云解析服务

最佳实践

文档版本 05

发布日期 2020-11-13

华为技术有限公司

商标声明


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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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。

目 录

1 设置 CAA 记录防止错误颁发 HTTPS 证书

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。

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。

背景

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1-1所示。

图 1-1 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。

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。

配置原则

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1-1**所示。

表 1-1 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： ● 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。

添加 CAA 记录集

1. 登录管理控制台。
2. 选择“网络 > 云解析服务”。
   进入云解析服务页面。
3. 在左侧树状导航栏，选择“域名解析 > 公网解析”。
   进入“公网域名”页面。
4. 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。
5. 单击“添加记录集”。
   系统进入“添加记录集”页面。
6. 设置CAA记录集的参数。
   - 类型：CAA – CA证书颁发机构授权校验
   - 线路类型：全网默认
   - TTL：5分钟
   - 值：
     0 issue "ca.abc.com"
     0 iodef "mailto:admin@domain.com"
7. 单击“确定”，完成CAA类型记录集的添加。

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.example.com +trace

2 为云服务器配置内网域名

背景

内网域名是指仅在VPC内生效的虚拟域名，无需购买和注册，无需备案。云解析服务提供的内网域名功能，可以让您在VPC中拥有权威DNS，且不会将您的DNS记录暴露给互联网，解析性能更高，时延更低，并且可以防护解析劫持。我们可以将VPC内承担内网域名解析功能的DNS称为内网DNS。

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，实现：

- 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。

操作场景

云解析服务作为内网DNS的典型应用场景如图2-1所示。

图 2-1 逻辑组网图

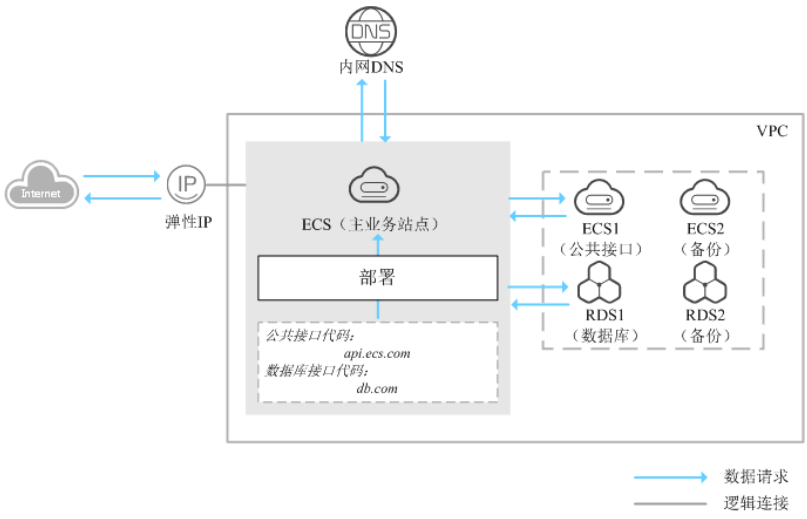


图2-1展示了某网站的逻辑组网，在一个VPC内，部署了ECS和RDS。其中：

- 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。

当该网站在运行过程中，因ECS1故障，需要将业务切换到备份的云服务器ECS2时，若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。

假如在部署该网站时，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，则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。

本文介绍为云服务器配置内网域名的操作指导。

数据规划

云服务器的内网域名规划如表2-1所示。

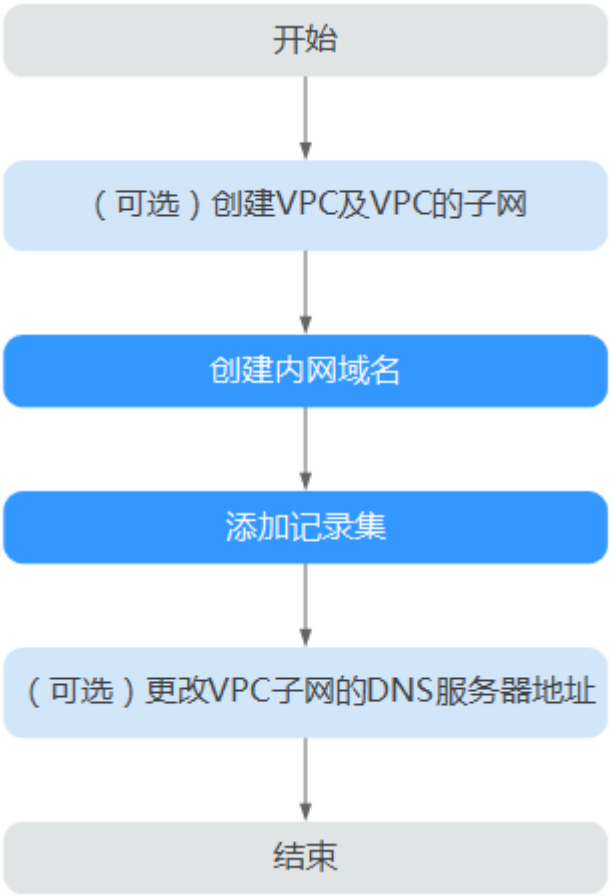
表 2-1 内网域名数据规划

设备	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。

操作流程

为云服务器配置内网域名的流程如图2-2所示。

图 2-2 内网域名配置流程



配置流程说明：

- “（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。
- “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。
- “（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。

