

移动解析 HTTPDNS

API 文档

产品文档



腾讯云

【 版权声明 】

©2013–2023 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。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默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

API 文档

配置信息说明

HTTP 请求方式查询

HTTPS 请求方式查询

AES、DES 加密解密说明

API 接入最佳实践

API 文档

配置信息说明

最近更新时间：2022-04-14 16:22:14

概述

在接入移动解析 HTTPDNS 过程中，您需在移动解析 HTTPDNS 控制台获取对应配置信息后才可正常接入，本文将对如何获取配置信息以及配置信息含义进行说明。

前提条件

已开通移动解析 HTTPDNS。具体操作请参见 [开通移动解析 HTTPDNS](#)。

操作指南

登录移动解析 HTTPDNS 控制台 [开发配置页](#)，即可查询到您的配置信息。如下图所示：

开发配置 授权ID: 1 开发文档 [🔗](#)

鉴权信息 ⓘ

备注 测试 [✎](#)

状态 解析中 暂停解析

DES加密 支持中

密钥 ***** [🔑](#) 2

AES加密 支持中

密钥 ***** [🔑](#) 3

HTTPS加密 支持中

Token ***** [🔑](#) 4

申请应用

应用名称	备注	iOS APPID	安卓 APPID	创建时间
	测试1	01C LK 5	0A 3Q 6	2021-04-12 10:12:44

- **授权 ID**：使 移动解析 HTTPDNS 服务中，开发配置的唯一 标识。调 移动解析 HTTPDNS 的 HTTP 解析接口 `http://119.29.29.28` 时中传 的授权 ID 参数。
- **DES 加密密钥**：调 移动解析 HTTPDNS 的 HTTP 解析接口 `http://119.29.29.98` 并使用 DES 加密方式时，对 DNS 请求数据进 加密时的加密密钥。
- **AES 加密密钥**：调 移动解析 HTTPDNS 的 HTTP 解析接口 `http://119.29.29.98` 并使用 AES 加密方式时，对 DNS 请求数据进 加密时的加密密钥。
- **HTTPS 加密 Token**：调 移动解析 HTTPDNS 的 HTTPS 解析接口 `https://119.29.29.99`，对 DNS 请求数据进 鉴权的 Token 信息。

说明：

若控制台无以下两项信息，请申请应用后再进行查看。具体操作请参见 [SDK 开通流程](#)。

- **iOS APPID**：使用移动解析 HTTPDNS 服务提供的 [iOS 端 SDK](#) 的 `appId`（应用 ID）鉴权信息。

-
- **Android APPID**: 使用移动解析 HTTPDNS 服务提供的 [Android 端 SDK](#) 的业务 appkey 鉴权信息。

HTTP 请求方式查询

最近更新时间：2022-05-30 16:06:59

概述

移动解析 HTTPDNS 通过 HTTP/HTTPS 接口对外提供域名解析服务，服务接入直接使用 IP 地址，服务 IP 有多个，移动解析 HTTPDNS 的 HTTP 请求方式查询入口以 119.29.29.98 为例。

说明：

- 开通移动解析 HTTPDNS 服务后，您需在移动解析 HTTPDNS 控制台添加解析域名后才可正常使用。详情请参见[添加域名](#)。
- 我们提供2个入口 IP 示例，HTTP 协议的服务 IP：119.29.29.98，HTTPS 协议的服务 IP：119.29.29.99。
- 请优先使用官方 SDK，如果场景特殊下无法使用 SDK，需要直接访问 HTTP API 接口，请加入[技术支持群](#)或者[提交工单](#)联系我们，我们将根据您的具体使用场景，为您提供多个服务 IP 和相关的安全建议。
- 考虑到服务 IP 防攻击之类的安全风险，为保障服务可用性，HTTPDNS 同时提供多个服务 IP，当某个服务 IP 在异常情况下不可用时，可以使用其它服务 IP 进行重试。

前期准备

使用请求接口 `http://119.29.29.98/d? + {请求参数}` 时，需使用以下配置信息。请前往移动解析 HTTPDNS 管理控制台 [开发配置页](#) 获取相关配置信息：

开发配置

授权ID:

1

[开发文档](#)

鉴权信息 ①

备注 测试

状态 解析中 暂停解析

DES加密 支持中

密钥 ***** 2

AES加密 支持中

密钥 ***** 3

HTTPS加密 支持中

Token *****

申请应用

应用名称	备注	iOS APPID	安卓 APPID	创建时间
	测试1	0IOS 3LK	0ANI 3Q	2021-04-12 10:12:44

- **授权 ID：**使 移动解析 HTTPDNS 服务中，开发配置的唯一 标识。调 移动解析 HTTPDNS 的 HTTP 解析接口 `http://119.29.29.98` 时中传 的授权 ID 参数。
- **DES 加密密钥：**调 移动解析 HTTPDNS 的 HTTP 解析接口 `http://119.29.29.98` 并使用 DES 加密方式时，对 DNS 请求数据进 加密时的加密密钥。
- **AES 加密密钥：**调 移动解析 HTTPDNS 的 HTTP 解析接口 `http://119.29.29.98` 并使用 AES 加密方式时，对 DNS 请求数据进 加密时的加密密钥。

