云解析 DNS

操作指南

操作指南

域名管理

域名管理

添加域名

非阿里云注册域名或子域如需使用云解析DNS，需要通过 **添加域名** 功能，将主域名或子域添加到云解析控制台，才可以启用域名解析服务。

阿里云注册域名

阿里云注册域名无需进行添加，域名注册完成后，可直接在域名控制台，点击“解析”进行DNS记录管理

1 . 登录 域名控制台

2 . 选择需要解析的域名，点击 **“解析”** 文字按钮

3 . 进入 **“解析设置”** 页面，可在此页面操作解析记录的增删改设置。

非阿里云注册域名

1 . 登录云解析控制台。

2 . 在域名解析页面， **全部域名**页签，点击 **添加域名** 按钮。

3 . 在 **添加域名** 对话框中，输入主域或子域，然后单击 **确定** 按钮。

4 . 添加域名完成后，即可在 **全部域名**页签下查看到此域名，说明域名添加成功。

删除域名

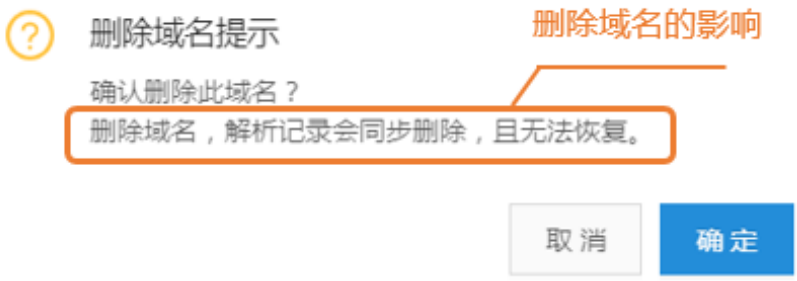
在云解析DNS控制台，删除域名是针对非阿里云注册域名使用，域名删除后解析记录会一并删除。（阿里云注册域名不支持删除操作）

操作步骤

1 . 登录云解析控制台。

2 . 在域名解析页面， **全部域名**页签，在操作栏点击 **更多**。

3 . 点击删除，会弹出删除域名的二次确认会话框，点击 **确认**



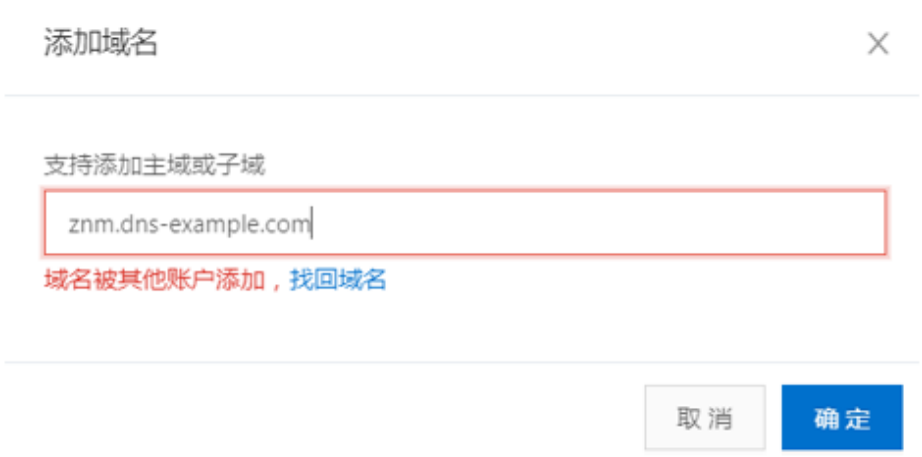
域名找回

域名找回 是指非阿里云注册域名，通过云解析DNS控制台在 **添加域名**时，提示域名已被其他账号添加。如果您是域名持有者，可以通过**域名找回**功能，将此域名找回到您当前操作的账号下，域名被找回至新账号下时，会同时删除之前的解析记录。

1 . 登录云解析控制台。

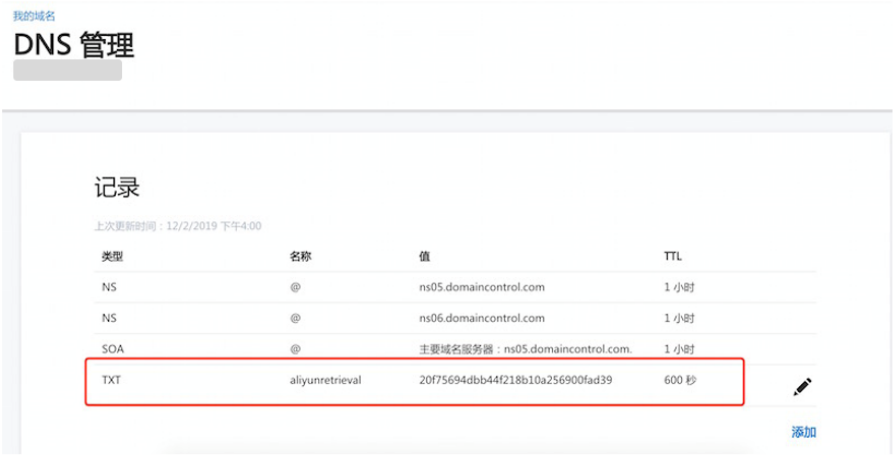
2 . 在域名解析页面， **全部域名**页签，点击 **添加域名** 按钮。

3 . 添加域名会话框提示域名已被其他账号添加，点击 **找回域名**



4 . 提示域名持有者身份验证，请复制TXT记录值，并且不要关闭此对话框。

5 . 到此域名当前的DNS服务商处，添加TXT记录。例如测试域名的DNS服务商在GODADDY管理，以下是在GODADDY控制台操作添加TXT记录



6．在域名当前DNS服务商，添加完TXT记录后，请返回云解析DNS域名持有者身份验证的对话框页面，点击**确认**按钮。然后云解析DNS通过自动扫描添加的TXT记录，如果扫描到TXT记录已正常添加，将会发送邮件通知您“域名找回成功”，并将该域名添加到发起域名找回请求的账号中。

域名分组管理

域名分组管理：是指对云解析DNS控制台中的域名，通过分组的方式进行归类和管理，包含创建分组、修改分组、删除分组、更换分组功能。

创建分组

1．登录云解析控制台。

2 . 在域名解析页面， **全部域名**页签，点击 **全部域名** 下拉框，点击 **+** 。

3 . 输入需要创建的分组名称，点击 **√** 创建分组完成。

修改/删除分组

1 . 在域名解析页面， **全部域名**页签，点击 **全部域名** 下拉框，单击分组名称旁边的编辑图标。最后输入需要更改的分组名称，点击 **√** 保存即可。

2 . 单击分组名称旁边的删除图标。删除分组，则该分组下的域名会同步从该分组中清空，可通过“全部域名”分组来管理域名。

更换分组

是指将域名添加到分组下、或者将域名从A分组移动到B分组下。

1 . 在域名解析页面，**全部域名**页签下，选中需要操作的域名，单击 **更换分组** 。

2 . 选择域名要添加的分组，点击 **确认**

3 . 成功将域名移动到分组下，可点击此分组名称查看。

分组规则说明

- “全部域名”属于系统分组，统计的是域名解析下的全部域名数量，系统分组名称不支持修改和删除。
- 域名在分组管理中具备唯一性，不支持一个域名同时存在多个分组中。
- 删除分组，则该分组下的域名会同步从该分组中清空，可通过“全部域名”分组来管理域名。
- 分组创建最大上限100个。
- 分组的名称的输入限制20个字符
- 分组管理可添加的域名数量不限
- 分组管理操作不支持日志查询

子域管理

概述

子域管理：是指云解析可实现为二级子域、三级子域、...等，提供独立的DNS托管和域名解析服务。

添加子域主流程：

① 添加域名

② 域名持有人验证（TXT验证）验证

③ 在子域下设置解析记录

④ 在主域下设置NS记录

详细参阅下文 **设置方法** 文档

名词定义

名词	定义
子域名	例如 www.aliyun.com 是 aliyun.com 的子域名
子域	例如主域名是aliyun.com，则www.aliyun.com是主域名的二级子域，test.www.aliyun.com是主域名的三级子域，二级子域、三级子域、...等统一称为子域
子域管理	云解析支持二级子域、三级子域、...等单独管理，子域可以独立管理域名解析

应用场景

子域托管，可以便于客户对主、子域名进行分别管理，适用于以下场景：

1 . 主域DNS服务器使用第三方DNS厂商，因某些特殊原因无法做到将DNS全量迁移到阿里云DNS，希望先迁移子域到云解析DNS使用。

2 . 跨国公司或集团类型客户，主域多属于总公司统一管理，而分公司则需要申请子域做单独管理使用。

3 . 政企/金融类型客户，一般使用的是自建DNS，但是使用和维护成本很高，用户可以将子域授权到云解析单独做管理。

设置方法

场景1：主域使用第三方DNS，子域使用阿里云DNS

1 . 登录 云解析DNS控制台

2 . 在域名解析页面，全部域名页签下，单击 添加域名 按钮

3 . 在 添加域名 会话框中，输入子域，单击 TXT授权校验 文字按钮 。

4 . 在域名持有者身份验证会话框中，复制主机记录和记录值。

提醒： 域名持有者身份验证允许复制主机记录、记录值后，在**未单击 验证 按钮的场景下**，可以先关闭此对话框，TXT记录验证的记录值有效期为1天，如单击验证，则最多支持3次验证，3次验证失败则会重置TXT记录值。待到主域名下完成添加完TXT记录后，再单击 验证 按钮进行TXT验证。

5 . 在 主域 的解析设置页面，根据域名持有人身份验证提供的主机记录和记录值 ，添加TXT记录。

记录类型	域名	记录值
TXT	alidnscheck.dns-example.com	60affd31e1a3420e92a32aeb4d8b4406

6 . 添加完成，确认TXT记录生效后，到验证会话框中，单击 验证 按钮。

7 . TXT验证通过，单击 验证成功 按钮。 子域会被自动添加到域名解析列表中，单击 子域进入解析设置页面，手动添加解析记录。

8 . 在主域下添加两条NS记录，分别指向云解析DNS为子域分配的DNS服务器。

提醒： NS记录以控制台提示的DNS服务器信息为准。

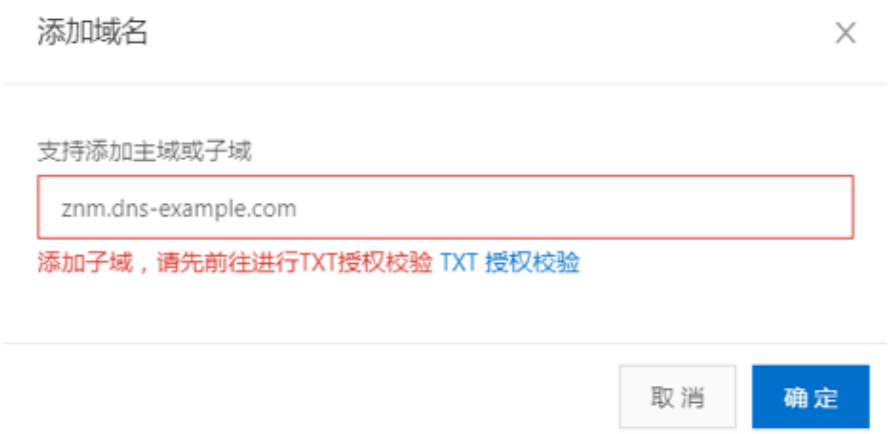
记录类型	域名	记录值
NS	znm.dns-example.com	ns1.alidns.com
NS	znm.dns-example.com	ns2.alidns.com

场景2：主域和子域都使用阿里云DNS，使用不同账号管理。

1 . 登录 云解析DNS控制台

2 . 在域名解析页面，全部域名页签下，单击 添加域名 按钮

3 . 在 添加域名 会话框中，输入子域，单击 TXT授权校验 文字按钮 。



4 . 在域名持有者身份验证会话框中，复制主机记录和记录值。

提醒： 域名持有者身份验证允许复制主机记录、记录值后，不能关闭对话框，否则系统会重新生成TXT记录，导致TXT验证失败。待到主域名下完成添加完TXT记录后，单击 验证 按钮。

5 . 在 主域 的解析设置页面，根据域名持有人身份验证提供的主机记录和记录值 ，添加

TXT记录。

6 . TXT记录确认生效后，到域名持有人身份验证会话框中，单击 验证 按钮。

提醒： 添加TXT记录的过程中，不能关闭验证会话框。否则系统会重新生成TXT记录，导致TXT校验失败。

7 . TXT验证通过，单击 验证成功 按钮。 子域会被自动添加的域名解析列表中，单击 子域进入解析设置页面，云解析会将主域下的子域自动同步到该子域下。

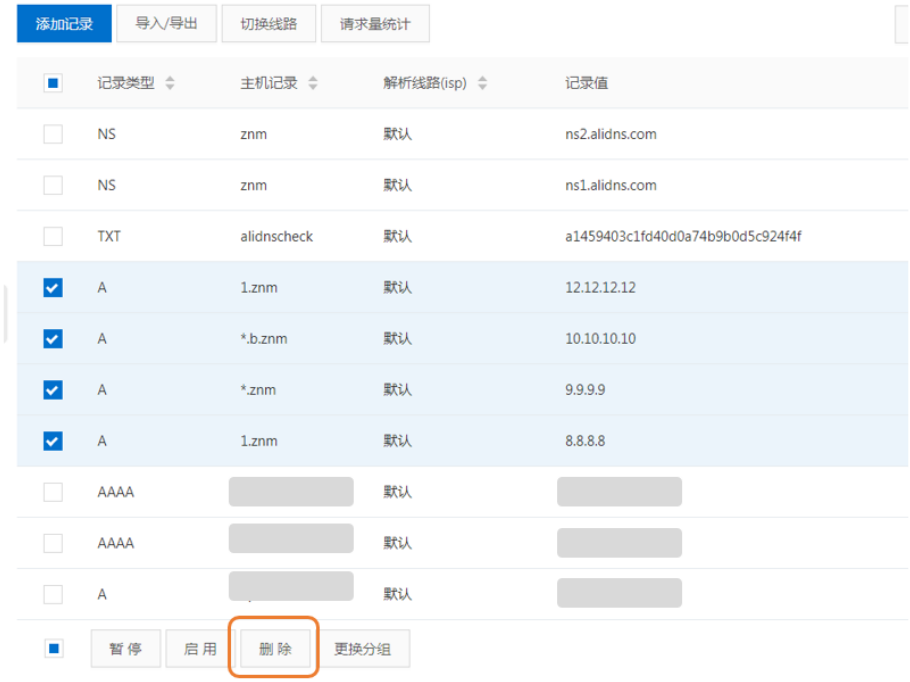

域名持有者身份验证
TXT记录验证：
请到域名当前DNS服务商处给该域名添加TXT记录
域名：dns-example.com
主机记录：alidnscheck
记录值：a1459403c1fd40d0a74b9b0d5c924f4f
添加完毕后点击"验证"按钮，验证通过后，即可成功创建域名
主域下存在当前子域的解析记录，迁移到子域后，子域涉及付费功能将会暂停使用。
已验证成功，确认添加域名


域名解析
公告：.com/.net/.cn/.xin/.top/.xyz/.vip/.club/.shop/.wang/.ren等域名注册成功后必须进行域名实名认证，否则会造成解析不生效，实
全部域名
请求量统计
版本套餐管理
更多服务
批量自动续费
添加域名
域名
记录数
DNS服务器
znm.dns-example.com
0
运行异常


解析设置 znm.dns-example.com
未查询到域名DNS服务器信息，请检查DNS服务器设置或域名实名认证相关。 展开
添加记录
导入/导出
请求量统计
无需人工操作，系统会自动将主域下的子域名同步到子域下
记录类型
主机记录
解析线路(isp)
记录值
A 1 默认 12.12.12.12
A *.b 默认 10.10.10.10
A * 默认 9.9.9.9
A 1 默认 8.8.8.8
暂停
启用
删除
更换分组

8 . 在子域的解析设置页面，获取分配的DNS服务器。然后到主域下添加两条NS记录，分别指向云解析DNS为子域分配的DNS服务器。

9 . 如主域下存在子域解析记录，子域名托管后会影响主域下的解析记录生效，需要在主域下删除子域解析记录，并在子域名解析设置页面进行解析设置。如果主域下没有子域，请忽略此步骤。



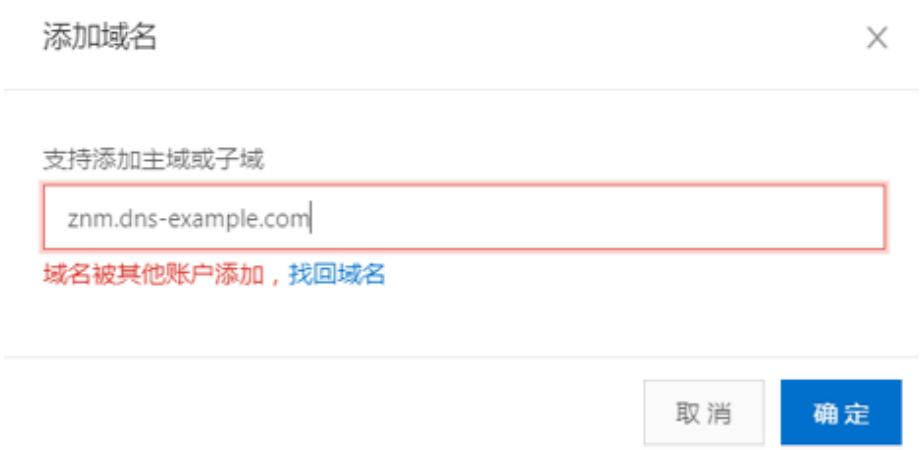
注意： 主域和子域使用的云解析版本需要保持一致，例如主域使用云解析付费版，那么子域也需要绑定云解析付费版。如果主域使用云解析付费版，那么请在子域添加完后，先将子域绑定到云解析付费版上，然后再到主域下添加NS记录。

场景3：主域和子域都使用阿里云DNS，但子域已被其他账号添加，需要找回子域。

1 . 登录云解析DNS控制台

2 . 在域名解析页面，全部域名页签下，单击 添加域名 按钮

3 . 在 添加域名 会话框中，输入子域，单击 域名找回 文字按钮 。



4 . 在域名持有者身份验证会话框中，复制主机记录和记录值。

提醒： 域名持有者身份验证允许复制主机记录、记录值后，不能关闭对话框，否则系统会重新生成TXT记录，导致TXT验证失败。待到主域名下完成添加完TXT记录后，单击 验证 按钮。

6 . 域名持有者身份验证通过后，子域和子域下的解析记录会被自动添加到发起找回的账号下。

产品规则

子域管理产品规则请参阅 子域管理产品规则限制 文档。

常见问题

请参阅 云解析DNS功能类FAQ 文档。

解析记录管理

添加解析记录

添加解析记录

解析记录类型

云解析支持的记录类型包含：

- A记录
- CNAME记录
- MX记录
- AAAA记录
- TXT记录
- URL显性/隐性转发
- NS记录
- SRV记录
- CAA记录

A记录

使用场景

添加 A 记录可实现将域名指向 IP 地址。

设置方法

1 . 登录云解析DNS控制台

2 . 在域名解析页面，全部域名页签下，单击域名，进入解析设置页面

3 . 在解析设置页面，单击 **添加记录** 按钮

4 . 添加记录会话框中各项参数的添加说明。

记录类型：选择 **A**

主机记录：一般是指子域名的前缀（如需创建子域名为www.dns-example.com, 主机记录输入 **www** ；如需实现dns-example.com，主机记录输入 **@** ）。

解析线路：选择 **默认** （默认为必选项，如未设置会导致部分用户无法访问)。

记录值：记录值为 IP 地址，填写 IPv4 地址。

TTL：为缓存时间，数值越小，修改记录各地生效时间越快，默认为10分钟。

CNAME 记录

使用场景

当需要将域名指向另一个域名，再由另一个域名提供 IP 地址，就需要添加 CNAME 记录，最常用到 CNAME 的场景包括做 CDN、企业邮箱、全局流量管理等。

设置方法

记录类型：选择 **CNAME**

主机记录：一般是指子域名的前缀（如需创建子域名为www.dns-example.com的解析, 主机记录输入 **“ www”** ；如需实现dns-example.com的解析，主机记录输入“@” ）

解析线路：默认为必填项，否则会导致部分用户无法解析。

记录值：记录值为 CNAME 指向的域名，只可以填写域名。

TTL：为缓存时间，数值越小，修改记录各地生效时间越快，默认为10分钟。

MX记录

使用场景

设置邮箱时，让邮箱能收到邮件，就需要添加 MX 记录。MX全称为mail exchanger，用于电子邮件系统发邮件时根据收信人的地址后缀来定位邮件服务器。例如，当有人发邮件给“vincen@example.com”时，系统将对“example.com”进行DNS中的MX记录解析。如果MX记录存在，系统就根据MX记录的优先级，将邮件转发到与该MX相应的邮件服务器上。

设置方法

以阿里云邮企业邮箱举例，需要配置的邮箱记录做示例：

记录类型：选择 **MX**

主机记录：一般是指子域名的前缀，（要做xxx@dns-example.com的邮箱，所以主机记录输入“@”；要做xxx@mail.dns-example.com，如果主机记录填 mail）。

解析线路：默认为必填项，否则会导致部分用户无法解析，邮件无法收取；

记录值：输入内容通过联系邮箱注册商提供。例如阿里云邮提供的需要配置的解析记录值是mx1.qiye.aliyun.com；

MX优先级：输入内容通过联系邮箱注册商提供，MX 优先级的数值越低，优先级别就越高（如下图，邮件会先尝试发送到 MX 优先级为 5 的mx1.qiye.aliyun.com，如果尝试失败，才会发送到 MX 优先级为10 的mx2.qiye.aliyun.com）。

TTL：为缓存时间，数值越小，修改记录各地生效时间越快，默认为10分钟。

注意：以上仅是对MX记录的设置为例，完整的创建邮箱，还需要同时设置CNAME、TXT记录，**具体需要配置的解析记录请联系您的邮箱厂商获取**，如果您的邮箱提供是阿里云邮箱，您可以参阅 **添加邮箱解析** 的操作文档

AAAA 记录

使用场景

当预期是实现访问者通过 IPv6 地址访问网站，可以使用 AAAA 记录实现。

设置方法

记录类型：选择 **AAAA**

主机记录：一般是指子域名的前缀（如需创建子域名为www.dns-example.com, 主机记录输入 **www**；如需实现dns-example.com，主机记录输入 **@**）

解析线路：**默认**为必选项，未设置会导致部分用户无法访问；

记录值：记录值为IP地址，填写 IPV6 地址

TTL：为缓存时间，数值越小，修改记录各地生效时间越快，默认为10分钟。

TXT 记录

使用场景

如果希望对域名进行标识和说明，可以使用 TXT 记录， TXT 记录多用来做 SPF 记录（反垃圾邮件）。

设置方法

记录类型：选择 **TXT**

主机记录：一般是指子域名的前缀（如需为子域名为 www.dns-example.com 添加 TXT 记录， 主机记录输入 **www**；如需为dns-example.com添加TXT记录，主机记录输入 **@**）

解析线路：**默认** 为必选项，未设置会导致部分用户无法解析。

记录值：常用情况TXT 记录是用来做 SPF 反垃圾邮件的，最典型的 SPF 格式的 TXT 记录例子为 “v=spf1 a mx ~all” ，表示只有这个域名的 A 记录和 MX 记录中的 IP 地址有权限使用这个域名发送邮件。

TTL：为缓存时间，数值越小，修改记录各地生效时间越快，默认为10分钟。

URL显性/隐性转发

使用场景

将一个域名指向另外一个已经存在的站点时，需要添加 URL 记录。

使用前提

添加 URL 转发记录时，转发前后的两个域名都需完成备案。

设置方法

示例：以 http://dns-example.com 跳转到 http://www.aliyun.com:80/ 为例。

1 . URL隐性转发

用的是iframe框架技术，非重定向技术；

实现效果

为浏览器地址栏输入http://dns-example.com 回车，打开网站内容是目标地址http://www.aliyun.com:80/ 的网站内容，但地址栏显示当前地http://dns-example.com

2 . URL显性转发

支持URL转发301永久重定向、302暂时性定向

实现效果

为浏览器地址栏输入http://dnswork.top 回车，打开网站内容是目标地址http://www.aliyun.com:80/ 的网站内容，且地址栏显示目标地址http://www.aliyun.com:80/

使用规则

添加 URL 转发记录时，转发前后的两个域名都需完成备案且备案接入商为阿里云。

- URL转发时记录值不能为IP地址
- URL转发不支持泛解析设置。
- URL转发的目标域名不支持中文域名。
- URL转发前域名支持HTTP，不支持HTTPS，转发后的目标地址支持HTTP、HTTPS。
- URL转发属于特殊商品，云解析不提供攻击防护服务，如遇攻击黑洞时无法使用URL转发，请将需要转发的主机记录配置为A或CNAME记录。

NS 记录

使用场景

如果需要把子域名交给其他 DNS 服务商解析，就需要添加 NS 记录。

设置方法

示例：域名 dns-example.com 使用阿里云解析，将子域名www.dns-example.com 的解析管理权从阿里云解析授权给腾讯云解析做管理。

记录类型：选择 **NS** 。

主机记录：一般是指子域名的前缀（如需将子域名为www.dns-example.com 的解析授权给腾讯云解析的DNS服务器进行解析管理，只需要在主机记录处填写 www 即可）。

解析线路：**默认**为必填项，未设置默认线路会导致部分用户无法解析。

记录值：记录值为要授权的 DNS 服务器域名，例如腾讯云解析的DNS服务器域名 f1g1ns1.dnspod.net。

TTL：为缓存时间，数值越小，修改记录各地生效时间越快，默认为10分钟。

SRV记录

使用场景

SRV 记录用来标识某台服务器使用了某个服务，常见于微软系统的目录管理。

设置方法

- 记录类型： 选择 **SRV** 。

  主机记录： 格式为 **服务的名字.协议的类型。**

  例如：_sip._tcp

- 解析线路：**默认** 为必选项，未设置默认线路会导致部分用户无法解析

  记录值：格式为 **优先级 权重 端口 目标地址** ，每项中间需以空格分隔。

  例如：0 5 5060 sipserver.example.com

  TTL：为缓存时间，数值越小，修改记录各地生效时间越快，默认为 **600秒。**

CAA记录

使用场景

CAA(Certificate Authority Authorization)，即证书颁发机构授权。是一项新的可以添加到DNS记录中的额外字段,通过DNS机制创建CAA资源记录，可以限定域名颁发的证书和CA（证书颁发机构）之间的联系。未经授权的第三方尝试通过其他CA注册获取用于该域名的SSL/TLS证书将被拒绝。

