ALIBABA CLOUD

# 阿里云

## 云解析 PrivateZone

## 用户指南

文档版本：20220630

阿里云

# 法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

# 通用约定

| 格式 | 说明 | 样例 |
| --- | --- | --- |
| 危险 | 该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。 | 危险<br>重置操作将丢失用户配置数据。 |
| 警告 | 该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。 | 警告<br>重启操作将导致业务中断，恢复业务时间约十分钟。 |
| 注意 | 用于警示信息、补充说明等，是用户必须了解的内容。 | 注意<br>权重设置为0，该服务器不会再接受新请求。 |
| 说明 | 用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。 | 说明<br>您也可以通过按Ctrl+A选中全部文件。 |
| > | 多级菜单递进。 | 单击**设置**> **网络**> **设置网络类型**。 |
| **粗体** | 表示按键、菜单、页面名称等UI元素。 | 在**结果确认**页面，单击**确定**。 |
| Courier字体 | 命令或代码。 | 执行 `cd /d C:/window` 命令，进入Windows系统文件夹。 |
| *斜体* | 表示参数、变量。 | `bae log list --instanceid`<br>*Instance_ID* |
| [] 或者 [a\|b] | 表示可选项，至多选择一个。 | `ipconfig [-all\|-t]` |
| {} 或者 {a\|b} | 表示必选项，至多选择一个。 | `switch {active\|stand}` |

# 目录

# 1.解析器（Resolver）

## 概述

解析器（Resolver）通过创建域名转发规则和DNS出站终端节点，可将阿里云vpc下PrivateZone 的dns请求流量转发到外部DNS系统，能够有效解决混合云、云上&云下的业务间调用场景。

## 开放地域

目前解析器功能开放的Region包括：北京、深圳、上海、杭州、张家口、呼和浩特、中国香港、美国（弗吉尼亚）共8个公共云Region；上海、深圳2个金融云Region。

## 操作流程


## 出站终端节点

## 一、创建出站终端节点

1. 登录到 云解析DNS控制台，并前往 PriviteZone 页面。
2. 依次选择 **解析器 - 出站终端节点 - 创建出站终端节点**，进行出站终端节点创建。


3. 出站终端节点创建配置。


- 终端节点名称

当前创建的终端节点名称，根据实际业务需求命名。

- 出站VPC

解析器所有出站的DNS查询流量都将经由此VPC进行流量转发。

> **注意**
>
> （1）出站终端节点一旦创建，不允许修改“出站VPC”，避免误操作造成线上流量中断。
>
> （2）目前开放区域请参考上述“开放地域”，并同步正在收集其他Region的开放优先级。如需申请其他Region，请**提交工单** 说明申请的Region。

- 选择安全组

安全组里面的规则将应用于出站VPC。

> **说明**
>
> 目前仅支持选择非托管安全组。何为托管安全组？

- 出站流量源IP地址 可用区域下子网中可用的IP地址（非ECS已占用IP地址）。为了保证高可用，解析器要求至少添加两个出站源IP地址，而且建议这2个IP地址分在不同的可用区，解析器允许添加的出站源IP地址最多为6个。

