

云解析服务

最佳实践

文档版本 01
发布日期 2025-01-06



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

目录

| | |
|--|----|
| 1 DNS 最佳实践汇总..... | 1 |
| 2 将第三方域名解析转入华为云 DNS..... | 5 |
| 3 通过云解析服务实现运营商线路解析和地域解析..... | 11 |
| 4 账号间转移域名解析..... | 15 |
| 5 将第三方域名转入华为云管理..... | 19 |
| 6 域名转入华为云如何避免影响 DNS 解析..... | 26 |
| 7 为 ECS 配置内网域名实现云服务器平滑切换..... | 28 |
| 8 通过 Nginx 配置 URL 转发..... | 36 |
| 9 设置 CAA 记录防止错误颁发 HTTPS 证书..... | 41 |
| 10 通过 Serving Stale 提高自建 DNS 的解析成功率..... | 52 |

1 DNS 最佳实践汇总

本文汇总了云解析服务（DNS）的常见应用场景，并为每个场景提供详细的方案描述和操作指南，您可以通过云解析服务和华为云上的其他服务，根据业务场景灵活构建DNS解析方案。

表 1-1 场景说明

| 场景 | 示例 | 云服务 | 说明 |
|------|---------------------------------------|--|--|
| 解析迁移 | 将第三方域名解析转入华为云DNS | 云解析服务 DNS | 用户域名解析当前已使用非华为云DNS服务商，为了改进解析速度、寻找更可靠的DNS服务或是业务集中管理便于更好控制DNS设置，可以将域名解析迁移至华为云DNS。 |
| | 账号间转移域名解析 | <ul style="list-style-type: none">云解析服务 DNS域名注册服务 Domains | 用户基于业务需求要更换DNS解析所在账号，可以将域名与DNS解析从当前华为云账号转移至其他华为云账号，或者单独转移DNS解析。 |
| | 域名转入华为云如何避免影响DNS解析 | <ul style="list-style-type: none">云解析服务 DNS域名注册服务 Domains | 部分域名服务商不提供单独的DNS服务，例如GoDaddy，在域名转出后会删除原有的域名解析数据。为避免影响DNS解析，可以先将域名解析转入华为云等待生效后再转入域名。 |
| 智能解析 | 通过云解析服务实现运营商线路解析和地域解析 | 云解析服务 DNS | 企业云上应用服务通常会使用多个运营商IP地址，传统DNS解析会随机选择一个IP地址返回给访问者，从而导致访问者因运营商或跨地域导致访问速度缓慢或访问质量差的情况。通过DNS智能解析的配置来实现用户的就近访问。 |

| 场景 | 示例 | 云服务 | 说明 |
|----|---|--|--|
| | 配置运营商线路解析 | 云解析服务 DNS | 运营商线路解析是云解析服务提供的按运营商维度来区分访问者来源的线路类型，DNS根据访问者的DNS服务器所在的运营商，对同一域名配置不同的解析记录，指向不同网络服务器的IP地址。 |
| | 配置地域解析 | 云解析服务 DNS | 地域线路解析是云解析服务提供的按地域维度来区分访问者来源的线路类型，DNS根据访问者的DNS服务器所在地域，对同一域名配置不同的解析记录，指向不同网络服务器的IP地址。 |
| | 配置自定义线路解析 | 云解析服务 DNS | 自定义线路解析，支持DNS根据访问者的IP地址返回特定的IP地址。 |
| | 配置权重解析 | 云解析服务 DNS | 当企业网站部署了多台服务器，每台服务器拥有独立的IP地址。通过配置域名的权重解析可以实现将不同用户的访问请求按比例分配到各个服务器上。 |
| | 通过全球加速实现海外用户加速访问国内网站 | <ul style="list-style-type: none">云解析服务 DNS全球加速 GA | 企业网站服务器部署在国内，由于跨国网络不稳定，跨境丢包等因素，海外用户在访问网站时经常出现丢包、时延大、网络抖动等问题，通过全球加速服务优化海外用户访问，实现访问加速。 |
| | 通过全球加速和CDN实现跨境访问加速 | <ul style="list-style-type: none">云解析服务 DNS全球加速 GA内容分发网络 CDN | 海外用户通过GA实现跨境加速访问大陆网站，网站的大量静态资源希望能够使用CDN缓存节省成本，可以通过CDN+GA的方案实现静态资源CDN缓存加速，动态请求GA回源加速。 |
| | 通过全球加速优化全球用户访问云下IDC应用（非华为云部署） | <ul style="list-style-type: none">云解析服务 DNS全球加速 GA | 企业网站服务器部署在中国大陆的非华为云数据中心的自建数据中心中，国内用户直接访问网站服务器的公网IP，但是由于跨国公网不稳定、大陆跨境经常丢包等因素，通过华为云全球加速优化海外用户访问，实现访问加速。 |

| 场景 | 示例 | 云服务 | 说明 |
|-------|-----------------------------|---|--|
| | 通过全球加速部署云上云下多活容灾 | <ul style="list-style-type: none">云解析服务 DNS全球加速 GA | 企业网站服务器部署在中国大陆的云下用户数据中心或自建机房中，基于可靠性考虑，希望在华为云部署实现多活容灾（或者华为云多个Region部署容灾），通过全球加速服务实现访问加速的同时实现高可靠多活容灾。 |
| 域名迁移 | 将第三方域名转入华为云管理 | <ul style="list-style-type: none">云解析服务 DNS域名注册服务 Domains | 华为云的域名注册服务与新网和西数合作，通过华为云注册的域名其注册商为新网或西数，由华为云提供域名管理服务。因此在从其他服务商处将域名转入华为云时，新注册商为“北京新网数码信息技术有限公司”或“成都西维数码科技有限公司”。 指将域名的管理权转入华为云，该操作是针对域名的管理权，不改变域名的“DNS服务器”设置以及域名的解析记录。 |
| 内网解析 | 为ECS配置内网域名实现云服务器平滑切换 | <ul style="list-style-type: none">云解析服务 DNS弹性云服务器 ECS云数据库 RDS | 网站运行时服务器故障，需要将业务切换到备份的云服务器时，如果云服务器没有配置内网域名，则需要通过修改主业务节点ECS的代码来重新设置云服务器的内网IP地址，该操作需要中断业务并重新发布网站，耗时耗力。 内网域名功能支持为VPC内每个云服务器创建一个内网域名，在部署该网站时，我们为云服务器申请了内网域名，且代码中设置的是云服务器的内网域名，仅需要通过修改内网域名解析记录即可实现云服务器的切换，无需中断业务，也不需要重新发布网站。 |
| URL转发 | 通过Nginx配置URL转发 | <ul style="list-style-type: none">云解析服务 DNS弹性云服务器 ECS | 用户服务器上部署了多个网站放置在不同目录下，或者购买了多个服务器部署了不同的网站，访问这些网站时可以配置域名转发到不同目录URL，即配置URL转发。 例如用户部署了博客、新闻、活动、应用商店等多个网站，可以为每个网站配置独立的域名转发到不同的URL进行访问。 |

| 场景 | 示例 | 云服务 | 说明 |
|------------|--|--|--|
| 配置CAA记录 | 设置CAA记录防止错误颁发HTTPS证书 | <ul style="list-style-type: none">云解析服务 DNS域名注册服务 Domains | <p>CAA (Certification Authority Authorization, 证书颁发机构授权) 是一项防止HTTPS证书错误颁发的安全措施, 遵从IETF RFC6844。</p> <p>假如浏览器将某个CA机构列入黑名单, 并宣称不再信任其颁发的HTTPS证书, 当您访问到部署了这些HTTPS证书的网站时, 会被提示HTTPS证书不受信任。</p> <p>公有云的云解析服务支持为公网域名设置CAA记录, 您可以通过在管理控制台为域名添加CAA解析记录。</p> |
| 提高DNS解析成功率 | 通过Serving Stale提高自建DNS的解析成功率 | 云解析服务 DNS | <p>Serving Stale是RFC 8767描述的用于提高DNS解析可靠性的一个标准。</p> <p>当Local DNS上的域名缓存过期, 由于权威DNS故障导致Local DNS无法刷新本地缓存时, 可以通过Local DNS的Serving Stale的能力使用过期的缓存结果应答请求, 避免客户端无法得到响应。</p> |

2 将第三方域名解析转入华为云 DNS

应用场景

用户域名解析当前已使用非华为云DNS服务商，为了改进解析速度、寻找更可靠的DNS服务或是业务集中管理便于更好控制DNS设置，可以将域名解析迁移至华为云DNS。

本文主要介绍如何将第三方域名解析平滑迁移至华为云DNS解析，避免您的业务因解析中断而受影响。

操作流程

将第三方域名解析转入华为云DNS的流程如图2-1所示。

图 2-1 第三方域名解析转入华为云 DNS 流程图



方案优势

- 华为云云解析服务提供多种解析类型，解析安全可靠，依托覆盖国内主流运营商以及海外六大洲线路的云解析服务，支持免费使用500个解析记录，为您的站点提供稳定、安全、快速的解析体验。
- 华为云基于域名注册服务、企业门户、云解析服务、ICP备案、SSL证书、华为云企业邮箱等华为云基础服务，为您提供适用于各行各业的产品与能力组合。

资源和成本规划

表 2-1 资源和成本规划

| 资源 | 资源名称 | 资源说明 | 数量 | 每月费用 (元) |
|-------|----------------|---|----------------------|----------|
| 公网域名 | 域名的名称 | 将域名解析转入华为云DNS服务，需要在DNS控制台创建公网域名后，再将解析记录集导入对应的域名下。 | 用户自定义迁移的域名数量 | 免费 |
| 解析记录集 | 根据具体的解析定义记录集名称 | 云解析服务的解析由不同类型的记录集实现，用于定义该域名支持的解析类型以及解析值。 导出后的解析记录需要按要求填写到华为云DNS解析记录的导入模板中。 | 用户自定义迁移的域名涉及的解析记录集数量 | 免费 |

步骤一：在原 DNS 服务商处导出域名解析记录

在域名原DNS服务商处导出DNS解析记录，建议您导出xlsx的文件格式。

详细内容请参见原DNS服务商的相关操作指导。

步骤二：在华为云 DNS 控制台添加域名

1. 进入[公网域名列表页面](#)。
2. 在页面右上角，单击“创建公网域名”。
3. 根据界面提示，填写需要迁移DNS解析的公网域名信息。

图 2-2 创建公网域名

创建公网域名

域名

例如: example.com

企业项目 ?