域名设置 CAA 记录，使网站所有者，可授权指定CA机构为自己的域名颁发证书，以防止HTTPS证书错误签发，从而提高网站安全性。

CAA记录的记录格式

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记录中。

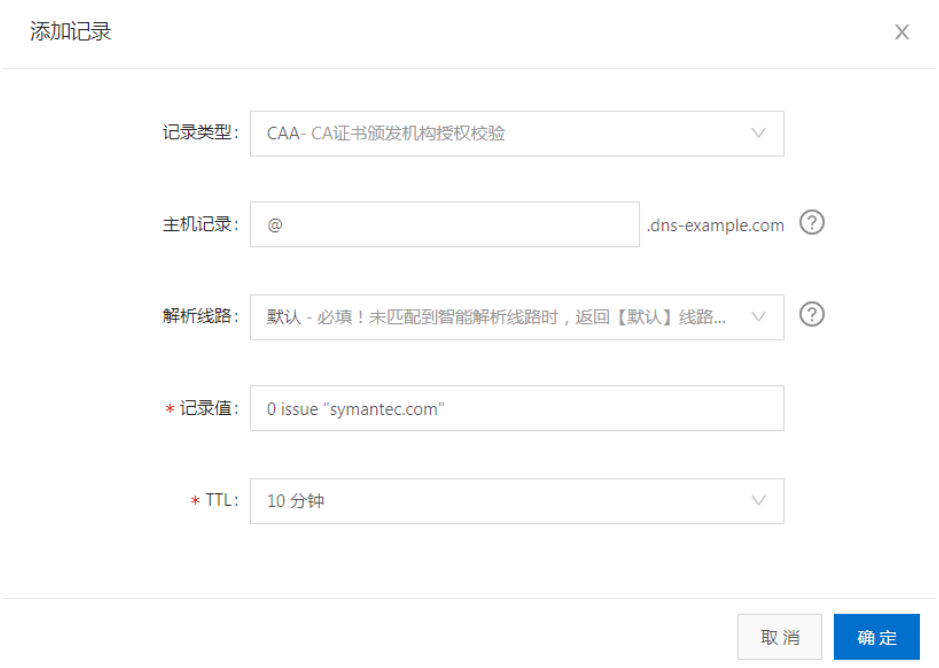
字段	说明
flag	无符号整数（目前仅支持0和128），用于标志认证机构。通常情况下填0，表示如果颁发证书机构无法识别本条信息，就忽略。
tag	支持 issue、issuewild 和 iodef。 - issue：CA授权单个证书颁发机构发布的**任何类型**域名证书。 - issuewild：CA授权单个证书颁发机构发布主机名的**通配符**证书。

	- 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。

设置方法

添加如下两条解析记录。

主机记录	记录值
@	0 issue “symantec.com”
@	0 iodef “mailto:admin@dns-example.com”



常见问题快速入口

在设置过程中如遇到问题，您可以参阅如下文档：

解析设置类常见FAQ

云解析DNS功能类FAQ

云·速成美站/云·企业官网解析方法

建站产品如何添加解析记录？
如果您购买了云·速成美站/云·企业官网，可选择以下两种方式解析域名。

一键解析：

登录云·速成美站/云·企业官网网站后台，绑定并单击解析域名，等待系统自动生成解析记录值后，即可单击一键解析完成解析。

手动解析：

1. 添加域名：登录云解析 DNS 控制台，单击**添加域名**。

2. 进入解析设置页面：单击**解析设置**，即可进入解析设置页面。
3. 添加记录：单击**添加记录**，记录类型请选择CNAME。
    - 主机记录：一般是指子域名的前缀（如需创建子域名为www.dns-example.com的解析, 主机记录输入“ www”；如需实现dns-example.com的解析，主机记录输入“@”）
    - 解析线路：默认为必填项，否则会导致部分用户无法解析。
    - 记录值：记录值为 CNAME 指向的域名，只可以填写域名。
    - TTL：即缓存时间。特性：数值越小，修改记录各地生效时间越快。默认为10分钟。

添加DKIM签名

概述

DKIM是一种身份验证方法，它使用公钥/私钥加密来验证电子邮件是否是由授权服务器生成的，由发送域管理员识别和配置。

联系邮箱服务商

DKIM主要是通过DNS中的TXT记录来配置实现，需要联系您的邮箱服务商获取selector Name 和TXT Record value。

操作步骤

登录云解析DNS控制台

点击域名，进入**解析设置**页面

在**解析设置**页面中，点击**添加记录**按钮，创建TXT记录。

TXT记录的添加规则，主机记录为输入default._domainkey

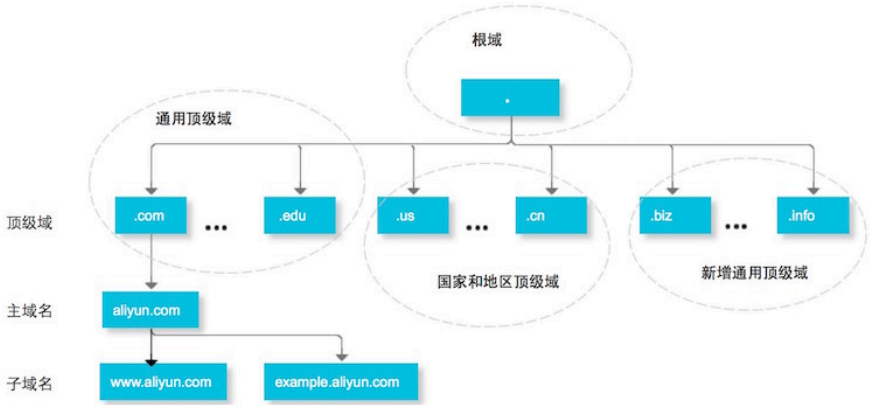
注意：此TXT记录中的“主机记录”和“记录值”均需要您联系您的邮件提供商提供，并在此输入即可。

- 点击**确定**后，可以联系您的邮箱提供商检查DKIM的有效性

如何设置子域名？

什么叫子域名

域名可以划分为各个子域，子域还可以继续划分为子域的子域，这样就形成了顶级域、主域名、子域名等。



举例：

- “.com”是顶级域名（一级域名）；
- “aliyun.com”是主域名（二级域名）；
- “example.aliyun.com”是子域名（三级域名）；
- “www.example.aliyun.com”是子域名的子域（四级域名）。

为什么要设置子域名

1、 因为一个主域名可以设置出不同的子域名，所以能够便于用户将不同的子域名应用到不同的业务中。

例如主域名是 aliyun.com，开发者则可以设置子域名 api.aliyun.com 为接口业务使用，子域名 pay.aliyun.com 为支付系统使用。

2、 实现访问者按照用户指定的子域名进行访问。

例如主域名是 aliyun.com，开发者设置子域名为 www.aliyun.com和aliyun.com 后, 访问者输入这两个域名时就可以实现访问。

如何设置子域名

1 、 首先需要确认要设置什么子域名

例如主域名为dns-example.com， 要让访问者能够实现通过 www.dns-example.com 和 dns-example.com 这两个子域名进行访问

2、 登录 云解析DNS控制台

3、 在域名解析列表中，单击 **域名** ，进入解析设置页面

4、 在解析设置页面， 单击 **添加记录**

- 记录类型：选择 **A**记录
- 主机记录：这里是您创建子域名的关键，例如需要创建 www.dns-example.com ，则在此处输入 **www** 即可； 如需创建dns-example.com，则在此处输入 **@** 即可。
- 解析线路：选择 **默认** 即可；
- 记录值： 这里输入网站服务器的IP地址（如果您不知道，可以联系您的服务器提供商或者网站空间服务商获取）
- TTL：选择 10 分钟即可。

5、 设置完毕后，您可以通过 域名检测工具 来检测解析是否已生效。

TTL 值设置方法

概述

TTL：TTL是Time-To-Live的缩写，指生存时间。而域名解析中提到的TTL值是指全国各地的localdns服务器中缓存解析结果的时间周期。

1 . 当各地的localdns服务器接接收到解析请求查询时，就会向权威DNS（例如云解析DNS）发起解析请求查询，获取到解析结果。

2 . localdns会将查询到的解析结果，保存到本地一段时间。保存的这个时间周期，就是根据TTL设置而来的。在保存的这个时间周期内，如果各地localdns再接收到此域名的解析请求查询，是不会再向权威DNS发起请求查询的，而是直接将本地保存的解析结果返回给用户。

3 . 当localdns本地缓存的时间到期后，就会清除该解析记录的缓存结果，清除后，如果各地localdns再接收到此域名的解析请求查询，则会重新向权威DNS（例如云解析DNS）发起解析请求查询，获取最新的解析结果。

应用场景

1 . 通过增大TTL值，减少DNS递归查询过程，实现提升域名解析速度。

一般情况，解析记录发生变更的频率是很低的，所以可以通过增大TTL值，让解析结果在全国各地 localdns 中的缓存时间变长，这样当用户访问网站时，就无需经过DNS的递归过程，而是最直接从客户本地DNS服务器将解析结果返回给用户，可以在一定程度上优化解析速度。

2 . 通过缩小 TTL 值，以减少更换空间IP地址时造成的不可访问时间。

当修改解析记录指向的IP地址时，因为缓存的原因，可能有些地方已经生效，但有些地方因为localdns 的缓存时间还没到期所以还未生效，造成的直接结果就是有的用户已经访问到了新的服务器地址，但有的用户还是访问的是旧服务器地址。建议方法如下：

先查看域名当前设置的 TTL 值，假设为1天。

修改 TTL 值为可设定的最小值，假设您购买的是云解析DNS旗舰版，那么可以将TTL值修改为1秒（云解析DNS版本不同，提供可设定的TTL最小值也不同，您可以参阅 版本对比 文档）。

等待1天，主要是等待全球各地的 localdns 缓存过期，缓存过期后会向权威DNS查询最新的解析结果（这里是TTL值从1天修改为1秒，所以需要等待上一次的缓存到期才会缓存此次修改的最新解析结果）

然后修改解析IP地址，因为上一步TTL值已修改为1秒，所以全国各地的localdns就能以最快的速度更新到最新的解析结果。

等全球各地的localdns都同步到最新的解析结果后（您可以通过 17测 测试全国各地localdns的解析生效情况），且测试没问题的情况下，最后对TTL值再进行修改。因为TTL设置1秒，相当于在全球各地的localdns上基本没有缓存效果，每次都需要经过DNS递归查询过程，会给解析速度造成影响。

注意： 有少部分localdns可能不遵循权威DNS的TTL设置规则，所以当您使用17测测试时，也许会发现部分地区的localdns的解析结果和设置不符，如果遇到此情况建议您再等待一段时间，然后再进行测试即可。

版本差异对比

云解析DNS不同版本提供的最低TTL值能力不同，如需购买 请点击进入

版本	免费版	个人版	企业标准版	企业旗舰版
最低TTL值	600秒	600秒	60秒	1秒

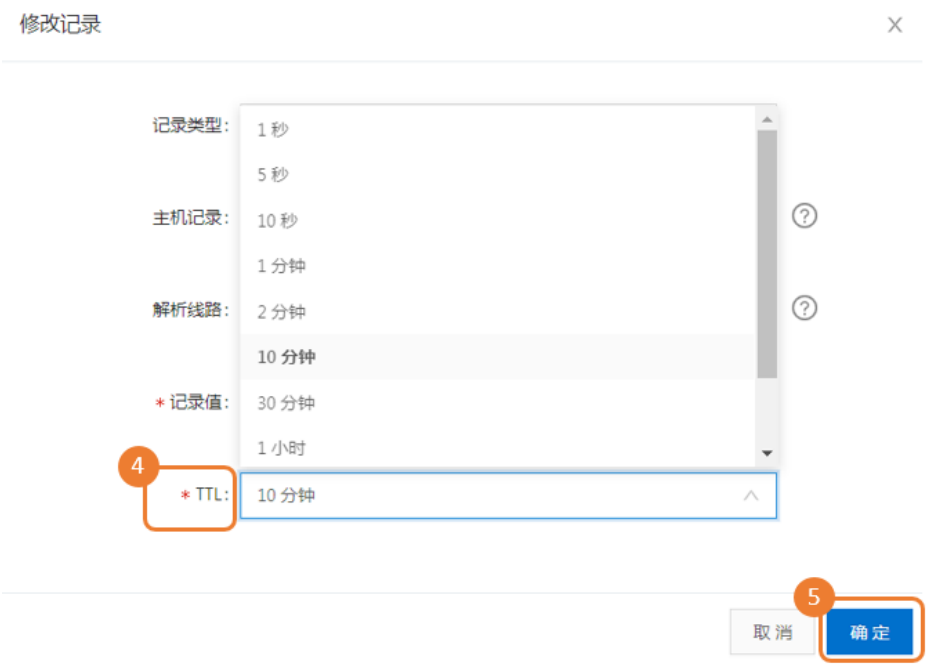
设置方法

1 . 登录 云解析DNS控制台

2 . 在域名解析页面，全部域名页签下，单击 **域名**，进入解析设置页面。

3 . 选择需要修改的解析记录，单击 **修改** 按钮

4 . 在修改记录会话框中，点击 **TTL选项框**，进行选择，并单击 **确认** 按钮。



泛解析设置方法

概述

泛解析：是指利用 “ * ” 来做子域名，实现所有的子域名都指向同一个IP地址（记录值）。例如域名 dns-example.com，设置泛解析 ***.dns-example.com** ，则该域名下所有的子域名（如 a.dns-example.com，b.dns-example.com，c.dns-example.com等）都将指向与 *.dns-example.com 相同的IP地址。

设置方法

1 . 登录 云解析DNS控制台

2 . 在域名解析页面，全部域名页签下，单击需要操作的域名，进入解析设置页面。

3 . 在解析设置页面，单击 **添加记录**按钮，在添加记录对话框中按照下图进行配置。

- 记录类型： 选择 **A** 记录
- 主机记录： 指子域名的前缀，这里输入 **“ * ”（星号）**
- 解析线路： **默认**为必选项，如未设置默认线路会造成部分用户无法解析。
- TTL值： 为缓存时间，数值越小，修改记录各地生效时间越快，选择默认配置 **10分钟。**

注意： 如TTL设置是10分钟，则等待10分钟后可以测试解析生效情况，设置完毕后您可以参阅如下关联文档。

- 泛解析解析规则
- 解析生效测试方法
- 解析生效时间

子域名级别

概述

子域名级别：域名按照层级可以分为顶级域、主域名、子域名等 。例如.com 是顶级域，主域名是example.com，子域名则是在主域名的前面添加自定义名称，例如像 www.example.com 、mail.example.com 这一类都可统称为子域名。域名的层级说明，您可以参阅 基本概念 文档。

示例说明

例如域名 dns-example.com.

- “.” 是根域
- “.com”是顶级域；
- “dns-example.com”是主域名（也可称托管一级域名），主要指企页名；
- “example.dns-example.com”是子域名（也可称为托管二级域名）；
- “www.example.dns-example.com”是子域名的子域（也可称为托管三级域名）。

设置方法

设置二级域名

1 . 登录 云解析DNS控制台

2 . 在域名解析页面，全部域名页签下，单击 **域名**，进入解析设置页面。

3 . 在解析设置页面，单击 **添加记录** 按钮，在**主机记录**参数处，输入“example” ，则二级域名为example.dns-example.com 。

设置三级域名

在解析设置页面，单击 **添加记录** 按钮，在**主机记录**参数处，输入“www.example” ，则二级域名为 www.example.dns-example.com 。

版本差异

功能/版本	免费版	个人版	企业标准版	企业旗舰版
子域名级别	5级	20级	20级	20级

修改记录

修改记录

修改记录， 主要是变更服务器的IP地址，修改记录类型/主机记录/解析线路/TTL值/也都属于修改记录的范围。

操作说明

1 . 登录云解析DNS控制台

2 . 在域名解析页面，全部域名页签下，单击 **域名**

3 . 在解析设置页面，对要修改的解析记录，单击 **修改**

删除记录

删除记录

删除记录，是指删除解析记录。删除后，会直接导致业务不可用，请谨慎操作。建议删除记录前，通过**导入/导出**功能将解析数据导出，做好备份工作。

设置方法

1 . 登录 云解析DNS控制台

2 . 进入域名解析页面，在全部域名页签下，单击 **域名**

3 . 在解析设置页面，对单条记录，单击 **删除** 按钮，确认删除会话框提示单击 **确认**按钮。

暂停/启用记录

暂停/启用记录

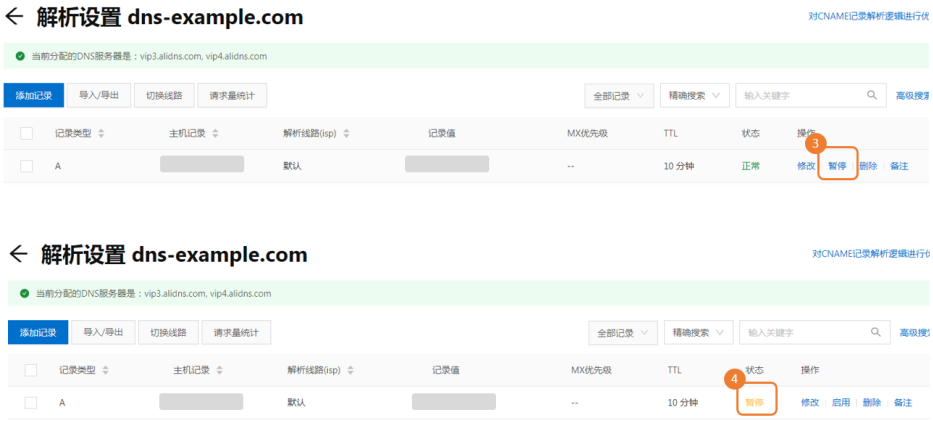
- 暂停记录：操作后解析请求过程无法查询到此条记录，暂停后解析生效时间是TTL的缓存时间。
- 启用记录：对于暂停的记录，可以恢复使用，启用后解析立即生效。

设置方法

1 . 登录 云解析DNS控制台

2 . 在域名解析页面，全部域名页签下，单击 **域名**

3 . 在解析设置页面，对需要操作的解析记录，单击 **暂停** 按钮，同时状态会显示为 **暂停**



4 . 在解析设置页面，对需要操作的解析记录，单击 **启用** 按钮恢复解析，同时状态会显示为 **正常**

注意： 暂停/启用记录，解析生效的测试您可以参阅 **解析生效测试方法** 文档

导入/导出记录

导入记录

导入记录：指将准备好的解析数据，导入到云解析DNS控制台中。

规则说明

1 . 导入记录分为增量更新 和 全量更新

增量更新：是指在进行导入操作时，已有的解析记录保持不变，然后添加新增的解析记录。

全量更新：是指在进行导入操作时，删除已有的所有解析记录，然后添加文件中的解析记录。

2 . 上传文件格式支持xls、xlsx或者zone文件，其中zone文件可以直接导入使用，而xls、xlsx请登录云解析控制台 **下载模板** 使用。

3 . 每次上传解析记录的最大上限为1000条，超出的记录不能正常导入成功。如果解析记录大于1000条，请拆分为多个文件并进行上传。

设置方法

1 . 登录 云解析DNS控制台

2 . 在域名解析页面，全部域名页签下，单击 **域名**

3 . 在解析设置页面，单击 **导入/导出** 按钮

4 . 在导入/导出页面，导入记录页签下，选择适合您的导入记录方式，单击 **上传文件** 按钮。

5 . 导入完成后，可在当前页面查看到导入结果。如单击 **完成** 按钮后，则会返回导入记录页面，导入结果数据将被清除。

模板说明

上传文件格式支持xls、xlsx ，请登录云解析控制台 **下载模板** 使用。需要您将从其他平台导出的解析数据，按

照此模板规则进行处理。

1 . 模板中对常用记录的填写方法给予了示例可供您参考。

2 . 模板中的示例是做参考使用的，在上传文件之前请删除这些示例。

3 . 模板中的解析线路填写方法，您可以参阅 智能解析 文档 。

4 . 模板支持记录的备注信息导入，备注信息输入字符上限 50个字符，超出部分不会导入。

5 . 模板支持记录的状态导入，记录状态支持输入暂停/正常，未输入代表 “正常” 。

记录类型	主机记录	解析线路	记录值	MX优先级	TTL值	状态(暂停/正常)	备注
A	www	默认	1.1.1.1		600	正常	示例，使用时请删除
A	www	移动	1.1.1.1		600	暂停	示例，使用时请删除
A	www	电信	1.1.1.1		600	正常	示例，使用时请删除
A	www	联通	1.1.1.1		600	正常	示例，使用时请删除
AAAA	www	默认	ff03:0:0:0:0:0:0:c1		600	正常	示例，使用时请删除
CNAME	@	默认	www.aliyun.com		600	正常	示例，使用时请删除
MX	@	默认	mx1.qiye.aliyun.com	5	600	正常	示例，使用时请删除
TXT	@	默认	v=spf1 include:spf1.staff.mail.aliyun.com -all		600	正常	示例，使用时请删除

导出记录

在导入/导出页面，导出记录页签下，选择**导出文件类型**，单击 **立即导出** 按钮

记录分组管理

概述

记录分组管理：可以将解析记录通过分组的方式进行归类和管理

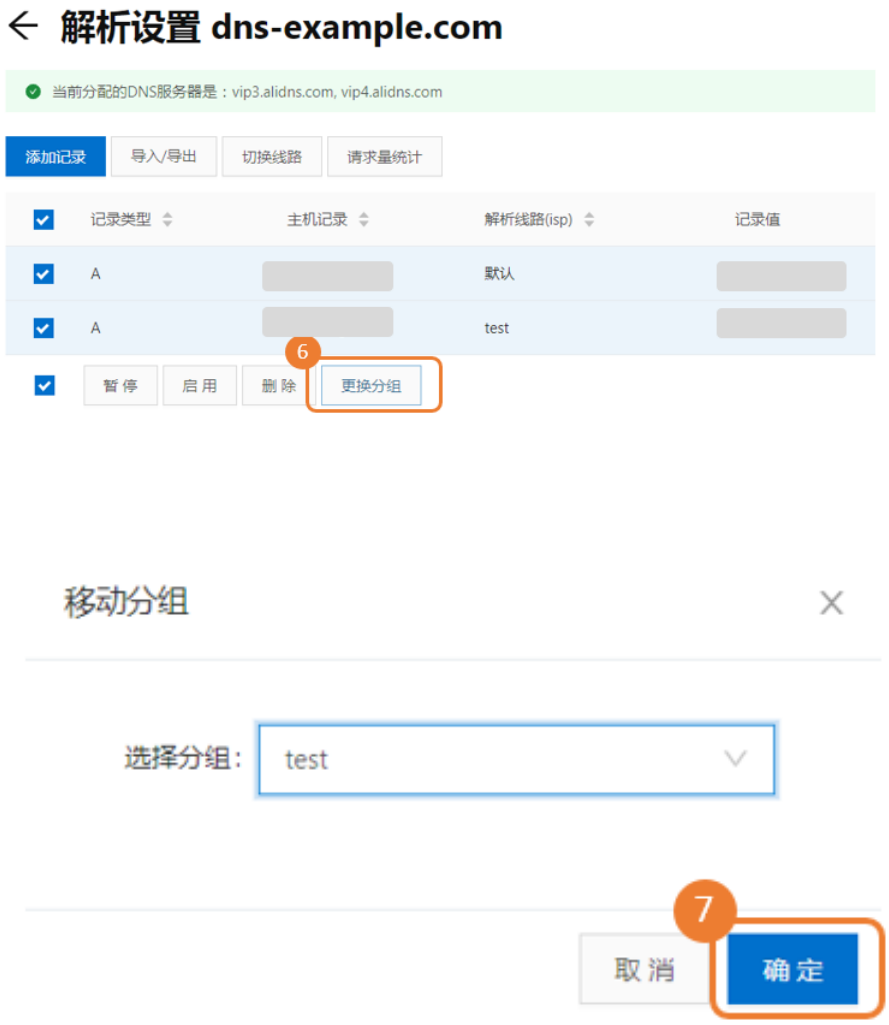
设置方法

1 . 登录云解析控制台。

2 . 在**域名解析**页面，全部域名页签下，单击 **域名** ，进入**解析设置**页面

3 . 在解析设置页面，点击 **全部记录** 下拉框，单击 **“+”** ，输入分组名称，点击 **“”** 保存，完成创建分组。

4 . 选中解析记录，单击 **更换分组** ，将选中的解析记录移动到创建的分组下，单击 **确定** 按钮。



5 . 将解析记录移动到创建的分组下，可以查看到该分组下的记录数量。

6 . 单击 分组名称后， 可查看属于该分组下的解析记录。

7 . 点击分组名称后的 编辑和删除图标，可以修改或删除此分组。

产品规则

- “全部记录”属于系统分组，统计的是选中域名下的全部解析记录数量，系统分组名称不支持修改和删除。
- 解析记录和记录分组的归属关系不受解析记录修改影响。
- 删除分组，则该分组下的解析记录会同步从该分组中清空，可通过“全部记录”分组来查看解析记录。
- 记录分组创建最大上限100个。
- 记录分组的名称的输入限制20个字符
- 记录分组管理可添加的解析记录数量不限
- 记录分组管理操作不支持日志查询

记录检索

概述

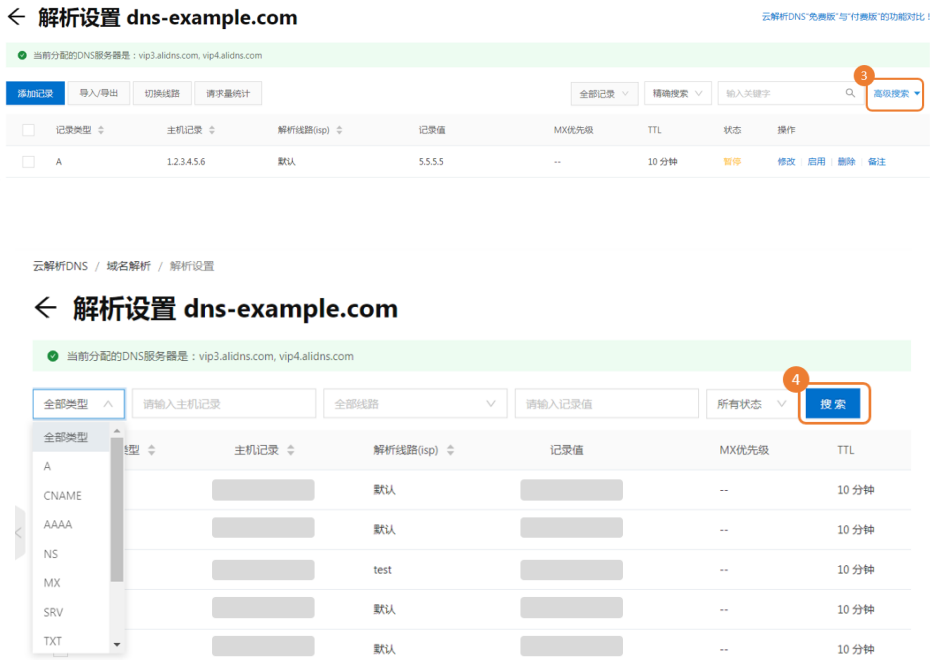
记录检索： 云解析DNS提供解析记录的高级检索功能，对于拥有大量解析记录的用户，可以 通过**记录类型、主机记录、解析线路、记录值、状态** 快速检索出指定的解析记录。