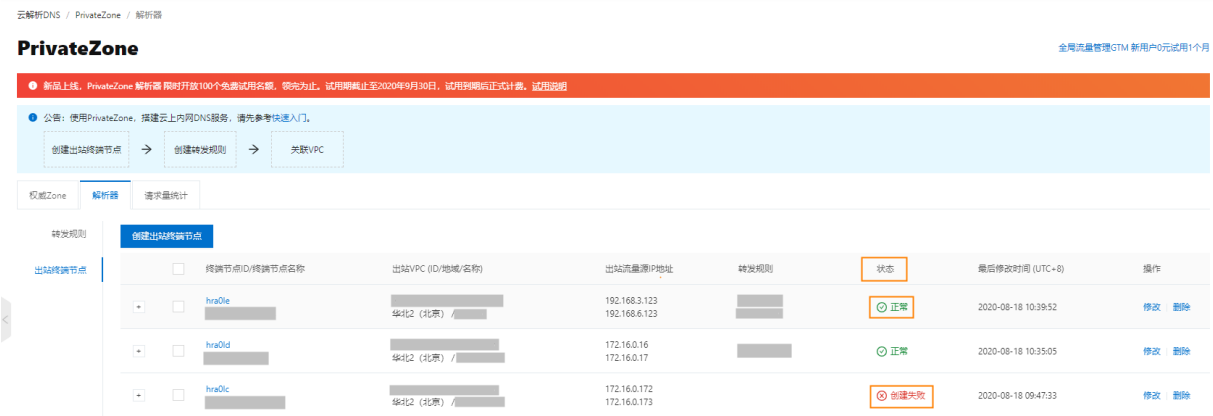
> 注意
>
> 若不进行IP地址的输入，则系统自动分配。

4. 点击 **确认** ，如果角色不存在 PrivateZone会创建一个服务关联角色。

**注：每次创建出站终端节点时，都会进行提示，但只有当角色不存在时才会创建。**


5. 出站终端节点列表会展示刚创建的节点及已经创建完成的节点。其中出站终端节点的状态包括：“正常”、“创建中”、“创建失败”、“修改中”、“修改失败”、“异常”。

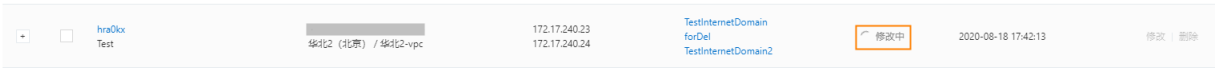
> 注意
>
> （1）创建终端节点，约需等待5-10分钟，如状态在“创建中”时，请耐心等待即可。
>
> （2）“创建中”的节点不允许修改和删除。如状态提示“异常”、“修改失败”，请**提交工单** 排查与处理。




## 二、修改出站终端节点

1. 登录到 云解析DNS控制台，并前往 PrivateZone 页面。
2. 依次选择 **解析器 - 出站终端节点**，点击终端节点后面的 **修改** ，对“终端节点名称”及“出站流量源IP地址”进行修改。


3. 修改完，点击确认后，列表中的终端节点状态会变更为“修改中”，且无法进行修改及删除。




## 三、删除出站终端节点

1.登录到 云解析DNS控制台，并前往 PrivateZone页面。

2.依次选择 **解析器 - 出站终端节点**，点击终端节点后面的 **删除** 。

> 注意
>
> 如当前出站终端节点已被关联转发规则，请先删除对应的转发规则，再操作删除出站终端节点。查看<转发规则（转发规则删除）>。

- 


## 转发规则

### 一、创建转发规则

1. 登录到 云解析DNS控制台，并前往 PrivateZone 页面。
2. 依次选择 **解析器 - 转发规则 - 创建转发规则**，进行转发规则创建。


3. 在创建转发规则页面中，进行配置。


- 规则名称

根据业务需要及业务含义进行规则命名。

- 规则类型

目前仅支持选择“转发至外部DNS系统”。

- 转发Zone

填写需要转发解析请求的Zone名称。

- 出站终端节点

使用该出站终端节点将DNS查询流量转发到目标IP地址列表中指定的IP地址。

- 外部DNS系统IP地址和端口

DNS查询流量被转发的目标服务器的IP地址和端口。（最多只能创建6个）

> **说明**
>
> 以下地址段内的IP地址为系统预留地址，不允许被配置为外部DNS系统的IP地址： 100.100.2.136-100.100.2.138,100.100.2.116-100.100.2.118