-请选择- 新建企业项目

高级配置(可选)

标签

如果您需要使用同一标签标识多种云资源, 即所有服务均可在标签输入框下拉选择同一标签, 建议在TMS中 [创建预定义标签](#)

+ 添加新标签

您还可以添加20个标签。

描述

0/255

取消 确定

4. 单击“确定”，完成公网域名的创建。
创建完成后，您可以在“公网域名”页面查看新创建的域名信息。

说明

单击操作列的“管理记录集”，可以看到系统已经为您创建了SOA类型和NS类型的记录集。其中，

- SOA类型的记录集标识了对此域名具有最终解释权的主权威服务器。
- NS类型的记录集标识了此域名的权威服务器。

您可以根据域名所在区域修改NS记录集的值，详细内容请参考[华为云DNS对用户提供服务服务的DNS是什么？](#)。

步骤三：在华为云 DNS 控制台导入域名解析记录

华为云云解析服务在导入DNS解析记录时，系统会按照预定模板扫描您的文件，请将原DNS服务商处导出的DNS解析记录按照华为云的导入模板重新填写后再导入。

1. 在域名列表中，单击创建的域名名称。
2. 单击“批量导入/导出”，进入批量导入/导出详情页面。

在进行批量导入前，首先需要完成导入模板的填写。

- a. 在批量导入/导出详情页面，单击“下载模板”，获取导入模板。
 - b. 按模板要求填写**步骤一：在原DNS服务商处导出域名解析记录**中获取的域名解析记录。
3. 单击页面右上角的“批量导入”，选择填写完成的导入模板，开始执行批量导入。
- 导入完成后，可以通过查看“导入成功记录”和“导入失败记录”检查解析记录导入是否成功。
- 导入成功记录：显示导入成功的记录数。
 - 导入失败记录：逐条显示导入失败的记录，您可以根据“失败原因”对导入失败的记录进行处理。

步骤四：在域名服务商处修改 DNS 服务器地址

前往域名服务商处修改域名DNS服务器地址，详细内容请参见[修改公网域名的DNS服务器地址](#)。

注意

- 一般情况下，DNS服务器地址修改后会快速同步到顶级域服务器并在互联网中生效。由于DNS服务商的NS记录的TTL值通常设置为48小时，可能存在某些地区Local DNS缓存了域名的NS记录，从而导致最长需要48小时才能刷新成新的NS记录，**为避免解析异常，在修改DNS服务器48小时内请避免变更解析记录。**
- DNS服务器地址修改后，域名解析仍有可能向原DNS服务商发起DNS查询，**在等待修改生效的期间内，请勿删除域名在原DNS服务商处的解析记录。**

步骤五：验证域名解析是否生效

- **使用ping验证解析**
 - a. 在本地主机打开cmd命令窗口。
 - b. 然后输入以下命令检查解析是否生效。

ping 域名

示例：检查域名example.com的解析是否生效，执行命令**ping example.com**

回显信息如**图2-3**所示，显示的IP地址与设置域名解析的IP地址保持一致，则说明解析已经生效。

图 2-3 使用 ping 检查解析是否生效

```
C:\Users\Administrator>ping example.com

正在 Ping example.com [93.184.216.34] 具有 32 字节的数据:
来自 93. 的回复: 字节=32 时间=265ms TTL=49

93. 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 265ms, 最长 = 265ms, 平均 = 265ms
```

- 使用 nslookup 验证解析

- a. 在本地主机单击“搜索”，输入cmd，打开命令窗口。
- b. 然后输入以下命令检查解析是否生效。

```
nslookup -qt=a 域名
```

或

```
nslookup 域名
```

示例：`nslookup example.com`

回显信息如图2-4所示，显示的IP地址与设置域名解析的IP地址保持一致，则说明解析已经生效。

图 2-4 使用 nslookup 检查 A 类型解析是否生效

```
C:\Users\Administrator>nslookup example.com
服务器: UnKnown
Address: 100.125.1.250

非权威应答:
名称:    example.com
Address: 2606:2800:220:1:248:1
          93.1
```

常见问题

- 添加解析记录后多久生效？

- 通常新添加的解析，添加成功后解析记录立即生效。
- 如果是修改已经添加的解析记录，解析生效时间不会迟于修改前的解析记录的TTL值。例如修改前TTL值为300s，则在300s内新的解析就会生效。如果本地DNS不存在缓存延时，则修改立即生效。
如果存在运营商强制延长域名记录缓存时间，则生效时间会略微延迟。

- 修改DNS服务器后多久生效？

修改DNS服务器可以很快同步到顶级域服务器并在网络中生效。但是，域名服务商处NS记录的TTL值通常设置为48小时，这样假如某些地区Local DNS缓存了域名的NS记录，则最长需要48小时才能刷新成新的NS记录，变更为修改后的DNS服务器。

因此，修改域名DNS服务器的生效时间请以域名服务商处的说明为准。在等待修改生效期间，请勿删除域名在原域名服务商处的解析记录，这样即使域名的新DNS没有生效，仍然可以通过访问原DNS进行解析，使域名的解析不中断。

相关阅读

- [域名过户](#)
- [域名转入华为云](#)
- [域名转出华为云](#)
- [域名账号间转移](#)
- [账号间迁移域名解析记录集](#)

3 通过云解析服务实现运营商线路解析和地域解析

应用场景

普通的域名解析只为用户返回解析结果，不会考虑访问者IP的来源和类型，这样，所有的访问者都被解析到同样的IP地址上，容易出现由跨运营商或者跨地域访问引起网络体验欠佳的问题。

云解析服务的智能线路解析功能支持按运营商、地域等维度区分访问者IP的来源和类型，对同一域名的访问请求做出不同的解析响应，指向不同服务器的IP地址。当联通用户访问时，域名解析服务器返回联通服务器的IP地址；当电信用户访问时，返回电信服务器的IP地址，解决了跨网访问慢的难题，从而实现高效解析。

除了按运营商线路及地域解析之外，云解析服务还支持按IP网段划分访问者的自定义线路解析，您可以更细粒度的设置解析线路，将访问者路由至不同的网站服务器。

对于部署了多台服务器的网站，如果想要实现解析的负载均衡，可以选择云解析服务的权重解析来实现。

本文指导用户通过华为云DNS服务智能解析配置以下业务场景：

- **中国大陆跨运营商访问：**在中国大陆地区实现跨运营商进行访问，智能DNS解析可以配置多个运营商IP地址，智能判断用户访问来源，并返回最合适的IP地址，实现用户的就近访问。
- **全球业务范围的智能访问：**对于需要在全全球范围内进行访问的企业，智能DNS解析可以判断用户处于中国大陆或全球范围，并能够根据具体的国家或地区返回相应的IP地址，以快速响应用户的访问。

方案架构

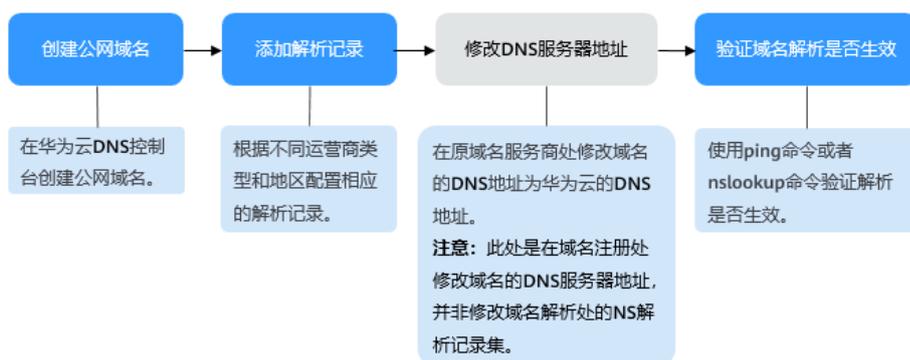
- **中国大陆用户根据运营商类型配置不同的IP访问地址**
 - 联通：1.1.xx.xx
 - 移动：2.2.xx.xx
 - 电信：3.3.xx.xx
 - 其他运营商（教育网、铁通、鹏博士等）：4.4.xx.xx
- **全球范围（不含中国大陆）用户根据所属地区配置不同的IP访问地址**
 - 亚太地区-中国香港：5.5.xx.xx

- 亚太地区-中国澳门：6.6.xx.xx
- 亚太地区-中国台湾：7.7.xx.xx
- 欧洲、北美洲、南美洲、非洲、大洋洲、南极洲、境外：8.8.xx.xx

操作流程

通过智能解析为不同运营商线路类型、不同地区用户配置域名解析的操作流程如图3-1所示。

图 3-1 运营商线路解析和地域解析配置流程



步骤一：创建公网域名

以huawei-example.com为例，详细操作流程请参见[创建公网域名](#)。

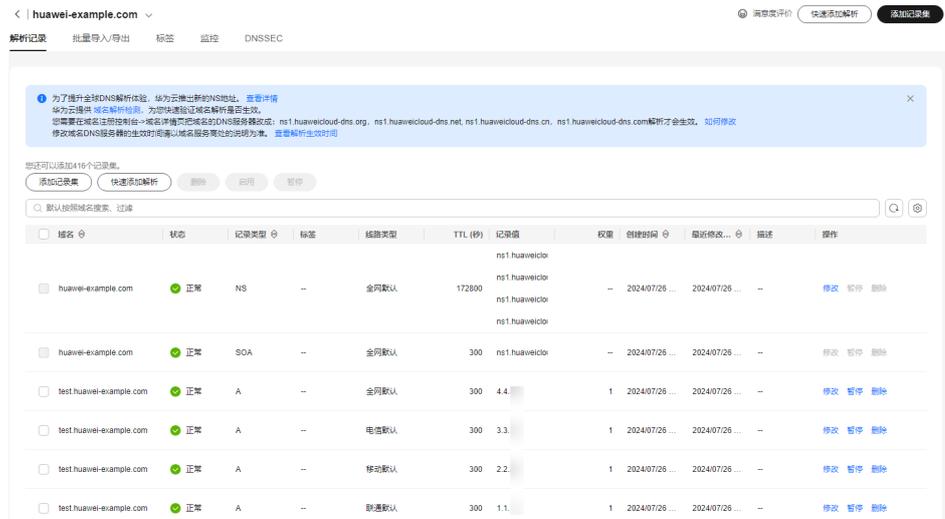
步骤二：添加解析记录

1. 在已添加公网域名的所在行，单击“管理解析”。进入域名的解析记录列表页。
2. 在域名解析记录列表页，单击“添加记录集”，配置子域名test.huawei-example.com的解析记录。
 - 中国大陆跨运营商访问，按照表3-1配置，云解析服务将访问者的运营商类型返回对应的解析记录IP地址。配置结果如图 [运营商解析记录](#)所示。

表 3-1 配置运营商解析

| 线路类型 | 运营商（访问者本地DNS出口IP来源） | 解析记录值 |
|---------|---------------------|-----------|
| 运营商线路解析 | 联通 | 1.1.xx.xx |
| | 移动 | 2.2.xx.xx |
| | 电信 | 3.3.xx.xx |
| 默认 | 其他（例如教育网、铁通、鹏博士等） | 4.4.xx.xx |

