云解析 DNS

实践教程

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或95716。

文档目录

实践教程
其他平台解析域名平滑转入腾讯云 DNSPod

最近更新时间：2025-12-30 10:38:52

概述

若您的 DNS 解析托管在其他 DNS 服务商进行托管，现您需转入至腾讯云 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腾讯云 DNSPod。

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云解析 DNS 套餐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：
  - 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 。
  - 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

步骤一：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，腾讯云解析 DNS 支持 xls、csv、txt、zone 文件格式。建议导出 zone 文件格式，若您使用 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。

步骤二：导入解析记录至 腾讯云 DNSPod

1. 登录 云解析 DNS 控制台 ，在左侧导航栏中选择**权威解析**，进入**权威解析**页面。
2. 在**权威解析**页面中，单击**添加域名**，如下图所示：

3. 输入您需要转入的域名并单击**确定**，如下图所示：

> **说明：**
> - 如果主账号开启了子账号强制打标签，那么子账号添加域名需打标签。
> - 如果要添加的标签数较多，可以使用**键值粘贴板**功能快速添加多个标签。
> - 更多关于腾讯云标签的介绍请参见 腾讯云标签概述 。

4. 域名添加完成后，在左侧导航栏中选择**批量操作**，再单击**导入记录**页签，进入**导入记录**页面。将准备好的解析记录数据，导入至腾讯云解析 DNS，具体操作请参见 批量导入记录 。如下图所示：

步骤三：修改 DNS 服务器地址

前往域名注册商处，将域名的 DNS 服务器地址修改为腾讯云 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：

步骤四：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。
> - 如果转入前需要指定 DNS 服务器验证，请先绑定域名至付费套餐（付费套餐不校验域名的 NS 服务器地址，也能正常提供解析服务），因为免费版套餐给不同用户分配专属 NS，云解析 DNS 会校验域名的 NS 服务器为专属 NS 才会正常提供解析服务。

DNS 解析实现智能解析

最近更新时间：2025-12-30 10:38:53

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. 登录 云解析 DNS 控制台，在左侧导航栏中选择**权威解析**，进入**权威解析**页面。
2. 在**权威解析**页面中，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。如下图所示：

3. 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**，记录值分别设置为3个不同的IP 地址：1.1.1.1（默认）、2.2.2.2（移动）、3.3.3.3（电信）。如下图所示：

4. 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. 登录 云解析 DNS 控制台，在左侧导航栏中选择**权威解析**，进入**权威解析**页面。
2. 在**权威解析**页面中，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。如下图所示：

3. 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**，记录值分别设置为 1.1.1.1（境外）、2.2.2.2（默认）。如下图所示：

4. 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 云解析 DNS 控制台，在左侧导航栏中选择**权威解析**，进入**权威解析**页面。
2. 在**权威解析**页面中，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。如下图所示：

3. 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**，记录值分别设置为 127.0.0.1（境外）、2.2.2.2（默认）。如下图所示：

4. 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。

自建 Nginx，实现 URL 转发和指定访问端口

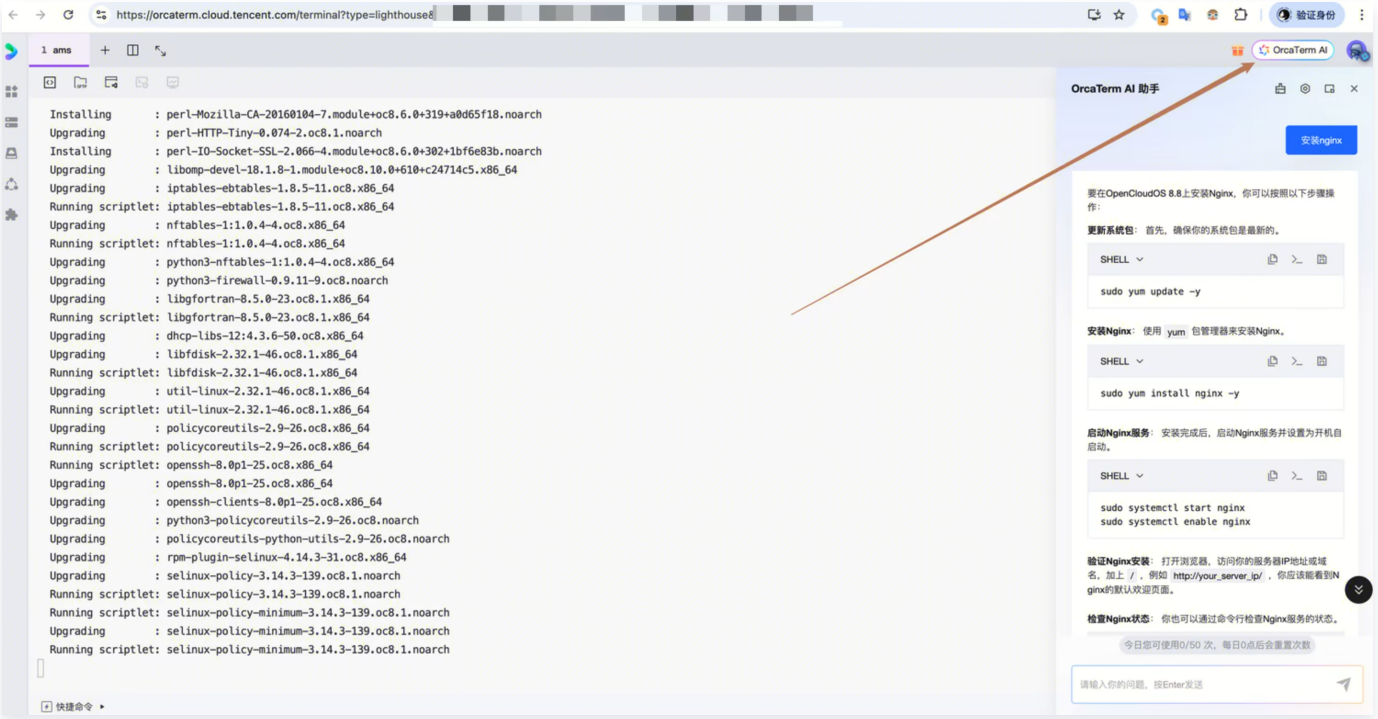
最近更新时间：2026-02-06 14:43:31

概述

如果您想实现自行搭建 URL 转发或指定访问接口，可以参考本文通过 Nginx 的转发功能实现。

配置前提

1. 安装 Nginx，本文实例使用 腾讯云轻量应用服务器，提供在线的 shell 控制台功能和文件编辑管理，也可以通过 OrcaTerm AI 直接查询 Nginx 安装教程：



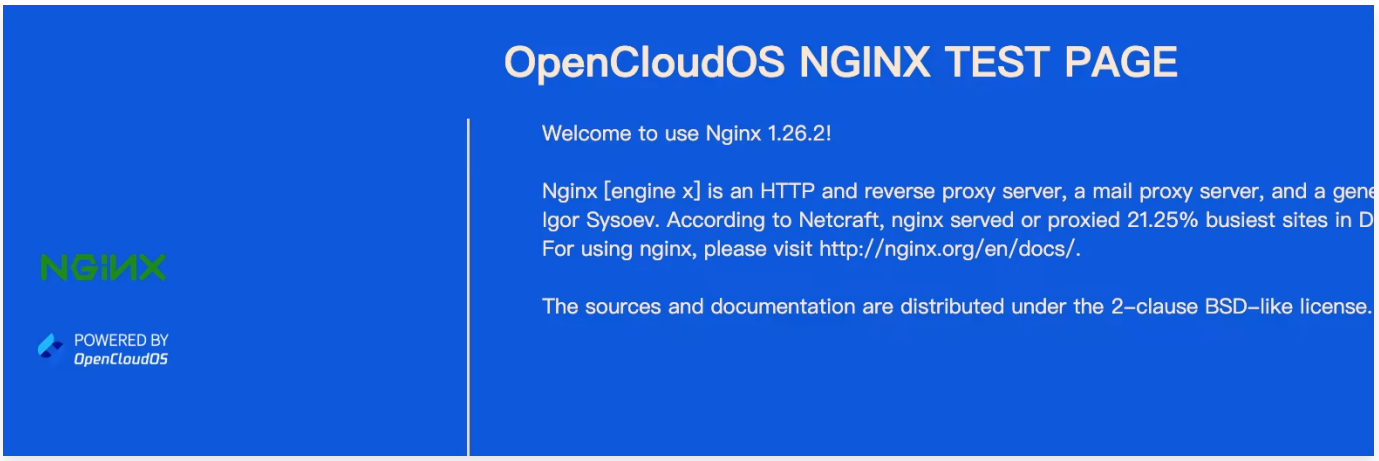
本文在轻量应用服务器上使用 yum 包管理器安装 Nginx，命令如下：

```
sudo yum install nginx -y
```

2. 启动 Nginx 服务，命令如下：

```
sudo systemctl start nginx
sudo systemctl enable nginx
```

3. 验证 Nginx 安装成功： 打开浏览器，输入 `http://你的服务器IP` ，可以看到 Nginx 的默认欢迎页面。



使用场景

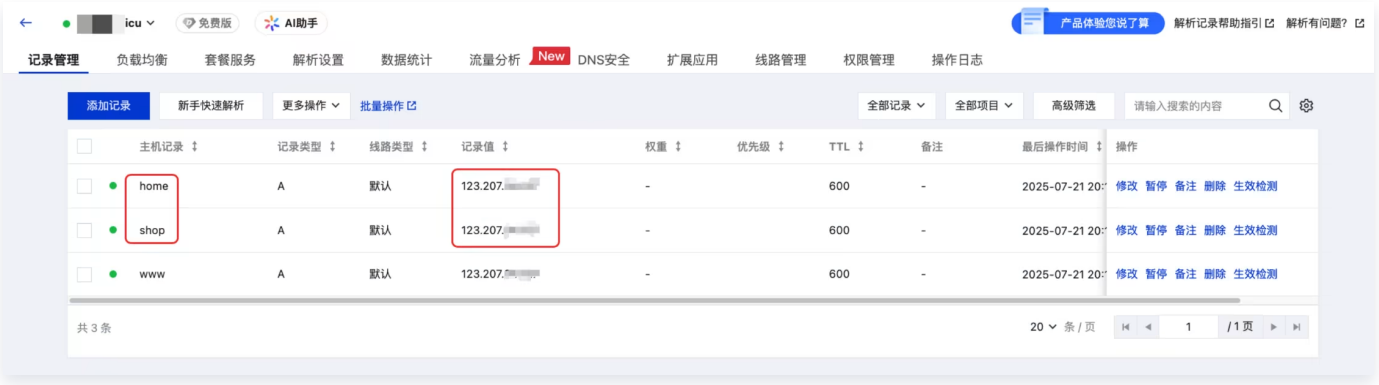
转发主要有3类使用场景：

- 场景1：显性转发，效果为浏览器地址栏输入 `http://a.com`，转发目标地址为 `https://cloud.tencent.com/`，浏览器显示转发目标地址的网站内容，且浏览器地址栏显示目标地址 `https://cloud.tencent.com/`。
- 场景2：隐性转发，效果为浏览器地址栏输入 `http://a.com`，转发目标地址为 `https://cloud.tencent.com/`，浏览器显示转发目标地址的网站内容，但地址栏显示当前地址 `http://a.com`。
- 场景3：端口转发，效果为浏览器地址栏输入 `http://a.com`，转发目标地址为 `http://a.com:8080`，浏览器显示转发目标地址8080端口的内容。

场景1. 显性 URL 转发操作场景

我们使用301/302实现显性 URL 转发，浏览器地址栏保持原始 URL，但内容从目标服务器获取。本例中，我们将 http://shop.11erotic.icu 域名显性转发到 http://www.example.com。

1. 在 云解析控制台 中添加好 shop.11erotic.icu 的 A 记录，记录值为 Nginx 服务器的公网 IP，这一步是为了让请求先到达 Nginx 服务器。



2. 使用文本编辑器（如 vi ）打开配置文件 nginx.conf：

```
sudo vi /etc/nginx/nginx.conf
```

3. 设置 server shop.11erotic.icu 通过301重定向转发到新 URL：

```
server {
    listen 80;
    server_name  shop.11erotic.icu;
    location / {
      return 301 http://www.example.com;
    }
}
```

您也可以选择使用302重定向 方式，两者的差别是 http 301响应码代表永久重定向，http 302响应码代表临时重定向。

```
server {
    listen 80;
    server_name  shop.11erotic.icu;
    location / {
      return 302 http://www.example.com;
    }
}
```

4. 重载 Nginx 服务配置。

```
sudo  systemctl reload nginx
```

5. 验证效果，通过 `curl -v http://shop.11erotic.icu` 进行验证：

```
curl  -v http://shop.11erotic.icu
```

如下图所示，HTTP 响应的转发字段 Location 信息和预设的 URL 地址一致，说明设置的 URL 转发已生效：

```
[redacted] ~ % curl -v http://shop.11erotic.icu
* Host shop.11erotic.icu:80 was resolved.
* IPv6: (none)
* IPv4: 123.20[redacted]
*   Trying 123.2[redacted]
* Connected to shop.11erotic.icu (123.20[redacted]) port 80
> GET / HTTP/1.1
> Host: shop.11erotic.icu
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 301 Moved Permanently
< Server: nginx/1.26.2
< Date: Mon, 31 Mar 2025 09:47:25 GMT
< Content-Type: text/html
< Content-Length: 169
< Connection: keep-alive
< Location: http://www.example.com
<
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
```

场景2. 隐性 URL 转发操作场景

我们使用**反向代理**实现隐性 URL 转发，浏览器地址栏保持原始 URL，但内容从目标服务器获取。本例中，我们将 http://home.11erotic.icu 域名隐性转发到 http://www.example.com。

1. 使用文本编辑器如 vi 打开配置文件 nginx.conf

```
sudo vi /etc/nginx/nginx.conf
```

2. 设置 server 段， home.11erotic.icu 通过 proxy_pass 转发到新 URL：

```
server {
    listen 80;
    server_name  home.11erotic.icu;
    location / {
      proxy_pass http://www.example.com;
    }
}
```