4. 配置完毕点击确认后，在转发规则列表中会生成一条转发规则。

> **注意**
>
> 转发规则中一旦创建，不允许修改“转发规则类型”、“转发Zone”、“出站终端节点”，如需修改可以先添加一条新的规则再删除这条旧的规则。


## 二、修改转发规则

1. 登录到 云解析DNS控制台，并前往 **PrivateZone** 页面。
2. 依次选择 **解析器 - 转发规则**。单击转发规则对应的 **修改** 操作按钮。


3. 进入转发规则编辑页面，进行“规则名称”、“转发目标IP地址和端口”修改。


## 三、删除转发规则

1. 登录到 云解析DNS控制台，并前往 PrivateZone 页面。
2. 依次选择 **解析器 - 转发规则**。单击转发规则对应的 **删除** 操作按钮。

> **注意**
>
> 如果当前转发规则已经进行了VPC关联，即“关联VPC状态”为已关联。则需要先进行取消VPC关联，再进行删除。取消VPC关联参考：关联VPC（取消关联VPC）。


- 已关联VPC删除报错


## 关联VPC

创建完 **转发规则** 后，需要进行 **VPC关联** ，转发规则才能对VPC内生效。

1. 登录到 云解析DNS控制台，并前往 **PriviteZone** 页面。
2. 依次选择 **解析器** - **转发规则**。单击转发规则对应的 **关联VPC** 操作按钮，选择要关联的VPC，点击 **确认** 。