接口描述

- 接口请求地址：http://119.29.29.98/d? + {请求参数}。
- 请求方式：POST 或 GET。
- 考虑到服务 IP 防攻击之类的安全风险，为保障服务可用性，我们同时提供多个服务 IP，如您直接通过 API 接口请求 HTTPDNS 服务，请加入 [技术支持群](#) 或者 [提交工单](#) 联系我们，我们将根据您的具体使用场景，为您提供多个服务 IP 和相关的安全建议。
- 入口 IP 的切换逻辑：当接入 IP 访问超时，或者返回的结果非 IP 格式，或者返回为空的时候，请采用其他入口 IP 接入，若所有 IP 均出现异常，请兜底至 LocalDNS 进行域名解析。

请求参数

参数名	参数含义	是否必选	取值	加密	说明
dn	被查询的域名	是	加密前的单个域名长度为253	是	需在移动解析 HTTPDNS 控制台已添加域名并且为传输加密后的字符串。 • 域名添加请参见 添加域名。 • 加密详情请参见 加密与解密算法使用说明。
id	用户标识	是	1 – 10000	否	如果使用 AES、DES 加密方式，必须传入 ID，不需要进行加密。
alg	选择使用何种算法	是	[aes/des]	否	默认使用 DES 算法，不同算法具有不同密钥。
ip	DNS 请求的 ECS（EDNS-Client-Subnet）值	否	IPv4/IPv6 地址值	是	默认情况下 HTTPDNS 服务器会查询客户端出口 IP 为 DNS 线路查询 IP，使用 “ip=xxx” 参数，可以指定线路 IP 地址。支持 IPv4/IPv6 地址传入，接口会自动识别。加密详情请参见 加密与解密算法使用说明 。
query	结果中返回被查询域名	否	1	否	单域名查询情况下，此参数要求返回结果中携带被查询域名。
timeout	超时返回时间	否	1000 – 5000，单位为毫秒	否	可用值[1000, 5000]，单位为 ms，查询超时时间，默认值为5秒。
ttd	查询结果是否返回 TTL 值	否	1	否	可用值 [1]，不携带此参数，默认为不传递TTL值。
type	查询类型	否	[aaaa/AAAA/addrs/ADDRS]	否	可用值 [aaaa,AAAA,addrs,ADDRS]。默认查询 A 记录，设置 AAAA/aaaa 查询 AAAA 记录，设置 addrs/ADDRS 同时查询 A 和 AAAA 记录。

参数名	参数含义	是否必选	取值	加密	说明
clientip	查询结果中返回的客户端 IP 地址	否	1	否	可用值 [1]，不携带此参数，默认为不传递 clientip 值。若此参数取值，则返回结果中地址值在 符号后，若携带有 ip 参数，返回的是 ip 参数的值，否则返回客户端地址 IP。

说明：

ECS (EDNS-Client-Subnet) 协议在 DNS 请求包中附加请求域名解析的用户 IP 地址，DNS 服务器可以根据该地址返回用户更快速访问的服务器 IP 地址。

请求说明

以 ID 为 xxx 为例。

注意：

- 以下示例为 AES/DES 加密方式，其中域名和 IP 参数均需要加密，例如，域名为 cloud.tencent.com 需要进行加密，授权 ID 不需要进行加密。
- 若 HTTPDNS 未查询到解析结果，将返回为空值。
- HTTP 已接入 BGP Anycast，并实现多地机房容灾，但为了服务质量更高的保障，建议您采用 [Failed over 策略](#) 进行接入。

请求 A 记录

- 输入示例：

```
curl "http://119.29.29.98/d?dn={cloud.tencent.com 加密后字符串}&id=xxx"
```

- 解密后返回格式：

```
2.3.3.4;2.3.3.5;2.3.3.6
```

- 格式说明：返回查询结果，多个结果以 ';' 分隔。

返回结果中携带 ttl 信息

- 输入示例：

```
curl "http://119.29.29.98/d?dn={cloud.tencent.com 加密后字符串}&id=xxx&ttl=1"
```

- 解密后返回格式：


```
2.3.3.4;2.3.3.5;2.3.3.6,120
```

- **格式说明：**返回查询结果，多个结果以 ';' 分隔。记录值与 ttl 值以 '|' 分隔。

返回结果携带查询线路 IP 地址

- **输入示例：**

```
curl "http://119.29.29.98/d?dn={cloud.tencent.com 加密后字符串}&id=xxx&clientip=1&ip={DNS 请求的 E  
CS 值加密后字符串}&ttl=1"
```

- **解密后返回格式：**

```
12.3.3.4;2.3.3.5;2.3.3.6,120|1.2.3.4
```

- **格式说明：**返回结果中携带线路 ip 地址，以 '|' 分隔。如果没有传入 “ip=xxx” 参数，则返回出口 IP 地址；否则返回 ip 参数中的地址。

同时请求 A 和 AAAA 记录

- **输入示例：**

```
curl "http://119.29.29.98/d?dn={cloud.tencent.com 加密后字符串}&id=xxx&clientip=1&ip={DNS 请求的 E  
CS 值加密后字符串}&type=addr&ttl=1"
```

