DNS 解析 DNSPod

最佳实践

产品文档

腾讯云

【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

最佳实践
其他平台解析域名平滑转入 DNSPod

最近更新时间：2022-05-18 16:07:46

概述

若您的 DNS 解析托管在其他 DNS 服务商进行托管，现您需转入至 DNSPod 进行解析，您可参考本文进行操作，本文将指导您如何将解析平滑转入至 DNSPod 解析。

前提条件

已在腾讯云注册账号并完成实名认证。

转入说明

- 转入前请确保所使用的 DNSPod 套餐是否支持导入的解析记录和功能。详情请参见 DNSPod 定价中心。
- 检查 CNAME 记录指向的域名是否配置解析，避免 CNAME 指向的域名未做配置导致的业务影响。
- 检查是否配置 DNSSEC 功能，若已配置您可以参考如下两种方式进行转入：
  i. 您可以到域名注册商处关闭 DNSSEC，等转入完成后，再进行 DNSSEC 配置。
  ii. 您也可以参考 DNSSEC 配置 进行操作，并到域名注册商处提交 DNSPod DNS 解析的 DNSSEC 配置。等转入完成后，在域名注册商处删除原 DNS 服务商的 DNSSEC 设置。

操作步骤

步骤1：原 DNS 服务商处导出解析记录

在您的原 DNS 服务商处导出解析记录文件，DNSPod 解析支持 ZONE 文件和 xls 文件格式。建议导出 ZONE 文件，若您的使用 xls 文件格式，您可 单击此处 下载导入模板进行编辑。导出操作请您咨询原 DNS 服务商。

步骤2：导入解析记录至 DNSPod

1. 登录 DNSPod 解析控制台，进入 “我的域名” 管理页面。
2. 在 “我的域名” 管理页面，单击**添加域名**，输入您需要转入的域名并单击**确认**。如下图所示：

> 说明：
> DNSPod 解析仅支持添加二级域名，暂不支持二级域名以下子域名。

3. 添加域名完成后，单击域名进入解析设置**记录管理**页签，依次单击**更多操作>批量导入记录**。如下图所示：

4. 在 “导入记录” 页签中，将准备好的解析记录数据，导入至 DNSPod DNS 解析。具体操作请参见 记录批量导入。如下图所示：


添加域名
取回域名
添加记录
修改记录
导入记录
导出记录
导出域名
选择域名
指定域名
指定分组
全部域名
请输入需要导入记录的域名，每行一个，最多支持 5000 个，
如：
example.com
example.cn
0/5000
从域名列表中选择
上传文件
点击上传或拖拽到此区域
使用说明
1. 上传文件格式支持 ZONE 文件、XLS 表格及 CSV 文件，建议先参考模板格式。
2. ZONE 文件是 DNS 服务器存储的配置文件，需要压缩为 ZIP 格式后才可上传。下载模板
3. XLS 表格文件必须先选择已有域名，否则无法上传。下载模板
4. CSV 文件必须先选择已有域名，否则无法上传。下载模板
5. 上传文件大小不得超过 10M。
批量导入

步骤3：修改 DNS 服务器地址

前往域名注册商处，将域名的 DNS 服务器地址修改为 DNSPod 提供的对应 DNS 服务器地址，具体操作请参见域名如何配置为 DNSPod 的 DNS 服务器。如下图所示：

步骤4：等待 DNS 服务器生效

修改 DNS 服务器地址完成后，请耐心等待全球各地 LocalDNS 缓存更新。因各地 LocalDNS 都缓存该域名原 DNS 服务器名称，所以修改 DNS 服务器地址完成后，域名 DNS 服务器地址的变更将会逐步同步到全球各地 LocalDNS 服务器中，请您耐心等待。

一般情况下在48小时内即可完成更新。

> **注意：**
> 更新期间 DNS 解析仍有可能向原 DNS 服务商发起 DNS 查询，所以在变更同步期间请不要删除原 DNS 服务商处的解析记录数据。

DNS 解析实现智能解析

最近更新时间：2021-09-03 11:27:08

操作场景

- **通过境内跨运营商或跨地区进行访问：** 中国大陆地区实现跨运营商进行访问，大多数都会使用多个运营商 IP 地址，由于传统 DNS 解析是随机或优选的方式将其中一个 IP 地址返回给访问用户，这种情况下容易造成访问用户跨网或跨地域访问速度慢或访问质量差，因此企业可通过 DNS 智能解析的配置来实现用户的就近访问。
- **通过全球范围进行访问：**若企业需要在全球范围内进行访问，通常会在境内和境外分别部署应用服务，因此企业可通过 DNS 智能解析的配置，判断用户处于境内或境外，可以更快速响应用户的访问。
- **通过智能解析限制某运营商或地域的访问者进行访问：**部分企业因某些原因，需要限制境外的用户访问企业的应用服务，因此企业可通过 DNS 配置智能解析，实现屏蔽境外访问者的访问诉求。