使用方法

1 . 登录 云解析DNS控制台

2 . 在域名解析页面，全部域名页签下，单击 **域名** ，进入解析设置页面。

3 . 单击 **高级搜索** 按钮，在 **记录类型、主机记录、解析线路、记录值、状态** 检索项中 根据您的需求，选择或输入对应的检索条件。检索方法支持单个检索条件、组合检索条件使用。



切换线路

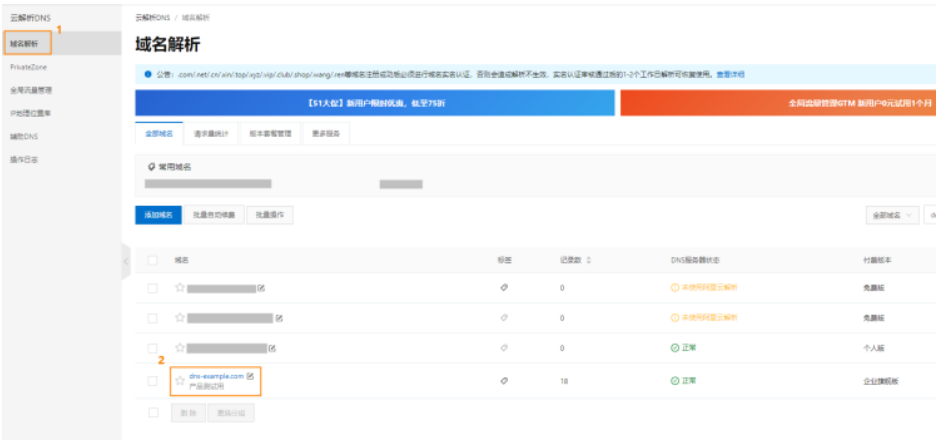
概述

结合云解析智能解析功能，为购买了云解析企业（标准、旗舰）版实例的用户提供了两种解析线路类型：运营商线路类型和地域线路类型。

设置方法

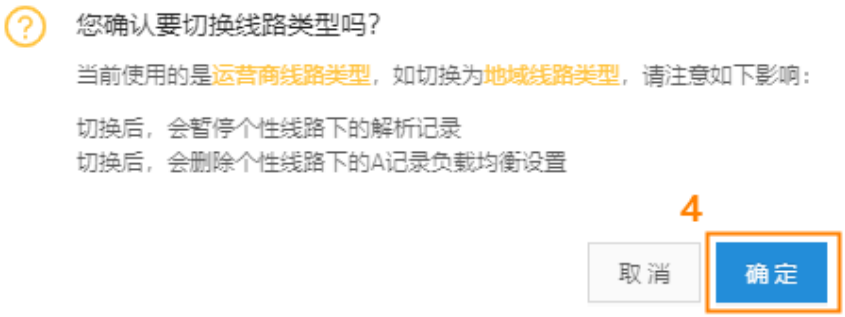
1 . 登录云解析DNS控制台。

2 . 在域名解析页面，全部域名页签下，单击域名，进入解析设置页面。



3 . 单击切换线路，可以查看到当前解析线路类型，或者查看解析线路列中括号的值：解析线路（isp）或者解析线路（地域）。

4 . 在切换线路设置页面，单击确定，完成线路切换。



注意：

当切换回原有线路类型，暂停的个性线路的解析记录**不会自动启用**，需要您**手动启用**

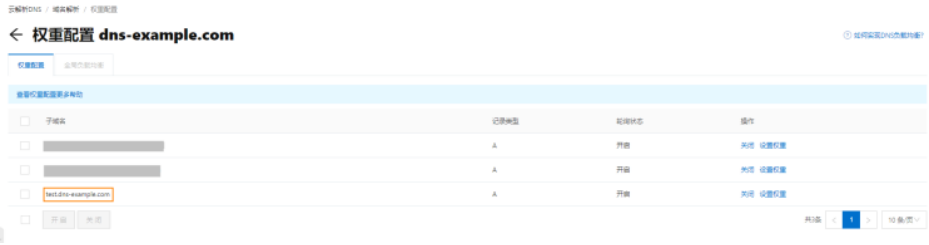
切换线路类型后，会暂停个性线路下的解析记录。

切换前：

切换后：

- 切换线路类型后，会删除个性线路下的A记录负载均衡设置

切换前：



切换后：

智能DNS解析

智能解析

概述

传统DNS解析，不判断访问者来源，会随机选择其中一个IP地址返回给访问者。而智能DNS解析，会判断访问者的来源，为不同的访问者智能返回不同的IP地址，可使访问者在访问网站时可获取用户指定的IP地址，能够减少解析时延，并提升网站访问速度的功效。

1 . 传统DNS解析示例

例如域名www.dns-example.com，有三台服务器，分别是联通IP，移动IP，电信IP，DNS解析配置如下：

- 将域名 指向 联通IP地址 （ 1.1.1.1 ）
- 将域名 指向 移动IP地址 （ 2.2.2.2 ）
- 将域名 指向 电信IP地址 （ 3.3.3.3 ）

可实现的解析效果：

传统DNS解析不判断访问者的来源，会将1.1.1.1、2.2.2.2、3.3.3.3三个地址全部返回给访问者的本地DNS，由访问者的本地DNS通过随机或者优选的方式将其中一个IP地址返回给访问者，传统DNS解析有可能会造成访问者跨网访问。

2 . 智能DNS解析示例

例如域名www.dns-example.com，有三台服务器，分别是联通IP，移动IP，电信IP，DNS解析配置如下：

- 解析线路配置 **默认线路** 指向 联通IP地址 （ 1.1.1.1 ）
- 解析线路配置 **移动线路** 指向 移动IP地址 （ 2.2.2.2 ）
- 解析线路配置 **电信线路** 指向 电信IP地址 （ 3.3.3.3 ）

可实现的解析效果

云解析会判断访问者的来源，为来源于移动运营商的访问者云解析返回2.2.2.2的解析地址，为来源于电信运营商的访问者云解析返回3.3.3.3的解析地址，其他来源的访问者云解析返回1.1.1.1的解析地址

实现原理

云解析是通过识别LOCALDNS的IP，来判断访问者来源。

如客户端LOCALDNS支持EDNS

因为云解析DNS支持 edns-client-subnet，所以在获取访问者来源IP时，优先获取 edns-client-subnet 扩展

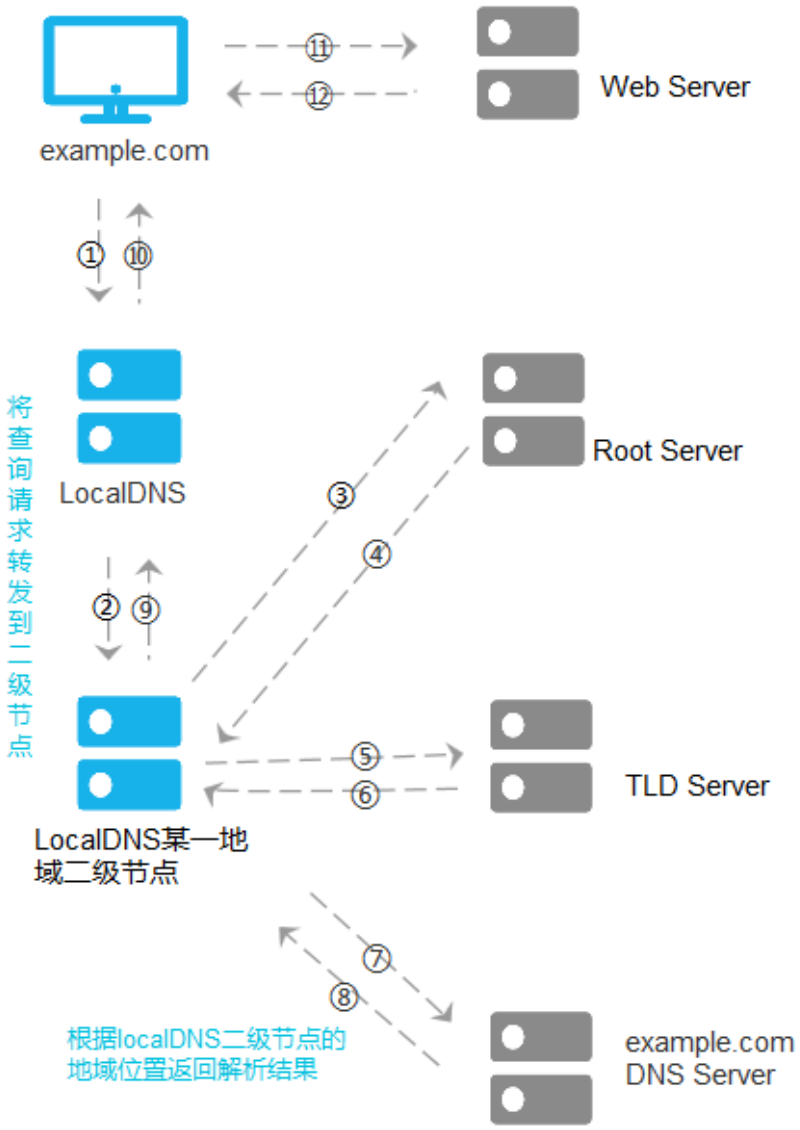
里携带的IP ，如果edns-client-subnet 扩展里存在IP，云解析DNS会以该IP来判断访问者的地理位置 ；如果不存在，则以 localdns出口ip来判断访问者的地理位置。

如客户端localDNS不支持EDNS

localDNS会迭代请至求云解析DNS，云解析DNS根据访问者本地DNS服务器的出口IP来判断访问者的地址位置，实现智能解析。

如客户端LocalDNS变相支持EDNS

用户发起DNS请求，递归到localDNS，则localDNS将本次请求发送到二级节点，通过二级节点向云解析DNS发起请求，此时**云解析DNS会根据localDNS二级节点的地域位置返回具体的细分线路解析结果。**



设置方法

1 . 登录云解析DNS控制台

2 . 在域名解析页面，全部域名页签下，单击 **域名**，进入 解析设置页面。

3 . 在解析设置页面，单击 **添加记录** 按钮

示例：

如果您拥有3台服务器，分别位于 电信、联通、移动，**添加记录**时，在**解析线路**选择时，按如下配置：

- 默认线路：电信IP（10.10.10.10）
- 联通线路：联通IP（1.1.1.1）
- 移动线路：移动IP（2.2.2.2）


添加记录
记录类型：
A- 将域名指向一个IPV4地址
主机记录：
www
.dns-example.com
4
解析线路：
默认 - 必填！未匹配到智能解析线路时，返回【默认】线路...
* 记录值：
10.10.10.10
* TTL：
10 分钟
取 消
确 定


添加记录
记录类型：
A- 将域名指向一个IPV4地址
主机记录：
www
.dns-example.com
5
解析线路：
中国联通
子级线路（细分选项，非必填）
* 记录值：
1.1.1.1
* TTL：
10 分钟
取 消
确 定

实现效果则是：

云解析会智能判断出访问者的来源，并返回配置的记录；

- 例如访问者来源于联通运营商，云解析则智能返回联通的IP地址1.1.1.1。
- 访问者如果来源于移动运营商，云解析则返回移动IP2.2.2.2。
- 访问者来源不属于联通和移动的运营商，则云解析返回默认线路配置的电信IP地址（10.10.10.10）。

以上解析线路的配置结果，可实现**根据不同的访问者来源智能返回指定的IP地址。**

支持线路

云解析DNS当前能够识别出用户来源的解析线路如下：

线路名称	线路省份
默认	全局
中国联通/中国电信/中国移动/中国教育网	山东、江苏、安徽、浙江、福建、上海 广东、广西、海南 湖北、湖南、河南、江西 北京、天津、河北、山西、内蒙古 宁夏、新疆、青海、陕西、甘肃 四川、云南、贵州、西藏、重庆 辽宁、吉林、黑龙江
中国鹏博士	安徽、北京、重庆、福建、甘肃 广东、广西、贵州、海南、河北、 黑龙江、河南、湖北、湖南、江苏、 江西、吉林、辽宁、内蒙古、宁夏、 青海、陕西、山东、上海、山西、

	四川、天津、新疆、西藏、云南、浙江
中国广电网	黑龙江、山东、内蒙古、宁夏、湖南、 贵州、青海、辽宁、河南、吉林、 甘肃、河北、江苏、安徽、福建、 海南、湖北、陕西、上海、陕西、 四川、天津、西藏、新疆、浙江、 北京、重庆、广东、广西、江西、云南

线路名称	大洲	国家（地区）
境外	-	-
境外	大洋洲	澳大利亚，新西兰，斐济，帕劳
境外	亚洲	阿联酋，香港，印度尼西亚，印度， 日本，柬埔寨，韩国，老挝， 缅甸，澳门，马尔代夫，马来西亚， 尼泊尔，菲律宾，沙特阿拉伯，新加坡， 泰国，台湾，越南，蒙古， 巴基斯坦，朝鲜，哈萨克斯坦，乌兹别克斯坦， 土耳其，伊朗，伊拉克，以色列， 科威特，黎巴嫩，卡塔尔
境外	欧洲	奥地利，瑞士，德国，西班牙， 法国，英国，意大利，荷兰， 俄罗斯，瑞典，捷克，比利时， 爱尔兰，丹麦，芬兰，冰岛， 匈牙利，波兰，斯洛伐克，白俄罗斯， 立陶宛，乌克兰，保加利亚，克罗地亚， 葡萄牙，罗马尼亚，斯洛文尼亚
境外	北美洲	加拿大，墨西哥，美国
境外	南美洲	阿根廷，巴西，哥伦比亚、委内瑞拉、 厄瓜多尔、秘鲁、玻利维亚、智利、 巴拉圭、乌拉圭
境外	非洲	南非，埃及，尼日利亚，安哥拉， 加纳，科特迪瓦，肯尼亚，塞舌尔， 阿尔及利亚，喀麦隆，摩洛哥，塞内加尔

线路名称	地区	省份
默认	-	-
中国地区	华东	山东、江苏、安徽、江西、浙江

		、福建、上海
中国地区	华南	广东、广西、海南
中国地区	华中	湖北、湖南、河南
中国地区	华北	北京、天津、河北、山西、内蒙古
中国地区	西北	宁夏、新疆、青海、陕西、甘肃
中国地区	西南	四川、云南、贵州、西藏、重庆
中国地区	东北	辽宁、吉林、黑龙江

版本对比

云解析DNS不同版本提供的解析线路不同，参考如下：

功能/版本	免费版	个人版	企业标准版	企业旗舰版
智能解析	联通/电信/移动/教育网/境外	联通/电信/移动/鹏博士/教育网/广电网，境外	分省（联通/电信/移动/鹏博士/教育网/广电网），境外/大洲/国家（地区）	包含所有固定智能解析线路，支持自定义IP范围解析

常见问题

您可以参阅 DNS解析设置FAQ 文档。

搜索引擎线路

概述

搜索引擎是指搜索引擎爬虫（又被称为网页蜘蛛，网络机器人），是一种按照一定的规则，自动地抓取万维网信息的程序或者脚本。

应用场景

网站被搜索引擎爬虫访问会耗费服务器的流量和带宽，可通过在**搜索引擎线路**专门指向一个服务器地

址，从而有效的控制蜘蛛的爬取路径。

临时闭站做SEO收录排名保护，可通过**搜索引擎线路**设置个搜索引擎专线，这样虽然站点关闭，但是蜘蛛爬虫还可以正常抓取网站信息，从而达到降低对站点SEO收入排名影响。

设置方法

例如为百度蜘蛛爬虫，指向专属的服务器IP地址2.2.2.2。此设置的效果是：百度蜘蛛会和服务器2.2.2.2 建立连接，访问并收集网页上的内容、图片等信息，使用户能在百度搜索引擎中搜索到您网站的网页、图片、视频等内容。

1 . 登录 云解析DNS控制台。

2 . 在域名解析页面，全部域名页签下，单击域名，进入解析设置页面。

3 . 在解析设置页面，单击 **添加解析**，点击解析线路的下拉框，选择需要配置的搜索引擎线路类型。

常见问题

1、 搜索引擎线路需要单独收费吗？

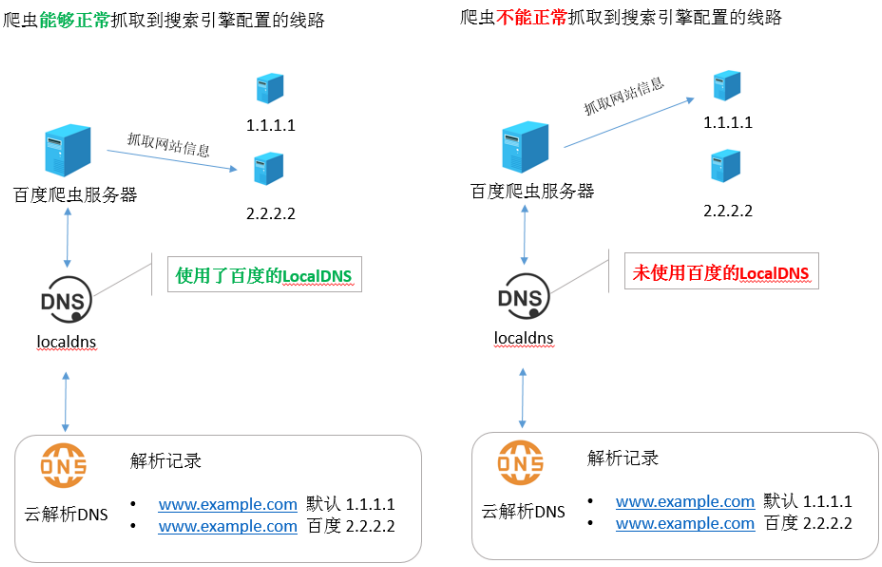
答： 免费。

2、搜索引擎线路都支持哪些搜索引擎商？

答：搜索引擎、谷歌、百度、必应、有道

3、为什么会出现搜索爬虫没有抓取到搜索引擎配置的线路？

答：以百度爬虫举例，如果百度爬虫服务器的本地DNS使用的不是百度的localdns，那么当DNS查询时，就会出现百度搜索爬虫无法抓取到搜索引擎配置的线路。如下图示例



云解析是通过识别LOCALDNS的IP，来判断访问者来源

自定义线路

概述

自定义线路，是可以定制DNS向来源于某个特殊IP段的DNS查询返回特定的IP地址。

设置方法

1 . 登录 云解析DNS控制台

2 . 在域名解析页面，全部域名页签下，单击 **域名**，进入 解析设置 页面。

3 . 在解析设置页面，左侧目录项中单击 **自定义线路**， 进入到自定义线路页面，单击 **添加线路**。

4 . 单击 添加线路 后，在 自定义线路 会话框中， 创建一个 **线路名称** 为test的自定义线路、并根据下列规则在 **IP地址范围** 输入框中输入IP段。

IP地址范围输入规则：

- IP与IP之间用 中横线 “-” 间隔；
- 每行一个IP段，最少1行最多50行；
- 只有一个IP填写 IP1-IP1，不同IP段不能交叉；
- 填写的IP段是本地机器使用DNS的出口IP地址，不是本地机器的出口IP地址。
- DNS的出口IP地址收集方法一：需联系所在网络的管理员，获取详细DNS出口IP地址。
- DNS的出口IP地址收集方法二：多执行几次命令获取IP地址 dig +short TXT whoami.ds.akahelp.net 或者 nslookup -q=txt whoami.ds.akahelp.net。

5 . 在左侧目录项中 单击 **解析设置**，进入解析页面后，并单击 **添加记录** 按钮，在添加记录的对话框中，解析线路选择在步骤4中创建的 **test** 线路。

修改DNS服务器

概述

修改DNS服务器，是指 **修改域名注册商处登记的DNS服务器名称**，该功能是由域名注册商提供。

操作指南

在阿里云注册的域名，DNS一般默认为阿里云解析DNS提供的DNS服务器地址。如果您有自己注册成功的

DNS服务器，且需要将域名的DNS修改为您自己的DNS，或将DNS修改为其他服务商的DNS，您可以参阅 域名DNS修改 文档 。

解析生效时间

修改DNS服务器，解析生效时间取决于本地DNS中缓存的域名DNS服务器名称的TTL时间，一般默认为48小时。解析生效原理

权重配置

概述

云解析DNS权重配置，指在DNS服务器中为同一个主机记录配置多个IP地址，在应答DNS查询时，所有IP地址按照预先设置的权重进行返回不同的解析结果，将解析流量分配到不同的服务器上，从而达到负载均衡的目的。

启用条件

权重配置的启用条件是域名下存在相同的主机记录、相同解析线路的多条A记录、CNAME记录、AAAA记录。

规则限制

权重配置仅适用于记录类型为“A记录、CNAME记录、AAAA记录”，且是**相同主机记录**、**相同线路**下的**多个记录值。具体使用规则如下：

限制	支持	不支持
记录类型	A记录、CNAME记录、AAAA记录	其他记录类型
记录状态	处于 **启用** 状态的记录	处于 **暂停**、**锁定** 状态的记录，以及泛解析记录
解析记录数量限制	单域名单线路下允许配置权重的最大解析记录数量：免费版支持10个，付费版支持90个。	—
权重值规则	权重值允许设置0-100，默认权	—

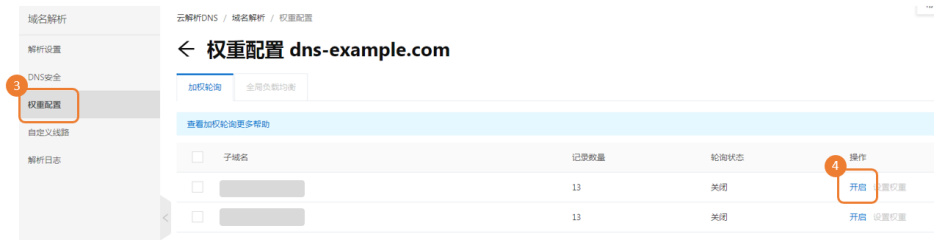
	重值比例为1:1 . 支持权重值设置为 “0” ，则云解析DNS不返回此解析记录值	
解析线路	可对默认线路配置带权重的A记录，也可以对具体的线路配置。**说明**：不同线路中，其权重相互独立。	针对不同线路，开启/关闭负载均衡。

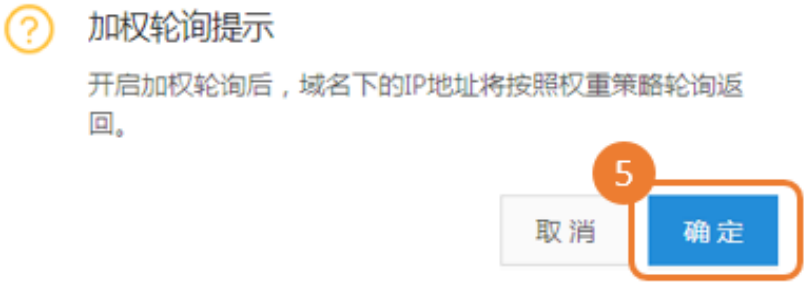
设置方法

1 . 登录到 云解析DNS控制台。

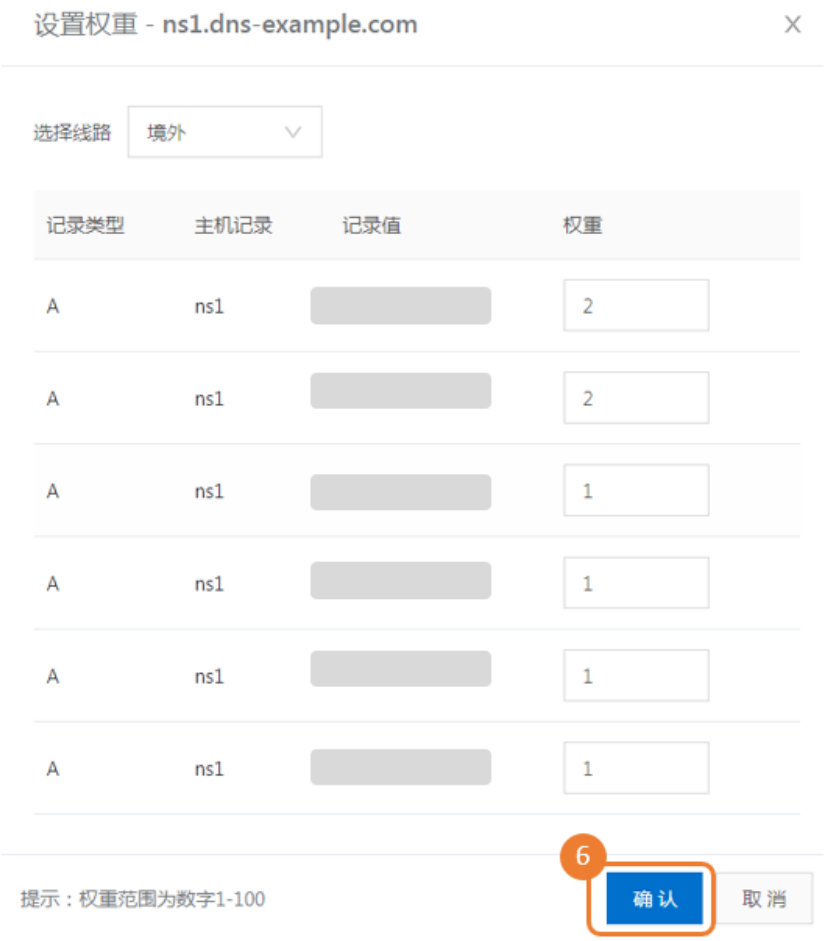
2 . 在域名解析页面，全部域名页签下，单击 **域名** ，进入解析设置页面。

2 . 在解析设置页面，点击左侧导航 **权重配置**，进入权重配置页面，单击 **开启** 按钮，一般开启是默认权重（1:1：1）的配置，在DNS请求应答中，云解析DNS会按照1:1:1的权重策略返回IP地址。





3 . 在权重配置页面，加权轮询页签下，单击 **设置权重** 按钮，配置权重后，在DNS请求应答中，云解析DNS会按照预先设置的权重返回IP地址。



实现效果

未开启权重配置的效果

假设您有 3 台服务器（IP 地址分别为1.1.1.1、2.2.2.2、3.3.3.3）提供同一服务（1个域名），且在解析设置中对应如下 3 条 A 记录：

记录类型	主机记录	解析线路	记录值
A	www	默认	1.1.1.1
A	www	默认	2.2.2.2
A	www	默认	3.3.3.3

当Local DNS访问云解析DNS，**云解析DNS将这3个解析记录全部返回给Local DNS**，Local DNS再将所有的IP地址返回给网站访问者，网站访问者的浏览器会随机访问其中一个IP。

在无DNS负载均衡的权威DNS中，这种方法能够在一定程度上减轻单台服务器的压力，但它不能区分服务器的差异，不能反映服务器的当前运行状态。

默认权重效果

权重配置开启，默认配置的是1:1:1权重，**云解析DNS会根据（默认权重1:1:1），轮询3个A记录，依次返回3个IP地址**，以响应网站访问者的请求。DNS解析结果如下所示：

```
User1 访问，返回 1.1.1.1
User2 访问，返回 2.2.2.2
User3 访问，返回 3.3.3.3
User4 访问，返回 1.1.1.1
User5 访问，返回 2.2.2.2
User6 访问，返回 3.3.3.3
……
```