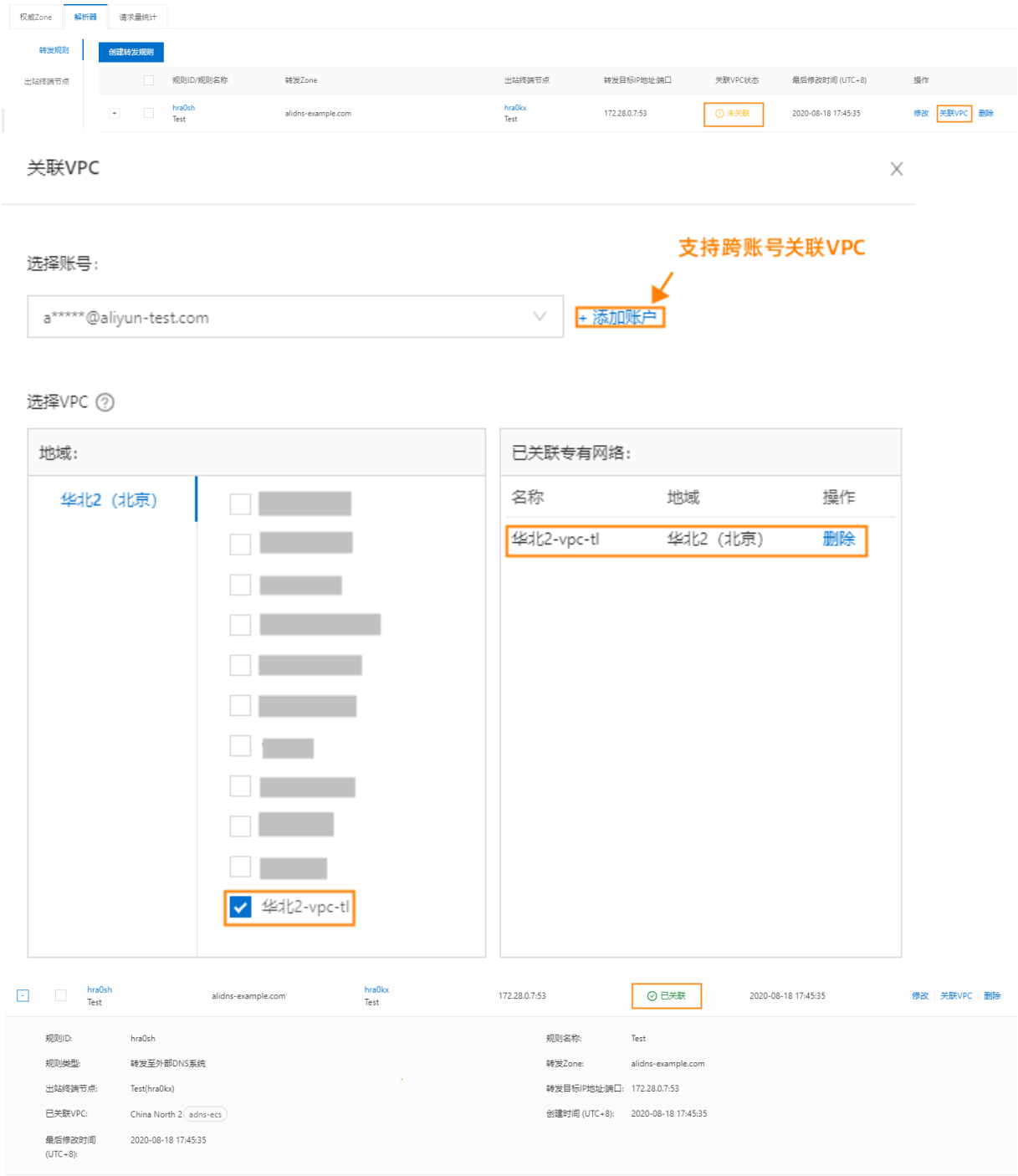
且支持跨账号关联VPC

**注意**

（1）转发规则可关联的VPC列表，必须与出站终端节点属于同一地域。

（2）不同转发规则，关联相同VPC情况下，转发Zone名称不允许相同；

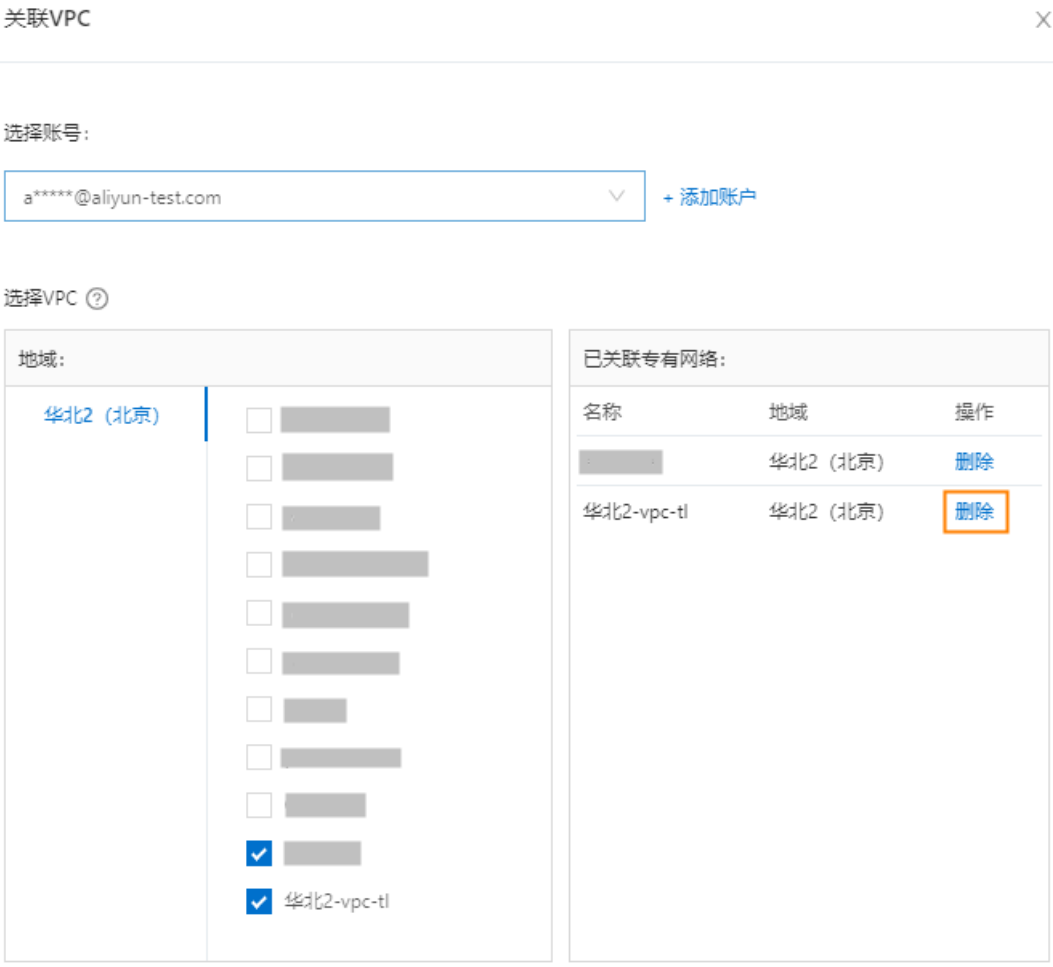
（3）转发规则与PrivateZone关联相同VPC情况下，转发Zone可以与PrivateZone中的Zone名称相同，且关联VPC内Zone解析请求由PrivateZone优先处理。