- **解密后返回格式：**

```
2.3.3.4;2.3.3.5;2.3.3.6,120-2402:4e00:0123:4567:0::2345;2403:4e00:0123:4567:0::2346,120|1.2.3.4
```

- **格式说明：**A 记录和 AAAA 记录之间以 '-' 分隔，A 记录在前，AAAA 记录在后。

返回结果中携带被查询域名

- **输入示例：**

```
curl "http://119.29.29.98/d?dn={cloud.tencent.com 加密后字符串}&id=xxx&clientip=1&ip={DNS 请求的 E  
CS 值加密后字符串}&query=1&ttl=1"
```

- **解密后返回格式：**

```
cloud.tencent.com.:2.3.3.4;2.3.3.5;2.3.3.6,120|1.2.3.4
```

- 格式说明：返回格式为“域名.:结果”的格式。

批量域名请求

- 输入示例：

```
curl "http://119.29.29.98/d?dn={cloud.tencent.com,www.qq.com,www.dnspod.cn 加密后字符串}&id=xxx&clientip=1&ip={DNS 请求的 ECS 值加密后字符串}&ttl=1"
```

- 解密后返回格式：

```
cloud.tencent.com.:2.3.3.4;2.3.3.5;2.3.3.6,120
www.qq.com.:3.3.3.4;3.3.3.5;3.3.3.6,180
www.dnspod.cn.:4.3.3.4;4.3.3.5;4.3.3.6,60|1.2.3.4
```

- 格式说明：多个域名返回内容之间以“换行符”分隔，ip 地址附加在所有记录值的最后。

请求异常或无记录说明

⚠ 注意：

- 以下示例为 AES/DES 加密方式，其中域名和 IP 参数均需要加密，例如域名为 cloud.tencent.com 需要加密，授权 ID 不需要进行加密。
- 如使用 HTTPS 加密方式，请求地址改为 119.29.29.99 并且必须要传入 token。

查询 A 记录

- 输入示例：

```
curl "http://119.29.29.98/d?dn={cloud.tencent.com 加密后字符串}&id=xxx"
```

- 解密后返回格式：空。
- 格式说明：没有记录，则返回空字符串。

返回结果中包含域名

- 输入示例：

```
curl "http://119.29.29.98/d?dn={cloud.tencent.com 加密后字符串}&id=xxx&type=addr&query=1&ip={DNS 请求的 ECS 值加密后字符串}"
```

- 解密后返回格式：

```
cloud.tencent.com|1.2.3.4
```

- 格式说明：0表示没有记录。

返回 A 与 AAAA 的记录

- 输入示例：

```
curl "http://119.29.29.98/d?dn={cloud.tencent.com 加密后字符串}&id=xxx&type=addr&query=1&ip={DNS 请求的 ECS 值加密后字符串}"
```

- 解密后返回格式：

```
cloud.tencent.com.:0-0|1.2.3.4
```

- 格式说明：0表示没有记录。如果某个记录存在，则该记录正常返回在结果中，例如 cloud.tencent.com.:2.3.4.5;3.3.3.3-0|1.2.3.4，表示 AAAA 记录无法查询到。

批量域名请求

- 输入示例：

```
curl "http://119.29.29.98/d?dn={cloud.tencent.com,www.qq.com,www.dnspod.cn 加密后字符串}&id=xxx&clientip=1&ip={DNS 请求的 ECS 值加密后字符串}&ttl=1"
```

- 解密返回格式：

```
cloud.tencent.com.:0  
www.qq.com.:3.3.3.4;3.3.3.5;3.3.3.6,180  
www.dnspod.cn.:4.3.3.4;4.3.3.5;4.3.3.6,60|1.2.3.4
```

- 格式说明：未查询到数据的域名则返回0。如果某个记录存在，则该记录正常返回在结果中。

HTTP 状态码

以下为接口业务逻辑相关的 HTTP 状态码。

状态码	描述
200 OK	如果接口调用正确，无论是否查询成功，均返回状态码200。
404 Not Found	接口不存在或 URL 实际上访问了某不存在的资源。
429 Too Many Request	访问过于频繁，超过了服务器限制。
501 Not Implemented	使用了非 “GET” 或 “POST” 请求方式。

HTTPS 请求方式查询

最近更新时间：2022-05-30 16:07:05

概述

移动解析 HTTPDNS 通过 HTTP/HTTPS 接口对外提供域名解析服务，服务接入直接使用 IP 地址，服务 IP 有多个，移动解析 HTTPDNS 的 HTTPS 请求方式查询入口以 119.29.29.99 为例。

说明：

- 开通移动解析 HTTPDNS 服务后，您需在移动解析 HTTPDNS 控制台添加解析域名后才可正常使用。具体操作请参见 [添加域名](#)。
- 我们提供2个入口 IP 示例，HTTPS 协议的服务 IP：119.29.29.99，HTTP 协议的服务 IP：119.29.29.98。
- 请优先使用官方 SDK，如果场景特殊下无法使用 SDK，需要直接访问 HTTPS API 接口，请加入 [技术支持群](#) 或者 [提交工单](#) 联系我们，我们将根据您的具体使用场景，为您提供多个服务 IP 和相关的安全建议。
- 考虑到服务 IP 防攻击之类的安全风险，为保障服务可用性，HTTPDNS 同时提供多个服务IP，当某个服务 IP 在异常情况下不可用时，可以使用其它服务 IP 进行重试。