图 3-2 运营商解析记录

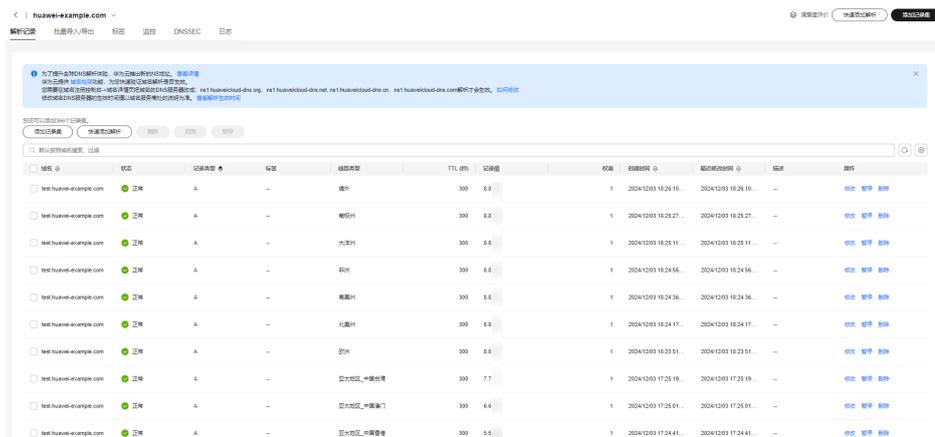


- 全球（不含中国大陆）业务范围的智能访问，按照表3-2配置，云解析服务将访问者所在地区返回对应的解析记录IP地址。
配置结果如图 地域解析记录所示。

表 3-2 配置地域解析

| 线路类型 | 地区（访问者本地DNS出口IP来源） | 解析记录值 |
|-------------|--------------------|-----------|
| 地域解析-亚太地区 | 中国香港 | 5.5.xx.xx |
| | 中国澳门 | 6.6.xx.xx |
| | 中国台湾 | 7.7.xx.xx |
| 地域解析-欧洲-默认 | 其他地区 | 8.8.xx.xx |
| 地域解析-北美洲-默认 | | |
| 地域解析-南美洲-默认 | | |
| 地域解析-非洲-默认 | | |
| 地域解析-大洋洲-默认 | | |
| 地域解析-南极洲-默认 | | |
| 地域解析-境外-默认 | | |

图 3-3 地域解析记录



| 域名 | 记录类型 | 记录值 | 记录类型 | TTL (秒) | 记录值 | 权重 | 生效时间 | 过期时间 | 备注 |
|-------------------------|------|-----|-----------|---------|-----|----|------------------------|------------------------|----|
| test.huawei-example.com | A | — | 默认 | 300 | 0.0 | 1 | 2024/12/03 18:26:10... | 2024/12/03 18:26:10... | — |
| test.huawei-example.com | A | — | 默认 | 300 | 0.0 | 1 | 2024/12/03 18:26:27... | 2024/12/03 18:26:27... | — |
| test.huawei-example.com | A | — | 北京 | 300 | 0.0 | 1 | 2024/12/03 18:26:41... | 2024/12/03 18:26:41... | — |
| test.huawei-example.com | A | — | 广州 | 300 | 0.0 | 1 | 2024/12/03 18:24:56... | 2024/12/03 18:24:56... | — |
| test.huawei-example.com | A | — | 南京 | 300 | 0.0 | 1 | 2024/12/03 18:24:36... | 2024/12/03 18:24:36... | — |
| test.huawei-example.com | A | — | 成都 | 300 | 0.0 | 1 | 2024/12/03 18:24:17... | 2024/12/03 18:24:17... | — |
| test.huawei-example.com | A | — | 深圳 | 300 | 0.0 | 1 | 2024/12/03 18:23:51... | 2024/12/03 18:23:51... | — |
| test.huawei-example.com | A | — | 亚太地区-中国香港 | 300 | 7.7 | 1 | 2024/12/03 17:25:19... | 2024/12/03 17:25:19... | — |
| test.huawei-example.com | A | — | 亚太地区-中国澳门 | 300 | 6.6 | 1 | 2024/12/03 17:25:01... | 2024/12/03 17:25:01... | — |
| test.huawei-example.com | A | — | 亚太地区-中国台湾 | 300 | 5.5 | 1 | 2024/12/03 17:24:41... | 2024/12/03 17:24:41... | — |

步骤三：修改 DNS 服务器地址

请确认您的域名已使用华为云DNS服务器地址解析，才能确保[步骤二：添加解析记录](#)配置的解析记录生效。

详细内容请参见[怎样查看并修改域名的DNS服务器地址？](#)

说明

更改后的DNS服务器地址将于48小时内生效，具体生效时间请以域名注册商处的说明为准。

步骤四：验证解析是否生效

方式一：通过[域名诊断](#)功能验证解析是否生效，详细内容请参见[诊断公网域名解析是否生效](#)。

方式二：通过nslookup命令验证解析是否生效，具体操作如下：

1. 在本地主机单击“搜索”，输入cmd，打开命令窗口。
2. 输入查询命令检查解析是否生效。
 - A类型解析：`nslookup -qt=a 域名`
 - 示例：`nslookup -qt=a test.huawei-example.com`

相关信息

- [解析不生效怎么办？](#)
- [网站无法访问排查思路](#)
- [为什么域名解析成功但网站仍然无法访问？](#)
- [为什么通过“https”方式无法访问网站？](#)

4 账号间转移域名解析

应用场景

用户因账号变更、资源集中管理或分离管理、企业业务重组或拆分、避免资源冲突等原因需要更换域名解析所属账号，需要将域名的DNS解析从当前华为云账号转移至其他华为云账号。

华为云域名注册和云解析服务支持用户跨账号转移域名解析，主要包括以下两种场景：

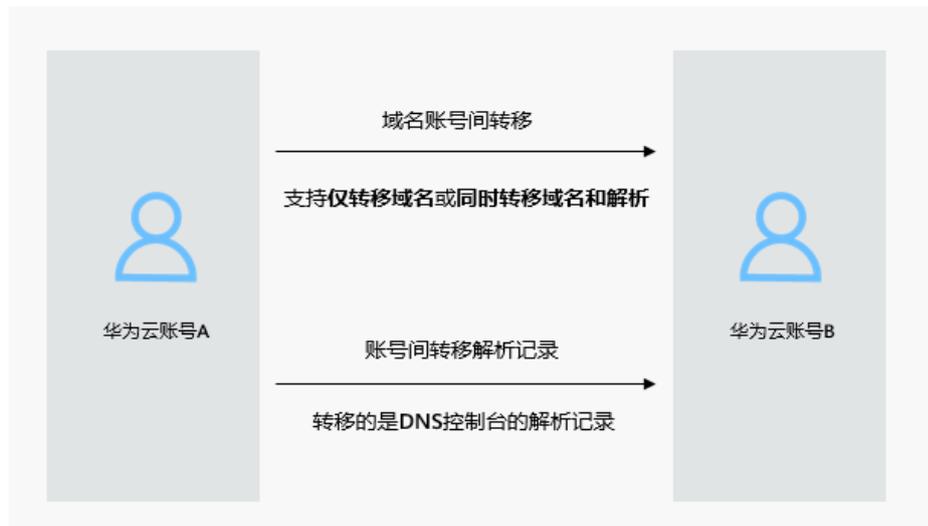
表 4-1 应用场景

| 用户场景 | 业务诉求 | 解决方案 |
|--------------------------------------|---------------|---|
| 域名和解析归属在同一账号。 例如：域名和解析同时归属在A账号下。 | 将解析从A账号转移至B账号 | 方案一：参考 域名账号间转移 ，选择“转移DNS”，将域名和DNS解析从账号A转移至账号B管理。 方案二：参考本实践的 操作步骤 ，将域名解析从账号A转移至账号B。 |
| 域名解析归属为不同账号。 例如：解析归属在A账号，域名归属在C账号 | | 参考本实践的 操作步骤 ，将域名解析从账号A转移至账号B。 |

方案架构

- **域名账号间转移**：在[域名注册控制台](#)对域名进行账号间转移，可同时转移域名和DNS解析，详细请参见[域名账号间转移](#)。
- **账号间转移解析记录**：登录原账号[DNS控制台](#)将域名解析记录转移至其他华为云账号，具体操作请参考本实践指导。

图 4-1 域名账号间迁移



约束限制

- 目标账号需要通过实名认证，并启用“华北-北京四”的项目。
- 仅支持转移本账号下的域名解析记录。
- 单次最多可转移1000个域名的解析记录。
- 批量转移域名仅适用于迁移公网域名解析，不支持迁移内网域名解析记录集。
- 域名转移前请先确保对方账户能正常登录云解析控制台页面进行域名操作。
- 批量转移域名任务为异步操作，转移期间请避免对转移中的域名进行操作，以免导致数据不同步。
- 不支持迁移使用自定义线路的域名解析记录集。
- 暂不支持中国站和国际站之间互转。

操作流程

本节主要介绍账号间转移解析记录的操作方法，具体流程如图4-2所示。

图 4-2 账号间转移域名解析流程图



操作步骤

1. 登录A账号的**DNS控制台**，进入公网域名列表页。
2. 在待转移DNS解析的域名所在行的“操作”列，选择“更多 > 转移域名”。
或者在列表上方的“批量操作”中，下拉选择“批量转移域名”。

3. 在批量转移域名界面，根据提示输入转移的域名信息。
 - a. 输入待转移的域名名称，一次最多转移1000个域名。
 - b. 输入转移后的华为云账号ID，即B账号的账号ID。
登录B账号管理控制台，鼠标移至页面右上角的用户名，在下拉菜单中单击“我的凭证”，即可查看账号ID。
4. 单击“提交”，提交域名转移申请。

📖 说明

操作完成后，您可以在“批量操作记录”页面查看操作名称、操作结果、操作时间和状态信息，还可以下载失败操作记录。

5. 登录B账号的[DNS控制台](#)，进入已转移DNS解析的域名解析记录列表页，查看转移结果。

相关阅读

表 4-2 域名与解析常见迁移操作

| 类型 | 说明 | 是否影响DNS解析 |
|--|---|--|
| 域名账号间转移 | <ul style="list-style-type: none"> • 仅转移域名：将域名的管理权从一个华为云账号转移至另一个华为云账号。 • 转移域名和DNS解析：将域名的管理权和DNS解析同时从一个华为云账号转移至另一个华为云账号。 | 否。 不改变域名的“DNS服务器”设置以及域名的解析记录，因此，不影响域名的正常解析。 |
| 账号间转移域名解析 | 将域名的解析记录从账号A转移到账号B | 否。 不改变域名的“DNS服务器”设置以及域名的解析记录，因此，不影响域名的正常解析。 |
| 域名过户 | 域名用户类型以及域名所有者的变更，即更换域名的实名认证模板。 | 否。 不改变域名的“DNS服务器”设置以及域名的解析记录，因此，不影响域名的正常解析。 |
| 域名转入华为云 域名转出华为云 | 域名转入和域名转出是指将域名的管理权转入或者转出华为云，该操作是针对域名的管理权。 | 否。 不改变域名的“DNS服务器”设置以及域名的解析记录，因此，不影响域名的正常解析。 |

| 类型 | 说明 | 是否影响DNS解析 |
|-----------|--|--|
| 域名转入华为云解析 | 域名转入华为云解析是指将域名的解析记录全部迁移到华为云，并修改域名的DNS服务器地址为华为云DNS。 | 是 如果本地DNS不存在缓存延时，则修改立即生效。 在解析迁移过程中，修改DNS服务器的生效时间通常受域名NS记录的TTL值以及Local DNS的缓存的影响，在迁移过程中有可能导致解析中断。 最长需要48小时才能更新，如果本地DNS不存在缓存延时，则修改立即生效。 |