权重设置效果

权重配置**开启**后，进行**权重设置**，在DNS请求应答中，IP地址按照预先设置的权重进行返回，可以实现将解析流量按照权重进行分配。例如，将上述3条解析记录的权重比设置为2:1:1时，则DNS解析结果如下所示：

```
User1 访问，返回 1.1.1.1
User2 访问，返回 2.2.2.2
User3 访问，返回 3.3.3.3
User4 访问，返回 1.1.1.1
User5 访问，返回 1.1.1.1
User6 访问，返回 2.2.2.2
……
```

特殊说明：

如果您在测试过程中，发现偶尔会出现DNS解析结果和权重配置不符的现象，这属于一种正常现象。因为加权

轮询是一个粗粒度的解析流量调度方式，它针对的是localdns的请求，而localdns在TTL时间内是只会向权威DNS（云解析DNS）请求一次。

例如您的域名被上海和北京两个地区的用户访问，假设上海用户使用的是localdnsA，北京用户使用到的是localdnsB。 当localdnsA和localdnsB向云解析DNS发起查询请求的时候，云解析DNS会按照用户配置的加权策略返回，但是在TTL时间内，使用相同localdns下的所有用户获取到的都是同一个解析结果。

DNS安全

概述

DNS是互联网的重要基础，例如WEB访问、Email服务在内的众多网络服务都和DNS息息相关，DNS的安全则直接关系到整个互联网应用能否正常使用。

云解析DNS安全针对DNS的DDoS攻击提供防护能力

DDoS（Distributed Denial of service）攻击通过僵尸网络利用各种服务请求耗尽被攻击网络的系统资源，造成被攻击网络无法处理合法用户的请求。主要表现为**Flood攻击**：通过发送海量DNS查询报文导致网络带宽耗尽而无法传送正常DNS 查询请求

云解析DNS安全提供的防御等级包含如下

DNS攻击基本防御：针对付费版本绑定的所有域名，提供基础DNS攻击保护能力，基础DNS攻击防御上限不超过每秒1000万次，适用于一般情况下的DNS攻击预防保障

DNS攻击全力防御：针对版本绑定的所有域名，提供全面的DNS攻击保护能力，能承受每秒过亿次的DNS攻击，适用于频繁受到DNS攻击时进行全力保护。

设置方法

DNS安全不需要单独做配置，以下为DNS防护数据的查看方法。

1 . 登录到 云解析DNS 控制台。

2 . 在 域名解析页面，全部域名页 签下，单击 **域名**，进入 解析设置页面

3 . 在 解析设置页面，左侧导航栏点击 **DNS安全**，进入 DNS安全页面

4 . 在 **DNS安全** 页面，您可以查看以下信息：

防护状态说明

在发生DNS查询攻击时，DNS防护状态包含：清洗开始、清洗结束、黑洞开始、黑洞结束。

> 清洗开始：如果DNS安全系统检测到用户域名持续遭受到大量异常请求，则会启用清洗策略，清洗策略是指对异常请求不做DNS查询响应。

清洗结束：如果DNS安全系统检测到用户域名遭受的异常请求正在减少，则会停止清洗策略。

黑洞开始：如果DNS安全系统检测到用户域名持续遭受到大量异常请求，且超过域名当前版本提供的安全防御上限，则会对该域名停止解析服务。

黑洞结束：域名解析在黑洞策略期间，如果DNS安全系统检测到用户域名遭受的异常请求恢复到安全防御上限内，则会自动恢复解析，恢复后需要等待TTL解析生效时间。

请求量统计

概述

请求量统计，统计的是从运营商localdns向云解析DNS发起的DNS查询的请求次数，此统计不等同于网站访问量，但是可以侧面反映出网站访问的情况。云解析DNS请求量统计支持域名、子域名维度。

产品限制

请求量统计仅限付费版DNS用户使用。 立即购买 付费版DNS

请求量统计数据最长支持90天查询。

应用场景

请求量统计在DNS迁移时，可以帮助用户侧面预测解析流量迁入云解析DNS的进度。

请求量统计可以帮助用户侧面评估业务的健康性，例如当请求量突然性增高或降低，都可能是业务运行出现了异常。

请求量统计可以作为衡量业务发展的一种指标，通过请求热度的分析，可以帮助用户盘点域名（业务资源）。

使用方法

1 . 登录 云解析DNS控制台

2 . 在域名解析页面，单击 **请求量统计** 页签，进入解析量统计页面。

3 . 在解析量统计页面，可以查询绑定付费版DNS的主域名的请求量统计数据。

4 . 在解析量统计页面，主域名请求量数据支持多种检索方法。

A ：单击 **无解析量** 按钮，可以快速检索出7天解析请求量为0的主域名。

B ：进入解析量统计页面，默认统计的是昨天的解析请求量数据；同时提供今天、7天、15天的快速查询项。

C ：支持自定义设置时间段，查询域名的解析请求量。

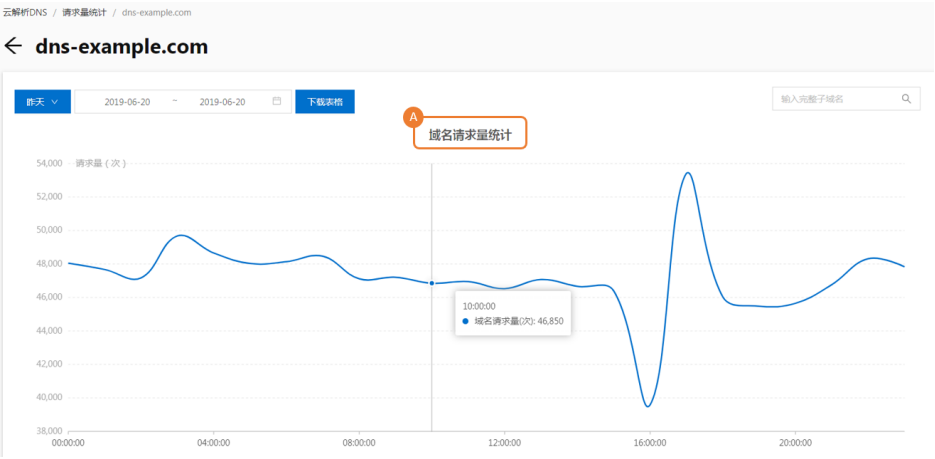
D ：支持主域名解析请求量统计的数据下载功能。

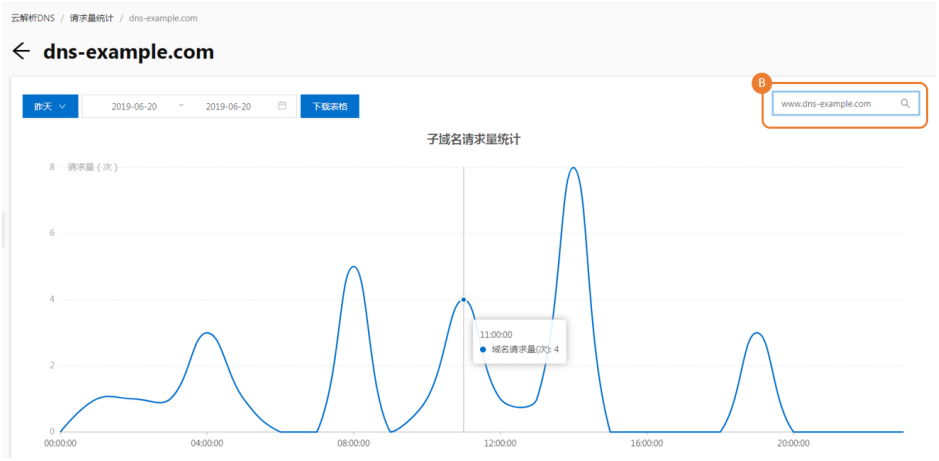
5 . 在操作下，单击 **详情** 按钮，进入子域名解析量请求统计页面。

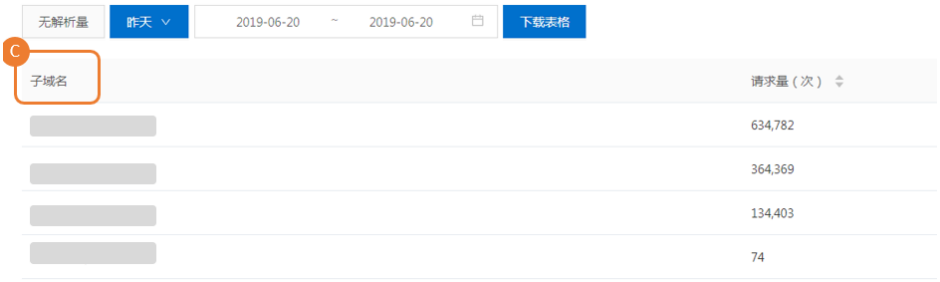
A ：进入子域名请求量统计页，默认统计的是 昨天 和 主域名的实时统计数据。

B ：输入框必须输入完整子域名，例如”www.dns-example.com” ，则展示子域名的实时统计数据。清空输入框，再单击**搜索图标**，则查询的是主域名请求量的实时数据

C ：默认查询的是 昨天 和 主域名下的全部子域名的解析请求量统计数据。







批量操作

批量添加域名

概述

批量添加域名： 是指将非阿里云注册域名，批量添加到云解析DNS的域名解析列表中。（阿里云注册域名无需添加，云解析会自动添加到域名解析列表中）

批量添加域名功能包含 **手动输入域名**、 **文件导入域名** 两种方法，其中如若添加的域名已被其他阿里云账号管理，可通过 **找回域名** 功能 发起批量找回。

手动输入域名

1 . 登录云解析DNS控制台。

2 . 在域名解析页面，全部域名页签下，单击 **批量操作** 按钮。

3 . 在 批量操作 页面， 批量添加域名页签下 ，选择 **手动输入域名**，在输入框中可直接输入需要添加的非阿里云注册域名，最后单击 **添加** 按钮。

4 . 批量任务提交后，任务处理结果 可在 **批量操作记录页签** 下，单击 **下载详情日志** 查看。

文件导入域名

1 . 选择 **批量添加域名** 页签，选中 **文件导入域名**

2 . 在 **文件导入域名** 页面中，单击 **下载模板** ，在 已下载的 **模板** 中，根据 模板示例 的格式填写。

3 . 点击 **上传文件** 按钮，选择填写完成的文件并上传。

4 . 批量任务提交后，在批量操作记录页签下，点击 **下载详情日志**

找回域名

找回域名：是指在批量添加域名时，发现域名已被其他阿里云账号添加，可以通过找回域名功能，批量将域名

找回到本账号管理。

1 . 在 **批量添加域名** 页签中，选中 **找回域名**功能项。

2 . 根据页面第一步，输入需要找回的域名，每行1个。

3 . 根据页面第二步，按照云解析提供的 **主机记录**、 **记录值**， 到各个域名当前所在的DNS厂商为域名添加 **txt记录**

4 . 点击 **找回** 按钮，提交批量域名找回任务。

5 . 批量域名找回任务的处理结果，在 批量操作记录页签下，点击 **下载详情日志**

使用限制

1 . 适用于非阿里云注册域名使用。（阿里注册的域名可使用 “批量管理域名-批量转移至其他账号”功能来进行域名DNS解析权限的跨账号转移）。

2 . 适用于找回已注册的域名，未注册的域名不能添加找回。

3 . 找回域名后，域名原有的解析记录将被删除，若域名绑定过付费版DNS则会同时解除绑定关系。

批量管理域名

概述

批量管理域名包含如下功能：

- 批量删除域名
- 更换分组
- 批量转移至其他账号

批量删除域名

批量删除域名：是指可以批量删除域名解析列表中的非阿里云注册域名。

使用限制

阿里云注册域名，不支持从云解析中删除。 第三方注册域名，从云解析中删除后，域名的解析记录会同步删除。 如删除的域名已绑定企业版DNS实例，删除后将解除绑定关系，企业版DNS功能将停止服务。

设置方法

1 . 登录云解析DNS控制台，

2 . 在域名解析页面，全部域名页签下，点击 **批量操作** 按钮

3 . 在批量操作页面，选批量管理域名页签， 输入即将要删除的域名，并单击 **批量删除域名** 按钮

4 . 批量删除的结果，在批量操作记录页签下，单击 **下载详情日志** 查看

更换分组

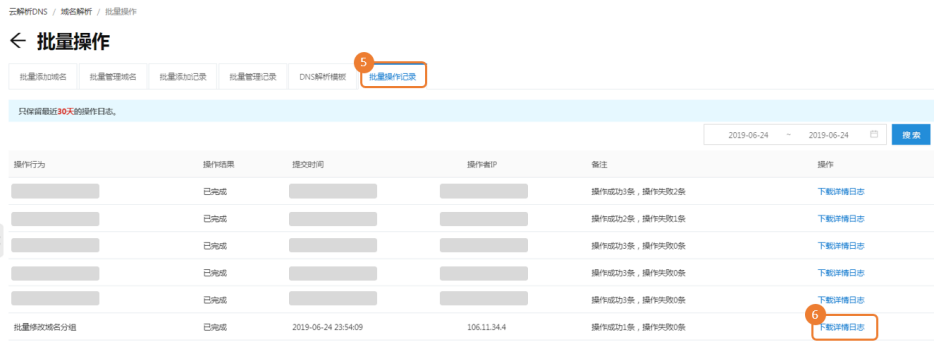
更换分组 是指 批量更换已有域名的分组。

设置方法

1 . 在批量操作页面，**批量管理域名** 页签下， 输入即将更换分组的域名，单击 **更换分组** 按钮。

2 . 在 **移动分组** 对话框中，选择 **目标分组** 然后单击 **确定。**

3 . 更换分组结果，在批量操作记录页签下，单击 **下载详情日志** 查看



批量转移至其他账号

批量转移至其他账号： 是指将将本账号下的域名解析转移至其他帐号管理。

规则

批量将域名转移至其他账号后，新帐户对域名解析有管理权限。权限包括DNS记录管理，但不包含域名注册相关管理权限。 域名解析转移至其他帐户后，可以通过批量添加域名，将域名解析再次找回本帐户。

设置方法

1 . 在批量操作页面，批量管理域名页签下， 输入需要批量操作的域名，单击 **批量转移至其他账号** 按钮。

2 . 按照对话框 **域名解析转移身份验证** 的提示信息，输入 **手机验证码** 和 **对方登录账号**

3 . 批量任务查询结果，在批量操作记录页签下，单击 **下载详情日志** 查看。

批量添加记录

概述

批量添加记录功能提供两种添加方式：分别是 **文本+设置方式** ，和 **文本方式** 添加记录。

使用前提

- 操作批量添加记录时，记录对应的域名需要在域名解析列表中，否则会导致添加记录失败。
- 非阿里云注册的域名，请先用 **批量添加域名** 功能将域名添加到云解析中，再 **批量添加解析** ；

- 添加的解析记录默认配置是：TTL时间 **10分钟**，解析线路 **默认**

文本+设置方法

示例 通过 **批量添加记录**，实现批量对两个域名添加相同解析记录：

dns-example.com 、 dns-example.cn

记录类型	主机记录	记录值
A	www	1.1.1.1

设置方法

1 . 登录云解析DNS控制台，

2 . 在域名解析页面，全部域名页签下，单击 **批量操作** 按钮

3 . 在批量操作页面，批量添加记录页签 ，选择 **操作方式一**

4 . 在输入框输入待添加记录的域名，每行输入1个域名，然后为这些域名指定统一的 **记录类型**、**主机记录**、**记录值**，单击 **添加** 按钮

5 . 批量添加记录结果，在批量操作记录页签，单击 **下载详情日志** 查看。

文本方法

在输入框内输入多条记录，单条记录格式为：域名 记录类型 主机记录 记录值。解析线路 **默认**，TTL 时间都**10 分钟**，不可自行定义。

1 . 点击 **批量添加记录** ，选择 **操作方式二**

2 . 输入框内按照格式要求，输入: **域名 记录类型 主机记录 记录值**，单击 **添加** 按钮。

3 . 批量添加记录结果，在批量操作记录页签，单击 **下载详情日志** 查看。

批量管理记录

概述

批量管理记录：包含批量修改解析记录和批量删除解析记录两项功能。

使用前提

解析记录对应的域名需要在域名解析列表中，否则会导致操作失败。

批量修改解析记录

批量修改解析记录：可设定解析记录修改前与修改后的解析值（主机记录、记录值），云解析可根据设定条件

完成批量修改。

设置方法

1 . 登录云解析控制台。

2 . 在 **域名解析** 页面中的 **全部域名** 页签下，单击 **批量操作**。

3 . 单击 **批量管理记录** 页签，选择 **批量修改解析记录**。

4 . 在输入框中输入需要修改解析记录的域名，不同域名之间以回车隔开。

5 . 设定解析记录修改前和修改后的具体值（主机记录、记录值），点击**确认**，云解析会根据设定条件进行批量修改。

6 . 批量修改解析记录结果，批量操作记录页签下，单击 **下载详情日志**

批量删除解析记录

批量删除解析记录 ：指在符合设定的删除条件下，批量删除解析记录。

设置方法

1 . 在 **域名解析** 页面中的 **全部域名** 页签下，单击 **批量操作**。

2 . 单击 **批量管理记录** 页签，选择 **批量删除解析记录**。

3 . 在输入框中输入需要删除解析记录的域名，不同域名之间以回车隔开。

4 . 对指定的 **主机记录或记录值** 设定删除条件，点击**确认**，云解析会删除符合此设定条件的解析记录。（同时也支持选择删除域名内含子域名的所有解析记录的设定。）

5 . 批量删除解析记录结果，批量操作记录页签下，单击 **下载详情日志**

DNS 解析模板

概述

DNS解析模板： 可实现为不同的域名批量添加或修改为相同的解析记录。

添加模板

添加模板包含两步：**输入模板名称、添加主机记录。**

设置方法

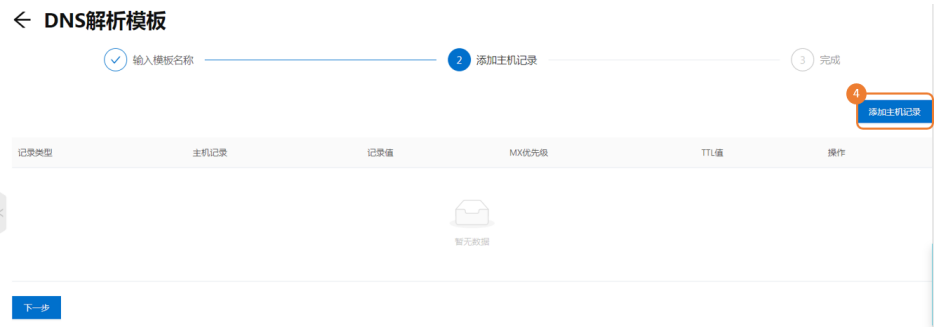
1 . 登录云解析DNS控制台。

2 . 在 **域名解析** 页面下的 **全部域名** 页签下，点击 **批量操作。**

3 . 在批量操作页面，DNS解析模板页签下，单击**添加模板** 按钮 。

4 . 输入 模板名称 ，并单击 **下一步** 按钮。

5 . 点击 **添加主机记录** 按钮，根据自己的需求添加解析记录，最后单击 **下一步**



6 . 点击 **返回**，返回到解析模板列表，点击 **设置域名**，输入域名， 输入的域名将会被统一添加上模板中设置的解析记录。

注意： 该功能会先删除输入的域名（含子域名）的所有解析记录，再按照模板添加新记录，删除记录会对当前解析造成影响，请了解此情况。

7 . 如点击 **修改** ，则会跳转至 **添加主机记录** 步骤，在此环节可以修改模板中的解析记录。 修改记录后，需要重新通过 **设置域名** 来将模板应用到添加的域名中。

删除模板

在批量操作页面， DNS解析模板页签下，选择要操作的模板，点击 **删除**，则会直接删除模板。 删除模板 不影响之前已引用此模板添加解析记录的域名

批量操作规则

云解析批量操作功能有如下限制：

操作类型	范围	说明
单次批量添加域名	1~10000	使用批量添加域名功能时，每次可以通过手动输入添加的域名数量。
单次通过文件批量添加域名	不超过 2 MB	使用批量添加域名功能时，每次可以导入的 excel 文件大小。
单次批量删除域名	1~10000	使用批量管理域名功能时，每次可以批量删除的域名数量。
单次批量更换域名分组	1~10000	使用批量管理域名功能时，每次可以批量更换分组的域名数量。
单次批量添加记录	1~10000	使用批量添加记录功能时，每次可以批量添加的记录数量。
单次批量修改解析记录	1~10000	使用批量管理记录功能时，每次可以批量修改的记录数量。
单次批量删除解析记录	1~10000	使用批量管理记录功能时，每次可以批量删除的记录数量。
单次批量设置域名的 DNS 解析模板	1~10000	使用批量设置域名功能时，每次可以通过手动输入批量设置的域名数量。

DNS监控

概述

DNS监控是利用全国节点，模拟用户每5分钟向域名发起一次DNS查询请求，可以实现监控用户本地运营商DNS的可用性和本地运营商DNS的查询响应时间。

优势

节点覆盖范围广： 全国部署节点1000+，覆盖国内主流运营商省份和地区。

实时监控告警：7x24小时监测，第一时间发出异常警告，有效帮助运维用户提前发现异常。

缓解DNS劫持： 实时监测域名劫持状态，可在一定程度上降低DNS劫持概率。

- **提升解析速度：** 减少公共DNS递归过程，加快域名解析速度。

使用前提

DNS监控使用的是云监控提供的全国节点，在进行DNS监控配置前，请先开通云监控按量付费。价格请参考云监控 **按量付费定价** ，或参考下图：

按量付费价格说明

计费项	价格
查询监控数据API调用数量	免费额度3330次/小时，超出部分按0.12元/万次收费
站点监控ECS探测点总数	免费额度50个，超出部分按0.003元/个/小时收费
云解析-分析与监控ECS探测点总数	免费额度50个，超出部分按0.0015元/个/小时收费
站点监控区分运营商探测点总数	0.014元/个/小时
云解析-分析与监控区分运营商探测点总数	免费额度50个，超出部分按0.007元/个/小时收费

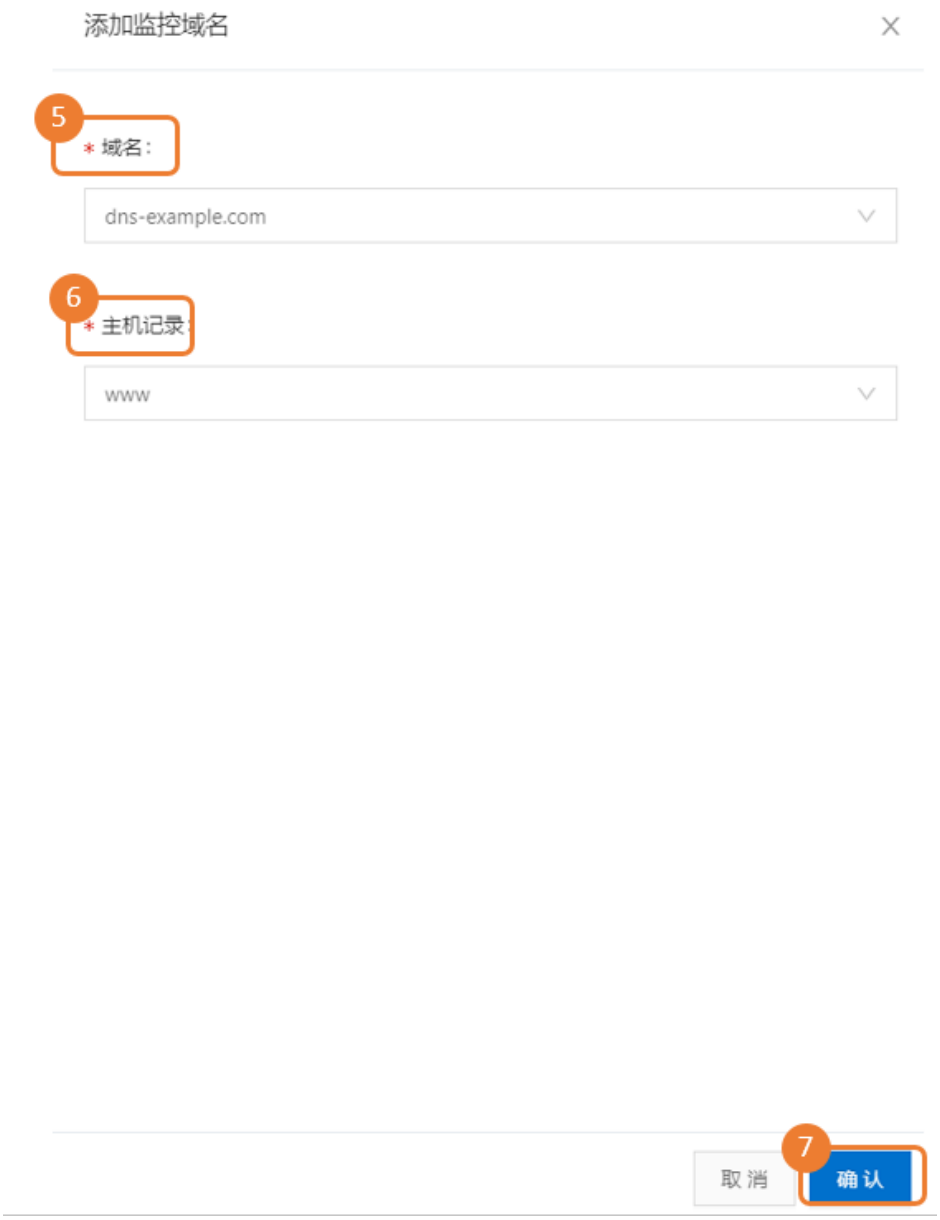
设置方法

1 . 登录 云解析DNS控制台

2 . 在域名解析页面， 更多服务页签， 在DNS监控模块，单击 **立即使用** 按钮。

3 . 在DNS监控介绍页面，单击 **点击授权** 按钮，在云资源访问授权页面，单击 **同意授权**。

4 . 在DNS监控页面，单击 **添加监控域名** 按钮，选择需要添加监控的主域名，然后选择需要添加的主机记录 。（如果主机记录为空，请到解析设置页面添加记录）