前期准备

使用请求接口 `https://119.29.29.99/d? + {请求参数}` 时，需使用以下配置信息。请前往移动解析 HTTPDNS 管理控制台 [开发配置页](#) 获取相关配置信息：

开发配置

授权ID:

[开发文档](#)

鉴权信息 ①

备注 测试

状态 解析中 暂停解析

DES加密 支持中

密钥 *****

AES加密 支持中

密钥 *****

HTTPS加密 支持中

Token ***** 1

申请应用

应用名称	备注	iOS APPID	安卓 APPID	创建时间
	测试1	0IOS ***** GLK	0AN ***** 3Q	2021-04-12 10:12:44

HTTPS 加密 Token：调 移动解析 HTTPDNS 的 HTTPS 解析接口 `https://119.29.29.99`，对 DNS 请求数据进 鉴权的 Token 信息。

接口描述

- 接口请求地址：`https://119.29.29.99/d? + {请求参数}`。
- 请求方式：POST 或 GET。
- 考虑到服务 IP 防攻击之类的安全风险，为保障服务可用性，我们同时提供多个服务 IP，如您直接通过 API 接口请求 HTTPDNS 服务，请加入 [技术支持群](#) 或者 [提交工单](#) 联系我们，我们将根据您的具体使用场景，为您提供多个服务 IP 和相关

的安全建议。

- 入口 IP 的切换逻辑：当接入 IP 访问超时，或者返回的结果非 IP 格式，或者返回为空的时候，请采用其他入口 IP 接入，若所有 IP 均出现异常，请兜底至 LocalDNS 进行域名解析。

请求参数

参数名	参数含义	是否必选	取值	加密	说明
dn	被查询的域名	是	字符串	否	需在移动解析 HTTPDNS 控制台已添加域名。具体请参见 添加域名 。
token	使用 HTTPS 方式的标识	是	整型数据	否	token 获取请参见 配置信息说明 。
ip	DNS 请求的 ECS（EDNS-Client-Subnet）值	否	IPv4/IPv6 地址值	否	默认情况下 HTTPDNS 服务器会查询客户端出口 IP 为 DNS 线路查询 IP，使用“ip=xxx”参数，可以指定线路 IP 地址。支持 IPv4/IPv6 地址传入，接口会自动识别。
query	结果中返回被查询域名	否	1	否	单域名查询情况下，此参数要求返回结果中携带被查询域名。
timeout	超时返回时间	否	1000 – 5000，单位为毫秒	否	可用值[1000, 5000]，单位为 ms，查询超时时间，默认值为 5 秒。
ttd	查询结果是否返回 TTL 值	否	1	否	可用值 [1]，不携带此参数，默认为不传递 TTL 值。
type	查询类型	否	[aaaa/AAAA/addr/ADDRS]	否	可用值 [aaaa,AAAA,addr,ADDRS]。默认查询 A 记录，设置 AAAA/aaaa 查询 AAAA 记录，设置 addr/ADDRS 同时查询 A 和 AAAA 记录。
clientip	查询结果中返回的客户端 IP 地址	否	1	否	可用值 [1]，不携带此参数，默认为不传递 clientip 值。若此参数取值，则返回结果中地址值在 符号后，若携带有 ip 参数，返回的是 ip 参数的值，否则返回客户端地址 IP。

🔍 说明：

- ECS（EDNS-Client-Subnet）协议在 DNS 请求包中附加请求域名解析的用户 IP 地址，DNS 服务器可以根据该地址返回用户更快速访问的服务器 IP 地址。
- 使用 HTTPS 方式，传输的数据会因为 TLS 通道而被加密保护，因此不需要主动对传入的数据额外加密。
- 出于安全和身份认证的考虑，需要传入 HTTPS Token 实现身份鉴权。

请求说明

以请求域名为 cloud.tencent.com，token 为 yyyy 为例。

⚠ 注意：

- 若 HTTPDNS 未查询到解析结果，将返回为空值。
- HTTP 已接入 BGP Anycast，并实现多地机房容灾，但为了服务质量更高的保障，建议您采用 [Failed over 策略](#) 进行接入。

请求 A 记录

- 输入示例：

```
curl "https://119.29.29.99/d?dn=cloud.tencent.com&token=yyyy"
```

- 解密后返回格式：

```
2.3.3.4;2.3.3.5;2.3.3.6
```

- 格式说明：返回查询结果，多个结果以 ';' 分隔。

返回结果中携带 ttl 信息

- 输入示例：

```
curl "https://119.29.29.99/d?dn=cloud.tencent.com&token=yyyy&ttl=1"
```

- 解密后返回格式：

```
2.3.3.4;2.3.3.5;2.3.3.6,120
```

- 格式说明：返回查询结果，多个结果以 ';' 分隔。记录值与 ttl 值以 ',' 分隔。

返回结果携带查询线路 IP 地址

- 输入示例：

```
curl "https://119.29.29.99/d?dn=cloud.tencent.com&token=yyyy&clientip=1&ip=1.2.3.4&ttl=1"
```