3. 重载 Nginx 服务配置。

```
sudo  systemctl reload nginx
```

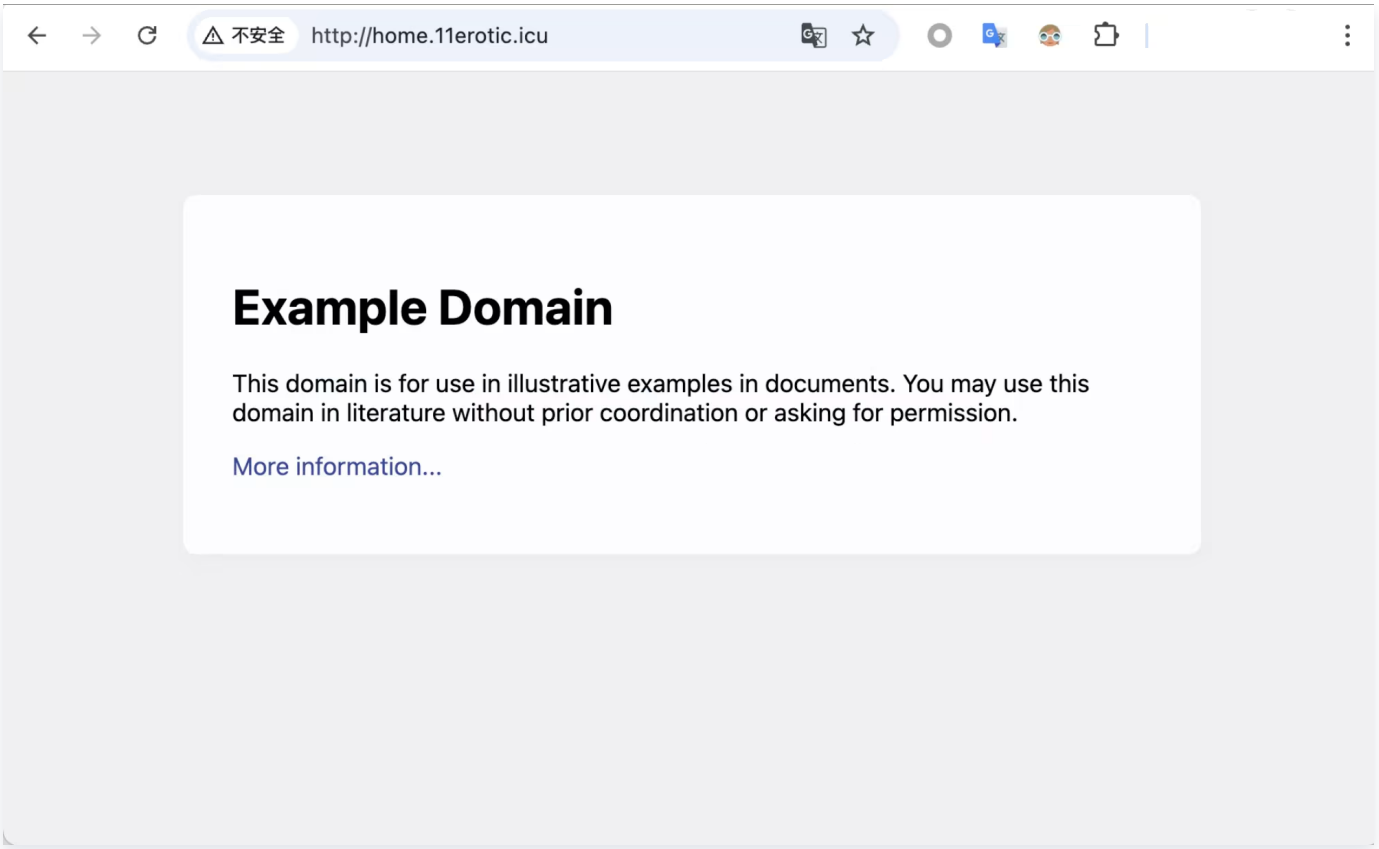
4. 验证效果，使用 `curl -v http://home.11erotic.icu` 进行验证：

```
curl  -v http://home.11erotic.icu
```

如下图所示，返回的内容已经是 http://www.example.com 的内容，说明设置的 URL 转发已生效：

```
* Connected to home.11erotic.icu (123.2[redacted]) port 80
> GET / HTTP/1.1
> Host: home.11erotic.icu
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Server: nginx/1.26.2
< Date: Mon, 31 Mar 2025 09:28:10 GMT
< Content-Type: text/html
< Content-Length: 1256
< Connection: keep-alive
< ETag: "84238dfc8092[redacted]:1736799080.121134"
< Last-Modified: Mon, 13 Jan 2025 20:11:20 GMT
< Cache-Control: max-age=1488
< X-N: S
<
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
```



场景3. 端口转发操作场景

使用文本编辑器如 vi 打开配置文件nginx.conf，配置自己的server，就能将不同子域名解析到不同端口了。本例中，我们将http://home.11erotic.icu 转发到http://home.11erotic.icu:8080。

1. 使用文本编辑器如 vi 打开配置文件nginx.conf

```
sudo vi /etc/nginx/nginx.conf
```

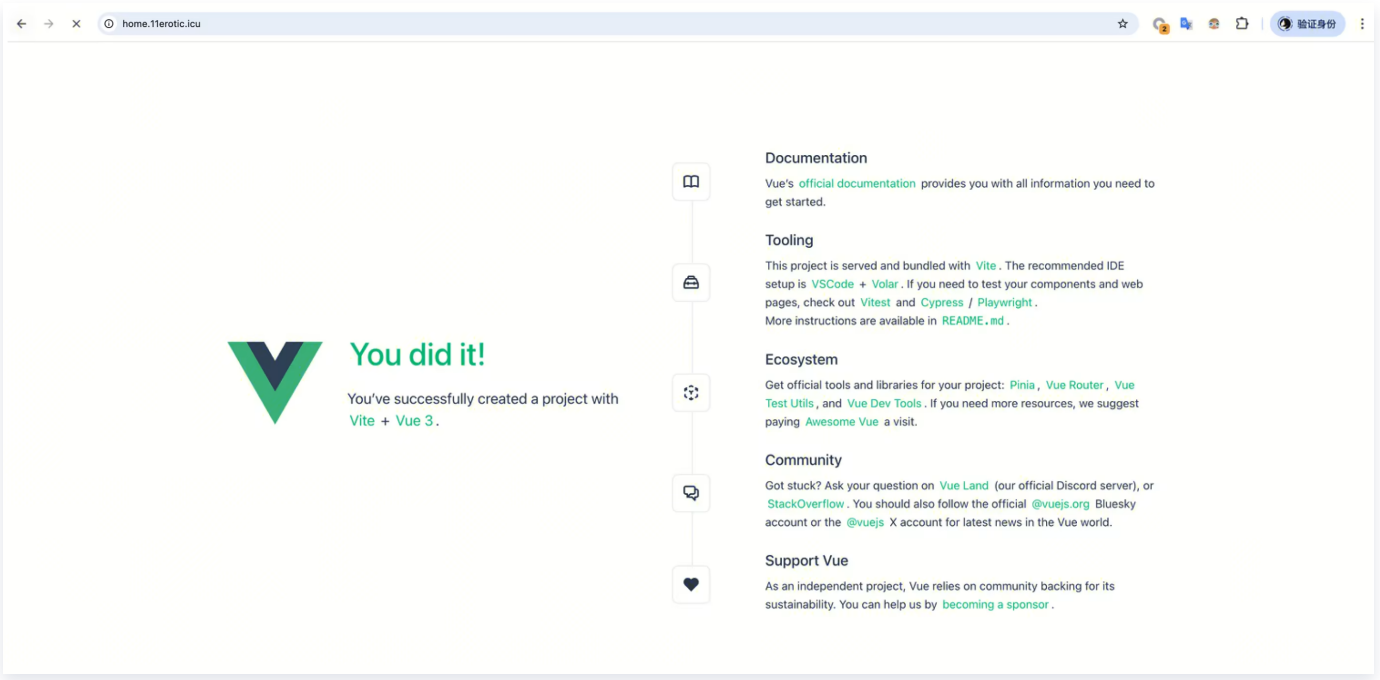
2. 设置 server段，home.11erotic.icu 通过 proxy_pass 转发到8080端口：

```
server {
    listen 80;
    server_name  home.11erotic.icu;
    location / {
      proxy_pass http://localhost:8080;
    }
}
```

3. 重载 Nginx 服务配置。

```
sudo  systemctl reload nginx
```

4. 验证效果，通过 http://home.11erotic.icu/ 访问8080端口应用，可以看到已成功转发。



使用 CAA 记录防止错误签发 SSL 证书

最近更新时间：2025-12-30 10:38:53

什么是 CAA?

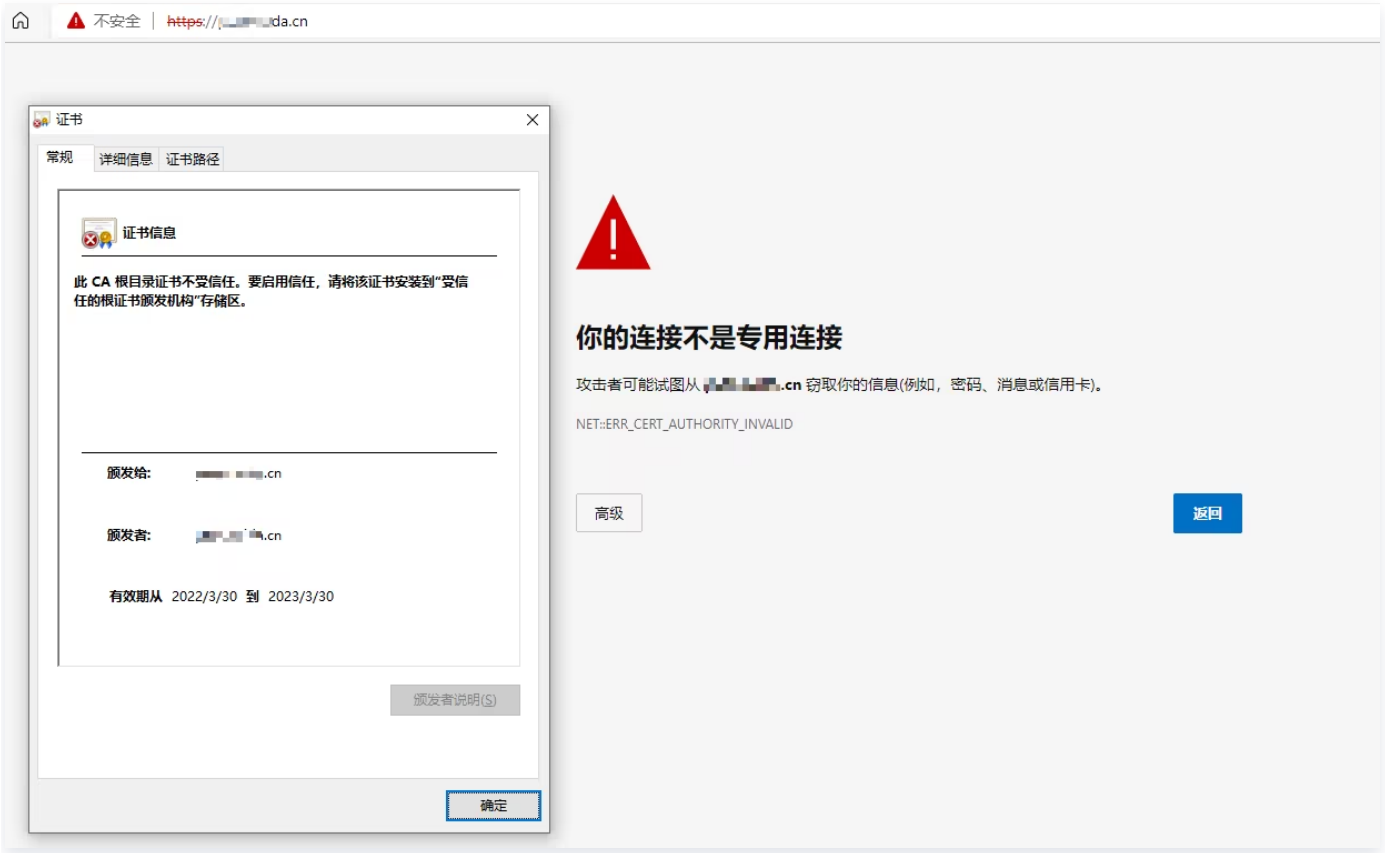
CAA（Certification Authority Authorization，证书颁发机构授权）是一项降低 SSL 证书错误颁发的控制措施，由互联网工程任务组（IETF）批准列为 IETF RFC6844 规范。2017年3月，CA 浏览器（CA/Browser Forum）论坛投票通过187号提案，要求 CA 机构从2017年9月8日起执行 CAA 强制性检查。

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，为避免您不被错误地颁发证书，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 记录值如下：

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，用于标识认证机构。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 云解析 DNS 控制台，在左侧导航栏中选择**权威解析**，进入**权威解析**页面。
2. 在**权威解析**页面中，选择并单击需要添加 CAA 记录的域名，进入该域名的**记录管理**页面，如下图所示：

3. 在**记录管理**页面中，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，请参见 TTL 如何填写?

