黑名单，为恶意URL配置鉴权。由于您只能统计分析昨天及以前的数据，分析滞后，会给您带来损失。

处理建议

CDN流量异常，会给您带来经济损失，建议您提前做好安全防护工作。具体操作方法如下：

- 通过报警设置功能，您可以设置带宽峰值和下行流量的报警规则。当流量达到时阈值时，系统自动通过电话、短信、邮件等方式通知您，及时采取措施。

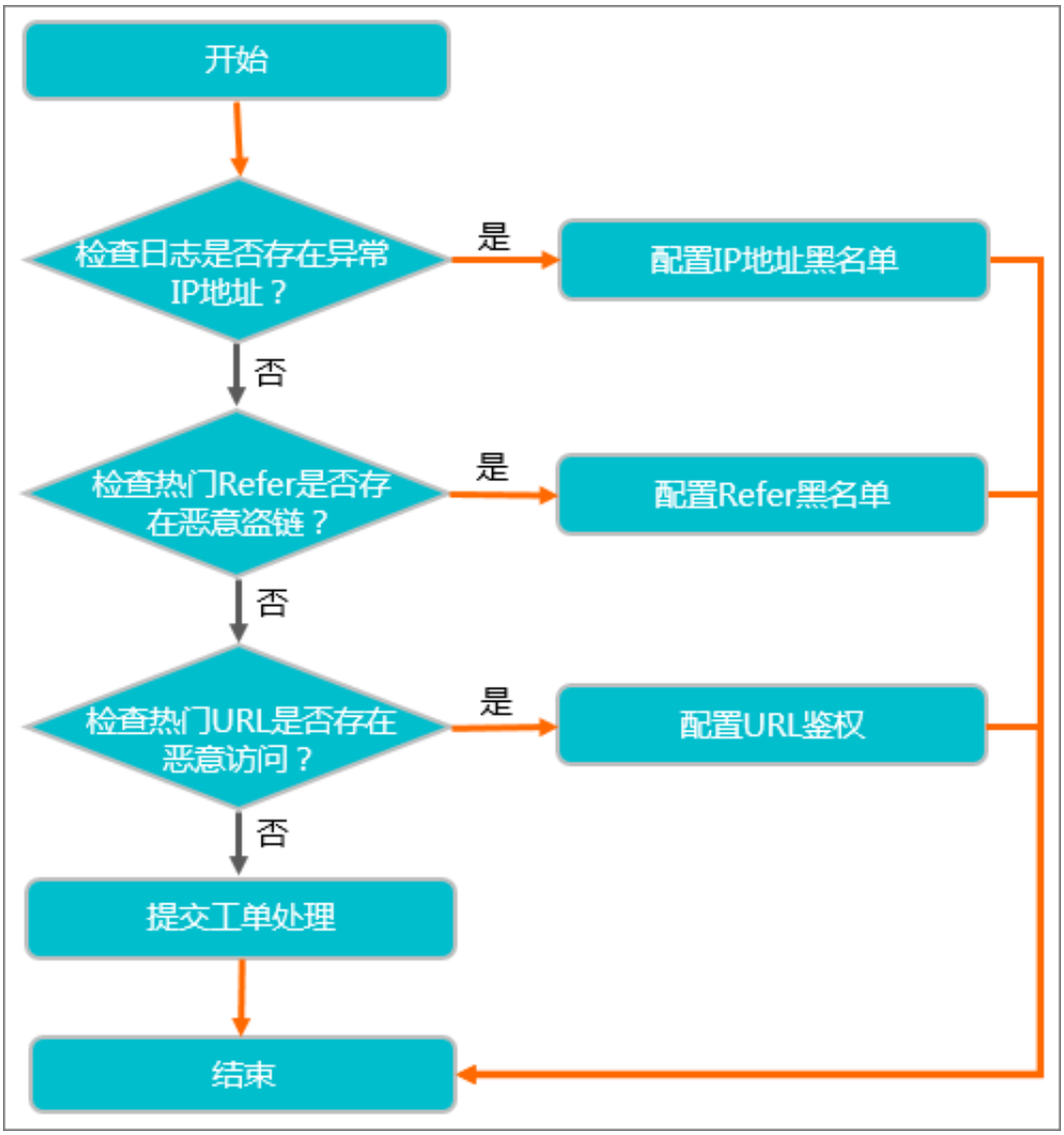
  设置报警规则的操作方法，请参见#unique_56。
- 通过CDN WAF防护功能，您可以配置Web应用攻击防护和精准访问控制。

  配置CDN WAF防护的操作方法，请参见#unique_57。
- 如果您的站点经常受到攻击，建议您使用安全加速SCDN。

  安全加速SCDN相关操作，请参见SCDN。

处理流程

CDN流量异常处理流程，如下图所示。



处理方法

1. 查看CDN日志是否存在异常IP地址访问资源。

   查看日志的操作方法，请参见#unique_58。

   - 是，将该IP地址配置为黑名单。

     配置IP黑名单的操作方法，请参见#unique_59。
   - 否，执行步骤 2。
2. 查看热门Refer是否存在恶意盗链。

   查看热门Refer的操作方法，请参见#unique_60。

   - 是，将该Refer配置为黑名单。

     配置Refer黑名单的操作方法，请参见#unique_61。
   - 否，执行步骤 3。
3. 查看热门URL是否存在恶意访问。

   查看热门URL的操作方法，请参见#unique_60。

   - 是，对该URL进行加密保护。

     配置URL鉴权的操作方法，请参见#unique_62。
   - 否，执行步骤 4。
4. 请提交工单处理。

CDN提供的安全防护功能，请参见CDN的安全防护功能。