（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. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 选择“网络 > 虚拟私有云”。
4. 在左侧树状导航栏，选择“虚拟私有云”。
5. 单击“创建虚拟私有云”，根据界面提示配置参数，关键参数的配置说明如表2-2所示。

表 2-2 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-北京一
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。	100.125.1.250 100.125.21.250

6. 单击“立即创建”，完成VPC以及VPC默认子网的设置。

创建内网域名

为云服务器ECS1和数据库RDS1创建内网域名。

1. 选择“网络 > 云解析服务”。
   进入云解析服务页面。
2. 在左侧树状导航栏，选择“域名解析 > 内网解析”。
3. 单击“创建内网域名”，开始创建内网域名。
4. 根据界面提示配置参数，参数说明如表2-3所示。

表 2-3 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
邮箱	可选参数。管理该内网域名的管理员邮箱。建议用户使用保留邮箱“HOSTMASTER@*域名*”作为此管理员邮箱。 更多关于Email的信息，请参见**SOA记录中的Email格式为什么变化了？**。	HOSTMASTER@ecs1.com
标签	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。 键和值的命名规则请参见**表2-4**。	-
描述	可选参数。域名的描述信息。长度不超过255个字符。	This is a zone example.

表 2-4 标签命名规则

参数	规则	举例
键	• 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	• 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

5. 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“名称”列的域名名称，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。
6. 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2-1**。

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2-5所示。

表 2-5 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2-4。	-
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2-1。

（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？**。

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-北京一”。
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“域名解析 > 内网解析”。
5. 在“内网域名”页面域名列表中，单击“名称”列的域名“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。

3 将域名迁移至华为云 DNS 进行解析

背景

如果要通过直接在浏览器中输入域名，访问网站或Web应用程序，您需要注册一个域名，并将该域名解析至网站的IP地址。

- 注册域名：通过域名注册商完成，域名注册商提供域名的注册、查询、续费等管理功能。您可以选择华为云作为您的域名注册商，参考**域名注册**完成网站域名的注册。
- 将域名解析至网站IP地址：通过在DNS服务商处为域名配置解析记录实现，DNS服务商提供域名的托管、解析等功能。您可以选择华为云的云解析服务作为DNS服务商，为域名提供DNS解析服务。

域名注册商和DNS服务商可以相同，也可以不同，无直接关系。

本文介绍如何将托管至其他DNS服务商处的域名迁移至华为云DNS进行解析。

操作场景

迁移至华为云DNS进行解析的域名包括以下两种情况：

- 通过其他域名注册商注册的域名，已使用第三方DNS服务商进行解析。
- 通过华为云注册的域名，已使用第三方DNS服务商进行解析。

上述两种情况，其域名迁移至华为云的操作相同，均可以参考本操作进行。

本文以托管至A服务商的域名example.com为例介绍域名迁移至华为云的操作过程。

前提条件

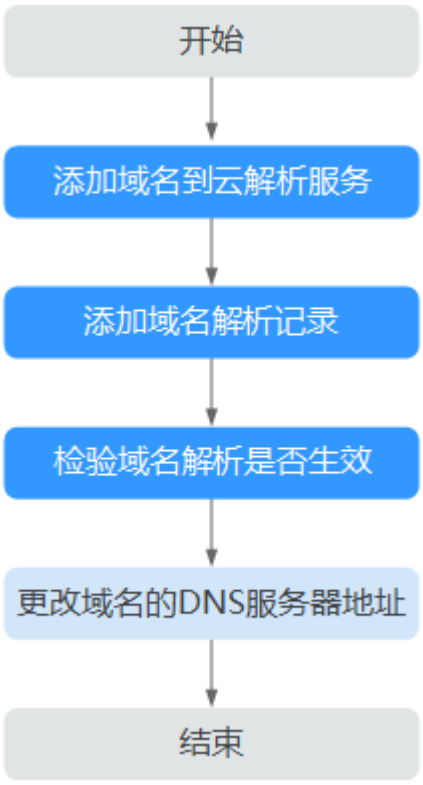
在域名迁移操作之前，需要确认并完成以下任务：

1. 检查华为云账号状态：检查待迁移至的华为云账号是否已经完成实名认证，若未完成请参考**华为云账号实名认证**完成账号的实名认证。
2. 获取域名当前DNS配置：将域名从其他DNS服务商迁移到华为云的云解析服务，需要在云解析服务中重现域名当前的DNS配置。您需要通过域名原服务商，导出域名当前的DNS配置。