4. 单击**确定**，完成添加。

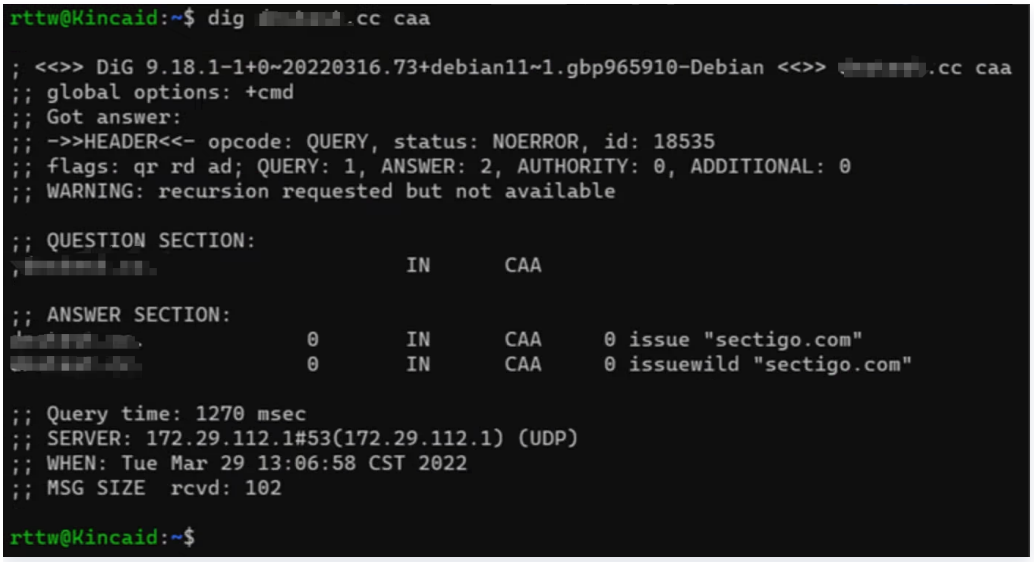
检查 CAA 记录

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，输入域名名称并选择 CAA 记录后单击检测，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：

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。

域名共享实践教程

最近更新时间：2025-12-22 15:57:32

操作场景

若您需使用域名共享功能，您可根据具体需求参考以下场景进行设置：

域名	授予权限	授权对象	域名示例	操作指南
二级解析域名	所有域名解析读写权	其他 DNSPod 用户（主账户）	dnspod.cn	场景1
	所有域名解析只读权		dnspod.cn	场景2
	名下部分记录读写权		www.dnspod.cn	场景3
	名下部分记录只读权		www.dnspod.cn	场景4

操作指南

场景1：需授权二级解析域名下所有域名解析全读写权限给其他 DNSPod 用户（主账户），例如 dnspod.cn

1. 登录 云解析 DNS 控制台，在左侧导航栏中选择**权威解析**，进入**权威解析**页面。
2. 在**权威解析**中，单击需要操作的域名名称，进入该域名的**记录管理**页面。

3. 选择**权限管理**页签，单击**添加域名共享**，如下图所示：

4. 在弹出的**添加域名共享**窗口中，输入需共享的腾讯云账号 ID，单击**添加**。

5. 勾选**共享主域名**和设置**全读写**权限，单击**确定**。如下图所示：

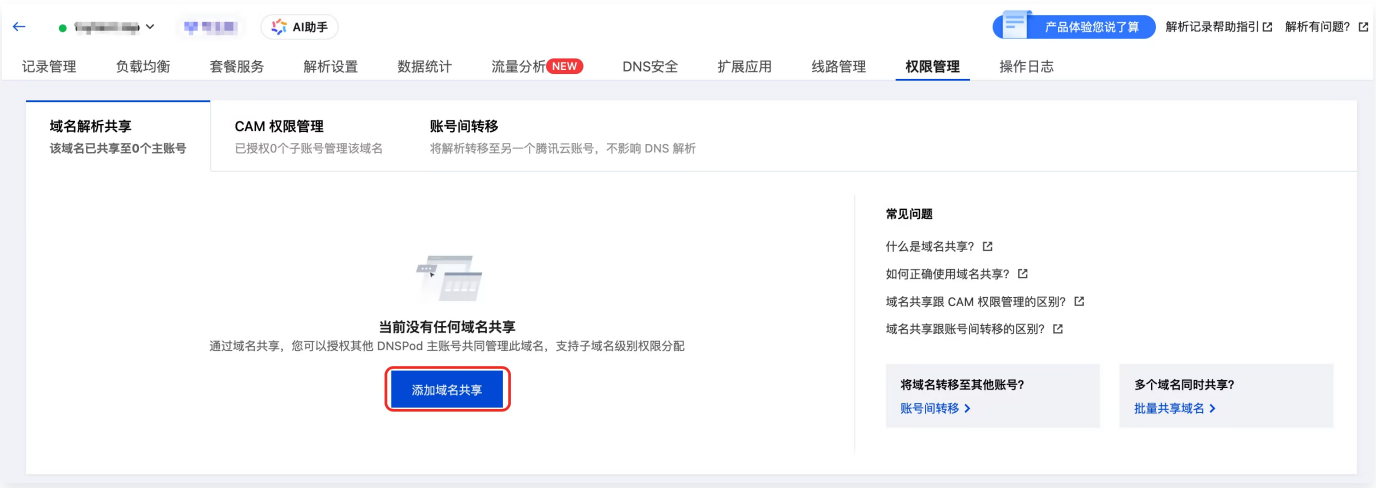
> **注意：**
> 完成设置后被授权云解析 DNS 用户将拥有该解析域名的所有设置权限，包括但不限于解析记录设置、自定义线路、功能设置等。但不能对解析套餐进行操作。

6. 添加成功后如下图所示：

场景2：需授权二级解析域名下所有域名解析只读权限给其他 DNSPod 用户（主账户），例如 dnspod.cn

1. 登录 云解析 DNS 控制台，在左侧导航栏中选择**权威解析**，进入**权威解析**页面。
2. 在**权威解析**页面中，单击需要操作的域名名称，进入该域名的**记录管理**页面。

3. 选择**权限管理**页签，单击**添加域名共享**，如下图所示：



4. 在弹出的**添加域名共享**窗口中，输入需共享的腾讯云账号 ID，单击**添加**。

5. 勾选**共享主域名**和设置**只读**权限，单击**确定**。如下图所示：

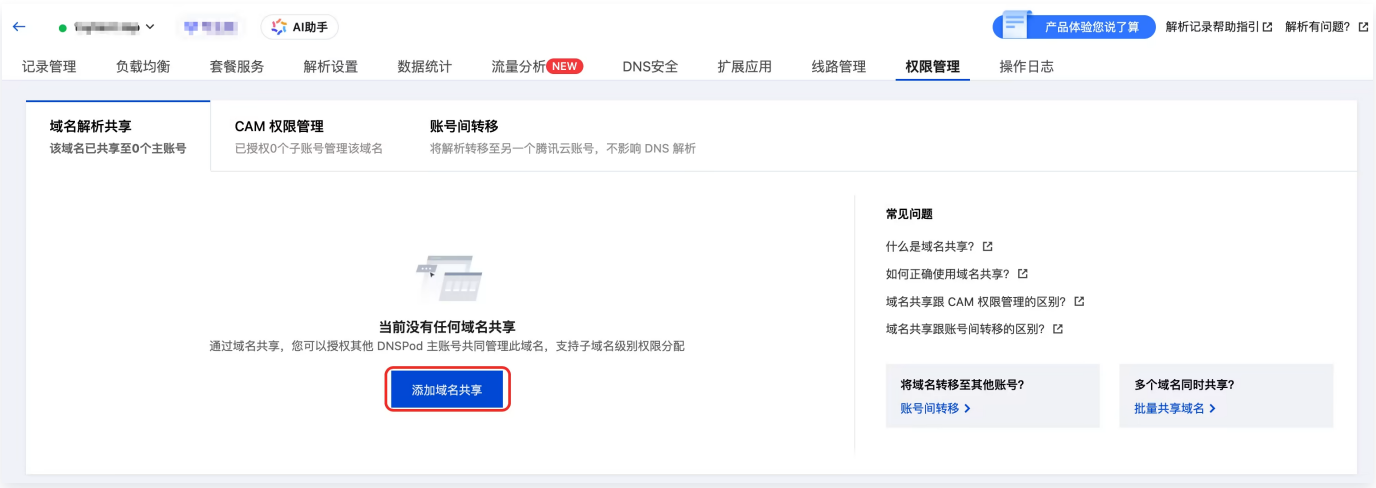
> **注意：**
> 完成设置后被授权云解析 DNS 用户将拥有该解析域名的所有设置只读权限。

6. 添加成功后如下图所示：

场景3: 需授权二级解析域名下部分记录读写权给其他 DNSPod 用户（主账户），例如 www.dnspod.cn

1. 登录 云解析 DNS 控制台，在左侧导航栏中选择**权威解析**，进入**权威解析**页面。
2. 在**权威解析**页面中，单击需要操作的域名名称，进入该域名的**记录管理**页面。

3. 选择**权限管理**页签，单击**添加域名共享**，如下图所示：



4. 在弹出的**添加域名共享**窗口中，输入需共享的腾讯云账号 ID，单击**添加**。

5. 勾选**共享部分记录**和设置**全读写**权限，单击**确定**。如下图所示：

> **注意：**
> 完成设置后被授权云解析 DNS 用户将拥有该解析域名子域名记录设置权限。但不能设置同级别或上级解析记录设置、自定义线路、功能设置等。也不能对解析套餐进行操作。

6. 添加成功后如下图所示：

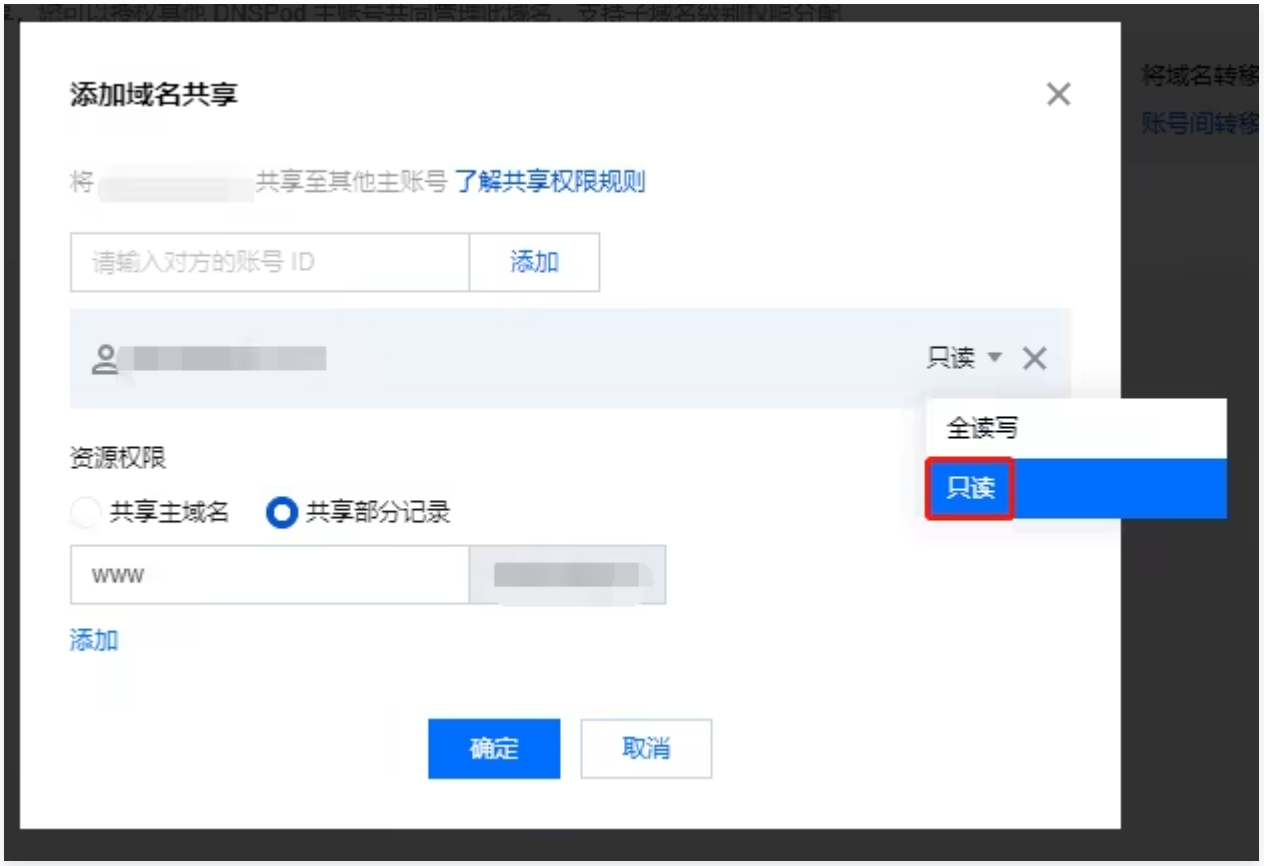
场景4: 需授权二级解析域名下部分记录只读权给其他 DNSPod 用户（主账户），例如 www.dnspod.cn

1. 登录 云解析 DNS 控制台，在左侧导航栏中选择**权威解析**，进入**权威解析**页面。
2. 在**权威解析**页面中，单击需要操作的域名名称，进入该域名的**记录管理**页面。

3. 选择**权限管理**页签，单击**添加域名共享**，如下图所示：

4. 在弹出的**添加域名共享**窗口中，输入需共享的腾讯云账号 ID，单击**添加**。

5. 勾选**共享部分记录**和设置**只读**权限，单击**确定**。如下图所示：



> **注意：**
> 完成设置后被授权云解析 DNS 用户将拥有该解析域名子域名记录只读权限。

6. 添加成功后如下图所示：

子域名托管解析实践教程

最近更新时间：2025-12-22 15:57:32

操作场景

若您需要将子域名托管在 云解析 DNS 解析并添加解析记录，您可参考本文进行操作。

> **说明：**
> - 子域名解析托管仅支持在 DNSPod 添加二级域名主域名（例如： dnspod.cn ）后才可进行子域名托管，不支持在控制台直接添加子域名进行托管。
> - 子域名托管解析实践教程建议在特殊场景下进行使用。若无特殊需求，建议直接托管二级域名主域名，管理更高效快捷。