5 . 在DNS监控页面，单击 **详情** 按钮。

6 . 在DNS监控详情页，单击 **修改监控** 按钮。

首次创建监控域名，DNS监控会自动为用户创建监控规则，点击**修改监控**，

解析地址：DNS监控会自动为您同步最新的解析地址。

监控节点：可以添加和修改探测节点。

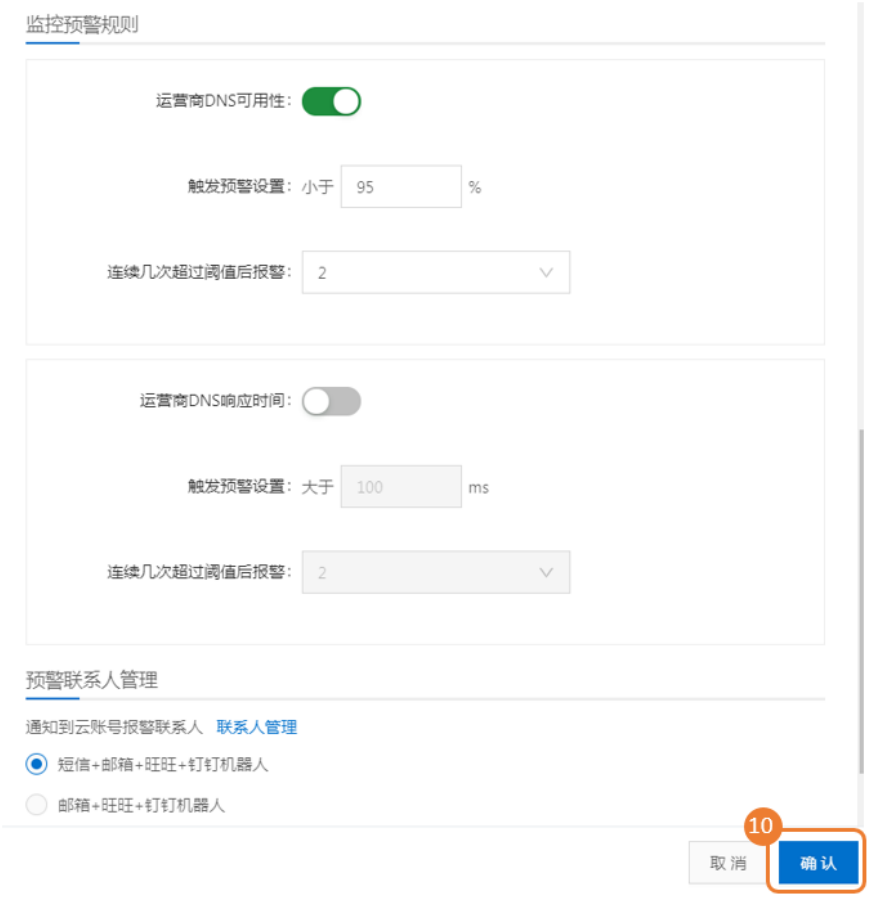
运营商DNS可用性： 默认开启，是指对用户本地DNS的可用性监测。

触发预警设置： 指对用户本地DNS可用性阈值的配置（例如95%），当监控用户本地DNS可用性小于设置的95%时，应触发异常告警提示。

连续几次超过阈值后报警：是对**触发预警设置**触发异常告警提示的限制规则，例如DNS监控每隔5分钟会探测一次，假设连续2次本地DNS可用性都低于95%，则会触发异常告警提示。

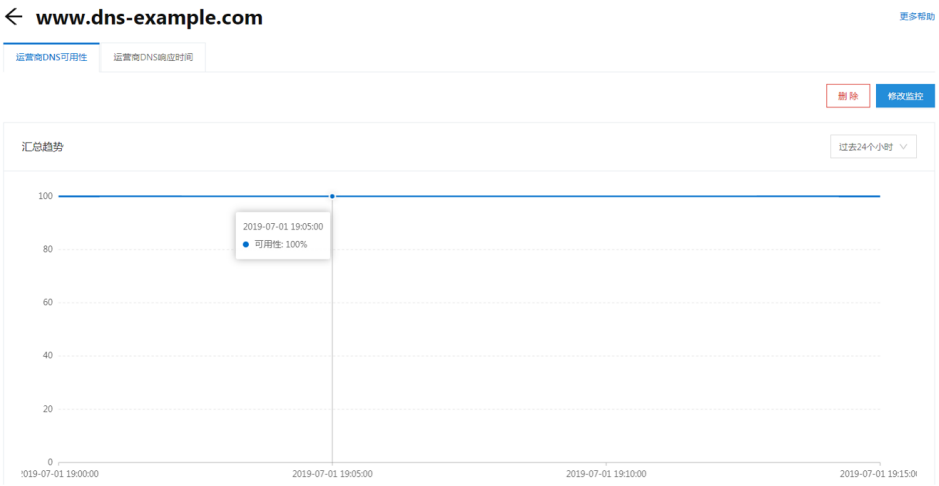
运营商DNS响应时间： 默认状态为关闭，关闭状态仍会继续做监测，但是如果监测出解析时间超过设置的上限，不会触发异常告警通知。如需要对DNS响应时间超出预期时触发异常告警通知，则点击按钮开启即可。默认创建的DNS查询响应时间是100ms，指通过监控节点，发起的本地DNS查询响应时间超过100ms时，会触发异常告警提示。


云解析DNS / 更多服务 / DNS 监控 / DNS监控详情
www.dns-example.com
更多帮助
运营商DNS可用性
运营商DNS响应时间
9
删除
修改监控
DNS监控详情
基本信息
提醒：DNS监控会自动为您同步最新的解析地址，更多帮助。
* 解析地址：
监测频率：5分钟
监控节点
提醒：运营商节点为付费服务，具体计费方法可参考云监控计费方法。
运营商
移动
鹏博士
联通
电信
阿里巴巴
区域 搜索区域...
暂无数据
城市 搜索城市
暂无数据
已选择探点 清空
阿里巴巴-上海市
阿里巴巴-深圳市
阿里巴巴-杭州市
阿里巴巴-青岛市
阿里巴巴-北京市



7 . 在DNS监控详情页， 单击 **运营商DNS可用性**页签。

- 可查看最近24小时的 运营商DNS可用性走势图。

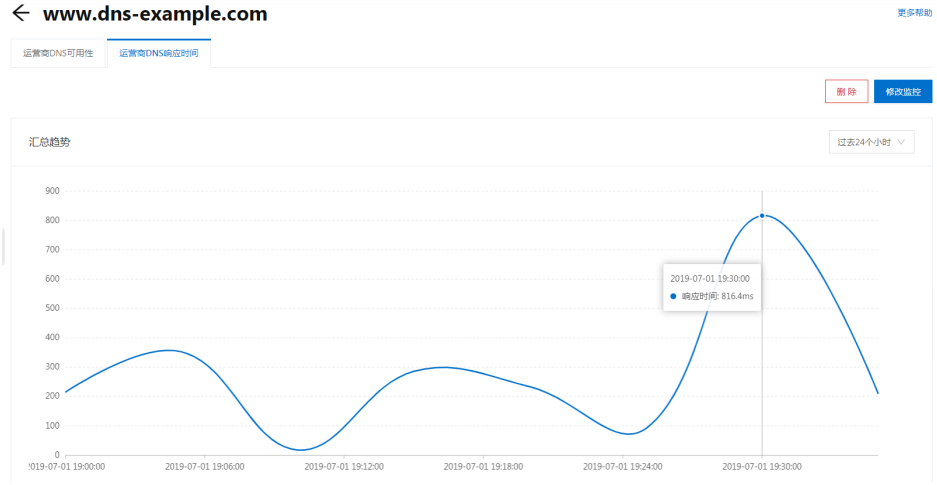


- 可查看本地运营商DNS监测到的异常数据：

运营商-城市	拨测时间	运营商DNS IP	拨测解析值	期望解析值	异常原因	异常状态码
西安市-电信	2019-04-17 15:27:09	114.114.114.114	-	3.3.3.3 4.4.4.4	解析超时或无响应	610
西安市-电信	2019-04-17 15:22:09	114.114.114.114	-	3.3.3.3 4.4.4.4	解析超时或无响应	610
西安市-电信	2019-04-17 12:31:57	114.114.114.114	-	3.3.3.3 4.4.4.4	解析超时或无响应	610

8 . 在DNS监控详情页， 单击 **运营商DNS响应时间** 页签。

- 可查看最近24小时运营商DNS响应时间的走势图。



- 可查看监控节点在地图上的解析时间分布状态、最快响应节点和最慢响应节点等数据。

触发异常告警的问题类型

DNS监控结果如出现下表中的问题类型，则判断 运营商DNS为不可用。

问题类型	异常状态码	异常原因说明
解析超时或无响应	610	监控节点向监控目标发送请求，但是最终未获取到目标地址或请求响应。
解析查询时出错	613	包括网络异常、域名状态异常、解析记录暂停、解析记录锁定、解析记录删除、IP不可用等未知异常。
解析内容不匹配	615	本地运营商DNS解析结果和解析设置不符，一般为DNS劫持
解析返回为空	616	域名被锁定（hold）

产品规则

1 . 解析功能变更对DNS监控的影响说明

操作域名删除、账号间转移、域名找回：则此域名会从DNS监控被自动删除。

解析记录删除：相同主机记录下仍有其它解析记录，DNS监控任务继续服务；相同主机记录下无其他记录，则DNS监控任务被自动删除。

解析地址变更：则DNS监控下的解析地址会同步更新

解析记录类型变更（限A记录和CNAME记录类型的切换）：相同主机记录同时存在A和CNAME，则DNS监控会删除此子域名的监控任务。

DNS监控的子域名只支持A、CNAME两种记录类型，如记录类型变更为其他解析记录类型，则DNS监控会删除此子域名的监控任务。

新增记录：相同主机记录不同解析线路下同时存在了A和CNAME记录 ，则DNS监控会删除此子域名的监控任务。

解析记录：DNS监控会删除此子域名的监控任务。

2 . 产品限制

DNS监控添加的子域名仅限A和CNAME两种记录类型使用。

DNS监控仅支持DNS托管在云解析DNS中的域名使用。

DNS监控不支持泛解析域名添加监测

相同主机记录但不同解析线路下，同时存在A和CNAME记录，DNS监控不支持使用。

DNS监控不支持添加其他账号下的域名使用。

辅助 DNS

概述

概述

辅助DNS 是云解析为使用自建DNS或第三方DNS的用户提供的 **DNS容灾备份服务**，当为域名 **开启辅助DNS**，则域名当前使用的DNS为 **主DNS** ，云解析则默认为 **辅DNS**，我们基于RFC标准协议，在主DNS和辅DNS之间建立区域数据传输机制，当主DNS遇到故障或者服务中断时，辅DNS仍可以继续提供解析服务，因此可以保障您的业务在全球范围稳定运行。

优势

容灾备份，降低业务中断风险

主DNS系统故障，辅助DNS可继续提供域名解析服务，保障业务可用性。

稳定可靠，保障业务稳定运行

云解析DNS提供100%SLA服务，全球DNS集群互相备份，服务永不宕机。

全球节点，提升域名解析效率

节点遍布全球，持续扩展的数据中心让跨域体验更流程

负责均衡，流量均摊降低负载

当辅助DNS与主DNS同时对外提供解析服务时，可以达到流量负载均衡的效果。

安全保障，实时攻击检测、全球2T带宽储备

当选择将主DNS隐藏，由辅DNS（云解析）对外提供解析服务，可更好地保障主DNS的安全。

开启辅助DNS

产品限制

辅助DNS面向云解析DNS企业旗舰版用户开放使用。立即购买

云解析目前只能作为 **辅DNS** 使用，您当前使用的DNS为 **主DNS**

域名开启辅助DNS后，在云解析解析设置中不能手动修改解析记录，所有解析记录都需要从主DNS同步过来。

辅助DNS功能适用于使用 **自建DNS** 或 **第三方DNS托管服务** 的用户。如使用的是 **第三方DNS托管服务**，请确认您当前的托管厂商也支持配置辅助DNS功能。

如使用的是 **自建DNS**，经测试，云解析辅助DNS与BIND v9.1.0以上版本兼容良好，且需要DNS服务器支持RFC标准的XFR、NOTIFY协议。

一、准备工作

开启辅助DNS，**首先** 需要在主DNS上完成配置，**然后** 在云解析DNS中开启辅助DNS。由于DNS系统的实现方式多样，以下以自建DNS（BIND 9.9.4及以上版本)为例说明如何配置主DNS。

1.生成TSIG密钥

可以通过 dnssec-keygen工具 生成TSIG密钥，命令如下：

dnssec-keygen -a HMAC-SHA256 -b 128 -n HOST test_key

如果长时间无法生成秘钥文件，可以尝试添加参数 -r /dev/urandom ，如下：

dnssec-keygen -a HMAC-SHA256 -b 128 -n HOST -r /dev/urandom test_key

命令说明

• -a ：指定加密算法，我们支持的HMAC-MD5、HMAC-SHA1、或HMAC-SHA256。

• -b： 指定密钥中字节的数量。密钥文件大小的选择依赖于所使用的算法，HMAC密钥必须在1和512位之间。

• -n： 指定密钥文件的所有者类型，可选值包括：ZONE、HOST、ENTITY、和USER。通常使用HOST或ZONE。

• test_key ：指定密钥文件的名称。该名称用于 使用BIND配置主DNS 中 allow-transfer 的填写，和 添加主DNS信息 中TSIG名称的填写。

• -r /dev/urandom：随机数生成器。

命令执行 后，在当前目录下会有 “**.key**”和 “**.private**” 的文件（例如：“ **Ktest_key.+157+64252.key** ”和“ **Ktest_key.+157+64252.private** ”）。“**.key**” 文件中包含了 **DNS KEY record**，这个record用于配置辅助DNS时，在**添加主DNS信息**时，用于**TSIG值**的填写；“**.private**” 文件中包含算法指定的字段。

2.使用BIND配置主DNS

在配置文件 **/etc/named.conf** 完成以下配置：

```
zone "域名（如：xxx.com）" IN {
type master;
allow-update { 127.0.0.1; };
allow-transfer {key test_key;};
notify explicit;
also-notify {47.92.14.234 port 53 key test_key;47.92.14.51 port 53 key test_key;};
file "zone_file";
};
```

配置含义说明

zone ：配置您指定的域名。

allow-transfer ：目前支持通过TSIG进行主辅DNS间通讯，此处请指定为允许服务器通过TSIG方式来更新的KEY名称。

说明：根据RFC标准协议，我们推荐使用事务签名（简称TSIG）来保证DNS消息的安全性。TSIG通常使用共享密钥和单向哈希函数来验证DNS消息，能较好地确保主辅DNS之间信息同步的安全性。您可以通过生成一个MD5、SHA256或SHA1型的TSIG密钥，生成后将TSIG同时配置到您的主DNS、辅DNS。具体操作请参考生成TSIG密钥。

also-notify ：当区域（ZONE）发生变更时，需要通知辅助DNS服务器IP地址，支持多个。此处请指定为云解析辅助DNS服务器：

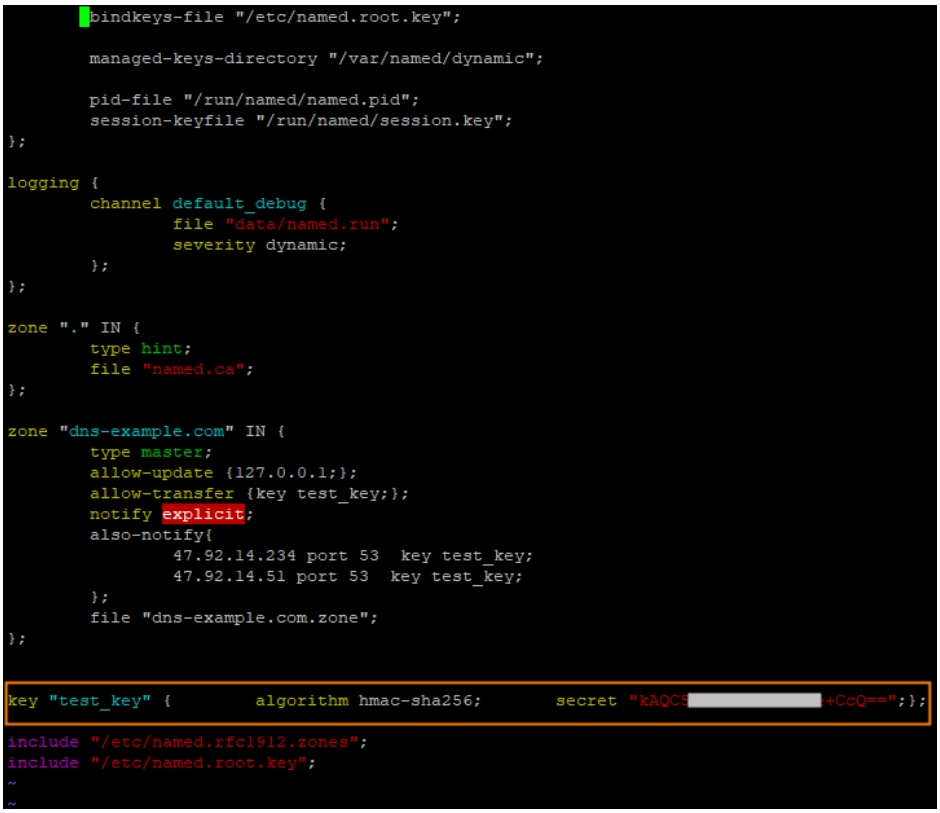
```
DNS服务器名称：
对应IP地址为：47.92.14.51,47.92.14.234
```

test_key ：指定密钥文件的名称。该名称用于 使用BIND配置主DNS 中 allow-transfer 的填写，和添加主DNS信息 中TSIG名称的填写。

3. 将生成的秘钥按照以下两种方式添加到 named.conf文件中

按如下格式粘贴到 named.conf中

```
key "test_key" {       algorithm hmac-sha256;       secret ".key文件中的加密串";};
```



- 通过include文件方式

需要通过include的方式添加到named.conf文件中，例如：

```
include "/etc/named/dns-key";
```

```
        bindkeys-file "/etc/named.root.key";

        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

zone "dns-example.com" IN {
        type master;
        allow-update {127.0.0.1;};
        allow-transfer {key test_key;};
        notify explicit;
        also-notify{
                47.92.14.234 port 53  key test_key;
                47.92.14.51 port 53  key test_key;
        };
        file "dns-example.com.zone";
};

include "/etc/named/dns-key";
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

/etc/named/dns-key文件格式如下

```
key "test_key" {
algorithm hmac-sha256;
secret ".key文件中的加密串";
};
```

注意： 配置文件**named.conf**中**完成配置**更改后，需要 **重启应用。**

1.重启命令：systemctl restart named

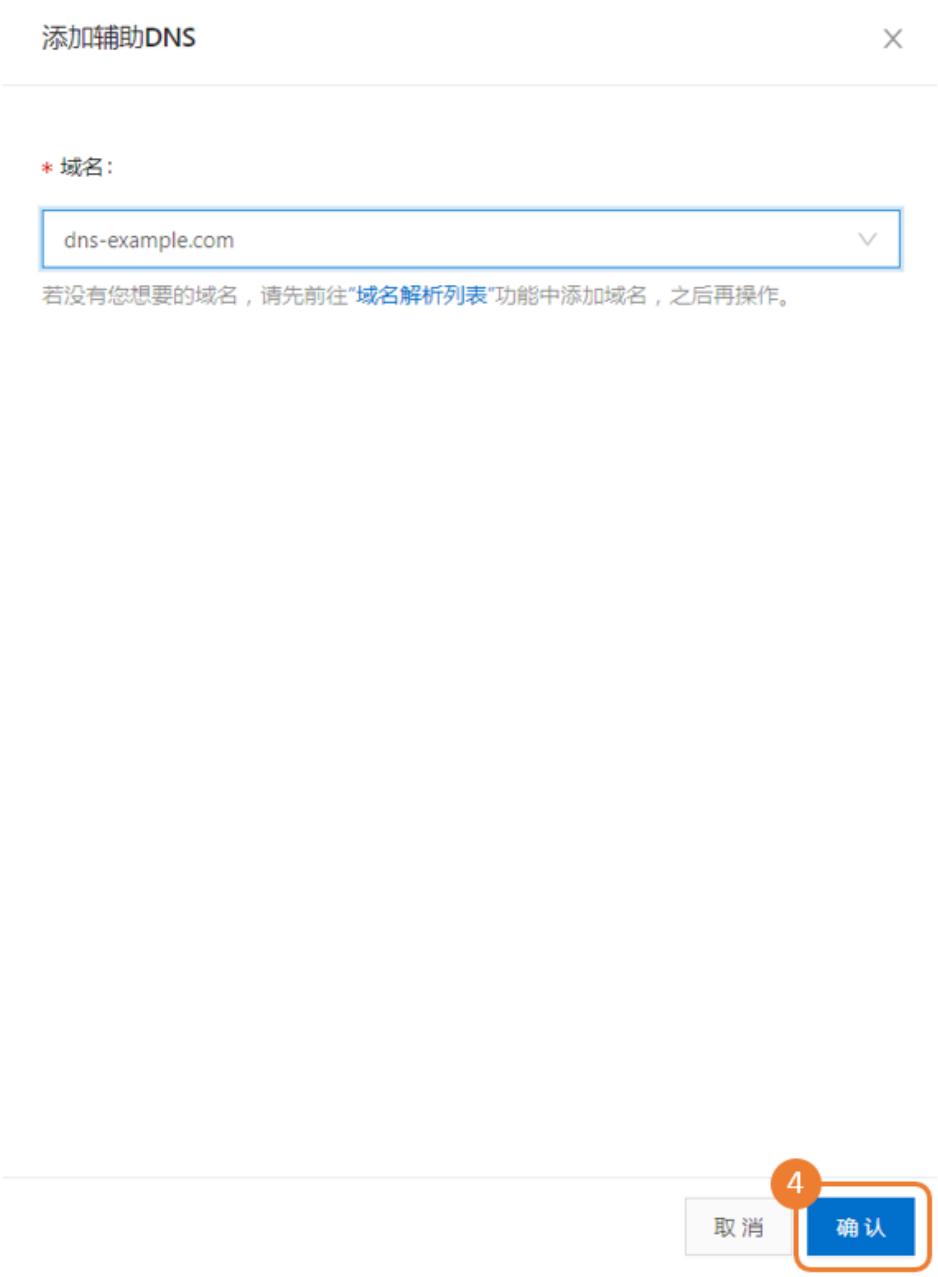
二、开始配置

4.辅助DNS配置

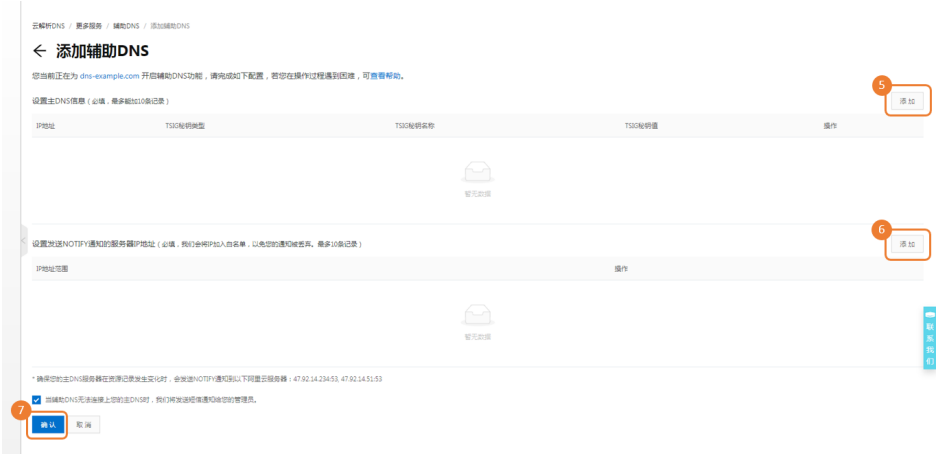
1 . 登录云解析DNS控制台。

2 . 在左侧目录单击 **辅助DNS** ，点击 **使用辅助DNS** 按钮

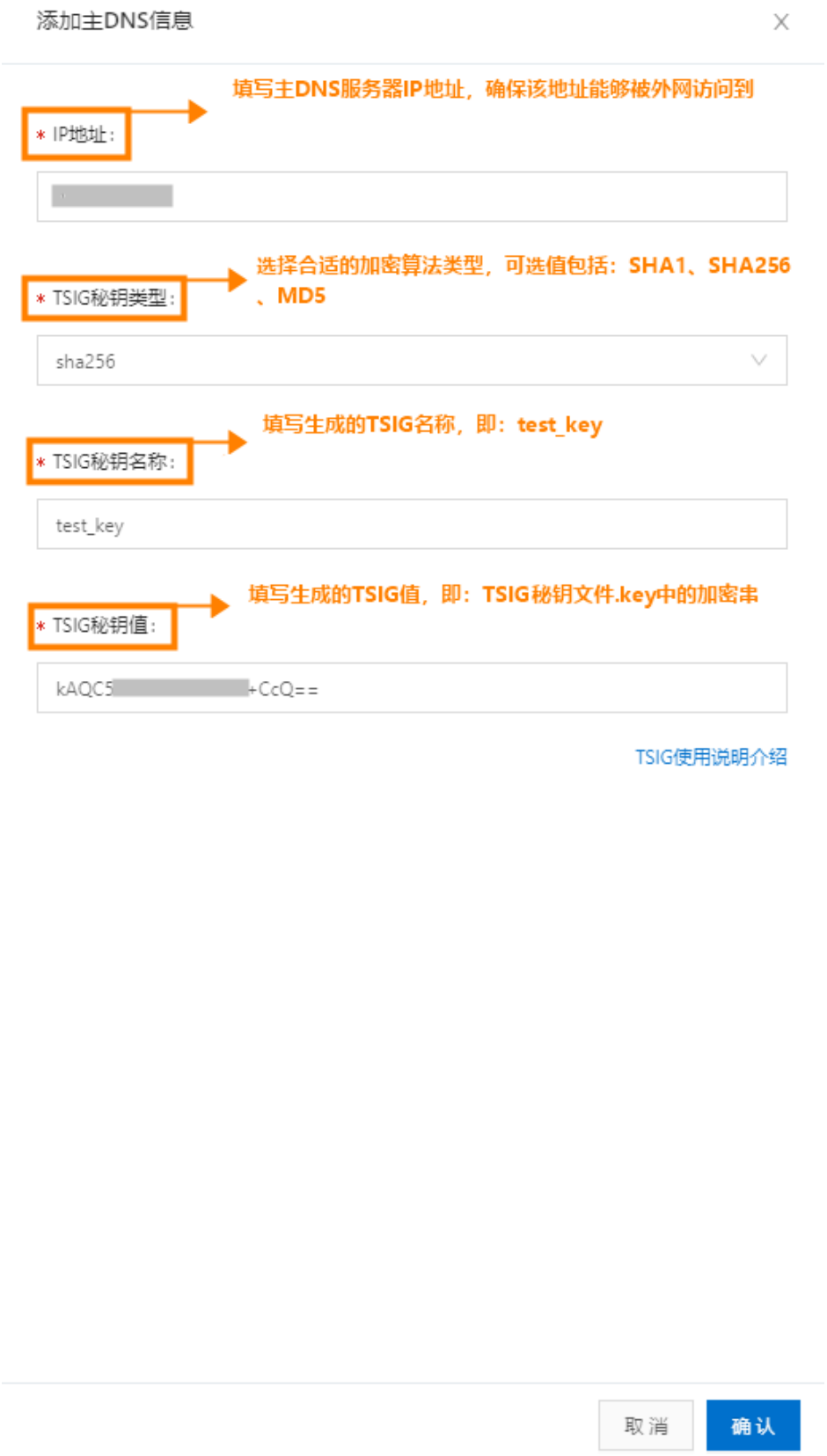
3 . 单击 **添加辅助DNS** 按钮，在添加辅助DNS的对话框中，选择需要开启辅助DNS的域名，并点击 **确认** 按钮 。



4 . 在辅助DNS页，完成三项配置： **设置主DNS信息** 、**设置发送NOTIFY通知的服务器IP地址**、 配置完毕后点击 **确认。**



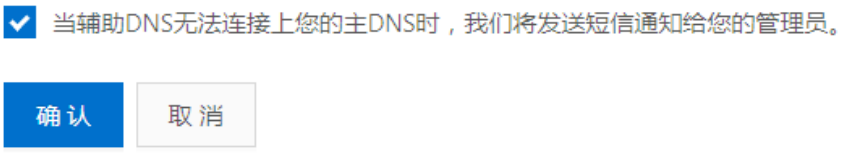
设置主DNS信息： 单击右侧 **添加**按钮，添加主DNS记录。



设置发送NOTIFY通知的服务器IP地址： 单击右侧 **添加**按钮，输入发送通知的服务器IP地址或IP段。

- 勾选是否使用故障通知：开启后，当出现主辅DNS连接中断时，云解析将短信通知您。最后点击 **确认**

。



5 . 完成上述辅助DNS的配置后，在辅助DNS页面的列表中可以看到添加的域名，说明该域名已开启辅助DNS。

主辅连接状态为 **正常**：说明辅助DNS可以正常连接到主DNS服务器。

主辅连接状态为为 **阻断**：则代表辅助DNS无法连接到主DNS服务器。请您检查如下2点。

① 辅助DNS配置参数信息是否填写正确，主DNS服务器的IP地址外网是否可以访问。

② 主DNS服务器目前是否正常运转。

③ 主DNS配置文件是否符合RFC规范，例如：SOA记录中的序列号值范围是1~2^32-1。若主DNS的SOA中序列号值超出范围，将导致辅助DNS停止同步主DNS的资源记录。具体可参考：**同步异常说明**

6 . 开启辅助DNS后，且**状态正常**。若希望跳过NOTIFY协议直接进行同步触发，则可进行以下操作。域名解析-单击开启辅助DNS的域名-解析设置-手动触发同步。

5.域名DNS配置

开启辅助DNS后，配合主DNS，有以下**三种**搭配方式：

1. 只配置主DNS

域名的所有解析由**主DNS**进行解析。辅助DNS进行**实时数据备份**。

根域名@的NS记录配置：

```
$TTL 3600
@       IN SOA  vip3.alidns.com. admin.dns-example.com. (
                                        6       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      vip3.alidns.com.
@       IN      NS      vip4.alidns.com.
@       IN      A       33.33.33.33
www     IN      A       55.55.55.55
@       IN      A       123.123.11.11
```

查看权威返回情况，执行dig dns-example.com NS @vip3.alidns.com结果：

```
; <<>> DiG 9.14.4 <<>> dns-example.com NS @vip3.alidns.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58064
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dns-example.com.               IN      NS

;; ANSWER SECTION:
dns-example.com.        86400   IN      NS      vip3.alidns.com.