5 将第三方域名转入华为云管理

应用场景

域名转入华为云，指将域名的管理权转入华为云，该操作是针对域名的管理权，不改变域名的“DNS服务器”设置以及域名的解析记录。

华为云的域名注册服务与新网和西数合作，通过华为云注册的域名其注册商为新网或西数，由华为云提供域名管理服务。因此在从其他服务商处将域名转入华为云时，新注册商为“北京新网数码信息技术有限公司”或“成都西维数码科技有限公司”。

本章节主要介绍如何将域名转入华为云管理。

📖 说明

- 某些域名服务商不提供单独的DNS服务，例如GoDaddy，在域名转出后会删除原有的域名解析数据。因此，从GoDaddy转入华为云的域名，其解析会失效。
- 在域名转移期间，不支持修改域名的“DNS服务器”设置，即不支持进行解析的迁移。
- 域名转入过程通常需要5~7天，取决于域名原注册商的转出确认时间。若您想要快速完成域名转入，请联系域名原注册商尽快完成转出确认。
- 为了保证在域名转入时，域名的解析不受影响，建议在域名转入操作前先将域名的解析迁移至华为云，待解析迁移完成后再进行域名转入操作。解析迁移的详细指导，请参见[将第三方域名解析转入华为云DNS](#)。

流程指导

域名转入华为云管理的流程如下：

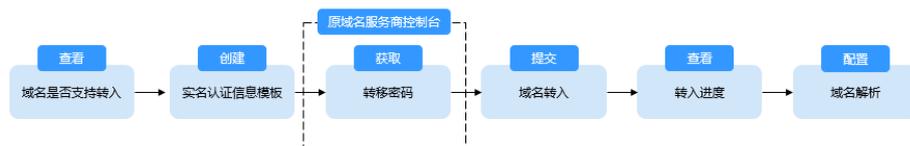
1. 在华为云控制台查看域名是否支持转入华为云。
2. 在原服务商处获取转移密码（auth-code）。
3. 在华为云控制台提交域名转入。
4. 查看转入进度。

系统自动校验转移密码，命名审核等，校验通过后注册局会向原服务商发送转出确认通知，原服务商确认后(不同服务商确认时间不同，可以催原服务商尽快确认转出)，域名开始转入。

5. （可选）如需使用华为云DNS解析您的域名，可参考[将第三方域名解析转入华为云DNS](#)将原服务商的解析记录转移至华为云。

视频指导：[域名转入华为云操作指导](#)

图 5-1 域名转入华为云流程图



方案优势

- 华为云域名注册服务提供域名的注册、购买、实名认证以及管理功能。
- 提供可靠稳定的域名解析服务，依托覆盖国内主流运营商以及海外六大洲线路的云解析服务，支持免费使用500个解析记录，为您的站点提供稳定、安全、快速的解析体验。
- 华为云基于域名注册、建站、云解析、备案、SSL证书等华为云基础服务，为您提供适用于各行各业的产品与能力组合。

资源和成本规划

表 5-1 资源和成本规划

| 资源 | 资源名称 | 资源说明 | 数量 | 每月费用（元） |
|----------|---------------|--|--------------|---------------------------|
| 实名认证信息模板 | 根据域名所有者定义模板名称 | 根据工信部域名实名认证的要求，在进行域名注册、域名过户（用户类型及域名所有者变更）、域名实名认证、域名转入等操作时，需要填写域名的用户信息。 建议您在进行上述操作前，首先创建域名的信息模板。 | 1 | 信息模板不计费 |
| 转入域名 | 域名的名称 | 域名转入是免费办理的。但因域名注册局的规定，转入时需在原期限上续费1年，因此，需支付域名续费1年的费用。 | 用户自定义迁移的域名数量 | 在华为云的价格详情中，点击域名类型查看相应的价格。 |

约束与限制

域名转入的约束限制较多，以下列举常见的域名转入华为云的约束限制，更多约束限制请参考[域名转入华为云](#)。

- 您必须是域名所有者，或者已经获得域名所有者的授权。
- 距域名注册成功超过60天。距域名最近一次转移成功超过60天。如果是国内域名（.中国和.cn），则距域名到期超过15天。
- 域名处于正常状态，本身无任何纠纷或欠费情况。
- 最多支持二级域名（example.com）的转入，不支持三级以上域名的转入（例如，abc.example.com）。

- 域名转入是免费办理的。但因域名注册局的规定，转入时需在原期限上续费1年，因此，需支付域名续费1年的费用。

步骤一：查看域名是否支持转入华为云

查看域名是否支持转入华为云。

1. 在华为云的[价格详情](#)中，点击域名类型。
2. 选择“转入”。
3. 选择“时长”。

查看域名后缀类型是否包含在转入价格列表中，如果包含则表示支持转入华为云，否则不支持转入华为云。

图 5-2 查看域名是否支持转入华为云

| 域名 | 简介 |
|-----------|-----------------|
| 英文.art | 艺术行业专属域名 |
| 英文.biz | 全球通用的商务域名 |
| 英文.black | 文化创意、广告设计行业推荐域名 |
| 英文.center | 各类商业和服务中心的专属域名 |

步骤二：创建实名认证的信息模板

您可以通过创建信息模板操作预先设置域名所有者的信息，并对信息模板进行实名认证。完成信息模板创建后，在域名转入时可以直接使用已经创建的信息模板设置域名信息。

信息模板的实名认证审核由注册局负责，一般1个工作日内即可完成审核（部分需要3~5个工作日）。

1. 登录[域名注册控制台](#)。
进入“域名列表”页面。
2. 在左侧树状导航栏中，选择“信息模板”。
3. 在页面右上角，单击“创建信息模板”。

图 5-3 创建信息模板



4. 设置“用户类型”
5. 根据实名认证证件内容填写“基本信息”区域。填写说明请参考[信息模板简介](#)。
6. 完成模板信息填写后单击“提交”，完成信息模板的配置。
7. 在左侧树状导航栏中，选择“信息模板”。

在信息模板列表中，可以查看已创建的信息模板。

此时，信息模板的“认证状态”为“实名认证审核中”。待信息模板的“认证状态”变为“已实名认证”，表示信息模板实名认证审核通过。

实名认证一般1个工作日内即可完成审核（部分需要3~5个工作日），请您耐心等待。

步骤三：获取转移密码

域名转入华为云前，必须在域名服务商处获取转移密码（auth-code）才能进行。

以下列服务商为例子，域名转入华为云需先获取原服务商的转移码（auth-code）。请在原服务商帮助中心搜索“域名转出”，查看获取转移码的方法。

说明

- 如果域名注册商是新网，则不支持将该域名转入华为云。
- 华为云的域名注册服务与新网合作，通过华为云注册的域名其注册商为新网，由华为云提供域名管理服务。因此在从其他服务商处将域名转入华为云时，新服务商为‘新网’。

步骤四：在华为云控制台提交域名转入

1. 登录[域名注册控制台](#)。
2. 在左侧树状导航栏，选择“域名转入”。
3. 在页面右上角，单击“域名转入”。
4. 在“域名转入”区域的文本框中，输入待转入域名以及转移密码。

填写格式：域名+空格+转移密码，例如：example.com password1。

每行填写一个域名，如需一次性转入多个域名，以换行符隔开。最多支持一次性转入5个域名。

图 5-4 输入域名和转移密码



说明

- 转移密码即**步骤1：获取转移密码**获取的转移密码。
 - 若用户已经提交了某一域名的转入申请，则不能重复提交该域名的转入申请，否则，系统会提示该域名已经存在。
5. 单击“立即转入”，系统进行转入域名的合法性校验。
 - 当转入域名因域名名称、域名状态等问题无法转入时，您需要根据提示的原因处理后，再次进行转入。
 - 当转入的域名全部合法，则直接进入下一步。
 6. 设置订单信息。

在“域名信息”栏，设置域名信息。

说明

- 域名转入仅支持选择已通过实名认证的信息模板，不限于用户类型，可以是个人用户或者企业用户。
7. 单击“立即购买”，进行订单确认。

若订单信息无误，阅读并勾选协议。
 8. 单击“去支付”。

选择支付方式后付款，提交域名转入。

步骤五：查看转入进度

系统自动校验转移密码，命名审核等，校验通过后注册局会向原服务商发送转出确认通知，原服务商确认后(不同服务商确认时间不同，可以催原服务商尽快确认转出)，域名开始转入。

在域名转入页面您可以查看转入进度。

1. 单击页面上方的“返回转入列表”，查看域名转入状态。
2. 单击域名“操作”列的“查看”，进入转入流程页面。

图 5-5 域名转入状态

| 域名 | 转入状态 | 提交时间 | 操作 |
|---------|------|-------------------------------|----|
| 163.com | 提交转入 | 2022/02/24 07:18:17 GMT+08:00 | 查看 |
| 1.com | 转入审核 | 2022/02/24 07:17:56 GMT+08:00 | 查看 |
| 163.com | 转入审核 | 2022/02/24 07:17:50 GMT+08:00 | 查看 |
| 164.com | 转入审核 | 2022/02/24 07:17:47 GMT+08:00 | 查看 |
| 20.com | 提交转入 | 2022/02/24 07:17:42 GMT+08:00 | 查看 |

在转入流程页面，可以对转入域名进行进一步操作，详细内容请参见[表5-2](#)。

表 5-2 域名转入后续操作

| 域名状态 | 说明 | 后续操作 |
|--------|--|--|
| 提交转入 | 域名转入提交完成，启动域名转入流程。 | 无需操作，等待系统转入处理。 若要取消转入，可以在转入流程页面通过单击“取消转入”实现。 |
| 审核中 | 域名转入进入审核阶段。 | 无需操作，等待系统转入处理。 若要取消转入，可以在转入流程页面通过单击“取消转入”实现。 域名转入过程通常需要5~7天。 |
| 转入成功 | 域名转入成功。 | 域名转入成功，需要对域名进行实名认证，详细操作请参见 实名认证域名 。 |
| 转入失败 | 域名转入失败。 | 根据界面提示的域名转入失败原因，进行处理： <ul style="list-style-type: none"> ● 用户取消转入 ● 域名转移密码错误 ● 注册局转移失败 ● 当前域名正在转入中 ● 域名服务商取消了该域名的转入操作 ● 通知邮件确认超时 |
| 转入密码错误 | 填写的转入密码不正确，无法转入域名。 | 需要重新核对转入密码后，再次执行转入操作。 |
| 转入撤销 | 执行“取消转入”操作后，域名转入进入“转入撤销”状态。 域名状态为“转入提交”和“审核中”的域名可以执行“取消转入”。 | 无需操作，域名转入流程结束。 |