若要进行取消VPC关联，请参考以下步骤：

1.单击已经关联VPC的转发规则后方的“关联VPC”操作按钮。

2.在关联VPC配置页面，删除已经关联的VPC，并单击确认。


关联VPC
选择账号：
a*****@aliyun-test.com
+ 添加账户
选择VPC
地域：
华北2（北京）
华北2-vpc-tl
已关联专有网络：
名称
地域
操作
华北2（北京）
删除
华北2-vpc-tl
华北2（北京）
删除

# 2.添加PrivateZone解析记录

在添加一个Zone以后，您需要先为其设置相应PrivateZone解析记录，然后才能将这个Zone关联到VPC。Zone关联VPC以后，在VPC环境内，Zone的PrivateZone记录会覆盖其公网解析记录。

## 操作步骤

参照以下步骤来为Zone添加PrivateZone解析记录：

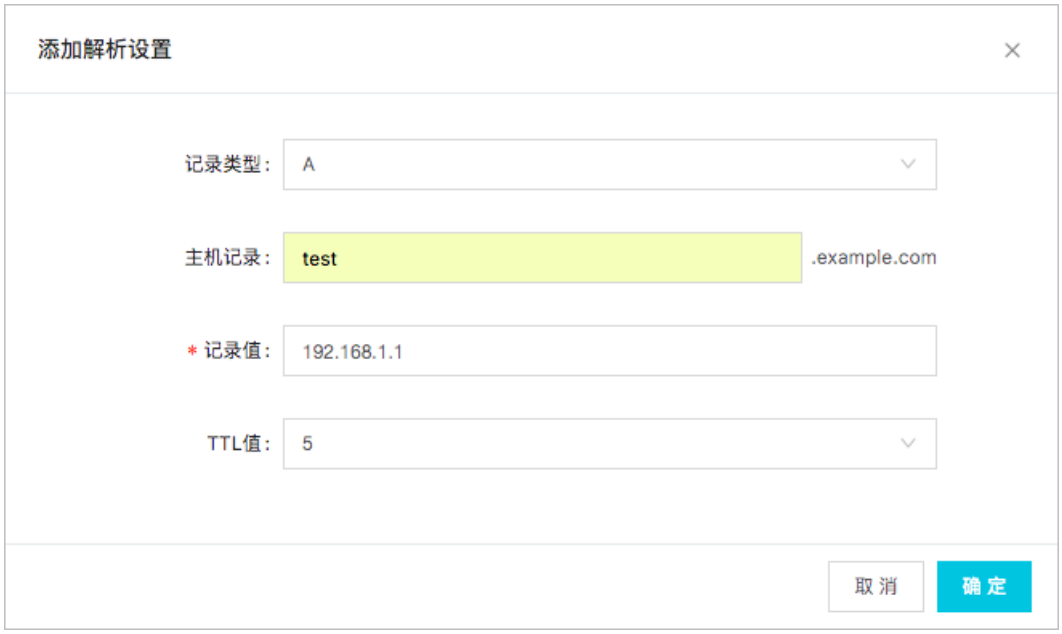
1. 登录到 云解析DNS控制台，并前往 **PriviteZone** 页面。
2. 找到需要配置PrivateZone解析记录的Zone，并单击其名称，进入解析设置控制台。
3. 在 **解析设置** 页面，单击 **添加记录** 为该Zone（私有域名）添加PrivateZone解析记录。