前提条件

该功能仅支持专业版及以上套餐，不支持免费套餐。若需使用您可购买套餐后再进行操作，具体操作请参见 购买解析套餐 。

操作步骤

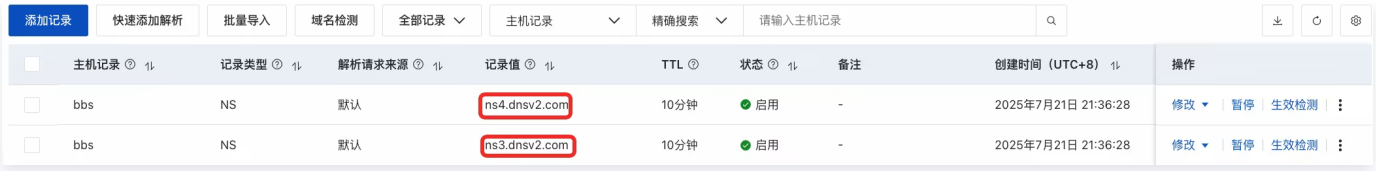
云解析 DNS 托管子域名

您需在您的原二级域名解析商处添加 NS 解析记录指向 腾讯云 DNSPod DNS 服务器地址。以下操作以阿里云为例。

> **说明：**
> 本文档仅供参考，具体以第三方页面为准；如有版权或其他问题，请及时联系 腾讯云在线客服 。

1. 登录阿里云 云解析控制台 。
2. 找到需设置的解析域名，并单击**解析设置**。如下图所示：

3. 在**解析设置**中，设置两条子域名的 NS 记录，记录值为**腾讯云 DNSPod DNS 服务器地址**。如下图所示：



> **说明：**
> 记录值请填写 腾讯云 DNSPod **付费套餐地址**，详情请参见 DNS 节点分布说明 。

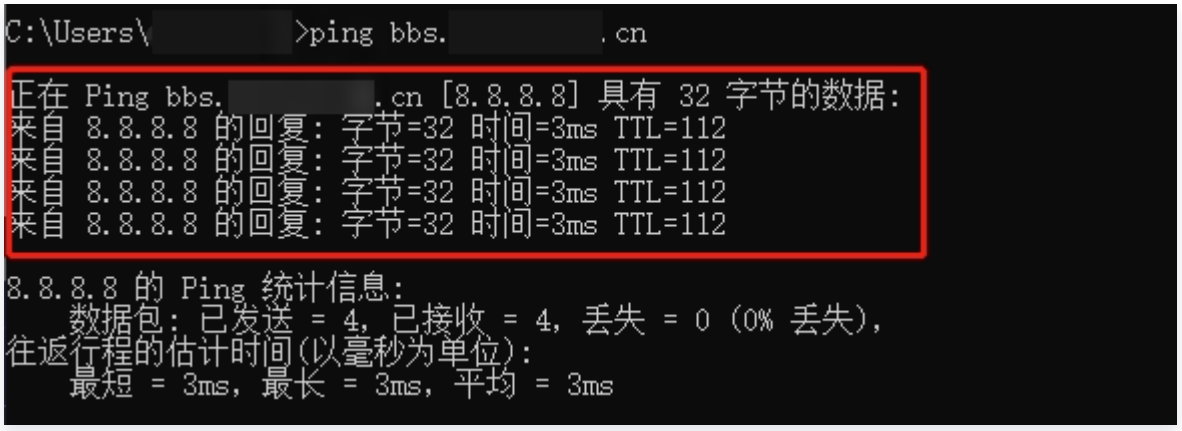
添加解析记录

1. 登录 云解析 DNS 控制台 ，在左侧导航栏中选择**权威解析**，进入**权威解析**页面。
2. 在**权威解析**页面中，找到需设置的解析域名，并单击域名名称，进入该域名的**记录管理**页面，如下图所示：

> **注意：**
> 添加解析记录的子域名需要先添加至域名列表，操作步骤请参见 添加子域名解析 。

3. 在**记录管理**页面中，您即可设置子域名对应解析记录。如下图所示：

4. 完成以上步骤后，请等待解析生效。解析生效后您即可访问设置的对应解析。如下图所示：



群晖（Synology）NAS 启用 DNSPod DDNS

最近更新时间：2025-08-26 15:21:42

操作场景

本文档指导您在群晖（Synology）NAS 上启用 DNSPod 提供的 DDNS（动态域名服务）。启用后，您可以在具备公网 IP 地址的情况下在外访问群晖（Synology）NAS。

> **说明：**
> 本过程中仅购买域名可能收取一定的费用，启用 DDNS 服务免费。

前提条件

- 具备群晖（Synology）NAS 管理员权限的账号。
- 具备 DNSPod 账号并完成 实名认证 。
- NAS 所在网络环境具备公网 IP 地址。

操作步骤

注册域名

> **说明：**
> 如果您已拥有可使用的域名，可忽略此步骤。

1. 登录 DNSPod 域名注册控制台 。
2. 在域名注册模块输入想要注册的域名并单击**查询**。如下图所示：

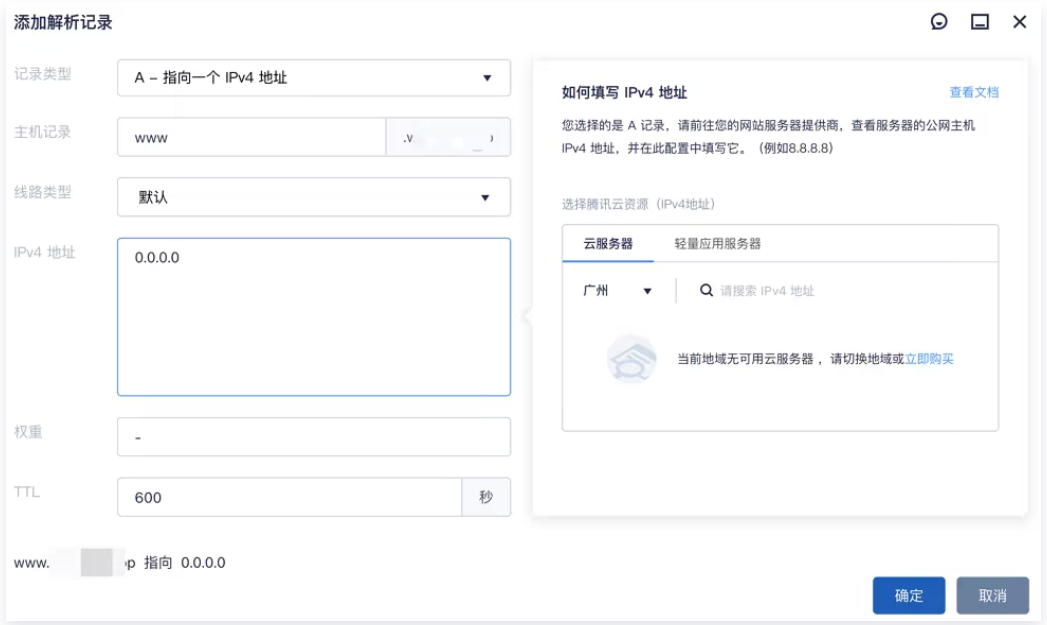
3. 挑选您心仪的域名并选择**立即加购** > **立即购买**。如下图所示：

4. 按照页面指引提交订单并完成支付即可完成购买。购买成功后，您可进入 我的域名 页面查看您注册的域名。

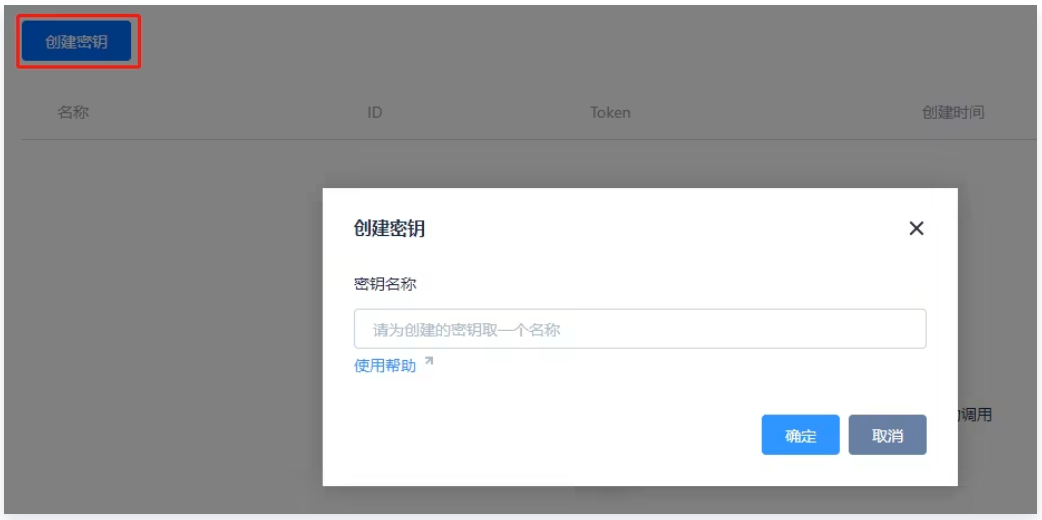
启用 DDNS

1. 在 我的域名 页面中，单击您已注册的域名，进入“记录管理”页面。
2. 单击**添加记录**，添加一条主机记录为 `www` ，记录值为任意 IP 的 A 记录。如下图所示：

> **说明**
> 记录值可以填写为任意 IP 地址，完成操作步骤后将会自动更新为您的公网 IP 地址。此处以 `0.0.0.0` 记录值为例。

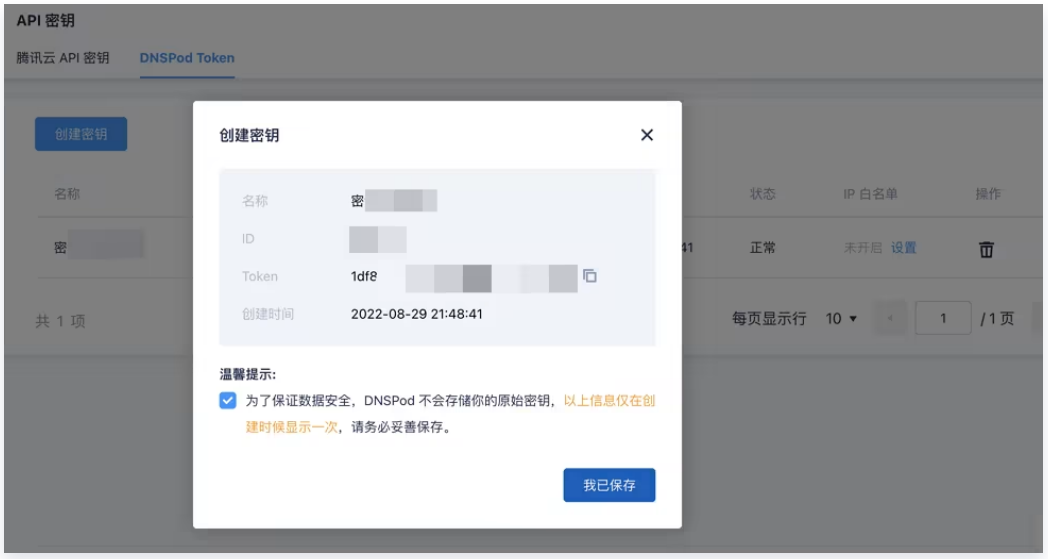


3. 进入 API 密钥 页面，选择 DNSPod Token 页签并单击创建密钥，输入自定义的密钥名称后，单击确定。

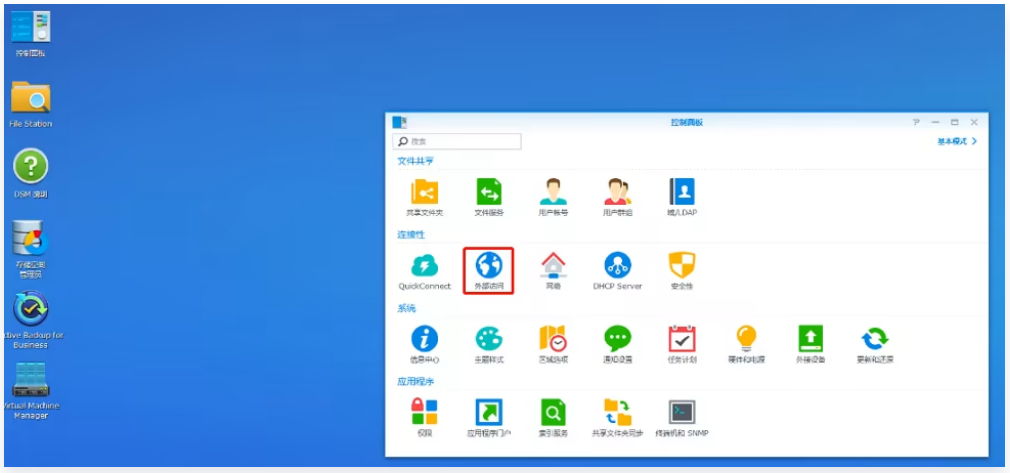


4. 密钥创建成功后，请妥善保管弹出窗口中的显示 ID 与 Token。

> **注意：**
> 以下信息仅在创建时显示一次，请您妥善保管。



5. 使用具有管理员权限的账号登录您的群晖（Synology）NAS，选择**控制面板** > **外部访问**。



6. 在 **DDNS** 页签中，单击**新增**。

7. 在弹出窗口中的“服务供应商”选单内下拉选择 DNSPod.cn，并填写相关信息。

- 主机名称：填写您购买的域名。
- 用户名/电子邮箱：填写您获取到的 DNSPod 的 Token ID。
- 密码/密钥：填写您获取到的 DNSPod 的 Token。

> **说明：**
> 您可单击**测试联机**，测试是否能成功联机。状态栏显示为正常，即代表成功联机。

8. 单击**确定**。
9. 单击**立即更新**，确认状态栏显示正常。如下图所示：

10. 返回 我的域名 页面，查看记录值的是否已变更为您的公网 IP 地址。
    若已变更为设置成功。未变更则请进行相关排查。

群晖（Synology）NAS 安装免费 SSL 证书

最近更新时间：2025-08-26 15:21:42

操作场景

本文档指导您如何在群晖（Synology）NAS 上安装免费 SSL 证书。

> **说明**
> 免费 SSL 证书由业界知名 CA 机构 TrustAsia 免费提供。

前提条件

- 具备群晖（Synology） NAS 管理员权限的账号。
- 具备 DNSPod 账号并完成 实名认证 。
- 已在群晖（Synology）NAS 上正确 部署 DNSPod DDNS 服务 。

操作步骤

申请及下载证书

1. 登录 DNSPod，并进入 我的域名 页面。
2. 单击 DDNS 域名，进入**记录管理**页面，检查该域名的 DDNS 记录值是否为群晖 NAS（Synology）中获取到的公网 IP 地址。确认无误后单击**扩展应用**页签，再单击 **SSL证书** 中的**立即申请**。如下图所示：

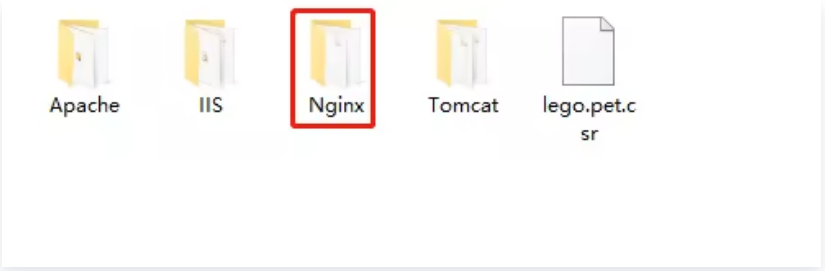
3. 在弹出的**申请 SSL 证书**窗口中，选择左侧**免费证书**，并单击**申请**。如下图所示：

4. 页面自动跳转到 SSL 证书控制台，根据指引输入**需要申请 SSL 证书的域名**，并提交证书申请。
5. 系统将自动在记录中添加一条“主机记录”为 `_dnsauth` 的 TXT 记录。域名身份验证通过后，您将收到短信、邮件等审核通过通知。
6. 来到 **我的域名** 控制台，查看申请了 SSL 证书的域名，若**服务**列显示为**绿色字体 SSL**，则表示申请成功。鼠标移动到 **SSL** 上，单击悬浮框中的**点此管理**进入证书详情页。如下图所示：