（可选）步骤六：将域名的解析记录转入华为云 DNS

如果只转移域名到华为云域名注册管理，无需执行此步骤。

如需将域名的解析转入华为云，此步骤必选。具体操作请参考[将第三方域名解析转入华为云DNS](#)。

常见问题

- **先转入域名还是先转入解析？**

您可以选择先转入域名，也可以先转入解析，并无逻辑上先后顺序的要求。

- 先转入域名，再转入解析：

将域名转入Domains控制台进行域名管理。域名转入过程中，不影响在原服务商的解析，且转入域名的过程不可以修改域名的DNS。

域名转入成功后再导出解析记录集，将域名解析转入华为云DNS控制台。

- 先转入解析，再转入域名：

先转入解析是指先将域名的解析记录转入DNS控制台解析，并修改原服务商的DNS地址为华为云DNS地址。

然后再转入域名到Domains控制台进行域名管理，转入域名的过程中域名的DNS不变。

- **域名转入失败或者取消，是否会退回已支付费用？**

域名转入的订单支付完成后，如果域名转入失败，或者取消了域名转入操作，则会自动全额退费至原华为云账号，请及时查收。

[更多域名转入常见问题](#)

6 域名转入华为云如何避免影响 DNS 解析

应用场景

域名转入华为云，指将您的域名从当前域名服务商（非华为云）转移至华为云域名注册服务进行管理。

本文主要介绍在域名转入华为云管理的过程中，如何避免影响域名解析。

域名当前 DNS 服务商为华为云 DNS

如果转入域名当前DNS服务商为华为云DNS，不论域名转入的目标账号与域名DNS解析所属账号是否一致，域名转入华为云管理过程均不会影响DNS解析。

📖 说明

当域名转入目标账号与DNS解析所属账号不一致时，如果用户希望在同一账号下管理域名和DNS解析，可以通过以下方式实现：

- **域名账号间转移**：将域名转移至DNS解析所属账号。
- **账号间转移域名解析**：将DNS解析转移至域名所属账号。

域名当前 DNS 服务商非华为云 DNS

如果域名当前DNS服务商非华为云DNS，您需要向对应DNS服务商确认域名转出是否会影响当前解析。

某些域名服务商不提供单独的DNS服务，例如GoDaddy，在域名转出后会删除原有的域名解析数据，导致域名解析失效。同时，域名转移期间，不支持修改域名的“DNS服务器”设置，即不支持进行迁移域名解析。

为保证在域名转入时域名解析不受影响，建议您在操作域名转入前先将域名解析迁移至华为云，详细内容请参见[将第三方域名解析转入华为云DNS](#)。待解析迁移完成后再转入域名。

 **警告**

由于转移域名解析需要修改DNS服务器地址，**请向当前域名服务商确认修改DNS服务器是否会立即停止域名解析。**

如果修改DNS服务器地址会立即停止域名解析，则不建议转移域名注册商。即使提前转移DNS解析，在修改DNS服务器的48小时内域名解析仍有可能向原DNS服务商发起DNS查询，导致解析失败或不稳定，请谨慎操作。

7 为 ECS 配置内网域名实现云服务器平滑切换

方案概述

应用场景

网站在运行过程中，当某一台ECS故障，需要将业务切换到备份的云服务器时，如果云服务器没有配置内网域名，则需要通过修改主业务节点ECS的代码来重新设置云服务器的内网IP地址，该操作需要中断业务并重新发布网站，耗时耗力。

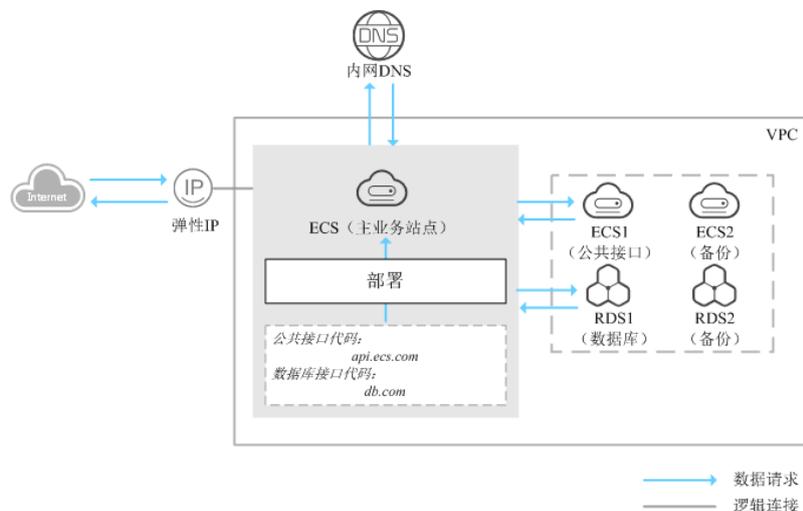
内网域名功能支持为VPC内每个云服务器创建一个内网域名，在部署该网站时，我们为云服务器申请了内网域名，且代码中设置的是云服务器的内网域名，仅需要通过修改内网域名解析记录即可实现云服务器的切换，无需中断业务，也不需要重新发布网站。

方案架构

图7-1展示了某网站的逻辑组网，在一个VPC内，部署了ECS和RDS。其中：

- ECS：作为主业务站点和业务入口。
- ECS1：作为公共接口。
- RDS1：作为数据库，存储业务数据。
- ECS2和RDS2：作为备份服务器和数据库。

图 7-1 逻辑组网图



方案优势

- 通过内网域名访问VPC内的云服务器，无需经过Internet，访问速度更快、安全性更高。
- 在代码中使用内网域名代替内网IP。当需要进行云服务器切换时，只需通过修改内网域名解析记录即可，无需修改代码。

资源成本和规划

本节介绍最佳实践中资源规划情况，包含以下内容：

表 7-1 内网域名资源规划

| 资源 | 内网域名 | 关联VPC | 内网IP | 记录集类型 | 说明 |
|------|-------------|---------|-------------|-------|---------------|
| ECS1 | api.ecs.com | VPC_001 | 192.168.2.8 | A | 公共接口ECS。 |
| ECS2 | api.ecs.com | VPC_001 | 192.168.3.8 | A | 备份公共接口ECS。 |
| RDS1 | db.com | VPC_001 | 192.168.2.5 | A | 数据库，用于存储业务数据。 |
| RDS2 | db.com | VPC_001 | 192.168.3.5 | A | 备份数据库。 |

表 7-2 资源和成本规划

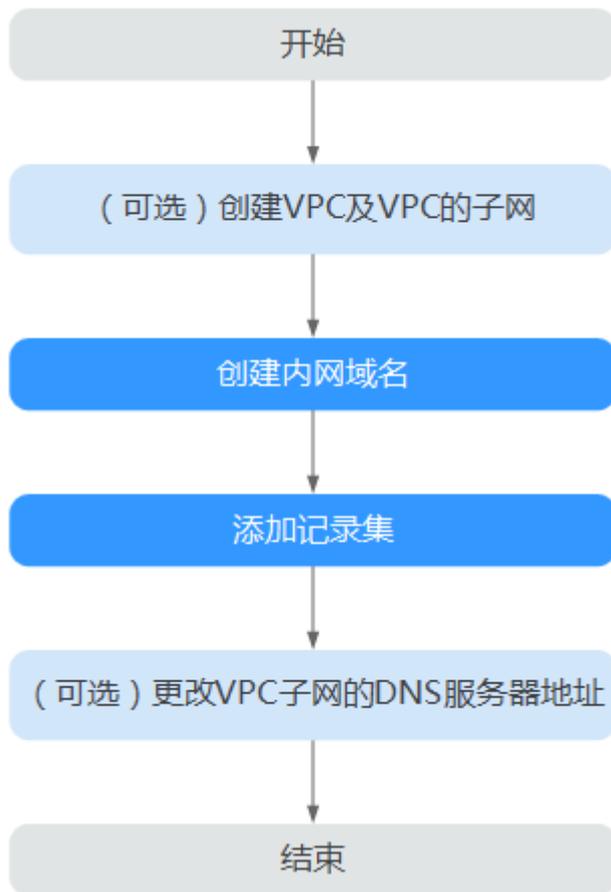
| 区域 | 资源 | 资源名称 | 资源说明 | 数量 | 每月费用(元) |
|--------|-----------|---------------------|--|----|--------------------------------------|
| 华北-北京四 | 虚拟私有云VPC | VPC_001 | 设置DNS服务器地址与华为云的内网DNS地址保持一致。 详细请参见 华为云提供的内网DNS地址是多少? | 1 | 免费 |
| | 弹性云服务器ECS | ECS ECS1 ECS2 | <ul style="list-style-type: none">• 内网域名: api.ecs.com• 关联VPC: VPC_001• ECS1: 公共接口ECS, 内网IP: 192.168.2.8• ECS2: 备份公共接口ECS, 内网IP: 192.168.3.8 | 3 | 详细请参见 弹性云服务器产品价格详情 。 |

| 区域 | 资源 | 资源名称 | 资源说明 | 数量 | 每月费用 (元) |
|----|----------|-----------------------|--|----|------------------------------------|
| | 云数据库 RDS | RDS1 RDS2 | <ul style="list-style-type: none"> 内网域名: db.com 关联VPC: VPC_001 RDS1: 数据库, 用于存储业务数据, 内网IP: 192.168.2.5 RDS2: 备份数据库, 内网IP: 192.168.3.5 | 2 | 详细请参见 云数据库产品价格详情 。 |
| | 云解析服务 | api.ces.com db.com | <ul style="list-style-type: none"> api.ces.com: 关联VPC: VPC_001 记录集类型: A, 值: 192.168.2.8 db.com 关联VPC: VPC_001 记录集类型: A, 值: 192.168.2.5 | 2 | 免费 |

为云服务器配置内网域名总流程

为云服务器配置内网域名的流程如[图7-2](#)所示。

图 7-2 内网域名配置流程



配置流程说明：

1. “（可选）创建VPC及VPC子网”：在管理控制台虚拟私有云服务页面完成配置，仅当您在网站部署阶段为云服务器配置内网域名时，执行本操作。
2. “创建内网域名”和“创建记录集”：在管理控制台云解析服务页面完成相关配置。
3. “（可选）更改VPC子网的DNS”：在管理控制台虚拟私有云服务页面完成配置，仅当您为已运行网站的云服务器配置内网域名时，执行本操作。