关于PrivateZone解析记录支持的记录类型及使用说明，请参考 PrivateZone解析记录支持的记录类型。

## 示例

### A记录

参照下图配置，为PrivateZone解析添加一条A记录。




### CNAME记录

参照下图配置，为PrivateZone解析添加一条CNAME记录。

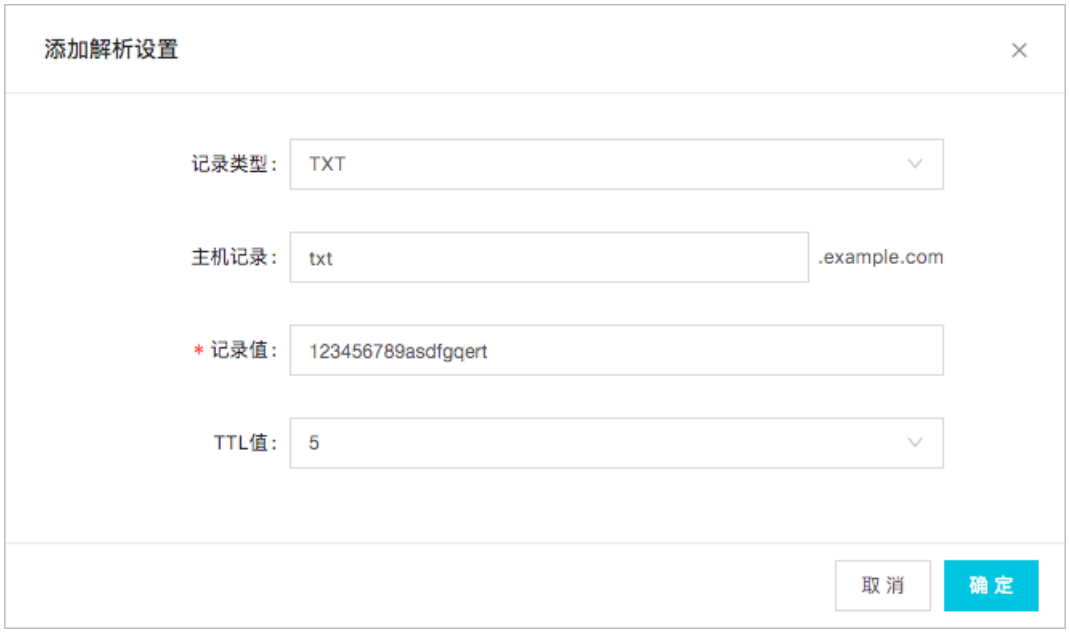

**注意**：相同主机记录的CNAME记录只能添加一条，且不能与其他任何记录共存。

## MX记录

参照下图配置，为PrivateZone解析添加一条**MX**记录。


## TXT记录

参照下图配置，为PrivateZone解析添加一条**TXT**记录。




## PTR记录

添加PTR记录前需要先配置反解Zone，具体操作请参考 反向解析及PTR记录。

### SRV记录

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。

- 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
- 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 **60秒**。