;; Query time: 32 msec
;; SERVER: 140.205.29.115#53(140.205.29.115)
;; WHEN: Tue Apr 14 17:57:58 中国标准时间 2020
;; MSG SIZE  rcvd: 73
```

查看递归解析返回情况，执行dig dns-example.com NS +trace +nodnssec结果：

```
; <<>> DiG 9.14.4 <<>> dns-example.com NS +trace +nodnssec
;; global options: +cmd
.                       86400   IN      NS      a.root-servers.net.
.                       86400   IN      NS      m.root-servers.net.
.                       86400   IN      NS      d.root-servers.net.
.                       86400   IN      NS      j.root-servers.net.
.                       86400   IN      NS      l.root-servers.net.
.                       86400   IN      NS      e.root-servers.net.
.                       86400   IN      NS      c.root-servers.net.
.                       86400   IN      NS      f.root-servers.net.
.                       86400   IN      NS      i.root-servers.net.
.                       86400   IN      NS      h.root-servers.net.
.                       86400   IN      NS      k.root-servers.net.
.                       86400   IN      NS      b.root-servers.net.
.                       86400   IN      NS      g.root-servers.net.
;; Received 824 bytes from 30.25.7.65#53(30.25.7.65) in 12 ms

com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
;; Received 868 bytes from 192.36.148.17#53(i.root-servers.net) in 77 ms

dns-example.com.        172800  IN      NS      vip3.alidns.com.
dns-example.com.        172800  IN      NS      vip4.alidns.com.
;; Received 553 bytes from 192.31.80.30#53(d.gtld-servers.net) in 174 ms

dns-example.com.        86400   IN      NS      vip3.alidns.com.
;; Received 73 bytes from 106.11.30.116#53(vip4.alidns.com) in 42 ms
```

2. 只配置辅助DNS

域名的所有解析由辅DNS（云解析）对外提供解析服务，可更好地保障主DNS的安全。

根域名@的NS记录配置：

```
$TTL 3600
@       IN SOA  ns1.dns-example.com. admin.dns-example.com. (
                                        3       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      ns1.dns-example.com.
@       IN      NS      ns2.dns-example.com.
@       IN      A       33.33.33.33
www     IN      A       55.55.55.55
ns1     IN      A       47.94.166.148
ns2     IN      A       47.94.166.148
@       IN      A       123.123.11.11
~
```

查看权威返回情况，执行dig dns-example.com NS @ns1.dns-example.com结果：

```
; <<>> DiG 9.14.4 <<>> dns-example.com NS @ns1.dns-example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39034
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: f991c9a26964f844f8aba4835e95866c4bc62c85c594b953 (good)
;; QUESTION SECTION:
;dns-example.com.               IN      NS

;; ANSWER SECTION:
dns-example.com.        3600    IN      NS      ns1.dns-example.com.
dns-example.com.        3600    IN      NS      ns2.dns-example.com.

;; ADDITIONAL SECTION:
ns1.dns-example.com.    3600    IN      A       47.94.166.148
ns2.dns-example.com.    3600    IN      A       47.94.166.148

;; Query time: 10 msec
;; SERVER: 47.94.166.148#53(47.94.166.148)
;; WHEN: Tue Apr 14 17:46:20 中国标准时间 2020
;; MSG SIZE  rcvd: 140
```

查看递归解析返回情况，执行dig dns-example.com NS +trace +nodnssec结果：

```
; <<>> DiG 9.14.4 <<>> dns-example.com NS +trace +nodnssec
;; global options: +cmd
.                       692     IN      NS      k.root-servers.net.
.                       692     IN      NS      i.root-servers.net.
.                       692     IN      NS      f.root-servers.net.
.                       692     IN      NS      a.root-servers.net.
.                       692     IN      NS      j.root-servers.net.
.                       692     IN      NS      h.root-servers.net.
.                       692     IN      NS      g.root-servers.net.
.                       692     IN      NS      l.root-servers.net.
.                       692     IN      NS      m.root-servers.net.
.                       692     IN      NS      c.root-servers.net.
.                       692     IN      NS      b.root-servers.net.
.                       692     IN      NS      e.root-servers.net.
.                       692     IN      NS      d.root-servers.net.
;; Received 824 bytes from 30.25.7.65#53(30.25.7.65) in 36 ms

com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
;; Received 840 bytes from 202.12.27.33#53(m.root-servers.net) in 92 ms

dns-example.com.        172800  IN      NS      ns1.dns-example.com.
dns-example.com.        172800  IN      NS      ns2.dns-example.com.
;; Received 112 bytes from 192.48.79.30#53(j.gtld-servers.net) in 176 ms

dns-example.com.        3600    IN      NS      ns1.dns-example.com.
dns-example.com.        3600    IN      NS      ns2.dns-example.com.
;; Received 140 bytes from 47.94.166.148#53(ns2.dns-example.com) in 13 ms
```

3. 主辅DNS都配置

LocalDNS根据一定的算法进行权威请求其中一组权威，由该权威进行解答返回。

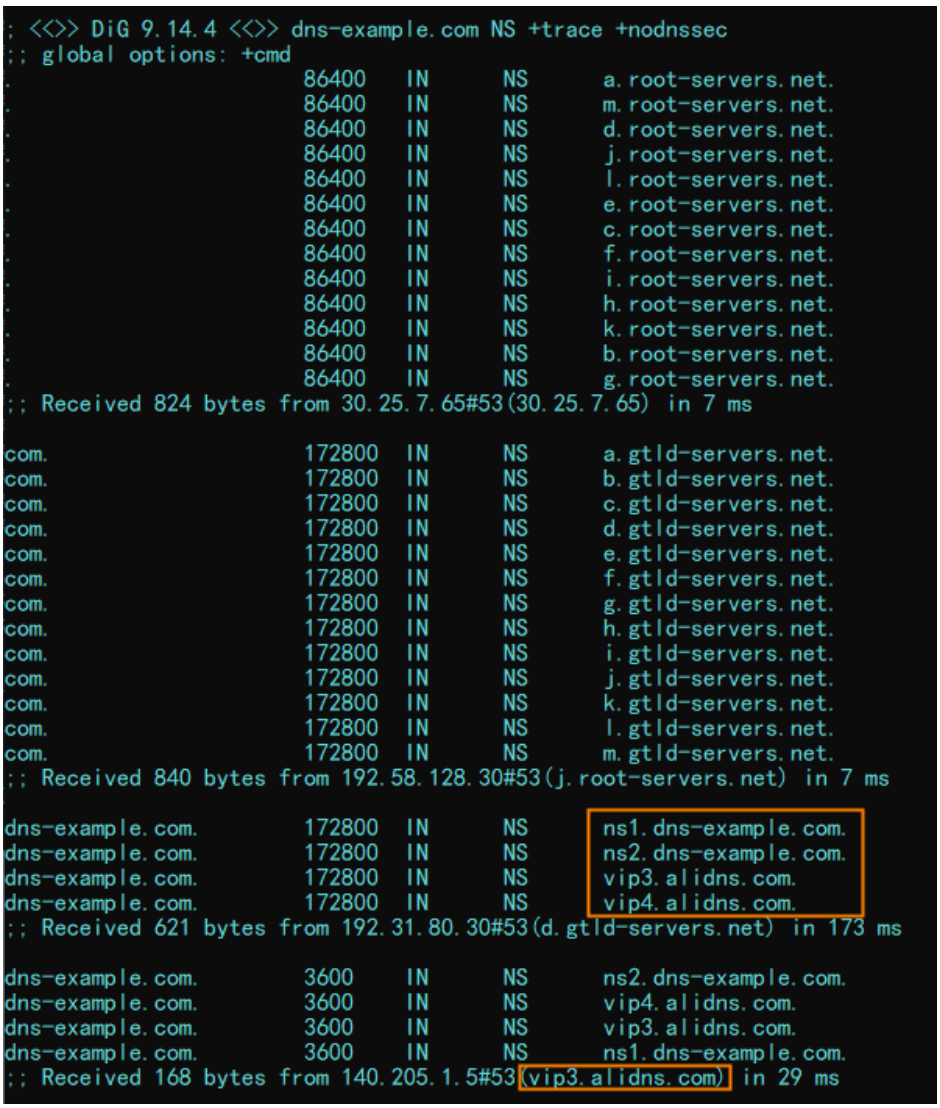
根域名@的NS记录配置：

```
$TTL 3600
@       IN SOA  ns1.dns-example.com. admin.dns-example.com. (
                                        3       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      ns1.dns-example.com.
@       IN      NS      ns2.dns-example.com.
@       IN      NS      vip3.alidns.com.
@       IN      NS      vip4.alidns.com.
@       IN      A       33.33.33.33
www     IN      A       55.55.55.55
ns1     IN      A       47.94.166.148
ns2     IN      A       47.94.166.148
@       IN      A       123.123.11.11
~
```

查看权威返回情况，执行dig dns-example.com NS @ns1.dns-example.com结果：

```
; <<>> DiG 9.14.4 <<>> dns-example.com NS @ns1.dns-example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5667
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 67409558b3081ebdab460c785e9571ad835b2274539b1ca1 (good)
;; QUESTION SECTION:
;dns-example.com.               IN      NS

;; ANSWER SECTION:
dns-example.com.        3600    IN      NS      ns2.dns-example.com.
dns-example.com.        3600    IN      NS      vip3.alidns.com.
dns-example.com.        3600    IN      NS      ns1.dns-example.com.
dns-example.com.        3600    IN      NS      vip4.alidns.com.

;; ADDITIONAL SECTION:
ns1.dns-example.com.    3600    IN      A       47.94.166.148
ns2.dns-example.com.    3600    IN      A       47.94.166.148

;; Query time: 10 msec
;; SERVER: 47.94.166.148#53(47.94.166.148)
;; WHEN: Tue Apr 14 16:17:49 中国标准时间 2020
;; MSG SIZE  rcvd: 185
```

查看递归解析返回情况，执行dig dns-example.com NS +trace +nodnssec结果：



连接主DNS

概述

连接主DNS：是指在主辅连接状态为 **阻断** 时，可支持手动触发连接主DNS。

注意：辅助DNS中的解析记录更新，一般是由主DNS发送NOTIFY来触发解析数据同步，或者是根据主DNS设置的刷新时间来触发解析数据同步（指时间到期则触发）。

操作步骤

登录云解析DNS控制台

进入辅助DNS页面，单击 **连接主DNS**按钮

修改辅助DNS

概述

修改辅助DNS：是指主DNS服务器信息如发生变更，则需要到云解析辅助DNS中，对 **设置主DNS信息**、 **设置发送NOTIFY通知的服务器IP地址**，进行更新配置。

操作步骤

1 . 登录云解析DNS控制台。

2 . 进入 **辅助DNS**页面，在辅助DNS列表页，在 操作项下点击 **同步配置** 按钮。

3 . 在 修改辅助DNS 页面，单击 **修改** 按钮，修改完后点击 **确认**。

4．修改配置参数完毕后，辅助DNS会主动向主DNS发起连接请求，来获取主DNS资源记录的最新数据。

关闭辅助DNS

概述

关闭辅助DNS：是指通过关闭辅助DNS，来实现停止主、辅DNS之间的数据同步行为。

操作步骤

1．登录云解析DNS控制台

2．在辅助DNS页面的同步开关处，单击关闭。

辅助DNS同步日志

概述

辅助DNS同步日志： 是指主-辅DNS同步的日志信息。

操作步骤

1 . 登录云解析DNS控制台。

2 . 在辅助DNS页面，单击 **辅助DNS同步日志** 按钮

3 . 在 **辅助DNS同步日志**页面，查看日志

同步异常说明

主DNS设置不符合RFC规范

开启辅助DNS，需确保主DNS的设置遵守RFC规范，**对于不符合RFC规范的设置，辅助DNS对应的处理方法如**

下：

SOA记录中的序列号值范围是1~2^32-1。若主DNS的SOA中序列号值超出范围，将导致辅助DNS停止同步主DNS的资源记录。

SOA记录中的刷新时间值范围是30-2^32-1。若主DNS的SOA中刷新时间超出范围，系统默认将其修改为30分钟。

目前辅助DNS最多可同步主DNS的资源记录条数为1万。若主DNS中资源记录超过1万，则本次辅助DNS的同步操作作废失效。

若您的设置中有不符合RFC规范之处，在辅助DNS同步主DNS资源记录时，会摒弃这些不符合规范的设置参数。

- 为确保主辅DNS之间连接通畅，请开放TCP 53端口。

主DNS的限制与影响说明

使用辅助DNS时，请注意以下主DNS上的限制和影响：

如主DNS服务器个数超过1个，您需要确保各个DNS服务器之间数据同步，否则会造成主辅DNS数据不一致的情况。且若所有主DNS都连接不上，系统将最终判定主DNS连接中断，并根据您的设置判断是否要触发短信通知。

主DNS中的解析记录，请确保其符合云解析DNS中对解析记录的要求，不能存在互相冲突的记录，具体请参考 解析记录中的冲突规则。

日志查询

概述

云解析DNS提供两个维度的日志查询，分别是操作日志、解析日志。

操作日志：指云解析DNS域名列表中的域名管理操作日志，可以查看操作时间、操作域名、操作行为。操作行为例如添加域名、删除域名、找回域名等操作。

解析日志：指在解析设置页面，解析记录的操作日志，可以查看操作时间，操作行为、操作者IP。操作行为例

如解析记录的增删改等。

例如对解析记录增删改的操作日志。

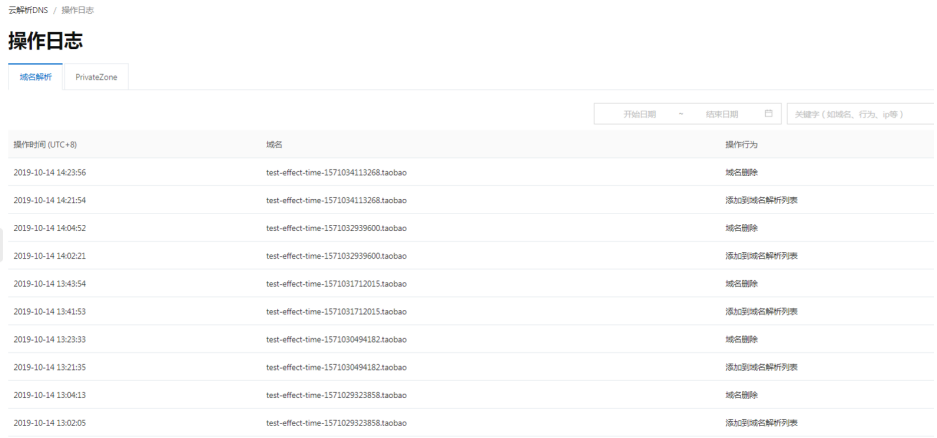
操作方法

操作日志

1 . 登录 云解析DNS控制台

2 . 左侧菜单选择 “操作日志”

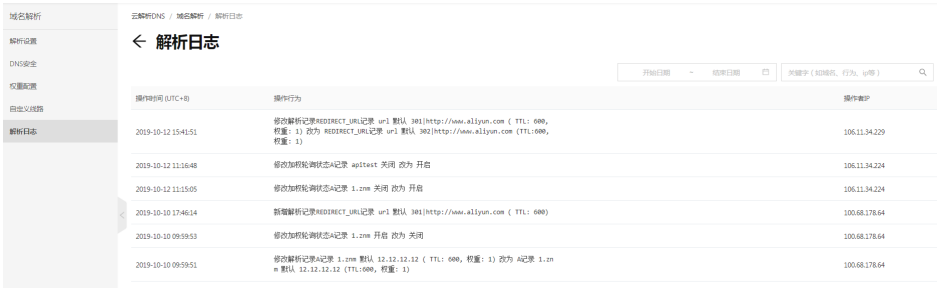
3 . 可在操作日志页面，查看域名管理的操作日志，例如添加域名、删除域名等。



解析日志

1 . 在域名解析列表页，选择需要查看解析日志的域名，单击域名进入解析设置页面。

2 . 在解析设置页面左侧菜单，单击解析日志，可查看解析记录增删改的日志信息。



权限管理

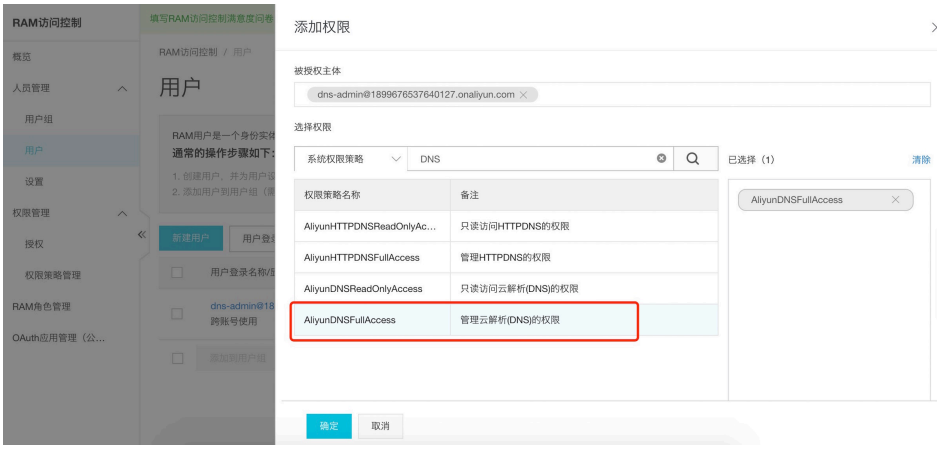
跨账号管理域名和DNS

场景描述

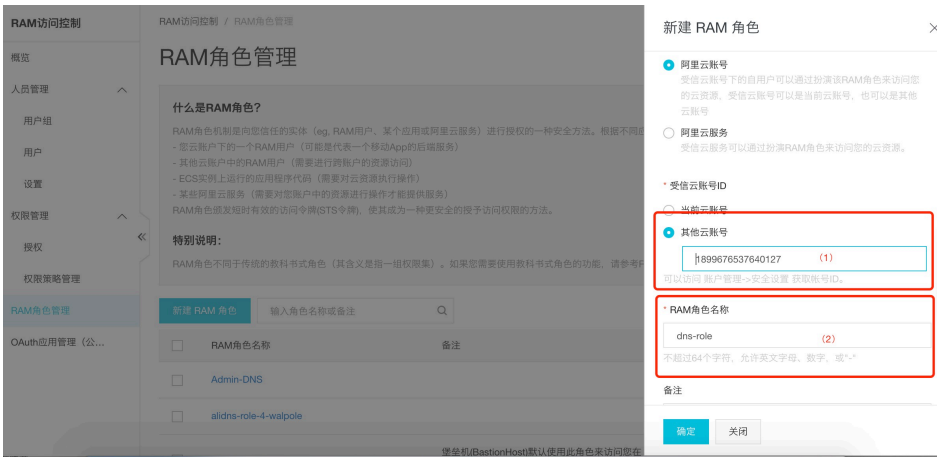
账号A和账号B，在账号B下建立RAM用户dns-account，dns-account可管理账号A下域名的权限；

使用指南

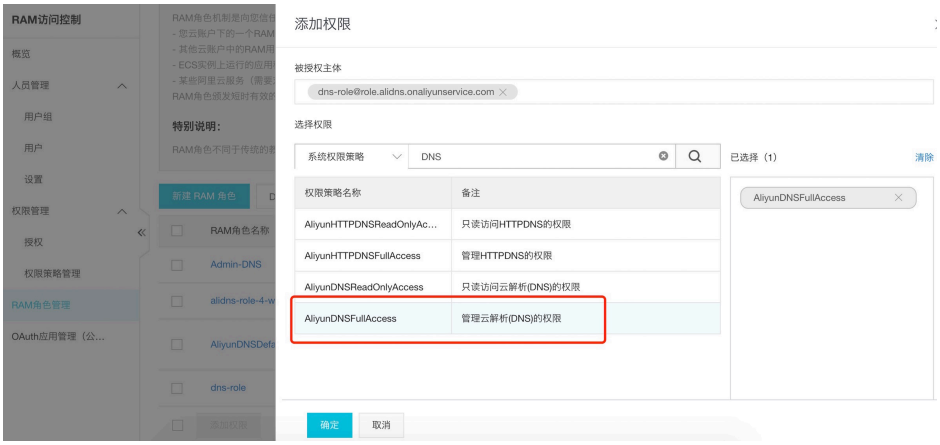
- 在账号A下为B账号先创建RAM用户dns-admin，再通过“**添加权限**”，选择系统权限“**AliyunDNSFullAccess**”



- 在账号A下为B账号先创建RAM用户角色dns-role，并输入B账号的ID

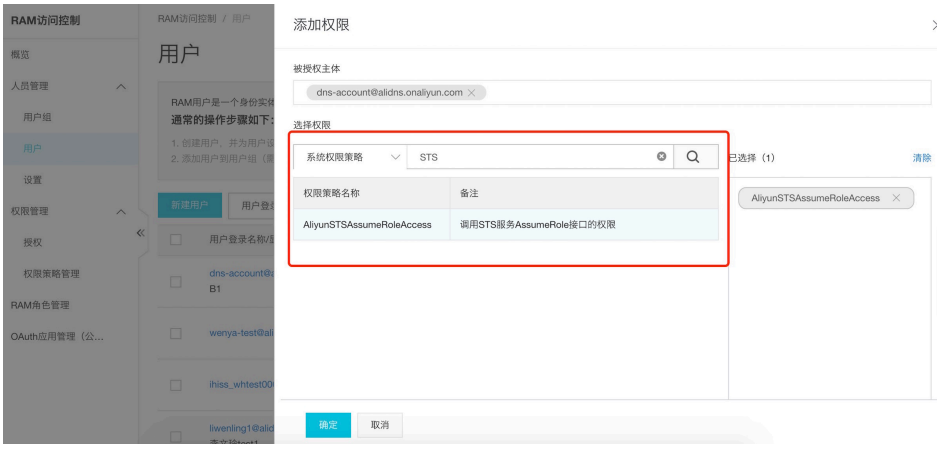


- 在A账号下，为RAM用户角色dns-role进行权限授权，点击“添加权限”，选择系统权限“AliyunDNSFullAccess”

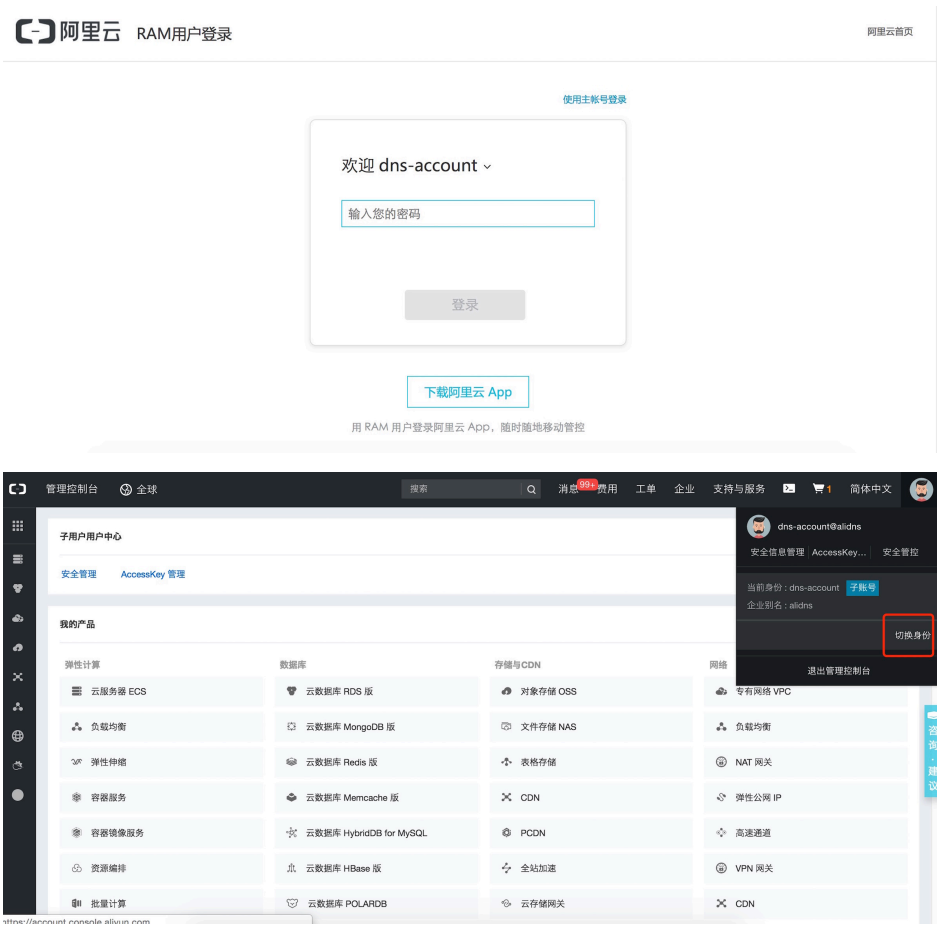


- 在B账号下创建RAM用户dns-account，并启用控制台登录。

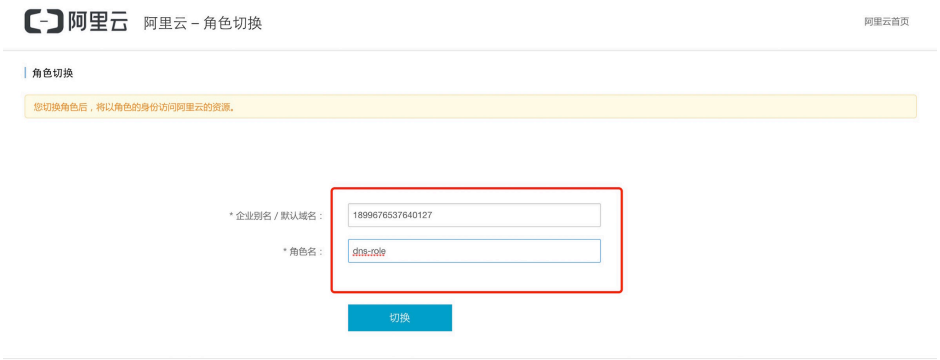
- 在账号B下为RAM用户dns-account分配STS跨账号管理权限



- 使用RAM用户dns-account登录控制台，并点击“切换身份”



- 点击切换身份后，输入A账号RAM用户的企业别名和创建的RAM角色DNS-role

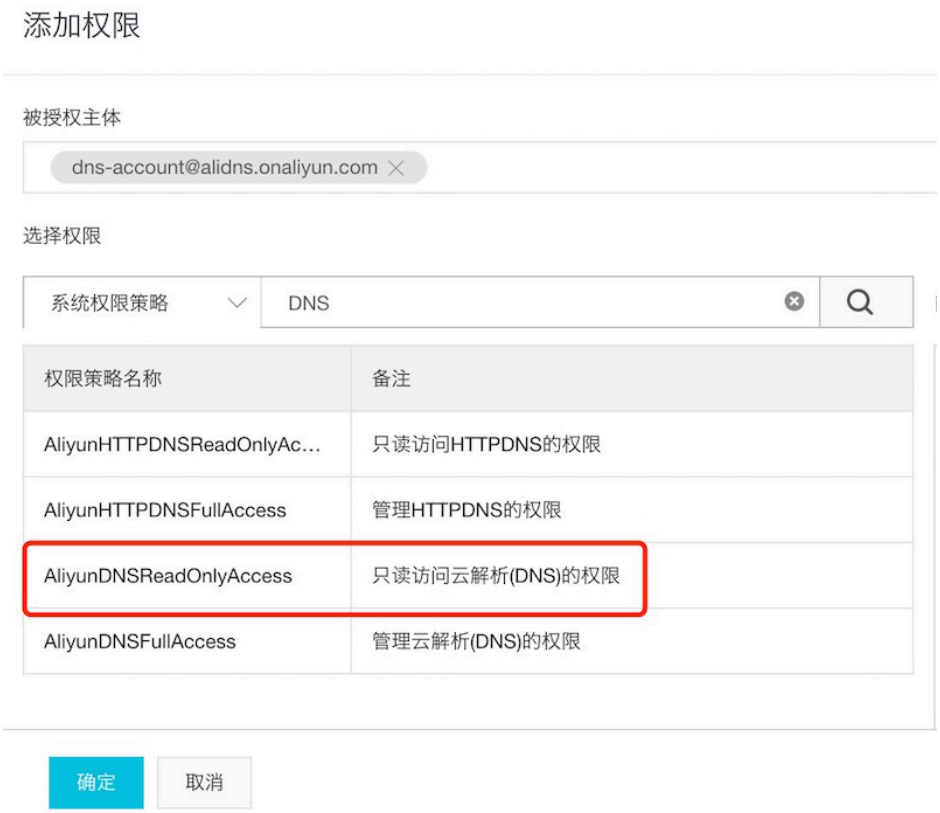


- 切换成功可最终实现通过B账号下的RAM用户DNS-account管理A账号下的RAM角色DNS-role。

权限管理

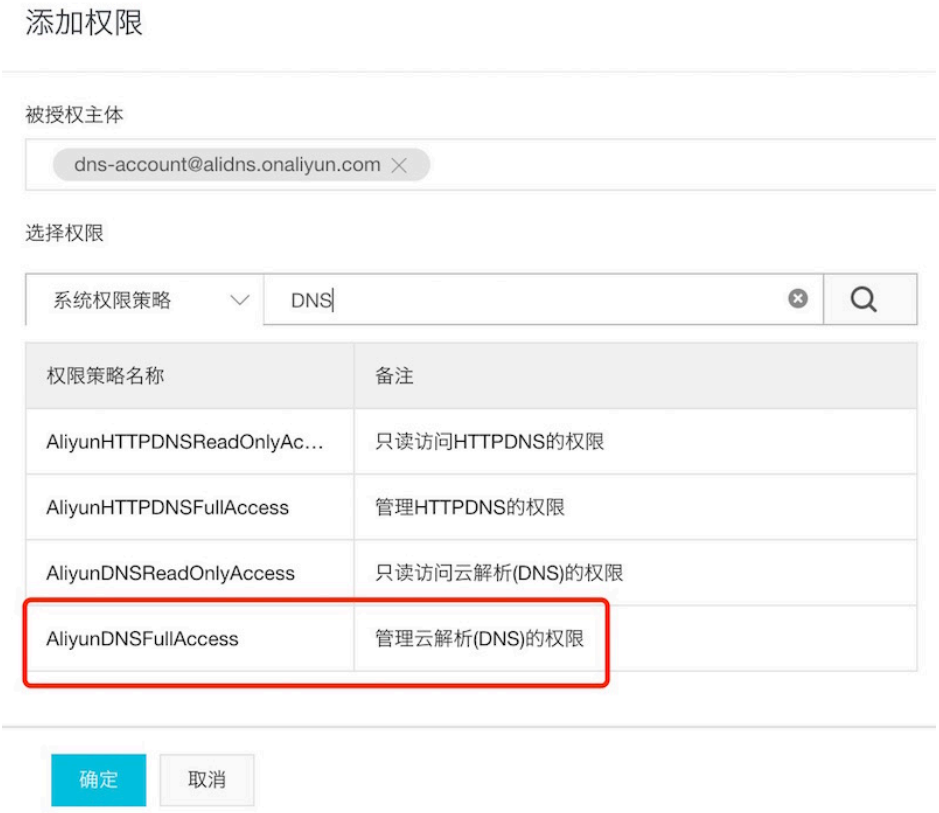
为一个子用户授权只读访问 云解析DNS 的权限

在 RAM 控制台中创建一个子用户，并为此子用户附加系统授权策略 “AliyunDNSReadyOnlyAccess”。附加授权策略的方式请参考 授权。



为一个子用户授予完全管理 云解析DNS 的权限

在 RAM 控制台中为此子用户附加系统授权策略 “AliyunDNSFullAccess”。



为一个子用户授权管理某个域名的DNS权限

该权限是指可以授权RAM用户管理某一个域名(例如example.com)的完全权限。

1. 新建权限策略

2. 脚本配置

脚本配置的示例如下：