- 解密后返回格式:

```
12.3.3.4;2.3.3.5;2.3.3.6,120|1.2.3.4
```

- 格式说明: 返回结果中携带线路 ip 地址, 以'|'分隔。如果没有传入 “ip=xxx” 参数, 则返回出口 IP 地址; 否则返回 ip 参数中的地址。

同时请求 A 和 AAAA 记录

- 输入示例:

```
curl "https://119.29.29.99/d?dn=cloud.tencent.com&token=yyyy&clientip=1&ip=1.2.3.4&type=addr&tll=1"
```

- 解密后返回格式:

```
2.3.3.4;2.3.3.5;2.3.3.6,120-2402:4e00:0123:4567:0::2345;2403:4e00:0123:4567:0::2346,120|1.2.3.4
```

- 格式说明: A 记录和 AAAA 记录之间以 '-' 分隔, A 记录在前, AAAA 记录在后。

返回结果中携带被查询域名

- 输入示例:

```
curl "https://119.29.29.99/d?dn=cloud.tencent.com&token=yyyy&clientip=1&ip=1.2.3.4&query=1&tll=1"
```

- 解密后返回格式:

```
cloud.tencent.com.:2.3.3.4;2.3.3.5;2.3.3.6,120|1.2.3.4
```

- 格式说明: 返回格式为 “域名.:结果” 的格式。

批量域名请求

- 输入示例:

```
curl "https://119.29.29.99/d?dn=cloud.tencent.com,www.qq.com,www.dnspod.cn&token=yyyy&clientip=1&ip=1.2.3.4&tll=1"
```

- 解密后返回格式:

```
cloud.tencent.com.:2.3.3.4;2.3.3.5;2.3.3.6,120  
www.qq.com.:3.3.3.4;3.3.3.5;3.3.3.6,180
```

```
www.dnspod.cn.:4.3.3.4;4.3.3.5;4.3.3.6,60|1.2.3.4
```

- **格式说明：**多个域名返回内容之间以“换行符”分隔，ip 地址附加在所有记录值的最后。

请求异常或无记录说明

查询 A 记录

- **输入示例：**

```
curl "https://119.29.29.99/d?dn=cloud.tencent.com&token=yyyy&id=xxx"
```

- **解密后返回格式：**空。
- **格式说明：**没有记录，则返回空字符串。

返回结果中包含域名

- **输入示例：**

```
curl "https://119.29.29.99/d?dn=cloud.tencent.com&token=yyyy&type=addr&query=1&ip=1.2.3.4"
```

- **解密后返回格式：**

```
cloud.tencent.com|1.2.3.4
```

- **格式说明：**0表示没有记录。

返回 A 与 AAAA 的记录

- **输入示例：**

```
curl "https://119.29.29.99/d?dn=cloud.tencent.com&token=yyyy&type=addr&query=1&ip=1.2.3.4"
```

- **解密后返回格式：**

```
cloud.tencent.com.:0-0|1.2.3.4
```

- **格式说明：**0表示没有记录。如果某个记录存在，则该记录正常返回在结果中，例如 cloud.tencent.com.:2.3.4.5;3.3.3.3-0|1.2.3.4，表示 AAAA 记录无法查询到。

批量域名请求

- **输入示例：**


```
curl "https://119.29.29.99/d?dn=cloud.tencent.com,www.qq.com,www.dnspod.cn&token=yyyy&clientip=1&ip=1.2.3.4&tthl=1"
```

• 解密后返回格式:

```
cloud.tencent.com.:0
www.qq.com.:3.3.3.4;3.3.3.5;3.3.3.6,180
www.dnspod.cn.:4.3.3.4;4.3.3.5;4.3.3.6,60|1.2.3.4
```

- 格式说明: 未查询到数据的域名则返回0。如果某个记录存在, 则该记录正常返回在结果中。

HTTP 状态码

以下为接口业务逻辑相关的 HTTP 状态码。

状态码	描述
200 OK	如果接口调用正确, 无论是否查询成功, 均返回状态码200。
404 Not Found	接口不存在或 URL 实际上访问了某不存在的资源。
429 Too Many Request	访问过于频繁, 超过了服务器限制。
501 Not Implemented	使用了非 “GET” 或 “POST” 请求方式。

AES、DES 加密解密说明

最近更新时间：2022-02-15 10:53:55

操作场景

使用 DES、AES 加密算法可以对请求参数进行加密，并对其响应数据解密，防止明文请求在传输过程中被恶意篡改。本文将指导您如何使用 DES、AES 加密算法。

-  说明：
- 使用 HTTPS 请求方式查询，传输的数据会因为 TLS 通道而被加密保护，因此不需要主动对传入的数据额外加密。

前提条件

- 已开通移动解析 HTTPDNS 并已获取授权 ID 和加密密钥及 HTTPS Token 等配置信息。详情可参见 [配置信息说明](#)。
- 已在移动解析 HTTPDNS 控制台添加需要查询的域名。详情可参见 [添加域名](#)。

操作流程

步骤1：确定加密方式。

目前移动解析 HTTPDNS，HTTP 请求查询方式支持 DES、AES、两种加密方式。

-  说明：
- 若您使用 HTTPS 请求查询方式，详情可参见 [HTTPS 请求方式查询](#)。
 - 使用对应的密钥和算法将要解析的域名进行加密（如需使用 ip 参数，也需要将该参数值进行加密），并将加密后的结果与 ID（不需要加密）作为请求参数。