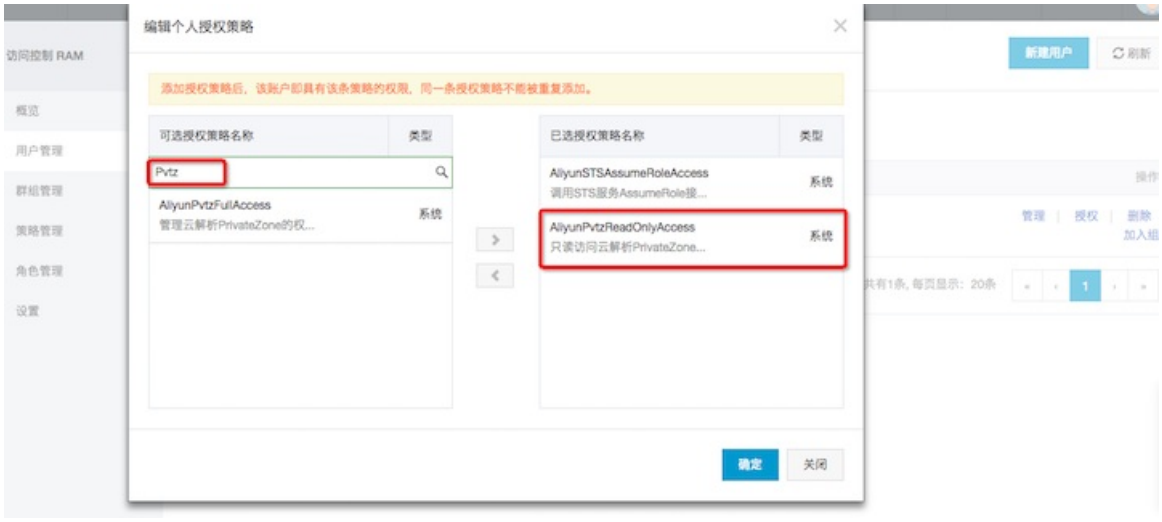
# 3.RAM授权

## 1、创建子用户

进入阿里云“访问控制RAM”控制台创建子用户，详细步骤参考请点击 。

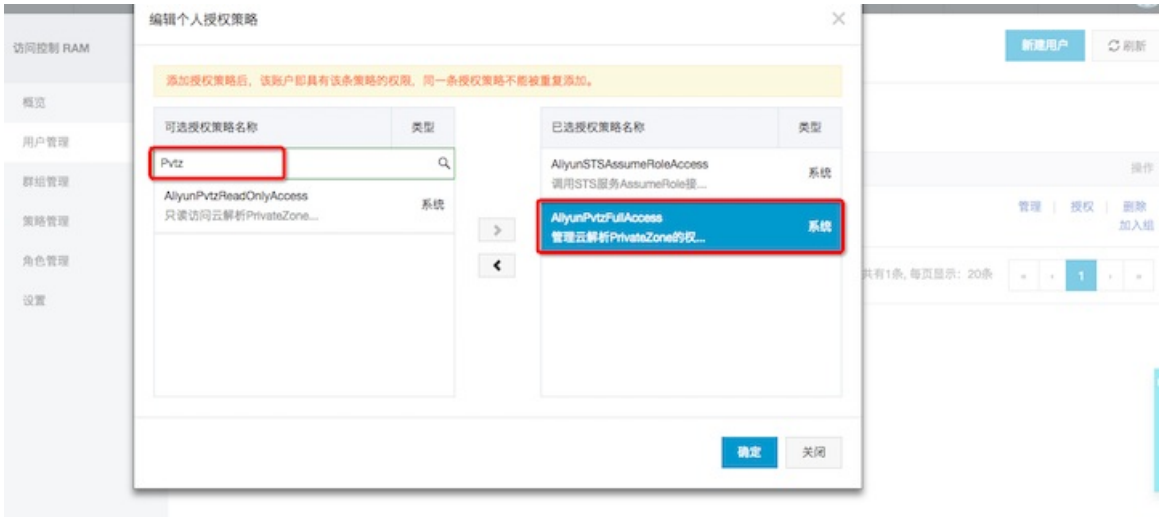
## 2、为一个子用户授予只读访问 PrivateZone 的权限

在 “访问控制RAM” 控制台中，点击“用户管理”右侧“授权”按钮，为子用户附加系统授权策略“AliyunPvtzReadOnlyAccess”。




## 3、为一个子用户授予完全管理 PrivateZone 的权限

在 “访问控制RAM” 控制台中为子用户附加系统授权策略 “AliyunPvtzFullAccess”。




## 4、为一个子用户授予管理一个 PrivateZone 的权限

您需要使用自定义授权策略功能。假设您的两个Zone ID 分别是 djiow001 和 djiow002。

- 首先，需要在“访问控制RAM”控制台的策略管理中，创建一条自定义授权策略，取名为“AliyunPvtzSingleAccess”，配置如下；


```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "pvtz:*",
      "Resource": [
                    "acs:pvtz:*:*:zone/djiow001",
                  "acs:pvtz:*:*:zone/djiow002"
                  ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "pvtz:DescribeUserServiceStatus",
        "pvtz:DescribeZones",
        "pvtz:DescribeRegions",
        "pvtz:DescribeVpcs"
      ],
      "Resource": "acs:pvtz:*:*:*",
      "Effect": "Allow"
    }
  ]
}
```

- 然后，将策略“AliyunPvtzSingleAccess”授权给子用户，即可完成指定Zone的授权；

# 4.操作审计日志

阿里云PrivateZone已与阿里云 ActionTrail 集成，您可以在 ActionTrail 中查看和检索用户行为日志，同时通过ActronTrail 将日志投递到日志服务 LogStore 或指定的 OSS Bucket 中，满足实时审计、问题回溯分析等需要。

## ActionTrail中记录的PrivateZone操作日志

PrivateZone 的操作审计日志主要包含的是 API 事件，其中 OpenAPI 事件在 ActionTrail 中记录的 eventType 取值为 ApiCall，其含义可以参考PrivateZone的API说明。

## PrivateZone 的日志样例

下面展示了一个 ActionTrail 中记录的 PrivateZone创建解析记录的日志，该条日志记录了 PrivateZone AddZoneRecord 操作记录的详细信息：


```