```
{
"Version": "1",
"Statement": [
{
"Action": "alidns:*",
"Resource": "acs:alidns:*:*:domain/example.com",
"Effect": "Allow"
},
{
"Action": [
"alidns:DescribeSiteMonitorIspInfos",
"alidns:DescribeSiteMonitorIspCityInfos",
"alidns:DescribeSupportLines",
"alidns:DescribeDomains",
"alidns:DescribeDomainNs",
"alidns:DescribeDomainGroups"
],
"Resource": "acs:alidns:*:*:*",
"Effect": "Allow"
}
]
}
```

更多云解析DNS权限定义

请参考 云解析DNS OpenAPI 文档中的 RAM鉴权 部分。

解析生效测试方法

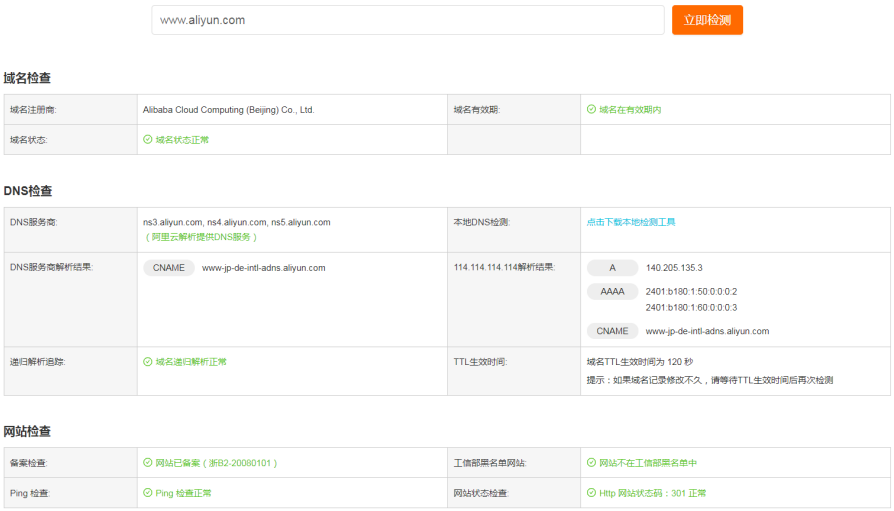
概述

测试域名解析生效的方法有以下四类

- 域名解析生效测试
- 本地域名解析生效测试
- 测试命令dig或nslookup
- 全国各地运营商解析生效测试

域名解析生效测试

可帮助用户快速排查域名、DNS、网站问题， 立即使用。



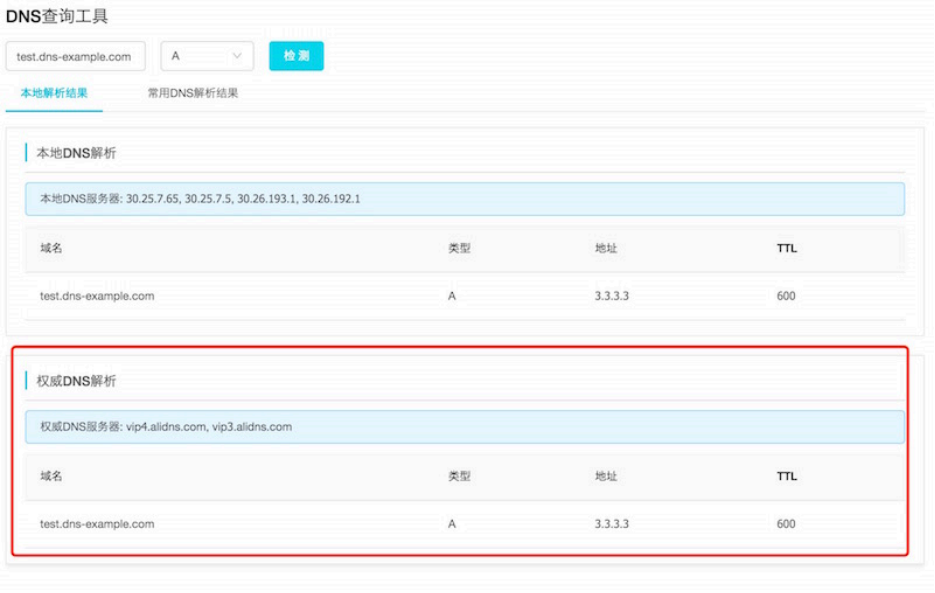
本地域名解析生效测试

此查询工具可以检测本地DNS、权威DNS、公共DNS的解析生效情况。

- 在线实时检测
- 苹果电脑下载
- windows电脑下载

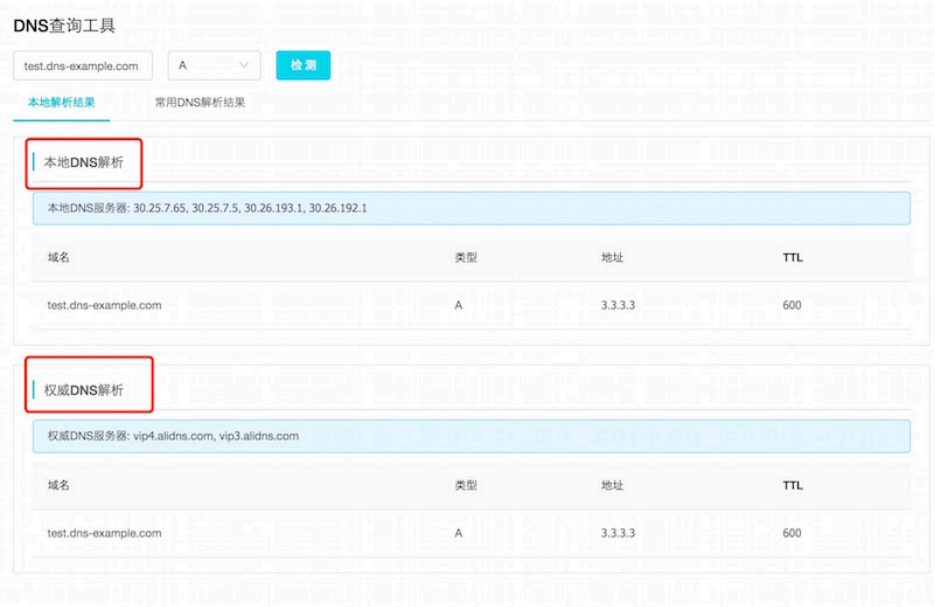
1 . 域名解析在云解析DNS上是否生效

判断方法：如果下图中权威DNS的查询结果，和您在云解析DNS设置的解析一致，则代表解析记录在云解析DNS上已生效。如查询结果与您的设置不一致，请 **提交工单** 联系阿里云售后为您处理。



2 . 域名解析在本地DNS上是否生效

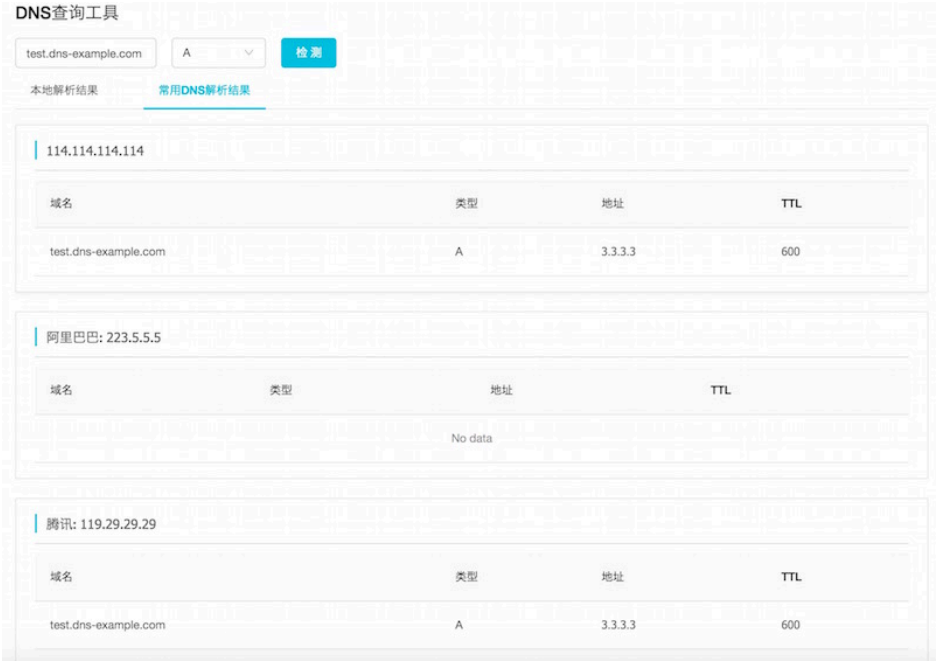
判断方法：对比权威DNS和本地DNS的查询结果，如果结果输出一致，则代表解析记录在本地DNS上已生效。如果本地DNS与权威DNS的查询结果不一致，则看下本地DNS的TTL缓存时间，可以等待该缓存时间到期后再进行测试。



3 . 域名解析在公共DNS上是否生效

大部分用户使用的本地DNS是用户在接入网络时由运营商自动分配的，例如电信、联通等。还有一部分用户的本地DNS接入的是公共DNS（例如114.114.114.114此类），都是负责DNS的递归查询环节。

判断方法：对比权威DNS和公共DNS的查询结果，如果结果输出一致，则代表解析记录在公共DNS上已生效。如果权威DNS与公共DNS的查询结果不一致，则看下公共DNS的TTL缓存时间，可以等待该缓存时间到期后再进行测试。



通过命令查询域名解析是否生效

一般常用的命令查询方法是dig或nslookup，判断方法是DNS查询返回的结果如何和您在云解析DNS中设置的一致，则代表解析已生效，如果不一致，则看下缓存时间，可以等待缓存到期后再进行测试。 dig命令安装下载方法

Linux CMD

1 . 最常用的查询命令

命令：dig test.dns-example.com

```
liwenlingdeMacBook-Pro:~ liwenling$ dig test.dns-example.com

; <<>> DiG 9.11.0-P1 <<>> test.dns-example.com +nocookie
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52070
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;test.dns-example.com.          IN      A

;; ANSWER SECTION:
test.dns-example.com.   600     IN      A       3.3.3.3

;; Query time: 40 msec
;; SERVER: 30.25.7.65#53(30.25.7.65)
;; WHEN: Thu Apr 04 17:51:17 CST 2019
;; MSG SIZE  rcvd: 65
```

解析未生效、或者未设置解析记录场景的示例

```
liwenlingdeMacBook-Pro:~ liwenling$ dig liwl.dns-example.com

; <<>> DiG 9.11.0-P1 <<>> liwl.dns-example.com +nocookie
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 2922
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;liwl.dns-example.com.          IN      A

;; AUTHORITY SECTION:
dns-example.com.        60      IN      SOA     vip1.alidns.com. hostmaster.hichina.com. 2019013016 3600 1200 86400 360

;; Query time: 53 msec
;; SERVER: 30.25.7.65#53(30.25.7.65)
;; WHEN: Thu Apr 04 18:02:56 CST 2019
;; MSG SIZE  rcvd: 116
```

2 . 根据记录类型进行查询，比如MX，CNAME，NS，PTR等，只需将类型加在命令后面即可

命令：dig test.dns-example.com cname

```
liwenlingdeMacBook-Pro:~ liwenling$ dig www.dns-example.com cname

; <<>> DiG 9.11.0-P1 <<>> www.dns-example.com cname +nocookie
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38280
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.dns-example.com.           IN      CNAME

;; ANSWER SECTION:
www.dns-example.com.    600     IN      CNAME   test.dnswork.top.

;; Query time: 47 msec
;; SERVER: 30.25.7.65#53(30.25.7.65)
;; WHEN: Thu Apr 04 17:58:40 CST 2019
;; MSG SIZE  rcvd: 78
```

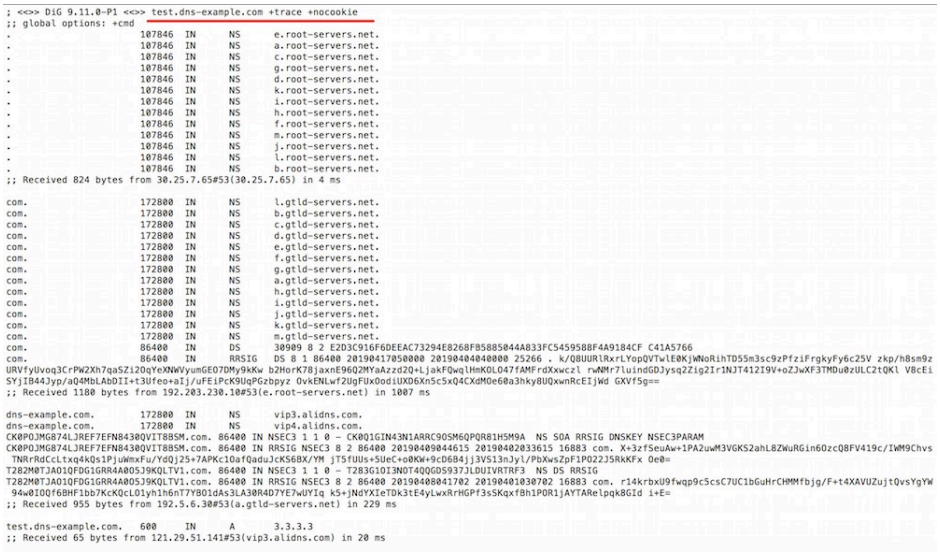
3 . 指定域名DNS服务器测试解析是否生效的命令，以下以指定云解析DNS服务器和公共DNS服务器作为查询解析是否生效的示例演示。

命令：dig test.dns-example.com @vip1.alidns.com

命令：dig test.dns-example.com @114.114.114.114

```
liwenlingdeMacBook-Pro:~ liwenling$ dig test.dns-example.com @vip1.alidns.com

; <<>> DiG 9.11.0-P1 <<>> test.dns-example.com @vip1.alidns.com +nocookie
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42702
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;test.dns-example.com.          IN      A

;; ANSWER SECTION:
test.dns-example.com.   600     IN      A       3.3.3.3

;; Query time: 149 msec
;; SERVER: 47.88.44.151#53(47.88.44.151)
;; WHEN: Thu Apr 04 18:09:31 CST 2019
;; MSG SIZE  rcvd: 65


liwenlingdeMacBook-Pro:~ liwenling$ dig test.dns-example.com @114.114.114.114

; <<>> DiG 9.11.0-P1 <<>> test.dns-example.com @114.114.114.114 +nocookie
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19170
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;test.dns-example.com.          IN      A

;; ANSWER SECTION:
test.dns-example.com.   38      IN      A       3.3.3.3

;; Query time: 34 msec
;; SERVER: 114.114.114.114#53(114.114.114.114)
;; WHEN: Thu Apr 04 18:10:23 CST 2019
;; MSG SIZE  rcvd: 65
```

4 . 另外一个重要的功能是dig+trace参数，使用这个参数之后将显示从根域逐级查询的过程,trace查询可以看到根域、 顶级域、以及一级域名的权威服务器的地址，及其各自的返回结果，这样对于追踪dns解析中的问题有很大的帮助。



5 . 需要逐级查询解析的递归过程，且指定localDNS

命令：dig 域名 @指定的localdns地址 +trace

```
; <<>> DiG 9.11.0-P1 <<>> test.dns-example.com @114.114.114.114 +trace +nocookie
;; global options: +cmd
.                       348792  IN      NS      a.root-servers.net.
.                       348792  IN      NS      f.root-servers.net.
.                       348792  IN      NS      i.root-servers.net.
.                       348792  IN      NS      l.root-servers.net.
.                       348792  IN      NS      b.root-servers.net.
.                       348792  IN      NS      m.root-servers.net.
.                       348792  IN      NS      e.root-servers.net.
.                       348792  IN      NS      j.root-servers.net.
.                       348792  IN      NS      d.root-servers.net.
.                       348792  IN      NS      h.root-servers.net.
.                       348792  IN      NS      g.root-servers.net.
.                       348792  IN      NS      k.root-servers.net.
.                       348792  IN      NS      c.root-servers.net.
;; Received 239 bytes from 114.114.114.114#53(114.114.114.114) in 34 ms

com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    86400   IN      DS      30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A
com.                    86400   IN      RRSIG   DS 8 1 86400 20190422050000 20190409040000 25
tGbsMNa6nOHErd6sFoTJKGHeJnRhLVIKOyrIJ 8n1P5yx3peUdORy46V2hFuFCdc6dnMPF4FjgDgjd+MT0HWxGWjDSHJ5
7IlkH29y8vMUyO448+B2c0f3AHiMoOjAV T3928H8l2IHhtgcRDrp0smttj4BJVDEhbR3ZkZvIcZHGIP4u17C2gqnT p
;; Received 1180 bytes from 202.12.27.33#53(m.root-servers.net) in 117 ms

dns-example.com.        172800  IN      NS      vip3.alidns.com.
dns-example.com.        172800  IN      NS      vip4.alidns.com.
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN NSEC3 1 1 0 - CK0Q1GIN43N1ARRC9OSM6QPQR81H5M9A
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN RRSIG NSEC3 8 2 86400 20190413044428 20190406
ox6whk+X9/+fITemoMGaXd4O58PuvunOfVdKyVpkp/Lw2fqd X//PtaGqQ51ZSy6iGY7V945u+FDcDG8NFjBvhCABaSN
T282M0TJAO1QFDG1GRR4A0O5J9KQLTV1.com. 86400 IN NSEC3 1 1 0 - T283G1OI3NOT4QQGDS937JLDUIVRTRF
T282M0TJAO1QFDG1GRR4A0O5J9KQLTV1.com. 86400 IN RRSIG NSEC3 8 2 86400 20190416041706 20190409
WcRZ+aFxQ2Uh9+kW4Yv96vwx+0a3DpfNQgvrkpHSCpSlZoT5 hMnTvqAEKmWOQ8sNWeY9TAEiyeGsT4pm7f6Wz1Ve7eO
;; Received 955 bytes from 192.33.14.30#53(b.gtld-servers.net) in 31 ms

test.dns-example.com.   600     IN      A       3.3.3.3
;; Received 65 bytes from 106.11.41.153#53(vip3.alidns.com) in 6 ms
```

6 . 查询域名使用的域名DNS服务器

命令：dig ns 域名（这里输入主域名即可）

```
liwenlingdeMacBook-Pro:~ liwenling$ dig ns dns-example.com

; <<>> DiG 9.11.0-P1 <<>> ns dns-example.com +nocookie
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19200
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 23

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;dns-example.com.               IN      NS

;; ANSWER SECTION:
dns-example.com.        85924   IN      NS      vip3.alidns.com.
dns-example.com.        85924   IN      NS      vip4.alidns.com.