实施步骤

步骤1 （可选）创建VPC及VPC的子网

当您在网站部署阶段为云服务器配置内网域名时，需要首先完成VPC及其子网的创建。

1. 进入[创建虚拟私有云页面](#)。
2. 根据界面提示配置参数，关键参数的配置说明如[表7-3](#)所示。

表 7-3 虚拟私有云关键参数说明

| 参数 | 说明 | 取值样例 |
|----------|--|----------------------------------|
| 区域 | 不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。 | 华北-北京四 |
| 名称 | VPC名称。 | VPC_001 |
| 网段 | VPC的地址范围，VPC内的子网地址必须在VPC的地址范围内。 目前支持网段范围： - 10.0.0.0/8~24 - 172.16.0.0/12~24 - 192.168.0.0/16~24 | 192.168.0.0/16 |
| 子网名称 | 子网的名称。 | Subnet |
| 子网网段 | 子网的地址范围，需要在VPC的地址范围内。 | 192.168.0.0/24 |
| 网关 | 子网的网关。 | 192.168.0.1 |
| DNS服务器地址 | 若要为VPC内的云服务器配置内网域名，需要设置DNS服务器地址与华为云的内网DNS地址保持一致。 | 100.125.1.250 100.125.129.250 |

3. 单击“立即创建”，完成VPC以及VPC默认子网的设置。

步骤2 创建内网域名

为云服务器ECS1和数据库RDS1创建内网域名。

1. 进入[内网域名列表页面](#)。
2. 单击“创建内网域名”，开始创建内网域名。
3. 根据界面提示配置参数，参数说明如表7-4所示。

表 7-4 创建内网域名参数说明

| 参数 | 参数说明 | 取值样例 |
|-----|------------------------------|-------------|
| 域名 | 域名。可以自定义，支持创建顶级域，但需符合域名命名规范。 | api.ecs.com |
| VPC | 内网域名要关联的VPC。 | VPC_001 |

| 参数 | 参数说明 | 取值样例 |
|------|--|-------------------------|
| 企业项目 | <p>内网域名关联的企业项目，用于将内网域名按照企业项目进行管理。</p> <p>说明 仅当用户使用的“账号类型”为“企业账号”时，显示该参数，且参数必选。</p> <p>配置原则：</p> <ul style="list-style-type: none"> - 如果不通过企业项目管理域名资源，则采用默认值“default”。 - 如果通过企业项目管理域名资源，则在下拉列表中选择已经创建的企业项目。 <p>在设置该参数前，您需要完成创建企业项目。</p> <p>更多关于企业项目的信息，请参考《企业项目管理用户指南》。</p> | default |
| 标签 | <p>可选参数。由键和值组成，用于搜索域名或为域名资源分组。当系统中配置多个域名时，可以选择配置此参数。</p> <p>键和值的命名规则请参见表7-5。</p> | - |
| 描述 | <p>可选参数。域名的描述信息。长度不超过255个字符。</p> | This is a zone example. |

表 7-5 标签命名规则

| 参数 | 规则 | 举例 |
|----|---|----------------|
| 键 | <ul style="list-style-type: none"> - 不能为空。 - 对于同一资源键值唯一。 - 长度不超过36个字符。 - 取值为不包含“=”、“*”、“<”、“>”、“\”、“”、“ ”和“/”的所有Unicode字符，且首尾字符不能为空格。 | example_key1 |
| 值 | <ul style="list-style-type: none"> - 不能为空。 - 长度不超过43个字符。 - 取值为不包含“=”、“*”、“<”、“>”、“\”、“”、“ ”和“/”的所有Unicode字符，且首尾字符不能为空格。 | example_value1 |

- 单击“确定”，完成内网域名api.ecs.com的创建。
创建完成后，您可以在“内网域名”页面查看新创建的域名信息。

说明

单击操作列的“管理记录集”，可以看到系统已经为您创建了SOA类型和NS类型的记录集。其中，

- SOA类型的记录集标识了对此域名具有最终解释权的主权威服务器。
- NS类型的记录集标识了此域名的权威服务器。

5. 重复执行3~5，完成内网域名db.com的创建。

内网域名规划请参见表7-1。

步骤3 创建记录集

为云服务器ECS1和数据库RDS1的内网域名添加到对应内网IP的解析记录。

1. 在“内网域名”页面的域名列表中，单击新创建域名的名称。
系统进入域名解析记录页面。
2. 单击“添加记录集”。
3. 根据界面提示填写参数配置，参数说明如表7-6所示。

表 7-6 添加 A 类型记录集参数说明

| 参数 | 参数说明 | 取值样例 |
|--------|--|------------------|
| 主机记录 | 域名前缀。 此处参数设置为空，表示解析的域名是api.ecs.com。 | - |
| 类型 | 记录集的类型，此处为A类型。 | A - 将域名指向IPv4地址 |
| TTL(秒) | 解析记录在DNS服务器的缓存时间，以秒为单位。 如果您的服务地址经常更换，建议TTL值设置相对小些，反之，建议设置相对大些。 | 默认为“5min”，即300s。 |
| 值 | 域名对应的IPv4地址。多个IPv4地址以换行符分隔。 此处设置为云服务器的内网IP。 | 192.168.2.8 |
| 标签 | 可选参数，由键和值组成，用于搜索记录集或为记录集资源分组。当系统中配置多个记录集时，可以选择配置此参数。 键和值的命名规则请参见表7-5。 | - |
| 描述 | 可选配置，对域名的描述。 | - |

4. 单击“确定”，完成为内网域名api.ecs.com添加A类型记录集。
5. 重复执行1~4，为内网域名db.com添加A类型的记录集。
域名db.com对应记录集的“值”设置为“192.168.2.5”。
记录集的详细数据规划请参见表7-2。

步骤4 （可选）更改VPC子网的DNS

当您为已运行网站的云服务器配置内网域名时，需要更改VPC子网的DNS。

为实现内网域名在VPC内的正常解析，您需要把VPC子网的DNS改成云解析服务提供的内网DNS。

更改VPC子网的DNS的操作请参见[怎样切换内网DNS?](#)。

步骤5 切换ECS

当ECS1发生故障，需要将业务切换到备份的云服务器ECS2上。此时，可以通过修改内网域名api.ecs.com的解析记录实现业务切换。

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择“华北-北京四”。
3. 选择“网络 > 云解析服务”。
- 进入云解析服务页面。
4. 在左侧树状导航栏，选择“内网域名”。
5. 在“内网域名”页面域名列表中，单击域名名称“api.ecs.com”进入域名解析记录页面。
6. 在A类型记录集中，单击“操作”列的“修改”。
7. 将“值”修改为“192.168.3.8”。
8. 单击“确定”，完成解析记录的修改。

此时，ECS到公共接口ECS1的访问会通过内网DNS解析到ECS2上，实现了ECS的切换。

----结束

8 通过 Nginx 配置 URL 转发

操作场景

用户服务器上部署了多个网站放置在不同目录下，或者购买了多个服务器部署了不同的网站，访问这些网站时可以配置域名转发到不同目录URL，即配置URL转发。

例如用户部署了博客、新闻、活动、应用商店等多个网站，可以为每个网站配置独立的域名转发到不同的URL进行访问。

本节操作介绍通过Nginx实现URL转发的操作步骤。

背景知识

URL转发一般分为URL显性转发和URL隐性转发，本节介绍的Nginx实现URL转发即URL显性转发。

- URL显性转发（Explicit URL Forwarding）
 - 显性转发是通过HTTP重定向实现的，通常采用的是301重定向或302重定向技术。通过显性转发将原URL重定向到新URL，从而使访问原URL的所有请求转发到新的URL地址。详细内容请参见[表8-1](#)。

表 8-1 301 重定向和 302 重定向对比

| 重定向类型 | 301重定向（HTTP 301 Moved Permanently） | 302重定向（HTTP 302 Found） |
|-------|------------------------------------|------------------------|
| 持久性 | 永久性重定向，表示资源已被永久移动。 | 临时性重定向，表示资源的移动是暂时的。 |

| | | |
|---------------|--|---|
| 用途 | <ul style="list-style-type: none"> 网站迁移：当网站从一个域名或URL迁移到另一个域名或URL时。 域名变更：当企业更改其域名或子域名时。 网站结构调整：当网站进行重大结构调整，导致大量URL变化时。 | <ul style="list-style-type: none"> 临时网站迁移：当网站进行临时迁移或维护时。 A/B测试：在进行网站测试或比较不同页面效果时。 临时URL变更：在某些情况下，可能需要临时更改URL，但不希望永久更改。 |
| SEO影响 | 有助于传递原URL的SEO价值（如链接权重）到新的URL，维护网站的搜索引擎排名。 | 不会传递原URL的SEO价值到新的URL，搜索引擎可能会认为这是临时的，不会更新其索引。 |
| 浏览器和缓存 | 重定向结果会被浏览器缓存，用户在刷新时会直接访问新的URL。 | 重定向结果通常不会被浏览器缓存，或者缓存时间较短，用户在刷新时可能会重新进行重定向。 |

- 显性转发是指DNS服务器明确配置了转发规则，将来自特定IP地址或网络的查询请求转发给指定的另一台DNS服务器。这种方式下，DNS管理员可以精确控制哪些查询需要被转发，以及转发到哪个服务器。
- 显性转发可以用于优化DNS查询的性能，例如，将来自某个地理位置的查询转发到该地区的DNS服务器，或者将特定类型的查询转发给专门的服务器。
- URL隐性转发（Implicit URL Forwarding）
隐性URL转发使用的是iframe框架技术，是指DNS服务器在没有明确配置转发规则的情况下，自动将无法解析的查询请求转发给其他DNS服务器。这种方式通常发生在主DNS服务器无法回答某个查询时，它会将请求转发给上级DNS服务器，直到找到能够解析该查询的服务器。
隐性转发是DNS查询的默认行为，确保了即使在没有显性转发规则的情况下，DNS查询也能够被正确处理。

步骤 1：在云服务器上安装 Nginx

本节操作使用工具为Nginx，且确认http_rewrite_module是开启的，一般默认为开启状态。

以CentOS 7系列为例，安装Nginx操作步骤如下：

1. 安装依赖包。

```
yum install -y gcc-c++
yum install -y pcre pcre-devel
yum install -y zlib zlib-devel
yum install -y openssl openssl-devel
```
2. 下载并解压安装包。

```
wget http://nginx.org/download/nginx-1.20.1.tar.gz
tar -zxvf nginx-1.20.1.tar.gz
```

3. 安装Nginx。
更换命令中“/usr/local/nginx”为实际希望安装路径。

```
cd nginx-1.20.1
./configure --prefix=/usr/local/nginx
make && make install
```

4. 安装完后验证是否安装成功。

```
cd /usr/local/nginx/sbin
./nginx -t
```

出现如下内容为安装成功。

```
nginx: the configuration file /usr/local/nginx/conf/nginx.conf syntax is ok
nginx: configuration file /usr/local/nginx/conf/nginx.conf test is successful
```