前提条件

- 1个可访问的域名，例如 dnspod.cn。
- 3个运营商 IP 地址，例如，**联通**线路解析至 1.1.1.1、**移动**线路解析至 2.2.2.2、**电信**线路解析至 3.3.3.3。

操作步骤

通过境内跨运营商或跨地区进行访问

1. 请登录 DNS 解析控制台，选择需要配置智能解析的域名，单击操作栏的**解析**进入该域名的**记录管理**页面。如下图所示：

2. 单击**添加记录**，创建3条子域名（例如，主机记录设置为 www）的 A 记录，线路类型分别设置为**默认**、**移动**、**电信**，记录类型分别设置为3个运营商 IP 地址：1.1.1.1（联通）、2.2.2.2（移动）、3.3.3.3（电信）。如下图所示：

www	A	电信	3.3.3.3	-	600	2020-07-13 19:31:31	修改 暂停 删除
www	A	移动	2.2.2.2	-	600	2020-07-13 19:31:46	修改 暂停 删除
www	A	默认	1.1.1.1	-	600	2020-07-13 19:31:56	修改 暂停 删除

配置后可以实现的效果：

- DNS 解析会智能判断出您访问的来源，并返回配置的记录 IP 地址。
- 若您本地 DNS 出口 IP 来源于移动运营商，DNS 查询获取的地址为 2.2.2.2。
- 若您本地 DNS 出口 IP 来源于电信运营商，DNS 查询获取的地址为 3.3.3.3。
- 若您本地 DNS 出口 IP 来源不属于电信或移动（例如来源于联通等）的场景下，DNS 查询获取的地址为 1.1.1.1。

通过全球范围进行访问

1. 请登录 DNS 解析控制台，选择需要配置智能解析的域名，进入该域名的**记录管理**页面。
2. 单击**添加记录**，创建2条子域名（例如，主机记录设置为 www）A 记录，线路类型分别设置为**境外**和**默认**，记录类型分别设置为 1.1.1.1（境外）、2.2.2.2（默认）。如下图所示：

www	A	境外	1.1.1.1	-	600	2020-07-13 19:34:19	修改 暂停 删除
www	A	默认	2.2.2.2	-	600	2020-07-13 19:34:33	修改 暂停 删除

配置后可以实现的效果：

- 若您本地 DNS 出口 IP 来源于境外，DNS 查询获取的地址为境外 IP 1.1.1.1。
- 若您本地 DNS 出口 IP 来源于非境外，DNS 查询获取的地址为移动运营商 IP 2.2.2.2。

通过智能解析限制某运营商或地域的访问者进行访问

1. 登录 DNS 解析控制台，选择并单击需要配置智能解析的域名，进入该域名的**记录管理**页面。
2. 单击**添加记录**，创建2条子域名（例如，主机记录设置为 www）A 记录，线路类型分别设置为**境外**和**默认**，记录类型分别设置为 127.0.0.1（境外）、2.2.2.2（默认）。如下图所示：

www	A	境外	127.0.0.1	-	600	2020-07-13 19:35:20	修改 暂停 删除
www	A	默认	2.2.2.2	-	600	2020-07-13 19:35:33	修改 暂停 删除

配置后可以实现的效果：

- 若您本地 DNS 出口 IP 来源于境外，DNS 查询获取的地址为 127.0.0.1（该地址可实现境外用户无法访问）。
- 若您本地 DNS 出口 IP 来源于非境外，DNS 查询获取的地址为移动运营商 IP 2.2.2.2。

使用 DNSPod 公共解析服务实现家庭网络净化

最近更新时间：2022-04-29 09:38:01

概述

Public DNS 是 DNSPod 推出的公共域名解析服务，可以为全网用户提供域名的公共递归解析服务。家里使用网络时，为避免访问到高风险网站以及各种广告等，您可使用 Public DNS 实现家庭网络净化。