7. 在证书详情页，单击**下载证书**，将证书的压缩包文件下载到本地。如下图所示：

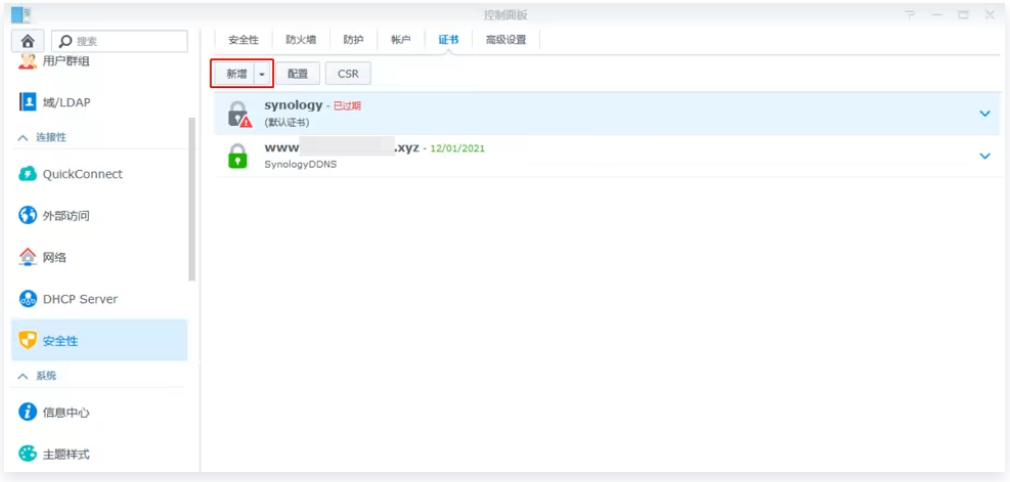
安装证书

1. 在本地解压后，打开 Nginx 文件夹。如下图所示：



> **说明**
> 文件夹内的 `.crt` 后缀文件为证书，`.key` 后缀文件为私钥。

2. 请使用具有管理员权限的账号登录您的群晖（Synology）NAS，选择**控制面板** > **安全性**，选择**证书**页签并单击**新增**。如下图所示：

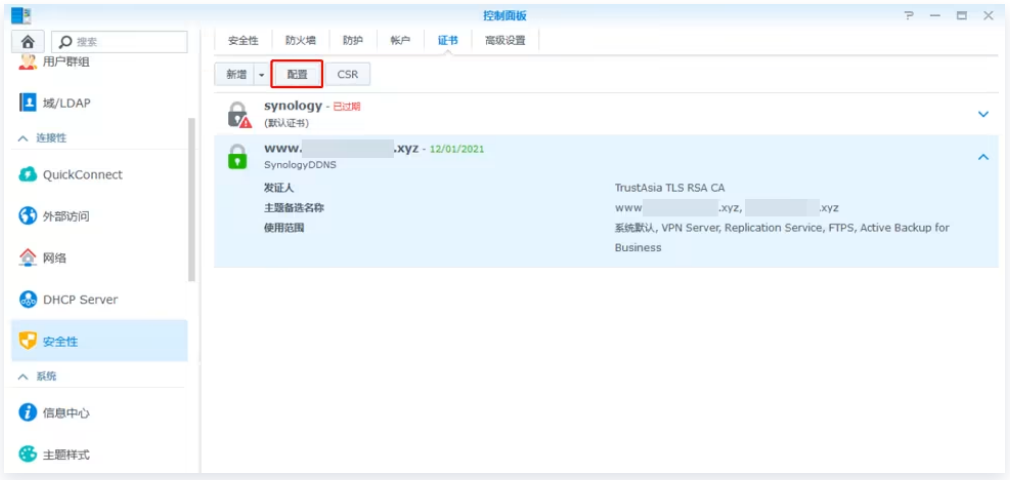


3. 在弹出的**创建证书**窗口中，选择**添加新证书**，并单击**下一步**。如下图所示：

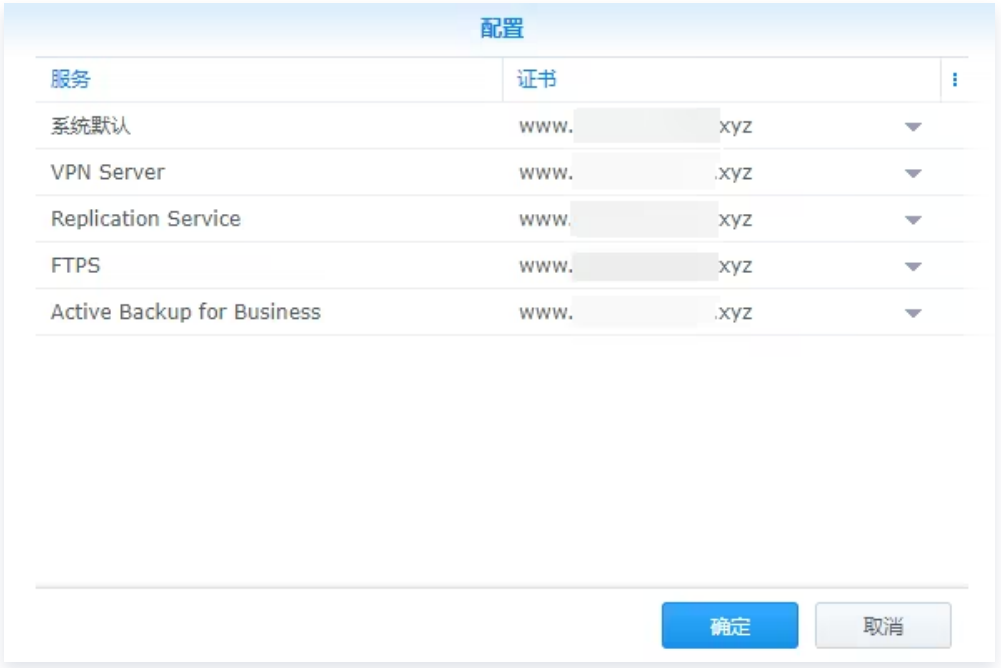
4. 请填入您的自定义描述，选择**导入证书**，并单击**下一步**。如下图所示：

5. 导入下载至本地的证书与私钥文件，上传后并单击**确定**。如下图所示：

6. 单击控制面板中的**配置**。如下图所示：



7. 在弹出的**配置**窗口中，将所有证书替换为新添加的 SSL 证书，并单击**确定**。如下图所示：



8. 使用 `https://域名:5001` 访问您的群晖（Synology）NAS，即可查看证书已被浏览器信任。如下图所示：

注意

若访问失败，请检查端口转发是否正确设置及 DSM 是否开启了 HTTPS 5001端口访问。

acme.sh 自动解析并申请证书

最近更新时间：2025-08-28 17:01:11

ACME（自动证书管理环境）是一个互联网工程任务组维护的协议，它允许自动化 Web 服务器证书的部署，acme.sh 是支持 ACME 协议流行的客户端之一，可以通过其实现 SSL 证书的自动申请、续期等。本文将为您介绍如何使用 acme.sh 自动申请证书。

安装 acme.sh

全新安装

适用于未安装 acme.sh 的用户，使用以下命令安装 acme.sh 客户端：

安装 acme.sh

```
curl https://get.acme.sh | sh -s email=my@example.com
```

或者：

```
wget -O -  https://get.acme.sh | sh -s email=my@example.com
```

> **说明：**
> 请将 my@example.com 替换为您的邮箱地址。

旧版升级

适用于已安装 acme.sh 的用户，请运行以下命令升级 acme.sh 客户端：

```
acme.sh --upgrade
```

获取腾讯云 SecretId 和 SecretKey

方式一：使用主账号 API 密钥

1. 登录 腾讯云控制台，进入 访问管理 页面，单击左侧菜单栏的 访问密钥，进入 API 密钥管理页面。

2. 单击**新建密钥**，创建 API 密钥，并记录保存 SecretId 和 SecretKey。

方式二：使用子账号 API 密钥

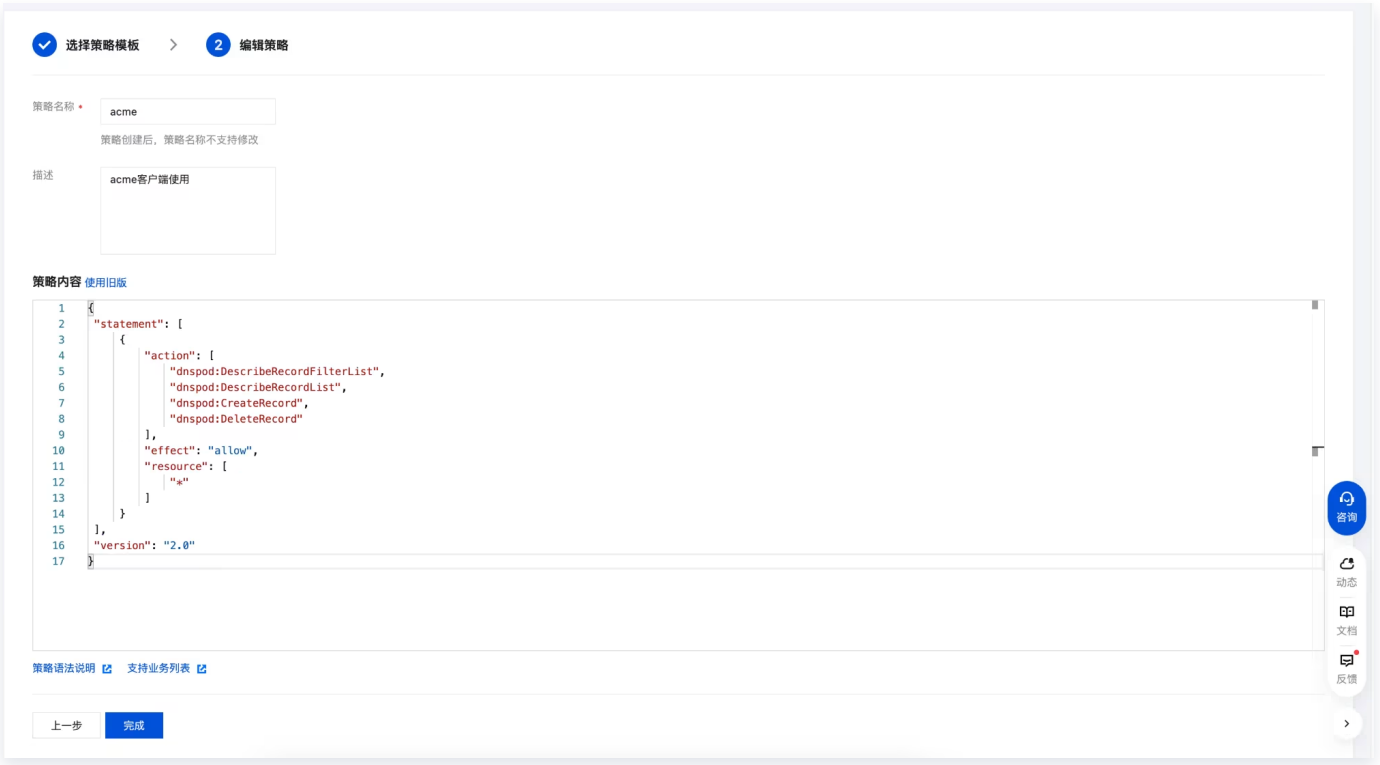
步骤一：新建权限策略

1. 登录 腾讯云控制台，进入 访问管理 页面，单击左侧菜单栏的 策略，进入**策略**页面，并点击**新建自定义策略**。

2. 选择**按策略语法创建 > 空白模板**，填写基本信息，并将策略语法修改为以下内容，并单击**完成**。

```
{
 "statement": [
     {
         "action": [
             "dnspod:DescribeRecordFilterList",
             "dnspod:DescribeRecordList",
             "dnspod:CreateRecord",
             "dnspod:DeleteRecord"
         ],
         "effect": "allow",
         "resource": [
             "*"
         ]
     }
```

```
  ],
  "version": "2.0"
}
```