操作流程

迁移域名的操作如图3-1所示。

图 3-1 迁移域名流程



添加域名到云解析服务

在云解析服务中，将待迁移域名托管至云解析服务。

说明

通过华为云注册的域名，系统会自动在云解析服务完成添加域名的操作，本步骤可以忽略。

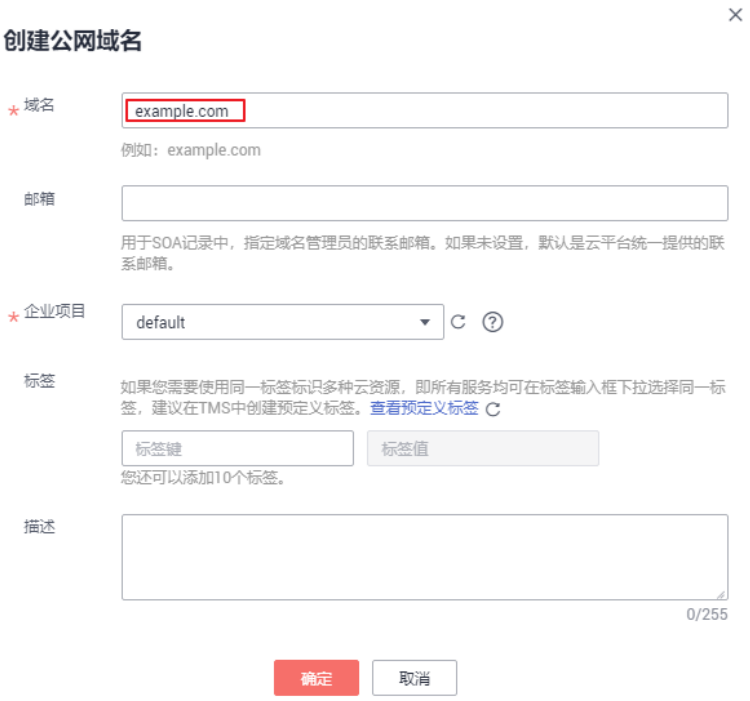
1. 登录管理控制台。
2. 将鼠标悬浮于页面左侧的“ ☰ ”，在服务列表中，选择“网络 > 云解析服务”。

   进入“云解析”页面。
3. 在左侧树状导航栏，选择“域名解析 > 公网解析”。

   进入“公网域名”页面。
4. 在页面右上角，单击“创建公网域名”。
5. 在“创建公网域名”页面中，输入注册的域名“example.com”，将域名添加至云解析服务。

   更多参数说明，请参见**创建公网域名**。

图 3-2 创建公网域名



6. 单击“确定”，完成公网域名“example.com”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。

图 3-3 公网域名列表

若提示“域名已经被其他租户创建。”，请参考**找回域名**。

说明

单击“名称”列的域名名称，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对用户提供域名服务的DNS是什么？**。

添加域名解析记录

需要在华为云平台为域名添加在原DNS服务商处的所有解析记录。域名原有的解析记录可以在原DNS服务商处查询并导出。

导出域名解析记录后，您可以批量导入域名解析记录。

1. 登录管理控制台。
2. 将鼠标悬浮于页面左侧的“ ☰ ”，在服务列表中，选择“网络 > 云解析服务”。

进入“云解析”页面。

3. 在左侧树状导航栏，选择“域名解析 > 公网解析”。

   进入“公网域名”页面。

4. 在域名列表中，单击创建的域名“example.com”，进入域名详情页面。
5. 在左侧导航栏，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，需要首先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. 按模板要求完成解析记录的填写。

      说明

      若您已经在域名的转出方导出了域名解析记录，需要将导出的内容填写到模板中，否则将无法导入成功。

6. 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。

检验域名解析是否生效

您可以在已经连接Internet的PC终端的DOS窗口使用如下三种命令测试域名解析是否生效，命令格式如下：

- nslookup [-qt=类型] 目标域名 权威DNS地址
- dig 类型 目标域名 @权威DNS地址

说明

- nslookup和dig命令中的“类型”可以输入解析记录类型（比如A，CNAME，TXT，MX等），用来查询指定类型的域名解析是否生效，如果不输入则默认查询A类型域名解析。
- 如果PC终端的操作系统没有自带dig命令，需要手动安装后才能使用。
- 上述命令均可以用于测试公网域名解析和内网域名解析是否生效。

更改域名的 DNS 服务器地址

1. 在域名服务商处修改域名解析服务器地址，具体以域名服务商官网操作指导为准。
2. 等待修改生效。

   通常，修改的DNS地址可以很快同步到顶级域服务器在互联网中生效。但是，DNS服务商的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。

   具体域名的DNS生效时间请以DNS服务商处的说明为准。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。这样在修改还未生效的地区由于已经缓存了域名以前的NS记录，仍然可以访问原DNS进行解析。