前提条件

已注册 DNSPod 账号。如需注册，具体可参考 注册 DNSPod。

操作步骤

基础操作

1. 登录 DNSPod 控制台，在左侧菜单中单击**公共解析 > 我的配置**，进入 “公共解析” 管理页面。
2. 在 “公共解析” 页面，单击**开始使用**，并选择**家庭用户**。如下图所示：

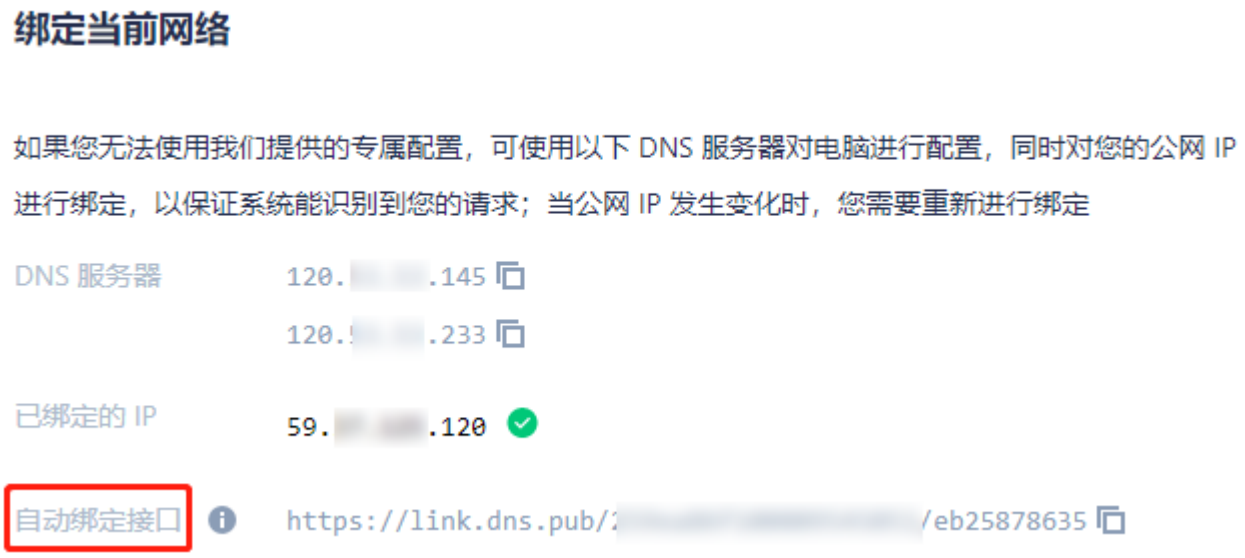
3. 单击**开始使用**，进入“配置项” 页签。如下图所示：

4. 在 “绑定当前网络” 模块中，查看**绑定当前网络 > 已绑定的 IP**，并单击**绑定**。
5. 在 “配置方式” 模块中，选择**路由器**，并按照内容进行配置。如下图所示：

6. 配置完成后，单击**拦截规则**页签，选择开启拦截威胁情报或者广告网址，从而达到防风险、去广告的效果。
   - **威胁情报**：全部开启。
   - **拦截列表**：EasyList 和 EasyList China 可选择开启其中一个，其余全部开启。
   - **分类目录**：除了游戏网站和视频网站，其余全部开启。
7. 开启后即可实现家庭网络净化。

进阶操作

如您家里路由器不支持 IPv6 地址，只支持 IPv4 地址，单击**配置项**页签，在 “绑定当前网络” 模块中，获取**自动绑定接口**。如下图所示：



- **若为智能路由器，可在智能路由器加个计划任务，间隔30分钟重复执行这条命令。**

```
wget -qO- https://link.dns.pub/8a8f7******7281/65******8e5
```

- **若为普通支持 IPv4 的路由器，并且全家共享拦截策略，则需在每次重启路由器或者外网 IP 变化后，复制自动绑定接口并在浏览器中打开。**

使用 CAA 记录防止错误签发 SSL 证书

最近更新时间：2022-05-26 14:59:42

什么是 CAA?