步骤 2：在云服务器上配置 Nginx 实现 URL 转发

以下步骤以访问测试域名www.example.cn跳转到华为云官网https://www.huaweicloud.com/xxx为例。

1. 打开Nginx配置文件，修改server模块中的server_name和location参数配置。
执行以下命令编辑nginx.conf文件，请将命令中路径替换为安装nginx的实际路径。

```
vi /usr/local/nginx/conf/nginx.conf
```

server_name: 访问的域名

location: 跳转的url地址。其中301是永久跳转，302是临时跳转，本例中使用的是302。具体差异请参考[背景知识](#)，并根据实际需求修改。

[图8-1](#)中域名和URL仅为示例，请根据实际需求替换域名和URL地址。

图 8-1 修改 Nginx 配置前

```
http {
    include        mime.types;
    default_type  application/octet-stream;

    #log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
    #              '$status $body_bytes_sent "$http_referer" '
    #              '"$http_user_agent" "$http_x_forwarded_for"';

    #access_log  logs/access.log  main;

    sendfile      on;
    #tcp_nopush  on;

    #keepalive_timeout  0;
    keepalive_timeout  65;

    #gzip  on;

    server {
        listen      80;
        server_name localhost;

        #charset koi8-r;

        #access_log  logs/host.access.log  main;

        location / {
            root    html;
            index  index.html index.htm;
        }
    }
}
```

图 8-2 修改 Nginx 配置后

```
http {
    include     mime.types;
    default_type application/octet-stream;

    #log_format main '$remote_addr - $remote_user [$time_local] "$request" '
    #               '$status $body_bytes_sent "$http_referer" '
    #               '"$http_user_agent" "$http_x_forwarded_for"';

    #access_log  logs/access.log  main;

    sendfile    on;
    #tcp_nopush on;

    #keepalive_timeout 0;
    keepalive_timeout 65;

    #gzip on;

    server {
        listen      80;
        server_name www.example.cn;

        #charset koi8-r;

        #access_log  logs/host.access.log  main;

        location / {
            root    html;
            index  index.html index.htm;
            return 302 https://www.huaweicloud.com;
        }
    }
}
```

2. 执行以下命令，重新加载配置文件并重启Nginx服务。

```
/usr/local/nginx/sbin/nginx -s reload
```

```
/usr/local/nginx/sbin/nginx -s reopen
```

步骤 3：在控制台设置域名解析到云服务器 IP

1. 登录DNS管理控制台，在左侧导航栏点击“公网域名”。
2. 单击“创建公网域名”，将域名添加至DNS控制台。
3. 点击域名进入解析记录集页面。
4. 单击“添加解析记录集”。
 - 主机记录置空。
 - 记录集类型选择A类型记录集。
 - 记录集的值填写为云服务器的IP地址。

步骤 4：验证 URL 转发是否生效

执行以下命令验证URL转发是否生效：

```
curl -v http://www.example.cn
```

如图8-3所示。回显信息和预设的URL地址一致，说明设置的URL转发已生效。

图 8-3 添加域名的 A 类型记录集

```
[root@ecs ~]# curl -v http://www.example.cn
* About to connect() to www.caiqichen.cn port 80 (#0)
*   Trying 128.193.100.100 ..
* Connected to www.caiqichen.cn (128.193.100.100) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: www.example.cn
> Accept: */*
>
< HTTP/1.1 302 Moved Temporarily
< Server: nginx/1.20.2
< Date: Thu, 26 May 2022 10:32:02 GMT
< Content-Type: text/html
< Content-Length: 145
< Connection: keep-alive
< Location: https://www.huaweicloud.com
<
<html>
<head><title>302 Found</title></head>
<body>
<center><h1>302 Found</h1></center>
<hr><center>nginx/1.20.2</center>
</body>
</html>
```

9 设置 CAA 记录防止错误颁发 HTTPS 证书

方案概述

应用场景

CAA (Certification Authority Authorization, 证书颁发机构授权) 是一项防止HTTPS证书错误颁发的安全措施, 遵从IETF RFC6844。从2017年9月8日起, 要求CA (Certification Authority, 证书颁发) 机构执行CAA强制性检查。

全球约有上百个CA机构有权发放HTTPS证书, 证明您网站的身份。假如浏览器将某个CA机构列入黑名单, 并宣称不再信任其颁发的HTTPS证书, 当您访问到部署了这些HTTPS证书的网站时, 会被提示HTTPS证书不受信任, 如图9-1所示。

图 9-1 HTTPS 证书错误颁发



CAA标准要求CA机构在为域名签发证书时执行CAA强制性检查:

- 如果检查域名的DNS解析记录, 发现未设置CAA字段, 则为该域名颁发证书。这种情况下, 任何CA机构均可为该域名签发证书, 存在HTTPS证书错误颁发的风险。
- 如果检查域名的DNS解析记录, 在CAA字段发现获得授权, 则为该域名颁发证书。
- 如果检查域名的DNS解析记录, 在CAA字段发现未获得授权, 则拒绝为该域名颁发证书, 防止未授权HTTPS证书错误颁发。

公有云的云解析服务支持为公网域名设置CAA记录，您可以通过在管理控制台为域名添加CAA解析记录。

方案优势

为网站的域名添加CAA解析记录可以使网站将指定CA机构列入白名单，仅授权指定CA机构为网站的域名颁发证书，提高网络的安全性。

约束和限制

CAA记录集的格式为：[flag] [tag] [value]，由一个标志字节的[flag]和一个[tag]-[value]（标签-值）对组成。

配置原则：

- flag：认证机构限制标志，定义为0~255无符号整型。常用取值为0。
- tag：仅支持大小写字母和数字0~9，长度1~15，常用取值：
 - issue：授权任何类型的域名证书
 - issuewild：授权通配符域名证书
 - iodef：指定违规申请证书通知策略
- value：域名或用于违规通知的电子邮箱或Web地址。其值取决于[tag]的值，必须加双引号。取值范围：字符串（仅包含字母、数字、空格、-#*?&_~=:;.@+^/!%），最长255字符。

不同应用场景下，设置CAA记录集的规则如表9-1所示。

表 9-1 CAA 记录配置规则

| 目的 | 样例 | 描述 |
|-------------|---|---|
| 设置单域名CAA记录 | 0 issue "ca.example.com" | 该字段表示只有ca.example.com可以为域名domain.com颁发证书，未经授权的第三方CA机构申请域名domain.com的HTTP证书将被拒绝。 |
| | 0 issue ";" | 该字段表示拒绝任何CA机构为域名domain.com颁发证书。 |
| 设置发送警报通知 | 0 iodef "mailto:admin@domain.com" | 该字段用于当第三方尝试为一个未获得授权的域名申请证书时，通知CA机构向网站所有者发送警报邮件。 |
| | 0 iodef "http://domain.com/log/" 0 iodef "https://domain.com/log/" | 该字段用于记录尝试在其他CA申请HTTPS证书的行为。 |
| 设置颁发通配符域名证书 | 0 issuewild "ca.example.com" | 该字段用于将通配符证书的颁发权限指定CA机构ca.example.com。 |

| 目的 | 样例 | 描述 |
|--------|--|---|
| 综合配置样例 | 0 issue "ca.abc.com" 0 issuewild "ca.def.com" 0 iodef "mailto:admin@domain.com" | 该字段表示域名domain.com： <ul style="list-style-type: none"> 授权CA机构ca.abc.com颁发不限类型的证书。 授权CA机构ca.def.com颁发通配符证书。 禁止其他CA机构颁发证书。 当有违反设置规则的情况发生，CA机构发送通知邮件到admin@domain.com。 |

资源成本和规划

本节介绍最佳实践中资源规划情况，包含以下内容：

表 9-2 域名资源规划

| 资源 | 公网域名 | 记录集类型 |
|-----|------------|-------|
| DNS | domain.com | CAA |

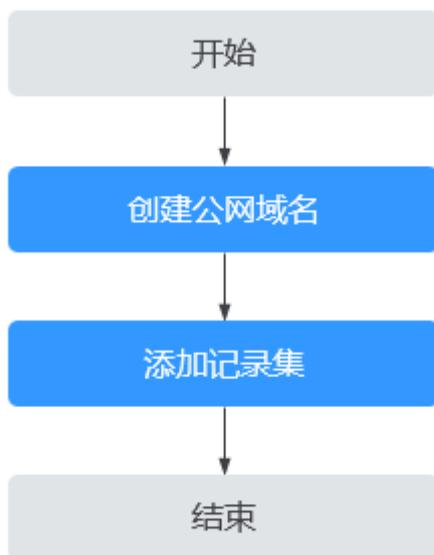
表 9-3 资源和成本规划

| 资源 | 资源名称 | 资源说明 | 数量 | 每月费用 |
|-------|-----------|--|----|------------------------------------|
| 域名注册 | 域名 | 公网域名：domain.com | 1 | 详细请参见 域名注册产品价格详情 。 |
| 云解析服务 | 公网域名解析记录集 | <ul style="list-style-type: none"> 公网域名：domain.com 记录集类型：CAA 值： 0 issue "ca.abc.com" 0 iodef "mailto:admin@domain.com" | 1 | 免费 |

设置公网域名的 CAA 记录流程

为公网域名添加CAA记录集的流程如[图9-2](#)所示。

图 9-2 设置公网域名 CAA 记录



实施步骤

步骤1 创建公网域名

1. 进入[公网域名列表页面](#)。
2. 在公网域名页面，单击“创建公网域名”。
3. 根据界面提示配置相关参数，参数说明如[表9-4](#)所示。

图 9-3 创建公网域名

创建公网域名 ✕

域名

企业项目 ?

—请选择— 新建企业项目

高级配置(可选)

标签

如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在TMS中 [创建预定义标签](#)

[+ 添加新标签](#)

您还可以添加20个标签。

描述

0/255

取消 确定

表 9-4 创建公网域名参数说明

| 参数 | 参数说明 | 取值样例 |
|----|---|------------|
| 域名 | 从域名注册商处获得的授权域名。 域名的格式请参见 域名格式与级别 。 | domain.com |

| 参数 | 参数说明 | 取值样例 |
|------|---|--------------------------------|
| 企业项目 | <p>公网域名关联的企业项目，用于将公网域名资源按照企业项目进行管理。</p> <p>说明 仅当用户使用的“账号类型”为“企业账号”时，显示该参数，且参数必选。</p> <p>配置原则：</p> <ul style="list-style-type: none">- 如果不通过企业项目管理域名资源，则采用默认值“default”。- 如果通过企业项目管理域名资源，则在下拉列表中选择已经创建的企业项目。 <p>在设置该参数前，您需要完成创建企业项目。</p> <p>更多关于企业项目的信息，请参考《企业项目管理用户指南》。</p> | default |
| 标签 | <p>可选参数。</p> <p>域名的标识，包括键和值，每个域名可以创建20个标签。</p> | example_key1 example_value1 |
| 描述 | <p>可选参数。</p> <p>域名的描述信息。</p> <p>长度不超过255个字符。</p> | This is a zone example. |

4. 单击“确定”。

步骤2 添加记录集

1. 在“公网域名”页面的域名列表中，单击待添加CAA记录集的域名domain.com。系统进入domain.com的域名解析记录页面。
2. 单击“添加记录集”。
- 系统进入“添加记录集”页面。
3. 根据界面提示配置相关参数，参数说明如[表9-5](#)所示。