{
  "eventId": "99680534-****-****-****-DCFD92E18FAB",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "99680534-****-****-****-DCFD92E18FAB",
    "RecordId": 175***657,
    "Success": true
  },
  "eventSource": "pvtz.aliyuncs.com",
  "requestParameters": {
    "Rr": "abc",
    "userClientIp": "100.**.***.69",
    "AcsHost": "pvtz.aliyuncs.com",
    "ZoneId": "d696741102e*******0ca13e934bd07",
    "RequestId": "99680534-****-****-****-DCFD92E18FAB",
    "Lang": "zh",
    "HostId": "pvtz.aliyuncs.com",
    "Ttl": 60,
    "Type": "A",
    "ServiceCode": "pvtz",
    "AcsProduct": "pvtz",
    "UserClientIp": "100.**.***.69",
    "Value": "5.*.*.5",
    "RegionId": "cn-hangzhou"
  },
  "sourceIpAddress": "Internal",
  "userAgent": "AlibabaCloud (Linux; amd64) Java/1.**_172-b9 Core/***.6 HTTPClient/ApacheHt
tpClient",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::PrivateZone::ZoneRecord": [
      "175***657"
    ]
  },
  "userIdentity": {
  updateZOne  "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false"
```

```
      }
    },
    "accountId": "12046******1685",
    "principalId": "12046******1685",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "PrivateZone",
  "additionalEventData": {
    "Scheme": "http"
  },
  "apiVersion": "2018-01-01",
  "requestId": "99680534-****-****-****-DCFD92E18FAB",
  "eventTime": "2021-01-08T04:56:37Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "AddZoneRecord"
}
```