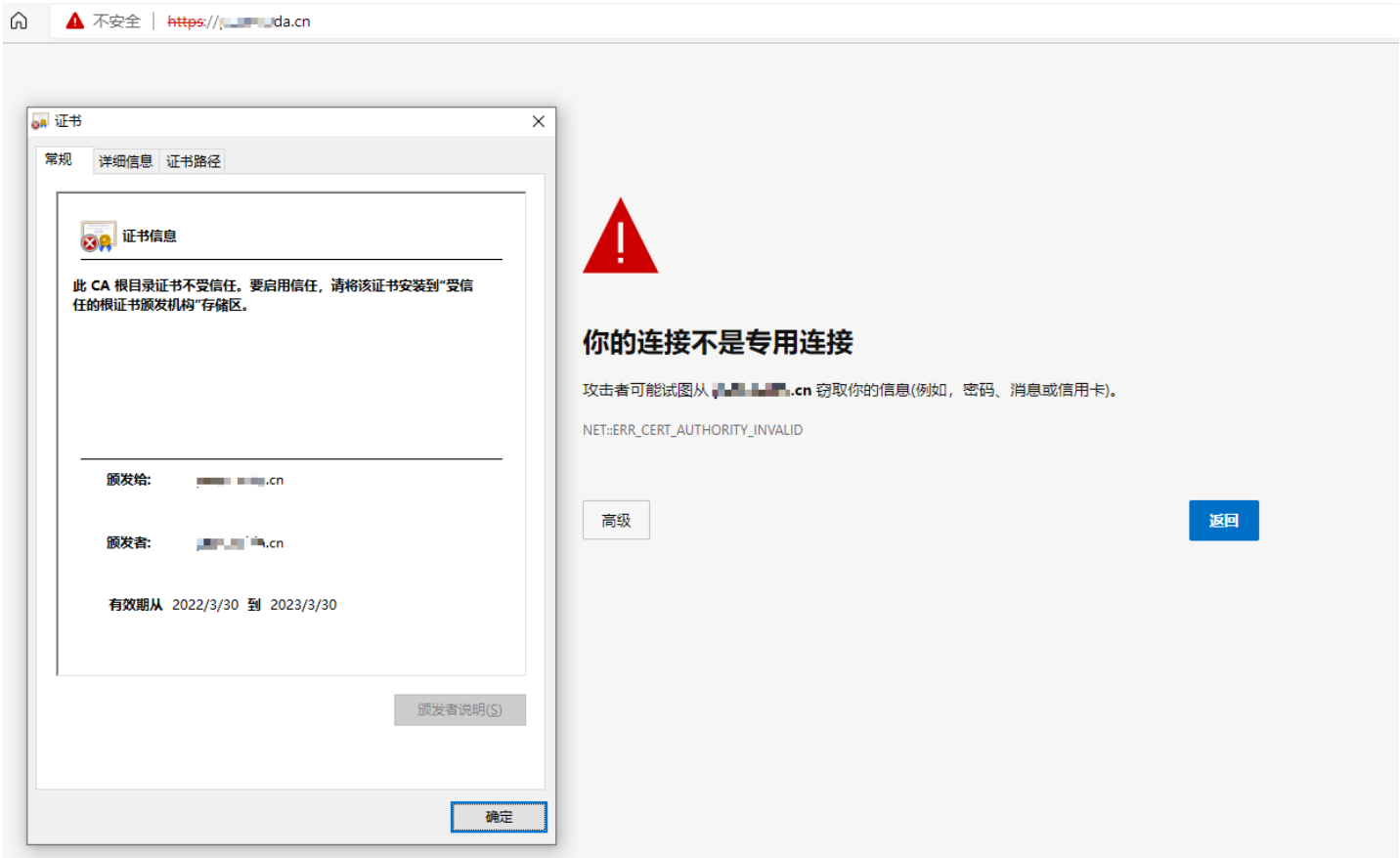
CAA（Certification Authority Authorization，证书颁发机构授权）是一项降低 SSL 证书错误颁发的控制措施，由互联网工程任务组（IETF）批准列为 IETF RFC6844 规范。2017年3月，CA 浏览器（CA/Browser Forum）论坛投票通过187号提案，要求 CA 机构从2017年9月8日起执行 CAA 强制性检查。

CAA 的作用?