步骤2：发送加密的请求。

步骤3：接受加密的应答。

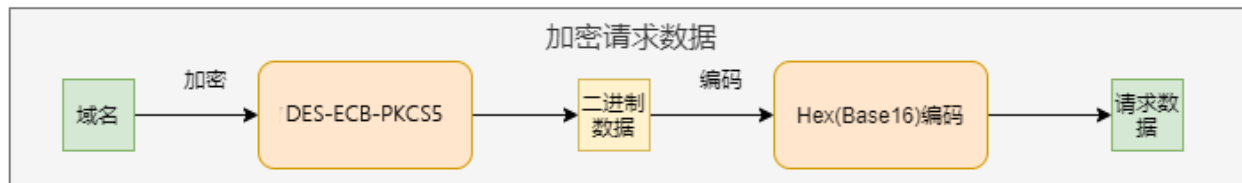
步骤4：将结果解密，即可获得所查询的域名对应的解析结果。

加密与解密算法使用说明

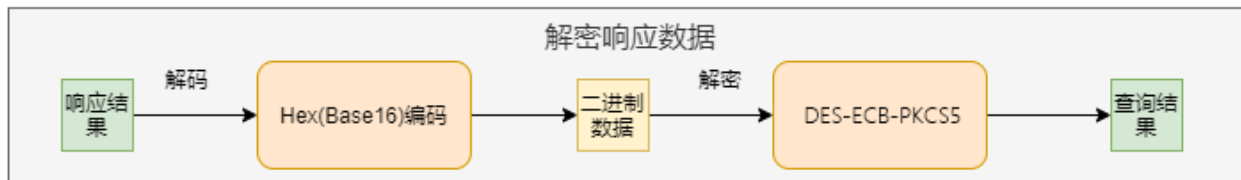
DES 算法

-  说明：
- 使用 DES 进行加密与解密，密码长度为8个字符，分组加密模式为 ECB，Padding 算法是 PKCS5Padding。

加密后数据使用 Hex（Base16）编码，将二进制数据转换为可见十六进制字符标识，Hex 编码后的数据长度将会加倍。具体流程如下图所示：



解密响应数据，先使用 Hex 解码为二进制数据，再使用 DES 算法解密为明文数据。具体流程如下图所示：



例如：您的域名为 `www.dnspod.cn`、加密密钥为：`dnspodpass`。流程如下：

1. 在 [HTTPDNS 控制台](#) 添加域名。
2. 使用 DES-ECB-PKCS5 加密算法与 [DES 加密密钥](#) `dnspodpass` 加密域名将得到加密字符串 `87ae992c1321f299da3c0210a9900ae7`。
3. 使用接口 `curl "http://119.29.29.98/d?dn=87ae992c1321f299da3c0210a9900ae7&id={授权ID}"` 请求 A 记录将得到数据长度加倍的加密字符串，如：`55915a682ea20840ff74aa6e7bebf11454ed0f4050a63e93e6e89521553a01a8`。
4. 得到加倍的加密字符串后，使用 DES-ECB-PKCS5 加密算法与 [DES 加密密钥](#) `dnspodpass` 进行解密后将得到明文的信息 `121.12.53.35;106.227.19.35`。