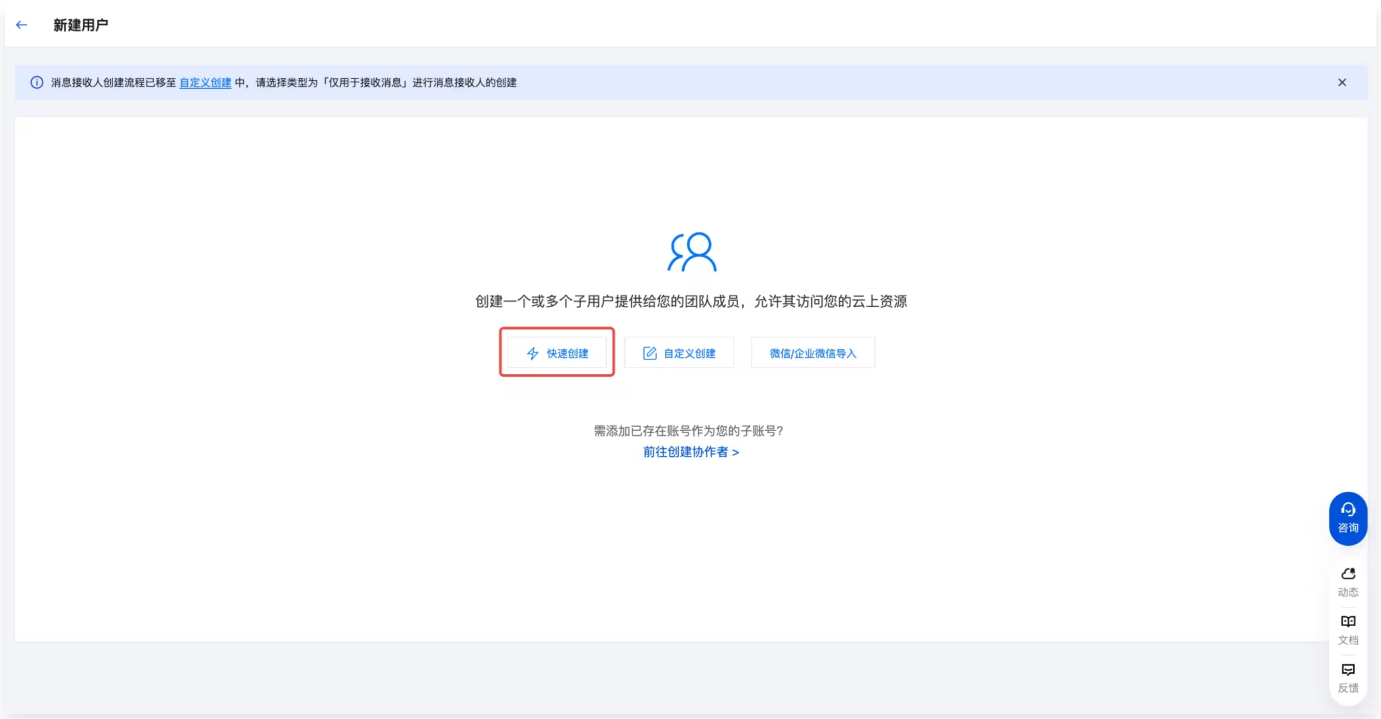
说明：

如您需要更精细的权限控制，可根据实际需求修改策略语法，如配置资源六段式等，详情请参见 CAM-云解析 DNS 。

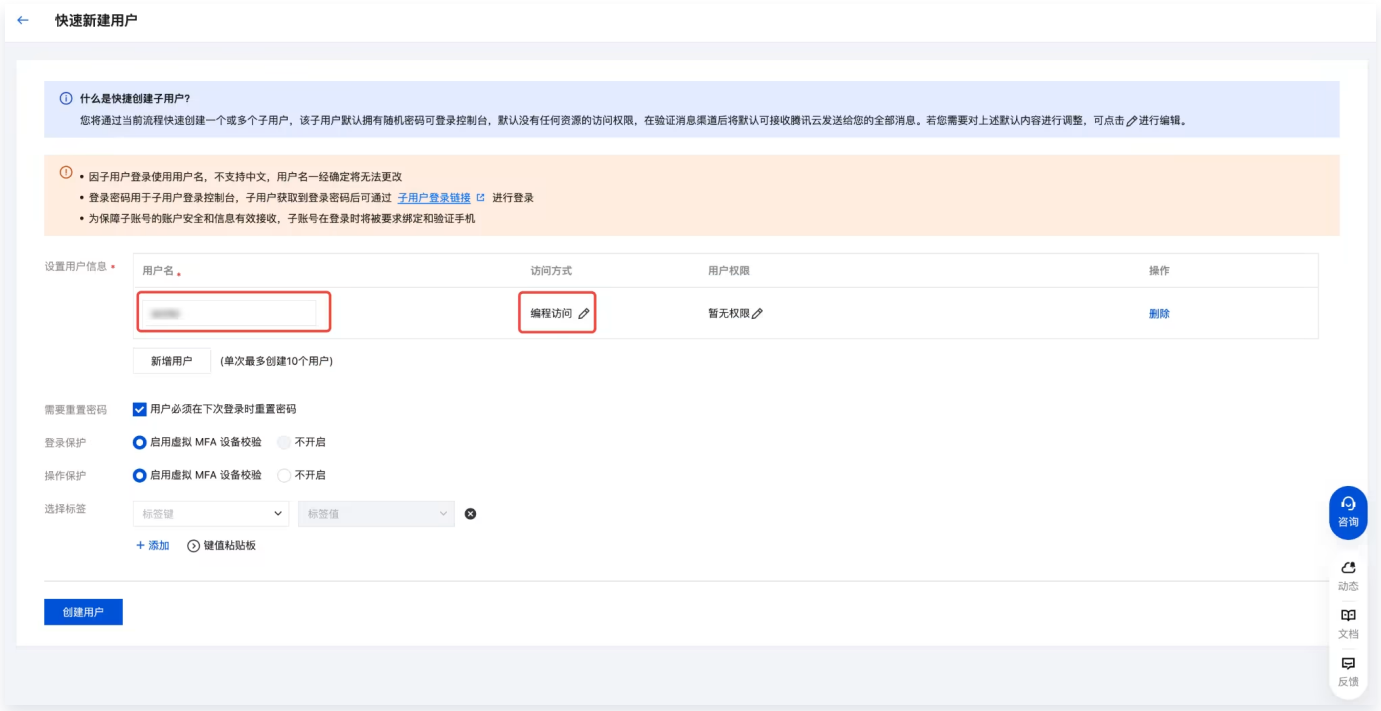
步骤二：新建子账号并关联权限策略

1. 登录 腾讯云控制台 ，进入 访问管理 页面，单击左侧菜单栏的 用户列表 ，进入用户列表页面，并单击**新建用户**。

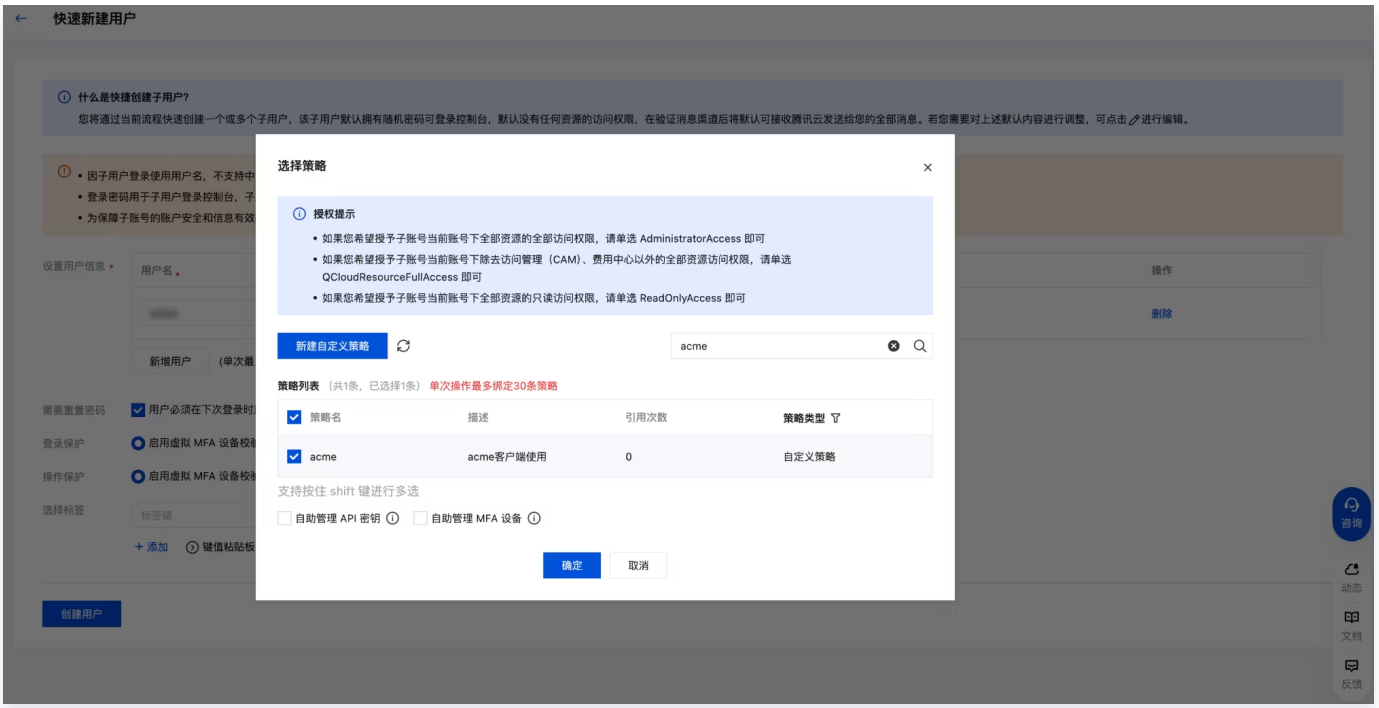
2. 在**新建用户**页面，选择**快速创建**。



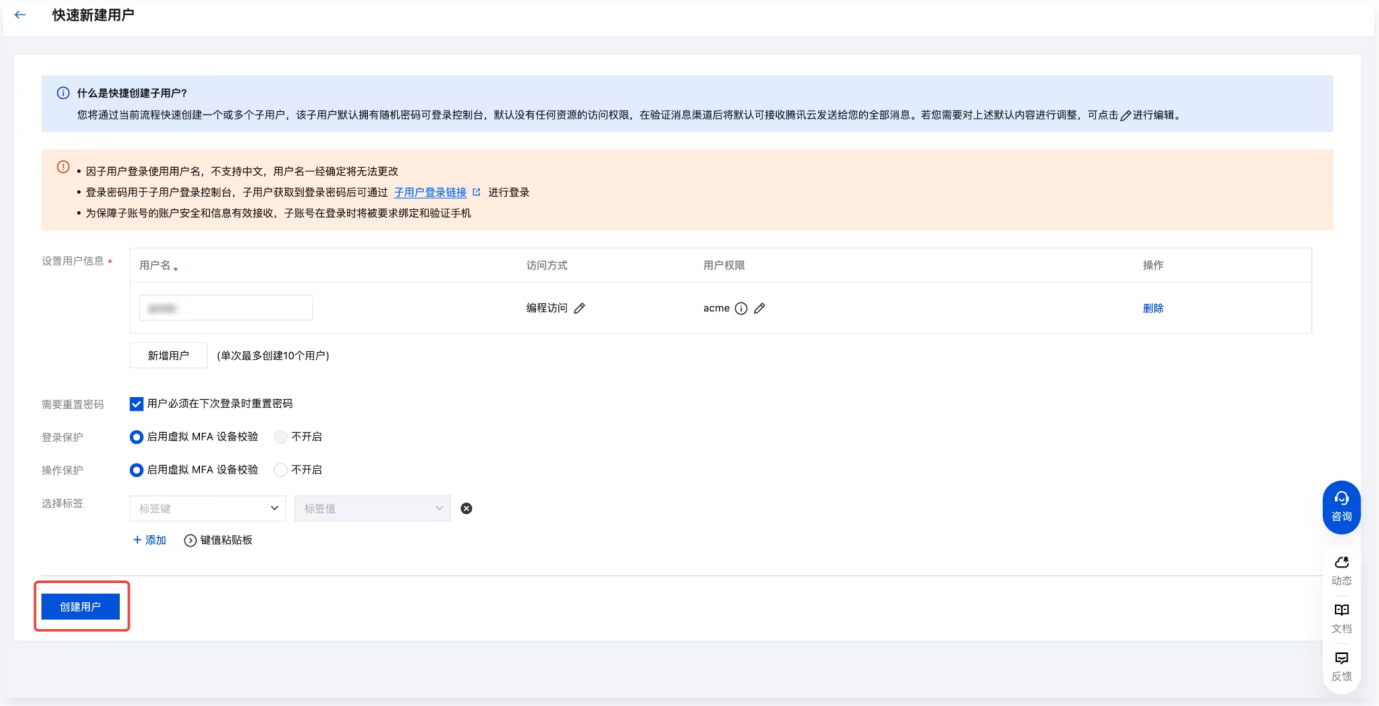
3. 在**快速新建用户**页面，填写用户信息，访问方式选择**编程访问**。



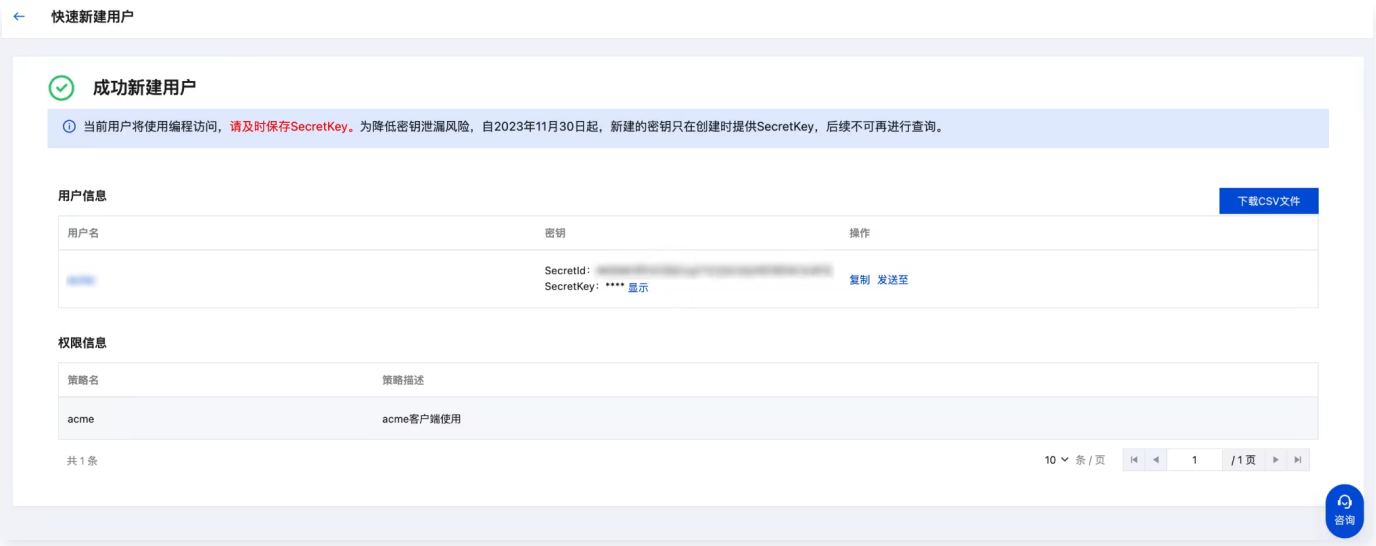
4. 配置用户权限，仅选择刚刚创建的权限策略，并单击**确定**。



5. 单击**创建用户**，完成子账号创建。



6. 记录保存 SecretId 和 SecretKey。



申请证书

1. 将获取到的 SecretId 和 SecretKey 导入环境变量中，以便 acme.sh 调用。

```
export Tencent_SecretId="<Your SecretId>"
export Tencent_SecretKey="<Your SecretKey>"
```

> **说明：**
> - <Your SecretId>：请输入您的 SecretId。
> - <Your SecretKey>：请输入您的 SecretKey。