域名所有者通过设置 CAA 解析记录来授权指定的 CA 机构为其颁发 SSL 证书，同时 CA 机构根据规范要求，在颁发 SSL 证书时会强制性检查域名 CAA 记录，如果检查发现未获得授权，将拒绝为该域名颁发 SSL 证书，从而防止未授权的 SSL 证书错误颁发，规避安全风险。如果域名所有者没有为其域名设置 CAA 记录，那么任何 CA 机构都可以为其域名颁发证书。

为什么要设置 CAA？

据权威部门统计，全球约有上百个证书颁发机构（CA）有权发放 SSL 证书，以证明您网站的身份，但是证书颁发机构由于某些原因，往往会被浏览器列入 “黑名单”，并被公开宣布将不再信任其签发的 SSL 证书。由于任何 CA 都可以为任何域名颁发证书，这使得 PKI 生态系统较为脆弱。因此，当您的网站部署了不被浏览器信任的证书颁发机构所颁发的证书，用户访问时，部分浏览器将提示 “HTTPS 证书不受信任”，影响您的业务正常使用。如下图所示：



因此，为避免您不被错误的颁发证书，建议您为域名设置授信的 CAA 记录，若您需指定仅支持腾讯云 SSL 证书为其颁发，腾讯云不同品牌 CAA 记录值以下：

证书品牌	记录值	
SecureSite	0 issue "digicert.com"	0 issuewild "digicert.com"
GeoTrust	0 issue "digicert.com"	0 issuewild "digicert.com"
TrustAsia	0 issue "trust-provider.com"	0 issuewild "trust-provider.com"
GlobalSign	0 issue "globalsign.com"	0 issuewild "globalsign.com"
WoTrus	0 issue "wotrus.com"	0 issuewild " wotrus.com"
DNSPod（国密标准（SM2））	0 issue "wotrus.com"	0 issuewild " wotrus.com"

说明：

0 issue 表示只有该 CA 机构可以为特定域名颁发证书， 0 issuewild 表示只有该 CA 机构可以为特定域名颁发通配符证书。

CAA 记录格式说明

CAA 记录的格式为：[flag] [tag] [value]，是由一个标志字节的 [flag] 和一个被称为属性的 [tag]-[value]（标签–值）对组成。您可以将多个 CAA 字段添加到域名的 DNS 解析记录中。

字段	说明
flag	可填写0或128，用于标志认证机构。通常情况下填0，表示如果颁发证书机构无法识别本条信息，就忽略。
tag	支持 issue、issuewild 和 iodef。 issue：CA 授权单个证书颁发机构发布的**任何类型域名证书**。 issuewild：CA 授权单个证书颁发机构发布主机名的**通配符证书**。 iodef：CA 可以将违规的颁发记录 URL 发送给某个电子邮箱。
value	CA 的域名或用于违规通知的电子邮箱。

添加 CAA 记录

> **说明：**
> 以腾讯云免费证书为例，为域名添加对应 issue 和 issuewild 记录。

1. 登录 DNSPod 管理控制台。
2. 在 “域名解析列表” 中，选择并单击需要添加 CAA 记录的域名，进入该域名的 DNS 解析记录管理页面。如下图所示：

3. 单击**添加记录**，填写以下记录信息。如下图所示：

- **主机记录**：填写子域名。例如为 www.dnspod.cn 添加 CAA 记录，您在 “主机记录” 处填写 “www” 即可。如果想添加 dnspod.cn 的 CAA 记录，您在 “主机记录” 处选择 “@” 即可。

- **记录类型**：选择 “CAA”。
  线路类型：选择 “默认” 类型，否则会导致部分 CA 机构无法进行认证。
- **记录值**：分别 填写 0 issue "sectigo.com" 与 0 issuewild "sectigo.com"。
- **权重**：不填写，可忽略。
- **MX 优先级**：不填写，可忽略。
- **TTL**：缓存的生存时间，默认600秒。如需修改，可参考 TTL 如何填写?