说明：

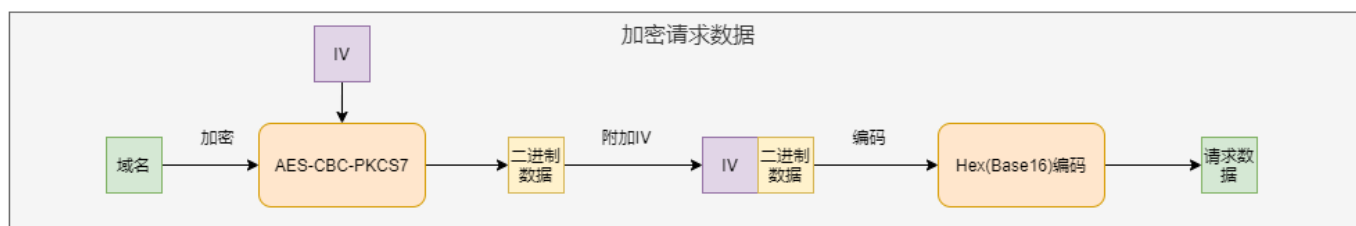
以上字符串仅做示例使用，用于正常请求将无法使用。

AES 算法

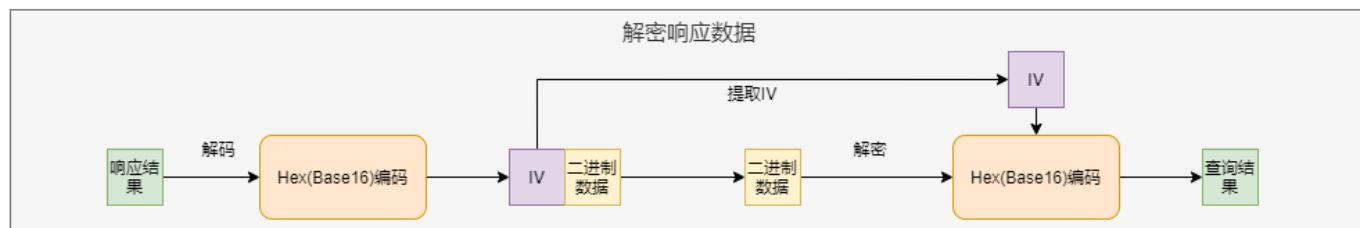
说明：

使用 AES 进行加密与解密，密钥长度为16个字符，分组加密模式为 CBC，Padding 算法是 PKCS7。

CBC 模式要求使用随机化 IV 作为初始加密与解密输入，因此该 IV 也会被带入到请求和响应中。加密后的数据，连同 IV 一起使用 Hex 编码，转换为可见十六进制标识。具体流程如下图所示：



解密时，使用 Hex 解码为二进制数据，前16字节为 IV 值，IV 后面为待使用 AES 算法解密的数据。使用 AES 算法解密后即
为明文数据。具体流程如下图所示：