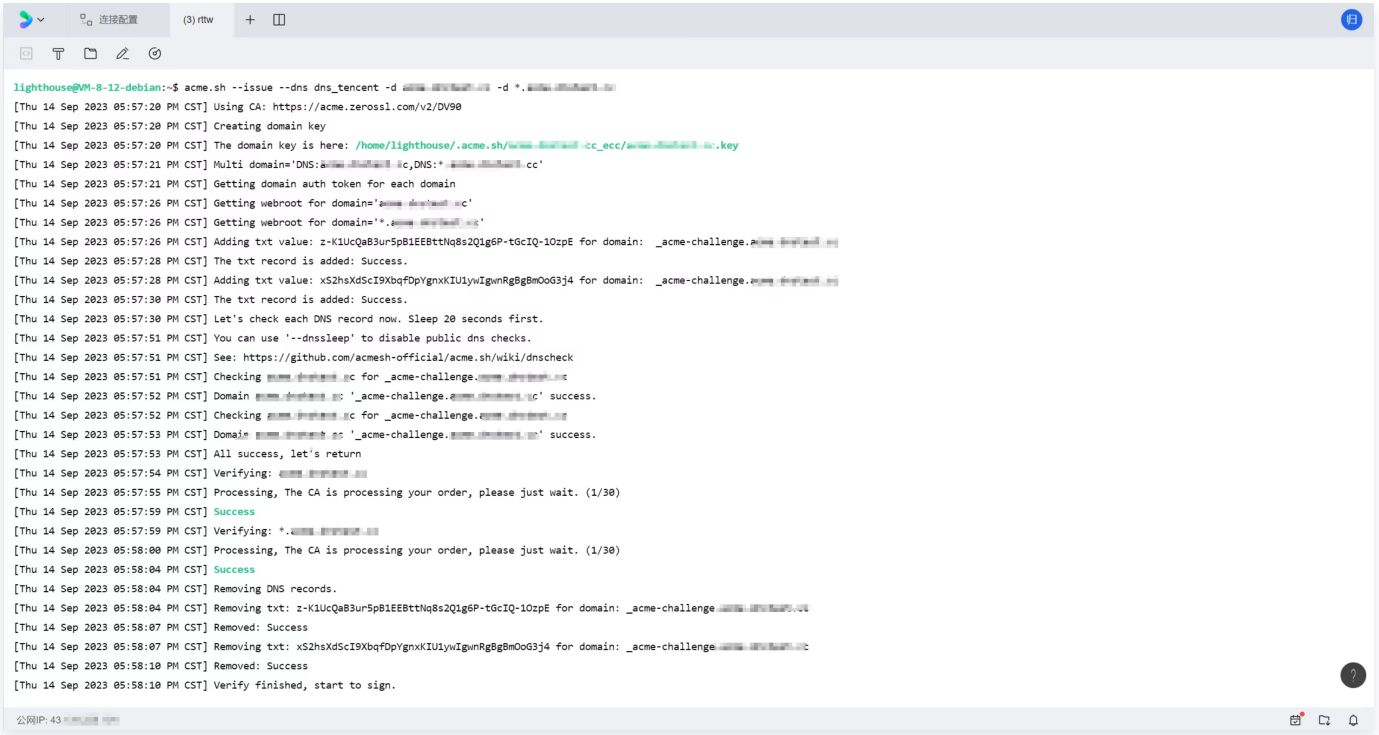
2. 使用 acme.sh 申请证书，例如：

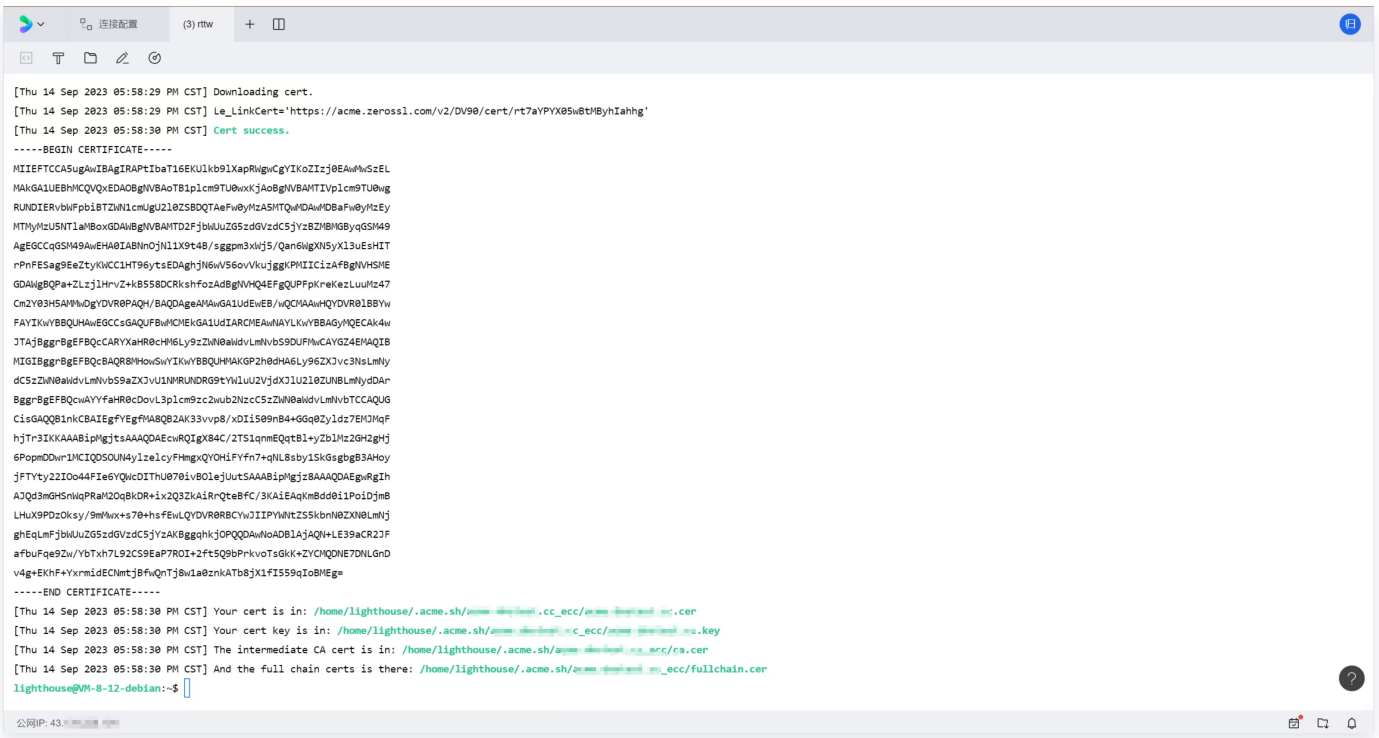
```
acme.sh --issue --dns dns_tencent -d example.com -d *.example.com
```

`example.com` 为演示域名，`*.example.com` 指 `example.com` 的所有下一级子域名，请将其替换为您的域名。运行后，acme.sh 将自动为您的域名 `example.com` 和其所有下一级子域名申请证书，并将证书文件保存在 `~/.acme.sh/example.com/` 目录下，并且会自动为您的域名配置证书自动续期任务，无需手动续期。

> **说明：**
> 证书品牌由 acme.sh 脚本决定，其申请的证书品牌通常为 Let's Encrypt、ZeroSSL 等。

运行结果如下：





后续操作

安装证书

> **警告：**
>
> acme.sh 不建议直接使用 `~/.acme.sh/` 目录下的证书文件，而是通过 acme.sh 提供的命令将证书安装到指定位置，以确保证书的正确使用和续期，详情请参见 Install the cert to Apache/Nginx etc，以下以 Nginx 为例。

```
acme.sh --install-cert -d example.com \
--key-file       /path/to/keyfile/in/nginx/key.pem  \
--fullchain-file /path/to/fullchain/nginx/cert.pem \
--reloadcmd     "service nginx force-reload"
```

注意：

请将 `example.com` 替换为您的域名，`/path/to/keyfile/in/nginx/key.pem` 和 `/path/to/fullchain/nginx/cert.pem` 替换为证书实际路径，`service nginx force-reload` 替换为您使用的 Web 服务重载命令。

完成申请后请将证书配置到您的网站中，以 Nginx 为例，示例如下：

```
server {
    listen 443 ssl http2;

    server_name example.com;

    # 请替换为证书实际路径
    ssl_certificate /path/to/fullchain/nginx/cert.pem;
    ssl_certificate_key /path/to/keyfile/in/nginx/key.pem;

    ssl_session_timeout 5m;
    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-
ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-CHACHA20-POLY1305;

    # 推荐设置为on，若您需要将其设置为off，只需将下面的命令中的"on"替换为"off"即可
    ssl_prefer_server_ciphers on;
    location / {
        root /nginx/www/html;
    }
}
```

注意：

完成后请重载服务。

联系我们

如果您在使用过程中遇到任何问题，欢迎报告 Issue，或者通过以下方式联系我们：

Issue： Report bugs to TencentCloud (DNSPod) DNS API 。

PTR 反向解析实践教程

最近更新时间：2025-09-15 15:15:22

操作场景

PTR 反向解析主要应用在邮件服务器中，因为多数垃圾邮件发送方使用动态分配或者没有注册域名的 IP 发送垃圾邮件，以逃避追踪，所以可以在邮件服务器中拒绝接收来自无法反向解析到域名的 IP 地址发送的信息，作为一种拒收垃圾邮件的手段，启用反向解析，可以拒绝接收所有没有注册域名发来的信息，从而提升腾讯云 IP 的信誉度。本文将指导您如何将已有的腾讯云 IP 在 DNSPod 进行反向解析至域名。

前提条件

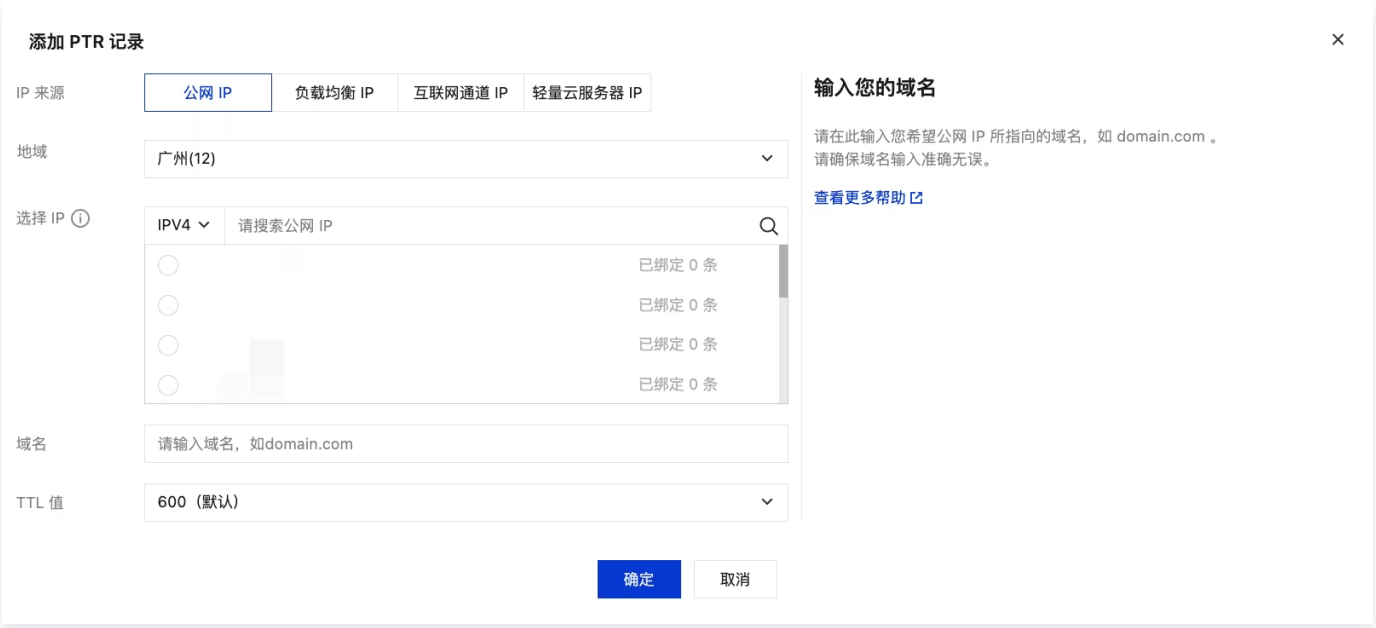
在开始执行操作前，请您确认以下信息：

- 您的账号需要拥有弹性公网 IP、负载均衡 IP、互联网通道 IP 或轻量云服务器 IP 的其中一个即可。如果没有，需要您提前准备 公网 IP 、负载均衡 IP 、互联网通道 IP 或 轻量云服务器 IP 。
- 您已购买 PTR 反向解析增值服务 。

添加 PTR 反向解析

1. 登录 云解析 DNS 控制台 ，选择左侧导航栏中的 反向解析 。
2. 在**反向解析**页面中，单击**添加 PTR 记录**。如下图所示：

3. 在弹出的**添加 PTR 记录**窗口中，参考以下信息进行配置。如下图所示：



- **IP 来源：**支持公网 IP、负载均衡 IP 、互联网通道 IP 或轻量云服务器 IP，请选择您已准备的腾讯云 IP 即可。
- **地域：**请按需选择。
- **选择 IP：**请按需选择。
- **域名：** 请输入您希望腾讯云 IP 所指向的域名名称。
- **TTL 值：** 请选择您的 TTL 值。TTL 值越小，解析生效越快，TTL值越大，解析生效越慢。一般情况下生效时间与设置的 TTL 值相同。

4. 单击**确定**，即可完成操作。

> **说明：**
> 添加完成后需要等待解析生效，一般情况下生效时间与设置的 TTL 值相同。

相关说明

PTR 配置要求 IP 归属为腾讯云， 如果您的需求是批量成功发送邮件，可以评估使用 腾讯云 SES 产品 。

怎么实现容灾切换

最近更新时间：2025-11-28 10:19:52

概述

容灾切换功能由智能全局流量管理 IGTM 产品为您提供。容灾切换可以对您的解析记录值（IP 或者域名）进行健康监控，当健康状态异常时，可以使用备用 IP 或域名，从而实现故障时的容灾切换。

前提条件

- 已开通 **IGTM 标准版或 IGTM 旗舰版**，并创建 IGTM 实例，详情请参见 创建实例 。

> **说明：**
> IGTM 探测节点使用腾讯云机器，若探测业务目的地址也是腾讯云 IP，网络访问将直接通过腾讯云内网，如果该目的地址外网 IP 不可用，但是内网 IP 可用，那么 IGTM 可能无法准确探测目的地机器是否可用。