;; ADDITIONAL SECTION:
vip3.alidns.com.        6380    IN      A       140.205.29.115
vip3.alidns.com.        6380    IN      A       170.33.23.13
vip3.alidns.com.        6380    IN      A       170.33.24.73
vip3.alidns.com.        6380    IN      A       106.11.30.115
vip3.alidns.com.        6380    IN      A       106.11.41.153
vip3.alidns.com.        6380    IN      A       116.211.173.141
vip3.alidns.com.        6380    IN      A       121.29.51.141
vip3.alidns.com.        6380    IN      A       14.1.112.21
vip3.alidns.com.        6380    IN      A       140.205.1.5
vip3.alidns.com.        6380    IN      A       140.205.228.171
vip3.alidns.com.        6380    IN      AAAA    2400:3200:1000:1::1
vip4.alidns.com.        6380    IN      A       170.33.23.14
vip4.alidns.com.        6380    IN      A       170.33.24.74
vip4.alidns.com.        6380    IN      A       106.11.30.116
vip4.alidns.com.        6380    IN      A       106.11.41.154
vip4.alidns.com.        6380    IN      A       116.211.173.142
vip4.alidns.com.        6380    IN      A       121.29.51.142
vip4.alidns.com.        6380    IN      A       14.1.112.22
vip4.alidns.com.        6380    IN      A       140.205.1.6
vip4.alidns.com.        6380    IN      A       140.205.228.172
vip4.alidns.com.        6380    IN      A       140.205.29.116
vip4.alidns.com.        6380    IN      AAAA    2400:3200:1000:1::2
```

7 . 可通过指定客户机IP，查询权威DNS返回的解析地址，来判断智能解析调度的精准度

命令：dig @权威DNS服务器 域名 +subnet=指定客户机IP

```
liwenlingdeMacBook-Pro:~ liwenling$ dig @vip3.alidns.com ns2.dns-example.com +subnet=1.1.1.1

; <<>> DiG 9.11.0-P1 <<>> @vip3.alidns.com ns2.dns-example.com +subnet=1.1.1.1 +nocookie
; (10 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8065
;; flags: qr aa rd; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; CLIENT-SUBNET: 1.1.1.1/32/24
;; QUESTION SECTION:
;ns2.dns-example.com.           IN      A

;; ANSWER SECTION:
ns2.dns-example.com.    86400   IN      A       140.205.1.2
ns2.dns-example.com.    86400   IN      A       140.205.29.114
ns2.dns-example.com.    86400   IN      A       140.205.228.52
ns2.dns-example.com.    86400   IN      A       14.1.112.11
ns2.dns-example.com.    86400   IN      A       47.88.44.152
ns2.dns-example.com.    86400   IN      A       47.88.44.151

;; Query time: 36 msec
;; SERVER: 140.205.1.5#53(140.205.1.5)
;; WHEN: Tue Apr 09 16:07:18 CST 2019
;; MSG SIZE  rcvd: 156
```

Windows CMD

1 . 查看本地DNS解析结果

命令：nslookup test.dns-example.com

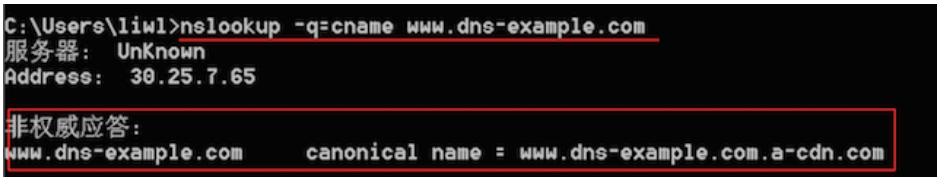
2 . 指定公共DNS，查询解析生效情况

命令：nslookup test.dns-example.com 114.114.114.114

3 . 查看权威是否生效

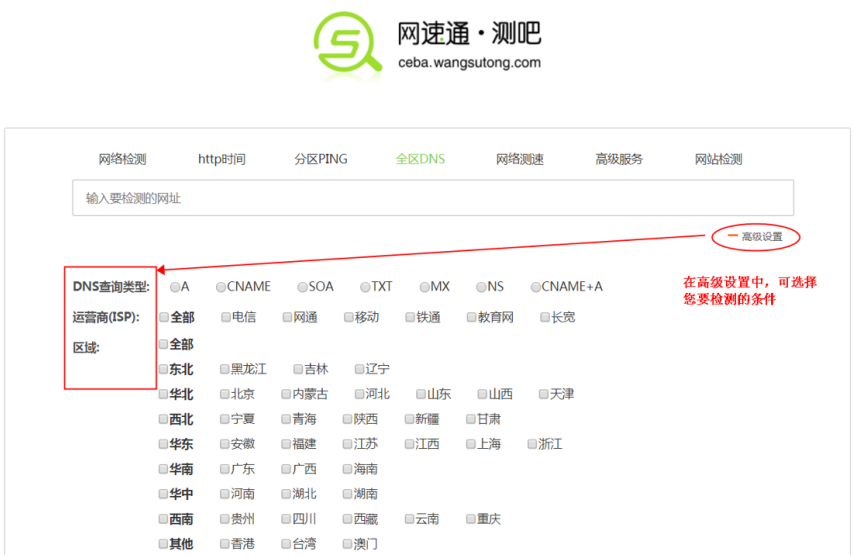
命令：nslookup test.dns-example.com vip3.alidns.com

4 . 查看非A记录结果，例如：CNAMEnslookup -q=CNAME www.dns-example.com



全国各地运营商解析生效测试

可以测试全国各地运营商DNS的解析生效情况，如果查询结果与设置的解析地址相同则代表已生效，如果查询结果与设置不符，则需要运营商DNS缓存时间到期再进行测试。立即使用



数据备份

概述

数据备份 可帮助用户实现DNS解析记录的定时备份、并支持平滑一键恢复到至指定备份版本，可以有效防止因解析记录丢失而造成的业务影响。

产品限制

1 . 数据备份是云解析DNS付费版功能，版本限制如下

版本	数据备份功能	定时备份时间
免费版	不支持	—
个人版	不支持	—
企业标准版	支持	按天备份
企业旗舰版	支持	按小时备份

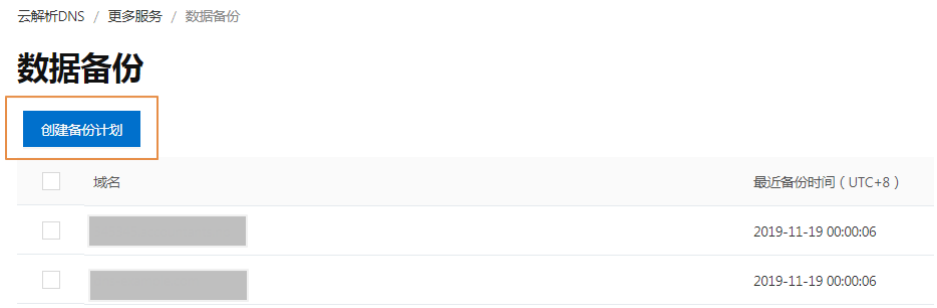
2 . 版本降级至个人版或免费版，则数据备份的 **备份管理**、**一键恢复**不可用，但可备份查看下载指定版本的备份记录，以及删除备份。

设置方法

1 . 登录 云解析DNS控制台

2 . 在域名解析页面，选择 **更多服务** 页签，选择数据备份，单击 **立即使用** 按钮。

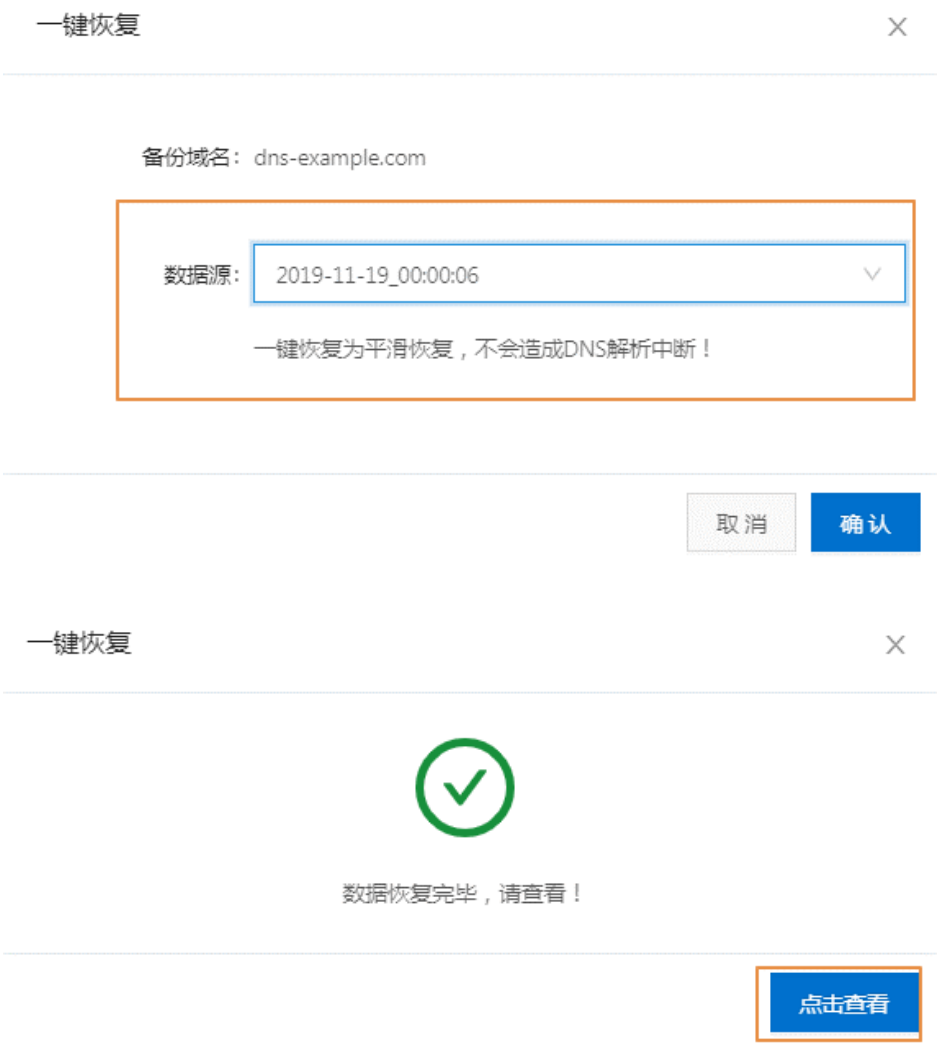
3 . 在数据备份页面下，单击 **创建备份** 按钮

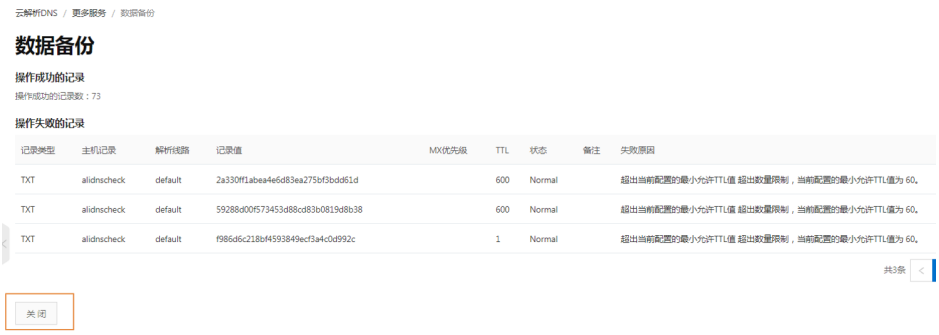


4 . 选择需要使用数据备份的域名，以及选择备份周期（备份周期请参考产品限制说明），创建备份成功。

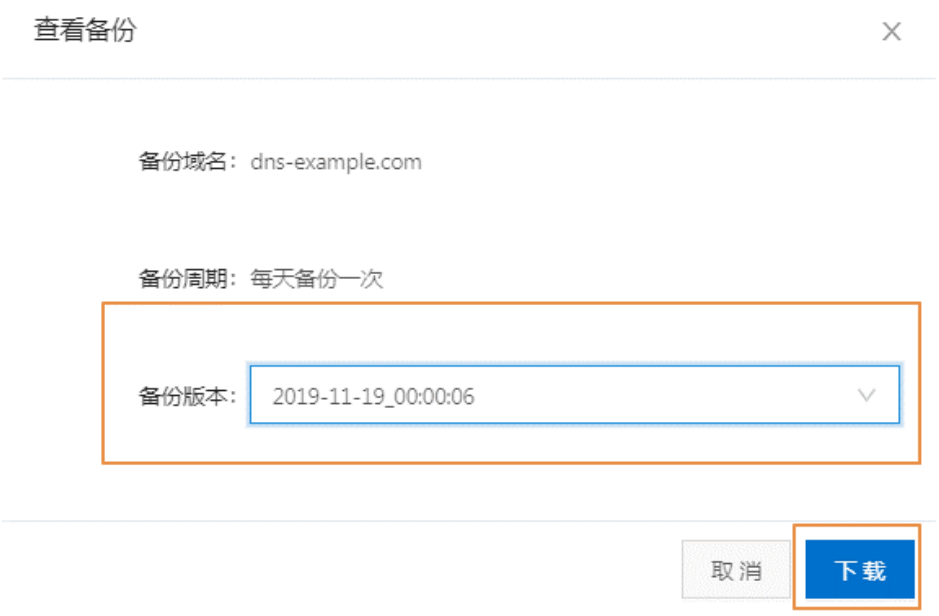
5 . 在数据备份列表中，单击 **备份管理**，可以对备份周期进行编辑修改。

6 . 在数据备份列表中，单击 **一键恢复**，可以将解析数据恢复到指定的备份时间。一键恢复是平滑恢复，不会影响业务中断。数据恢复后，可以点击 **立即查看** 按钮，查看数据恢复结果。





7 . 在数据备份列表中，单击 **查看备份**，可选择指定备份时间的解析数据进行下载。



8 . 在数据备份列表中，单击 **删除备份**，则会删除此条数据备份计划，并不会影响解析数据。

DNSSEC设置方法

什么是DNSSEC

域名系统安全扩展（DNS Security Extensions），简称DNSSEC。开启DNSSEC，可有效防止DNS欺骗和缓存污染等攻击。它是通过数字签名来保证DNS应答报文的真实性和完整性，能够保护用户不被重定向到非预期地址，从而提高用户对互联网的信任，并保护您的核心业务。

DNSSEC使用注意事项

DNSSEC目前面向付费版DNS用户（不限版本）开放使用。

使用子域名独立托管DNS功能，则不支持开启DNSSEC。

使用辅助DNS功能，则不支持开启DNSSEC。

DNS付费版到期，如计划不再使用DNS付费版时，需先到域名注册商删除DS记录，然后在云解析DNS控制台关闭DNSSEC，避免造成解析失败情况。

已开启DNSSEC服务，且使用 “域名账号间转移” 功能时，指将域名从A账号转移到B账号， 需先到域名注册商删除DS记录，然后在云解析DNS控制台关闭DNSSEC，避免造成解析失败情况。

已开启DNSSEC服务，且使用 “跨账号转移DNS解析” 功能时，指将域名DNS解析从A账号转移到B账号，需先到域名注册商删除DS记录，然后在云解析DNS控制台关闭DNSSEC，避免造成解析失败情况。

已开启DNSSEC服务，使用 “解绑域名” 功能呢时，需先到域名注册商删除DS记录，然后在云解析DNS控制台关闭DNSSEC，避免造成解析失败情况。

DNSSEC功能，需要域名解析服务商和域名注册服务商均需支持DNSSEC，方可生效，目前云解析DNS和阿里云域名注册商均支持此项服务。

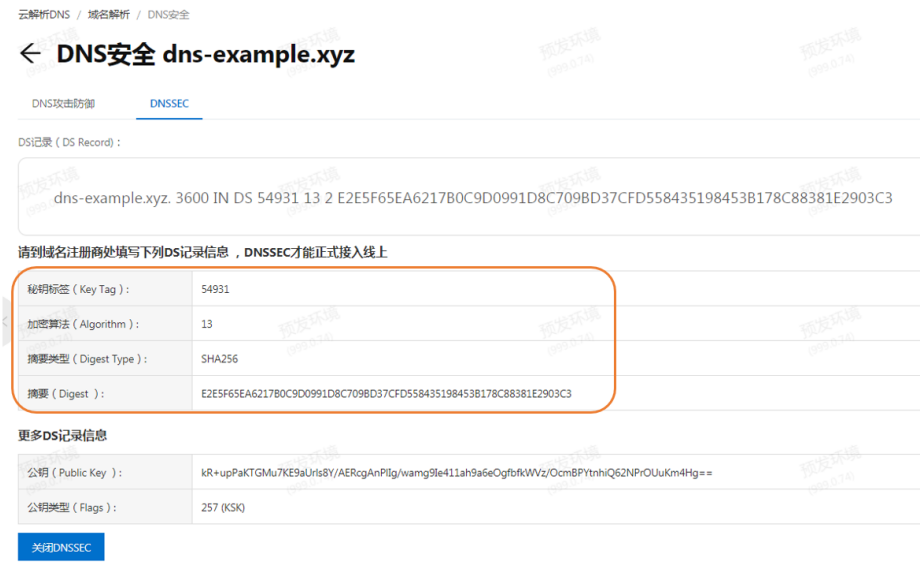
DNSSEC设置方法

① 登录 云解析DNS控制台

② 选择需要开启DNSSEC的域名，点击 **解析设置** 按钮。

③ 菜单选择 **DNS安全**， 页签选择 **DNSSEC**， 单击 **开启DNSSEC** 按钮

④ 复制DS记录信息如 **Key Tag** 、**Algorithm**、**Digest Type**、**Digest**， 然后到域名注册商处增加一条DS记录。



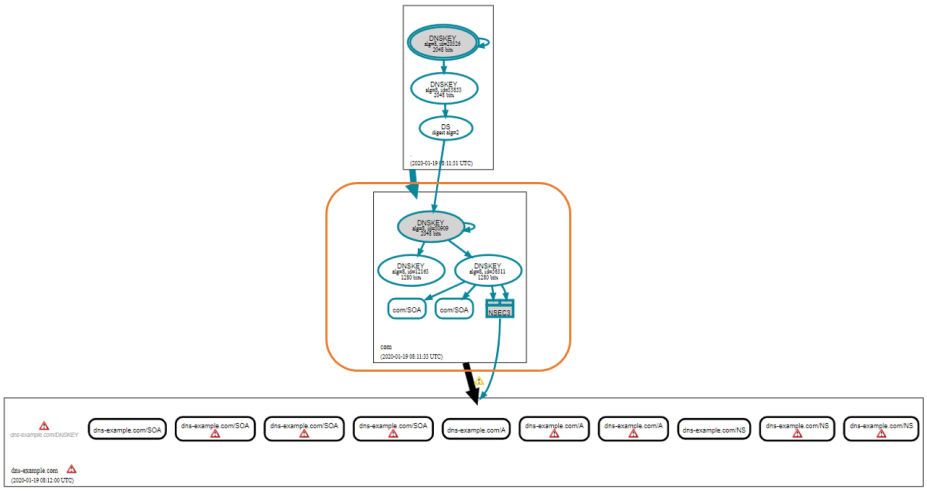
⑤ 以阿里云域名注册商为例， 请参考 **域名系统安全扩展（DNSSEC）配置** 文档

DNSSEC生效测试方法

请使用 **测试工具** 测试。

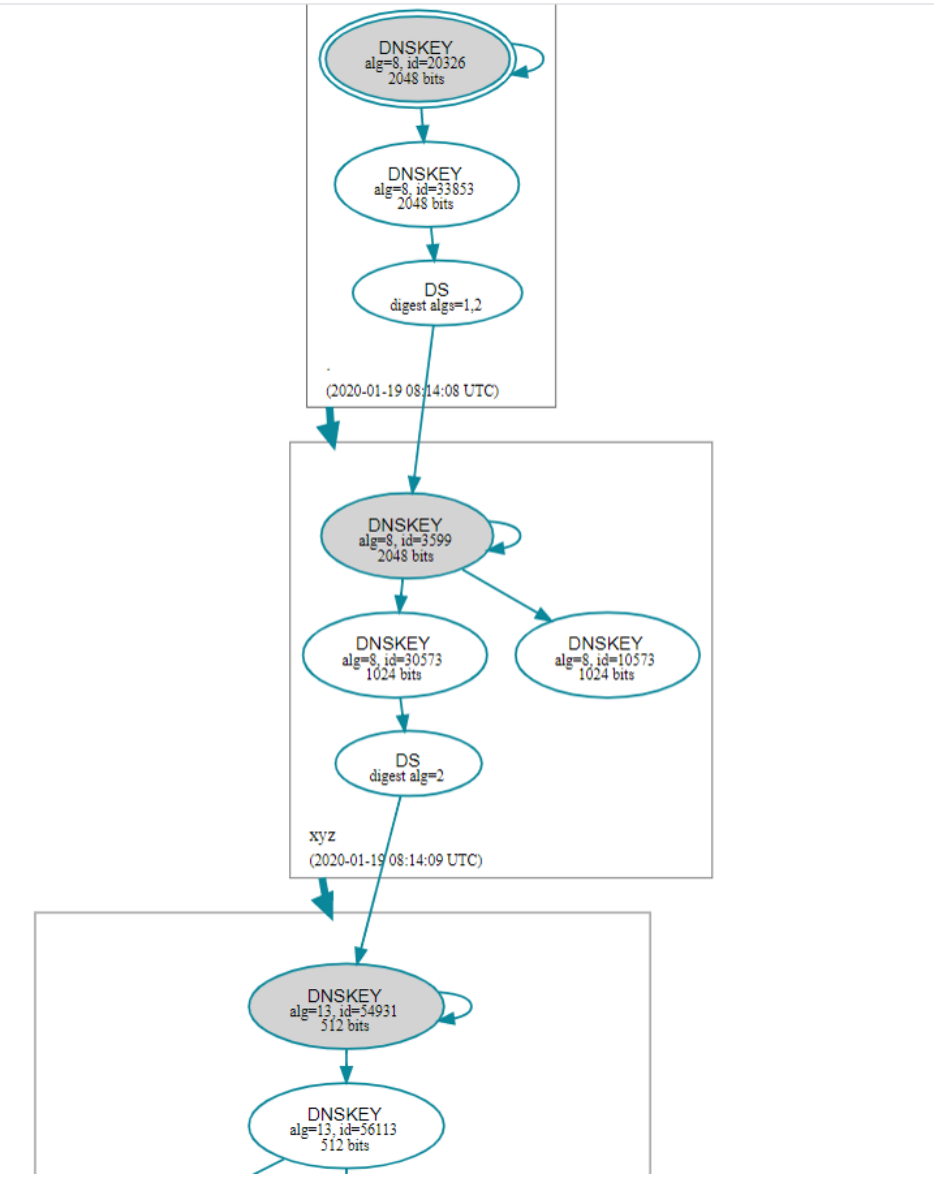
检测DNSSEC是否开启

以dns-example.com为例，例如在圈中区域未展示有 **DS** 代表未开启DNSSEC服务



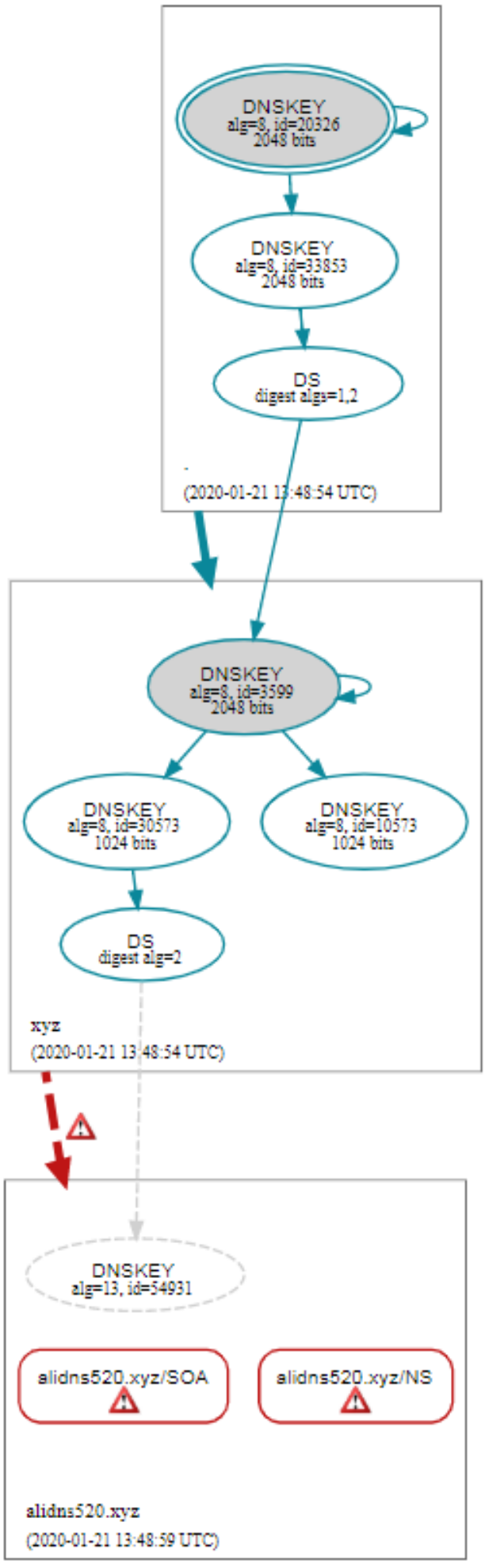
DNSSEC已生效

测试页面中如每一级都显示出了 **DS**，且无红色报错框，说明已开启DS，并已生效。



DNSSEC未生效

例如当测试页面如出现红框报错，则代表DNSSEC未生效，可通过 **提交工单** 排查。


DNSKEY
alg=8, id=20326
2048 bits
DNSKEY
alg=8, id=33853
2048 bits
DS
digest algs=1,2
.
(2020-01-21 13:48:54 UTC)
DNSKEY
alg=8, id=3599
2048 bits
DNSKEY
alg=8, id=30573
1024 bits
DNSKEY
alg=8, id=10573
1024 bits
DS
digest alg=2
xyz
(2020-01-21 13:48:54 UTC)
DNSKEY
alg=13, id=54931
alidns520.xyz/SOA
alidns520.xyz/NS
alidns520.xyz
(2020-01-21 13:48:59 UTC)

DNS联动刷新功能介绍

概述

DNS记录删除或修改的解析生效时间往往不是实时的，它会受到TTL设置的影响，也会受到运营商/公共递归DNS的设置影响，少则5分钟，长则48小时（请参阅 解析生效时间FAQ 文档）。阿里云解析DNS为了减少解析生效时间，与阿里公共递归DNS配合，发布了联动刷新功能，显著减少解析生效时间到5秒以内。

启用条件

联动刷新功能启用的条件：云解析DNS的收费版用户（包括全局流量管理GTM用户）自动生效。这些用户注册的域名的记录变更请求会实时同步到阿里公共递归DNS上。

注意：域名联动刷新的功能暂不支持泛域名。

适用人群

主要适用于对解析快速生效有强烈需求的客户，快速的DNS解析生效时间能够让业务流量调度更加灵活和迅速，容灾切换场景更加有效；

注意：一般互联网用户也可以通过设置阿里公共DNS，来获得域名解析生效加速的好处（注：阿里云解析DNS上有将近一半的国内备案域名，阿里巴巴经济体的域名也支持联动刷新）

接入方式

针对自有域名已经注册到云解析DNS的收费版用户（包括GTM用户），需要改变你们的应用客户端（移动app或pc客户端）或者缓存服务器（CDN节点）解析DNS的方式，选择阿里公共递归DNS来做DNS解析。

应用层DNS解析方式有多种方式：

1 . 用传统的DNS接口，访问阿里公共DNS 。注：需要应用发起DNS查询，使用UDP协议，端口号是53。

2 . 使用DoH的方式，阿里公共递归服务器提供两种DoH的方式，一种是wireformat二进制版，一种是DNS Json格式。具体请参阅：《阿里公共DNS安全传输服务》。

3 . 使用DoT的方式， 具体请参阅：《阿里公共DNS安全传输服务》。