图 9-4 添加 CAA 类型记录集

添加记录集

主机记录

主机记录指域名前缀，例如 example.com 常用的解析如下：
网站解析：主机记录与www，解析的域名是www.example.com
网站解析：主机记录为空，解析的域名是example.com
子域名：主机记录与cdn，解析的域名是cdn.example.com
邮箱解析：主机记录与mail，解析的域名是 mail.example.com
泛解析：主机记录写*，解析的域名是 *.example.com，匹配example.com的所有子域名

* 记录类型

* 别名 是 否

将此记录集关联到一个华为云服务资源实例，与CNAME记录集相比，别名支持一级主域名。

* 线路类型

全网默认：必选。未匹配到已设置的线路时，会返回默认解析结果。
运营商线路：可选。根据访问用户所在运营商网络调度到最佳访问地址。
地域线路：可选。根据访问用户所处地理位置调度到最佳访问地址。

* TTL (秒)

TTL指解析记录在本地DNS服务器的缓存时间。如果您的服务地址经常更换，建议TTL值设置相对小些，反之，建议设置相对大些。

* 记录值

CAA记录：指定要授权的证书颁发机构，使其可以给域名或者子域名颁发证书。最多可以输入50个不重复记录，每行一个。
格式：
[flag] [tag] [value]
例如：
0 issue "ca-example.com"
0 issuewild "ca-example.com"
0 iodef "mailto:admin@domain.com"

表 9-5 添加 CAA 类型记录集参数说明

| 参数 | 参数说明 | 取值样例 |
|------|--|--------------------|
| 主机记录 | 解析域名的前缀。 例如创建的域名为“domain.com”，其“主机记录”设置包括： <ul style="list-style-type: none">- www：用于网站解析，表示解析的域名为“www.domain.com”。- 空：用于网站解析，表示解析的域名为“domain.com”。主机记录置为空，还可用于为空头域名“@”添加解析。- abc：用于子域名解析，表示解析的域名为“domain.com”的子域名“abc.domain.com”。- mail：用于邮箱解析，表示解析的域名为“mail.domain.com”。- *：用于泛解析，表示解析的域名为“*.domain.com”，匹配“domain.com”的所有子域名。 | 置空 |
| 类型 | 记录集的类型，此处为CAA类型。 添加记录集时，如果提示解析记录集已经存在，说明待添加的记录集与已有的记录集存在限制关系或者冲突。 详细内容请参见 为什么会提示解析记录集已经存在？ 。 | CAA - CA证书颁发机构授权校验 |
| 别名 | 用于是否将此记录集关联至云服务资源实例。 <ul style="list-style-type: none">- 是：为此记录集关联云服务资源实例。- 否：不为此记录集关联云服务资源实例。 | 否 |
| 别名记录 | “别名”参数设置选择“是”时，该项必选。 用于设置记录集关联的华为云服务资源实例。 记录集支持关联的华为云服务资源实例包括：企业门户、Web应用防火墙。 | - |

| 参数 | 参数说明 | 取值样例 |
|--------|--|------------|
| 线路类型 | <p>解析的线路类型用于DNS服务器在解析域名时，根据访问者的来源，返回对应的服务器IP地址。</p> <p>默认值为“全网默认”。</p> <p>仅支持为公网域名的记录集配置此参数。</p> <ul style="list-style-type: none"> - 全网默认：默认线路类型，当未根据访问者来源设置解析线路时，系统会返回默认解析结果。 - 运营商线路解析：根据访问者所在运营商，设置解析线路。 - 地域解析：根据访问者所在地域，设置解析线路。 - 自定义线路：根据访问者所属IP网段。 | 全网默认 |
| TTL(秒) | <p>解析记录在本地DNS服务器的缓存时间，以秒为单位。</p> <p>默认值为“300秒”。取值范围为：1~2147483647</p> <p>如果您的服务地址经常更换，建议TTL值设置相对小些，反之，建议设置相对大些。</p> <p>更多TTL相关内容请参见什么是TTL值?。</p> | 5分钟，即300s。 |

| 参数 | 参数说明 | 取值样例 |
|----|---|---|
| 值 | <p>指定要授权的证书颁发机构，使其可以给域名或者子域名颁发证书。</p> <p>最多可以输入50个不重复记录，多个记录之间以换行符分隔。</p> <p>填写格式: [flag] [tag] [value]</p> <p>配置规则:</p> <ul style="list-style-type: none">- flag: 认证机构限制标志，定义为0~255无符号整型。常用取值为0。- tag: 仅支持大小写字母和数字0~9，长度1~15，常用取值：<ul style="list-style-type: none">▪ issue: 授权任何类型的域名证书▪ issuewild: 授权通配符域名证书▪ iodef: 指定违规申请证书通知策略- value: 域名或用于违规通知的电子邮箱或Web地址。其值取决于[tag]的值，必须加双引号。取值范围: 字符串（仅包含字母、数字、空格、-#*?&_~=:;.,@+^/!\%），最长255字符。 | <pre>0 issue "ca.abc.com" 0 iodef "mailto:admin@domain.com"</pre> |
| 权重 | <p>可选参数，返回解析记录的权重比例。默认值为1，取值范围: 0~1000。</p> <p>仅支持为公网域名的记录集配置此参数。</p> <p>当域名在同一解析线路中有多条相同类型的解析记录时，可以通过“权重”设置解析记录的响应比例。。</p> | 1 |
| 标签 | <p>可选参数，记录集的标识，包括键和值，每个记录集可以创建20个标签。</p> | <pre>example_key1 example_value1</pre> |
| 描述 | <p>可选参数，对域名的描述。</p> <p>长度不超过255个字符。</p> | The description of the hostname. |

4. 单击“确定”，完成CAA类型记录集的添加。

---结束

验证 CAA 解析记录是否生效?

CAA解析记录可以通过dig+trace命令查看域名是否生效以及具体的解析过程。如果操作系统没有自带dig命令，需要手动安装后才能使用。

命令格式为：dig [类型] [域名] +trace。

示例如下：

```
dig caa www.domain.com +trace
```

10 通过 Serving Stale 提高自建 DNS 的解析成功率

什么是 Serving Stale

Serving Stale是RFC 8767描述的用于提高DNS解析可靠性的一个标准。当Local DNS上的域名缓存过期，由于权威DNS故障导致Local DNS无法刷新本地缓存时，可以通过Local DNS的Serving Stale的能力使用过期的缓存结果应答请求，避免客户端无法得到响应。

📖 说明

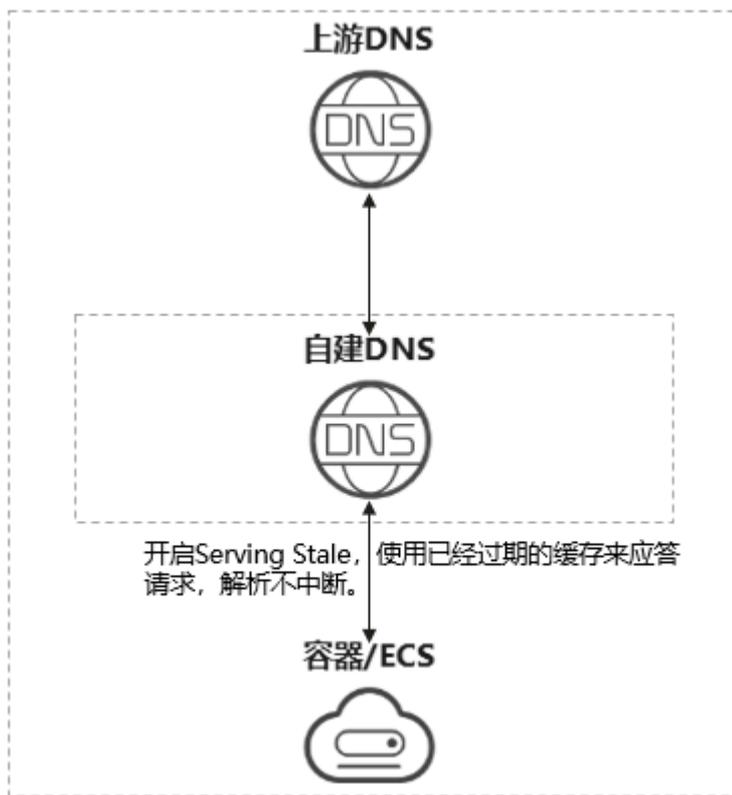
- 上游DNS服务器故障时，使用过期的缓存应答请求，可能导致域名在上游DNS更新后，自建DNS不能及时给客户端响应最新的结果。
- Serving Stale功能是使用在自建DNS缓存已经过期的缓存来应答客户端，未缓存过的域名不适用。

Serving Stale 的使用场景

如下图中，容器/ECS使用了自建DNS做域名解析，当自建DNS的上游DNS由于故障而无法应答时：

- 如果自建DNS未开启Serving Stale能力，容器/ECS解析域名会失败。
- 如果自建DNS开启了Serving Stale能力，自建DNS使用过期的缓存来应答容器/ECS，解析不中断。

图 10-1 Serving Stale 的使用场景



如何开启 Serving Stale

- **bind9开启Serving Stale**: 如果您的自建DNS用的是bind, 可以在bind的options配置中增加相关配置项并重载/重启您的DNS服务来生效。
- **coreDNS开启Serving Stale**: 如果您的自建DNS是coreDNS或者您需要优化k8s集群的域名解析时延, 可以在cache配置项中开启Serving Stale。

bind9 开启 Serving Stale

bind9支持版本: 9.16.3及以上

- 配置文件: named.conf
- 配置位置: options
- 配置项说明

| 配置项 | 默认值 | 建议值 | 功能说明 |
|---------------------|---------------------|------|----------------------|
| stale-cache-enable | no | yes | 启用缓存保持功能。 |
| stale-answer-enable | stale-answer-enable | yes | 启用stale-cache来应答。 |
| max-stale-ttl | 1day | 1day | stale-cache缓存保持多长时间。 |

| 配置项 | 默认值 | 建议值 | 功能说明 |
|--------------------|-----|-----|---|
| stale-refresh-time | 30s | 30s | bind刷新stale-cache的时间间隔，即多长时间向权威DNS请求一次，并刷新缓存。 |
| stale-answer-ttl | 30s | 30s | 使用stale-cache回复response时，报文中的TTL值。 |

- 配置样例：

```
options {
  stale-cache-enable yes;
  stale-answer-enable yes;
};
```

coreDNS 开启 Serving Stale

coreDNS插件中已支持Serving Stale能力，允许coreDNS无法连接上游DNS服务器时使用已过期的本地缓存来应答。

coreDNS支持版本：1.6.6

- 配置格式：serve_stale [DURATION] [REFRESH_MODE]
- 配置项说明：
 - DURATION：过期缓存的使用时长，默认值为1h。
 - REFRESH_MODE：支持配置为verify、immediate。
 - verify：在将过期的缓存发送到客户端之前，先验证上游的DNS是否可用。该方式可能会增加客户端的解析时延。
 - immediate：立即将过期的缓存作为响应发送给客户端。
- 配置样例：

```
cache {
  serve_stale 1h immediate
}
```