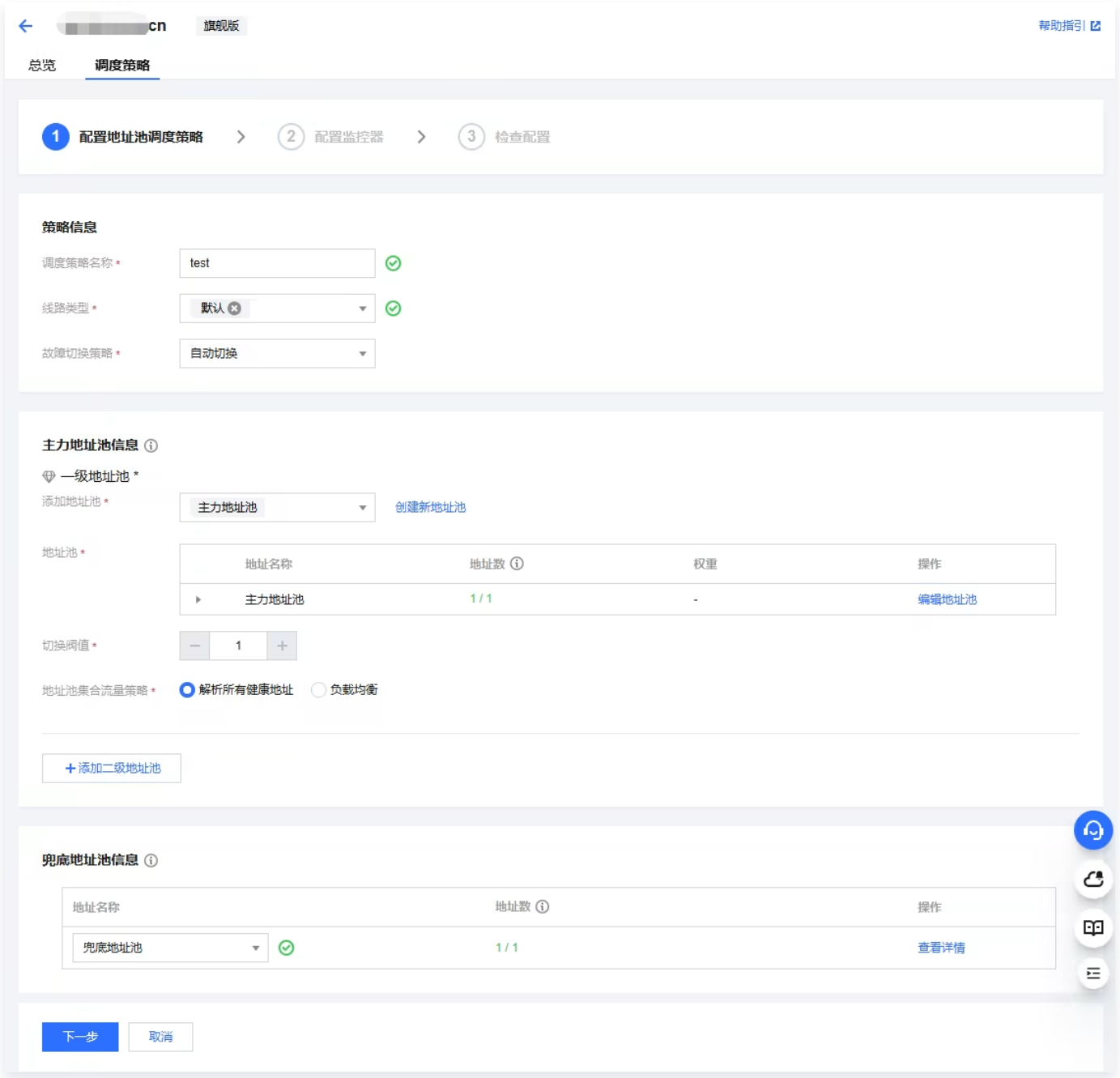
- 已配置地址池，详情请参见 地址池配置 。

操作步骤

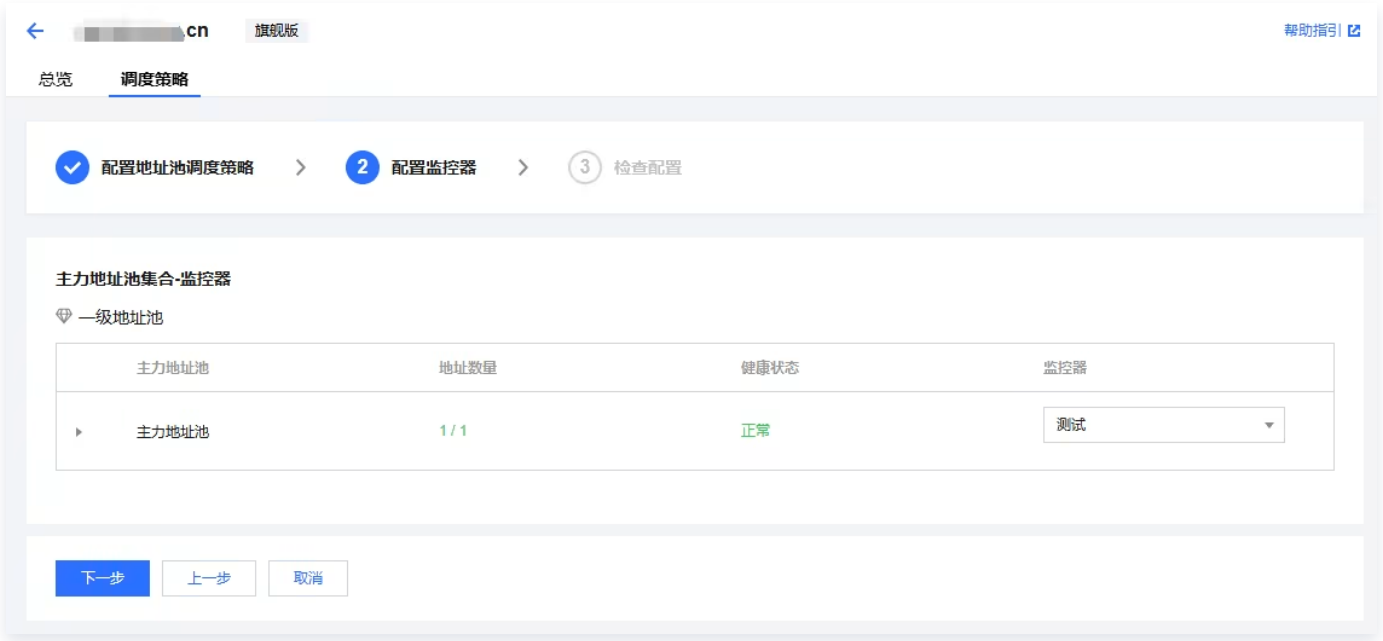
1. 登录 智能全局流量管理 IGTM 控制台，进入**我的实例**页面。
2. 在**我的实例**页面，单击需要配置容灾策略的**域名**，进入实例详情页面。如下图所示

3. 在实例详情页面中，选择**调度策略**页签，单击**新建调度策略**。

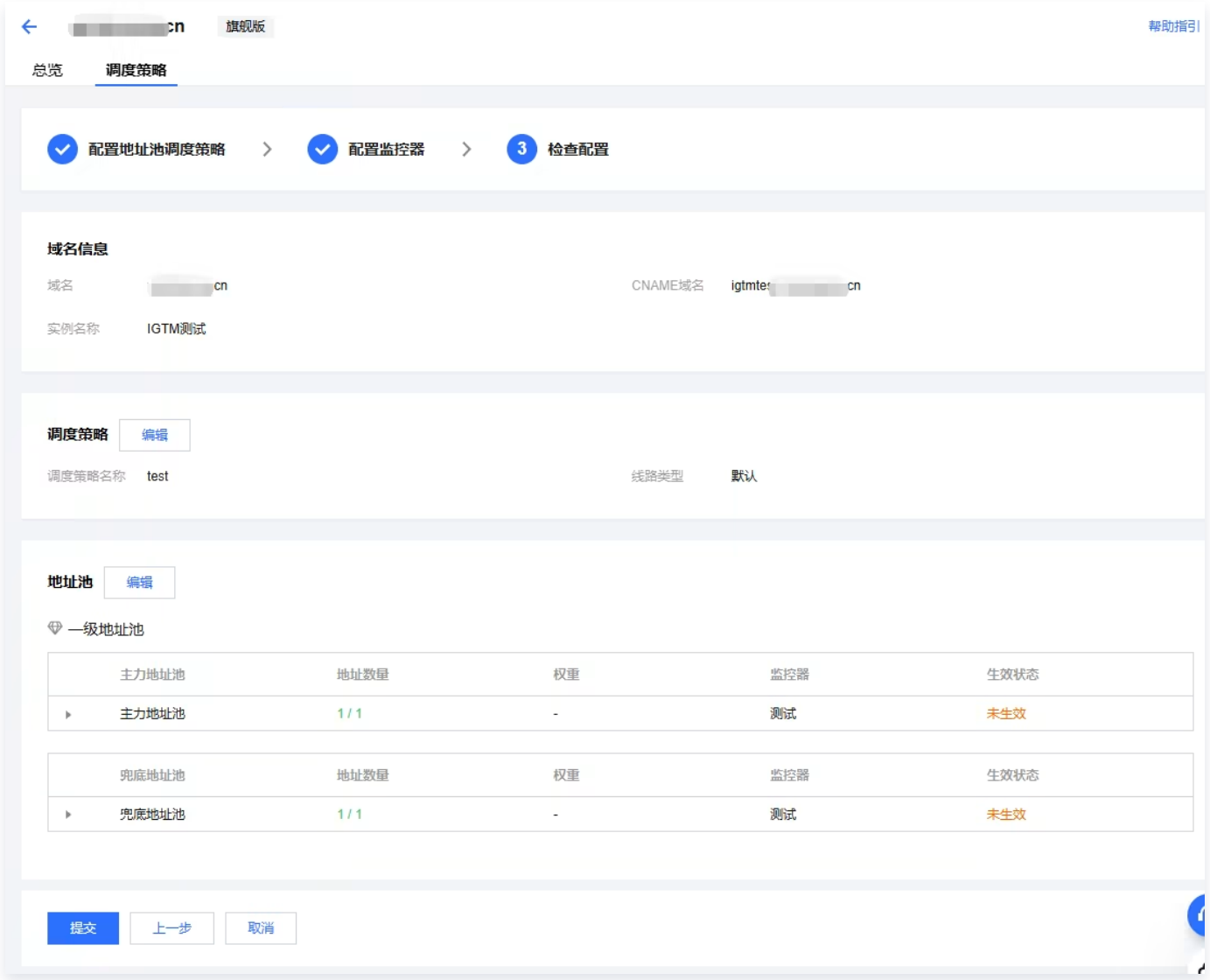
4. 配置地址池调度策略，单击**下一步**。



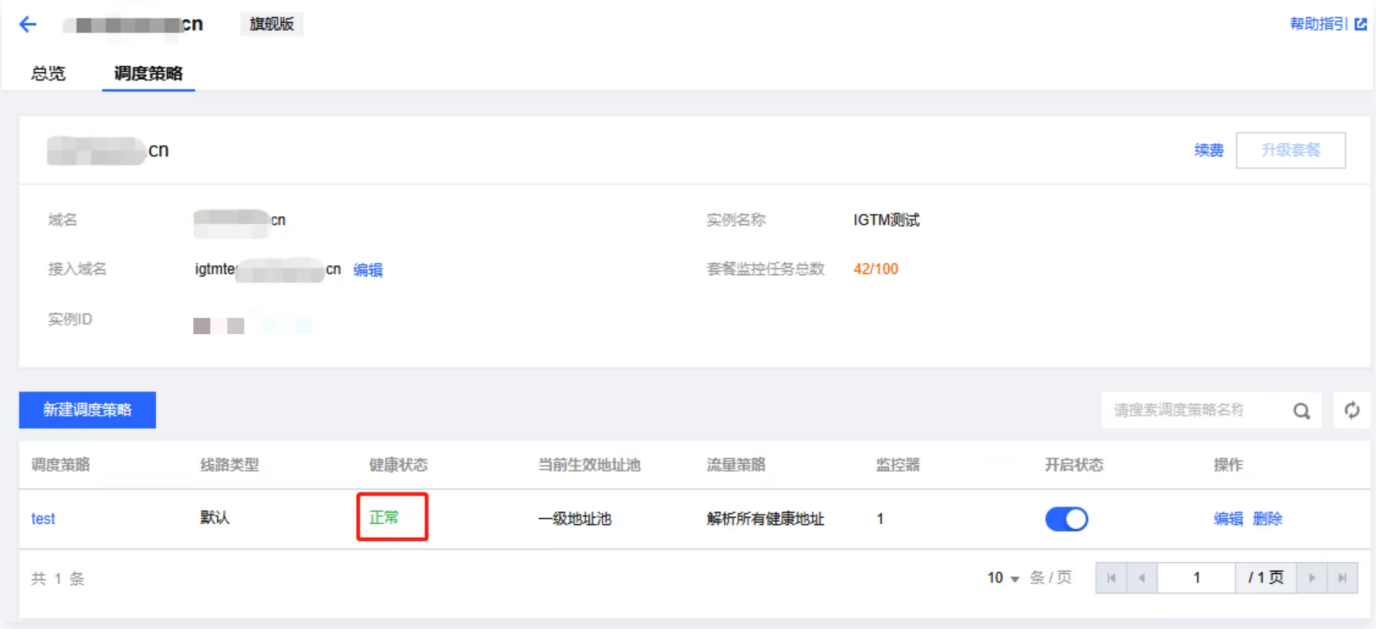
5. 配置监控器，单击**下一步**。


cn
旗舰版
帮助指引
总览
调度策略
配置地址池调度策略
2 配置监控器
3 检查配置
主力地址池集合-监控器
一级地址池
主力地址池
地址数量
健康状态
监控器
主力地址池
1 / 1
正常
测试
下一步
上一步
取消

6. 检查配置，并单击**提交**。


cn
旗舰版
帮助指引
总览
调度策略
配置地址池调度策略
配置监控器
3 检查配置
域名信息
域名
cn
CNAME域名
cn
实例名称
IGTM测试
调度策略
编辑
调度策略名称
test
线路类型
默认
地址池
编辑
一级地址池
主力地址池
地址数量
权重
监控器
生效状态
主力地址池
1 / 1
-
测试
未生效
兜底地址池
地址数量
权重
监控器
生效状态
兜底地址池
1 / 1
-
测试
未生效
提交
上一步
取消

7. 策略配置完成后，在调度策略页面中，可以查看容灾切换策略状态。



技术支持

操作过程中如果出现问题，请您联系 技术支持 协助您解决。