4. 单击【 确定 】，完成添加。

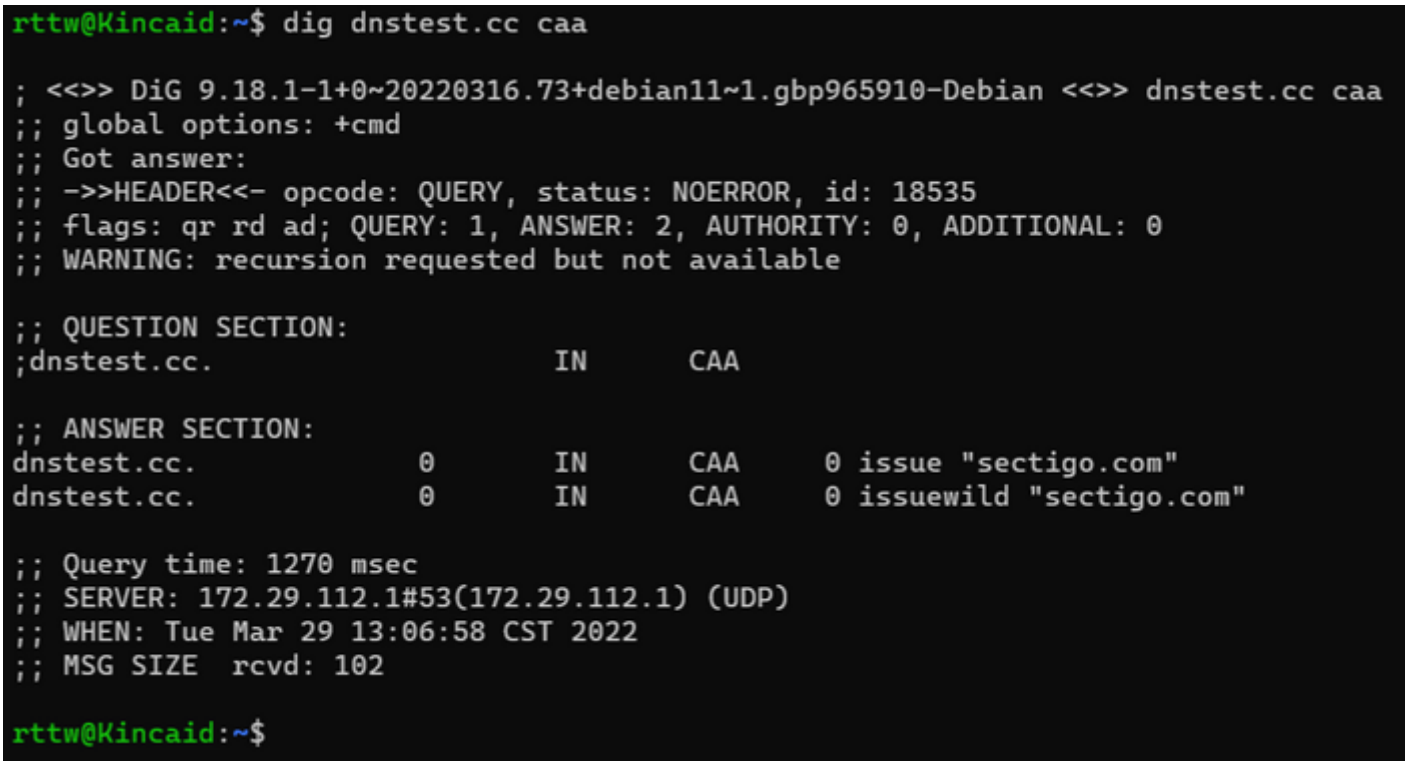
检查 CAA 记录

可通过以下两种方式检查已添加的 CAA 记录：

dig 命令

```
dig 域名名称 CAA
```

返回值为空或包含 0 issuewild "sectigo.com" 和 0 issue "sectigo.com" 即为正常。如下图所示：



DNS 诊断工具

前往 DNS 诊断工具，输入主域名并选择 CAA 记录后点击检测，返回值为空或包含 0 issuewild "sectigo.com" 和 0 issue "sectigo.com" 即为正常。如下图所示：

DNS 诊断工具

DNS解析诊断 | 域名型SSL验证

dnstest.cc | CAA | 检测

通过DNS检测可以快速查出不同的地区不同的网络对你的域名解析速度，及域名DNS信息。

检测结果

地区	耗时（秒）	TTL（秒）	值
中国	0.26s	5s	0 issue "sectigo.com"
		5s	0 issuewild "sectigo.com"
香港	0.20s	5s	0 issue "sectigo.com"
		5s	0 issuewild "sectigo.com"
美国	0.37s	5s	0 issue "sectigo.com"
		5s	0 issuewild "sectigo.com"

说明：

若出现检测失败或只有部分地区可以正常检测的情况，请检查域名 DNS 解析设置。