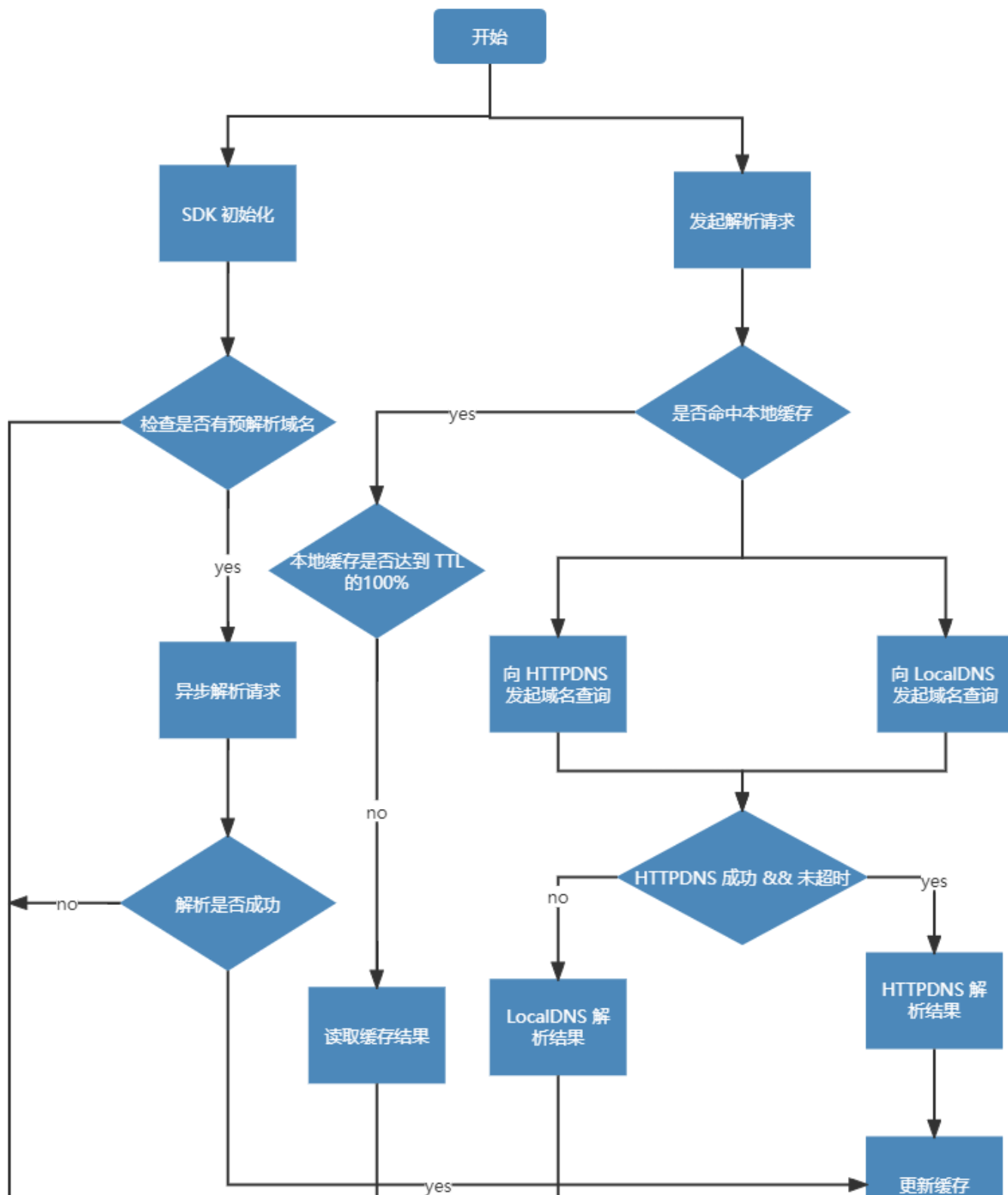


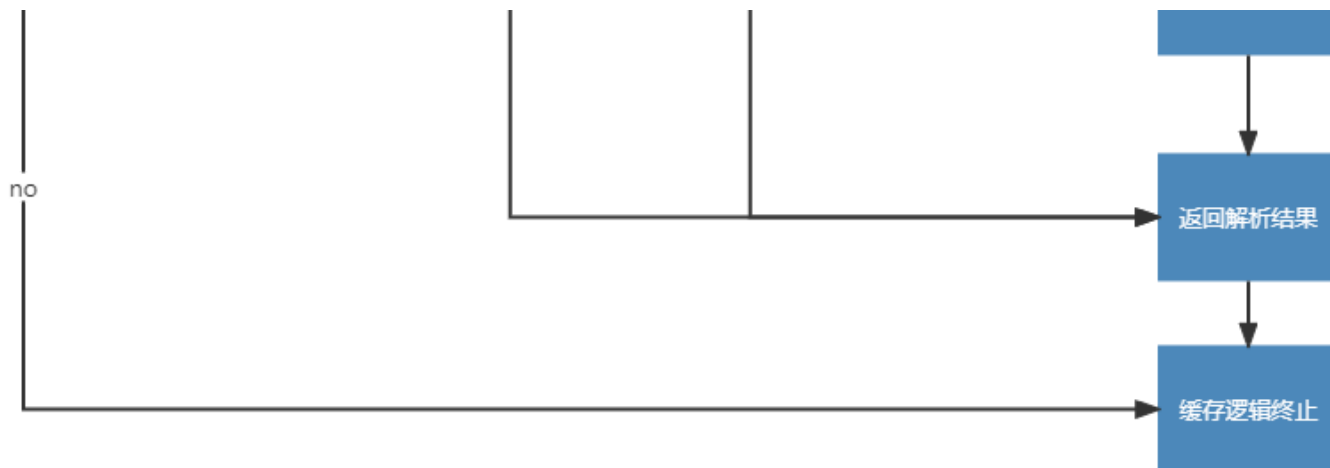
API 接入最佳实践

最近更新时间：2022-04-28 18:02:33

客户端接入流程

接入 HTTPDNS 过程中，需要改造移动客户端的域名解析机制，流程参考如下：





设计策略

改造过程中需要遵循以下两个设计策略：

Failed over 策略

虽然 HTTPDNS 已经接入 BGP Anycast，并实现了多地跨机房容灾，但为了保证在最坏的情况下客户端域名解析依然不受影响，建议您采用以下的 Failed over 策略：

1. 先向 HTTPDNS 发起域名查询请求。
2. 如果 HTTPDNS 查询返回的结果不是一个 IP 地址（结果为空、结果非 IP、连接超时等），则通过本地 LocalDNS 进行域名解析。超时时间建议为5s。

缓存策略

移动互联网用户的网络环境比较复杂，为了尽可能地减少由于域名解析导致的延迟，建议在本地进行缓存。缓存规则如下：

- **缓存时间：**缓存时间建议设置为120s至600s，不可低于60s。
- **缓存更新：**

缓存更新应在以下两种情形下进行：

- **用户网络状态发生变化时：**

移动互联网用户的网络状态由3G切换 Wi-Fi，Wi-Fi 切换3G的情况下，其接入点的网络归属可能发生变化，用户的网络状态发生变化时，需要重新向 HTTPDNS 发起域名解析请求，以获得用户当前网络归属下的最优指向。

- **缓存过期时：**

当域名解析的结果缓存时间到期时，客户端应该向 HTTPDNS 重新发起域名解析请求以获取最新的域名对应的 IP。为了减少用户在缓存过期后重新进行域名解析时的等待时间，建议在 75%TTL 时就开始进行域名解析。例如，本地缓存的 TTL 为 600s，那么在第 $600 * 0.75 = 450s$ 时，客户端就应该进行域名解析。

除了以上几点建议外，减少域名解析的次数也能有效的减少网络交互，提升用户访问体验。建议在业务允许的情况下，尽量减少域名的数量。如需区分不同的资源，建议通过 url 来进行区分。

其他注意事项

为了让您更好的改造移动客户端，请改造前阅读以下注意事项：

- 请尽量将不同功能用同样域名，资源区分通过 url 来实现，减少域名解析次数（用户体验好，容灾切换方便。多一个域名，即使域名已命中缓存，至少多100ms的访问延迟）。
- 设置的缓存 TTL 值不可太低（不可低于60s），防止频繁进行 HTTPDNS 请求。
- 接入移动解析 HTTPDNS 的业务需要保留用户本地 LocalDNS 作为容灾通道，当 HTTPDNS 无法正常服务时（移动网络不稳定或 HTTPDNS 服务出现问题），可以使用 LocalDNS 进行解析。
- Android 程序中可能出现404错误，但浏览器中正常，可能为权限问题或者其他问题。详情请参考 [Android 请求返回 404](#)。
- bytetohehex&hextobyte，需自己实现接口，进行16进制字符串与字节的转换。
- HTTPS 问题，需在客户端 hook 客户端检查证书的 domain 域和扩展域看是否包含本次请求的 host 的过程，将 IP 直接替换成原来的域名，再执行证书验证。或者忽略证书认证，类似于 curl -k 参数。
- HTTPDNS 请求建议超时时间2 - 5s左右。
- 在网络类型变化时，例如，4G切换到 Wi-Fi，不同 Wi-Fi 间切换等，需要重新执行 HTTPDNS 请求刷新本地缓存。