ALIBABA CLOUD

阿里云

云解析 PrivateZone

最佳实践

文档版本：20220601

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

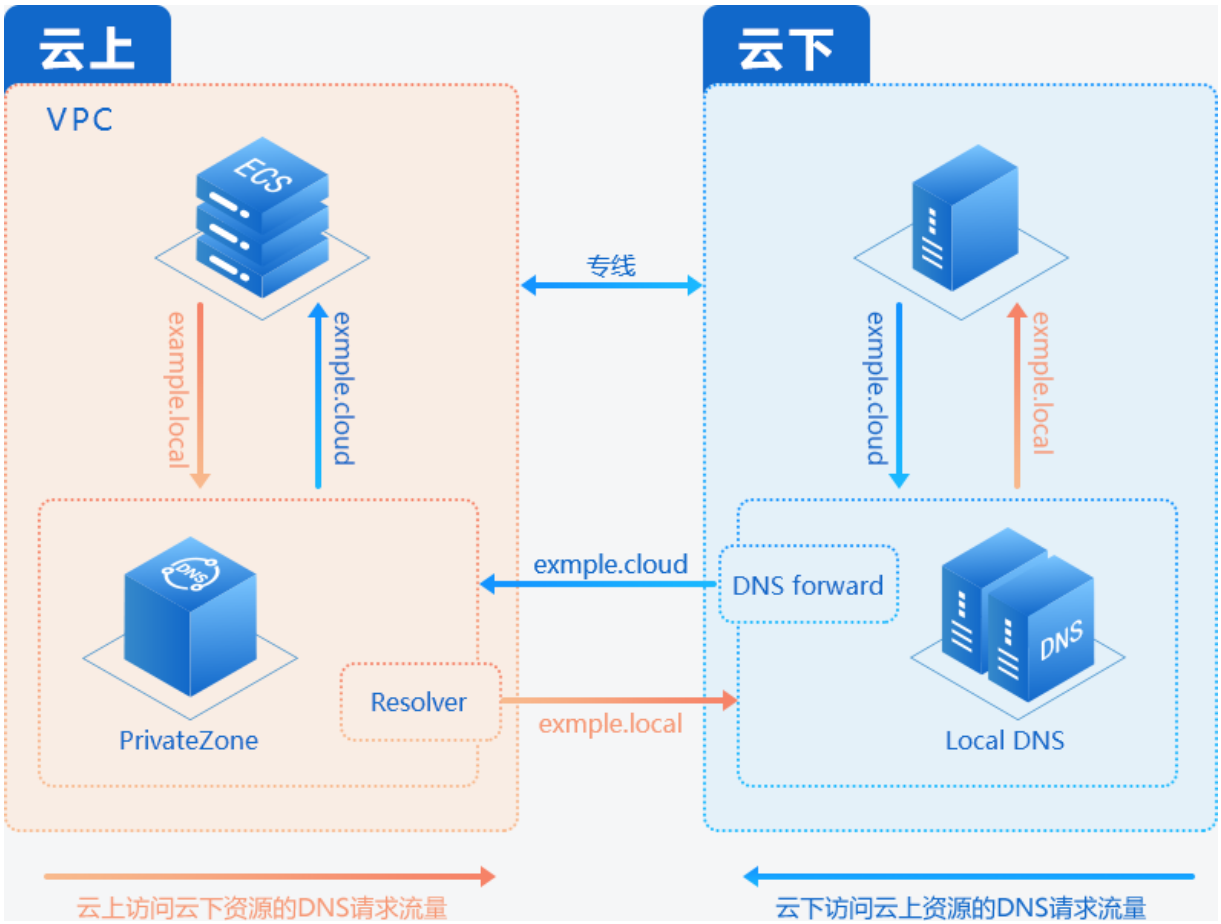
格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**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` *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.PrivateZone&VPN网关联动实现云上访问云下资源

背景描述

自建IDC和 阿里云VPC分别属于两套网络环境，但部署在自建IDC和阿里云VPC内的业务都需要通过DNS解析进行业务间调用，并且分别管理两套数据不仅给运维工程师带来重复性工作的增加，同时也会产生数据一致性管理的风险，给业务带来很高的不确定性，所以需要在自建IDC和阿里云VPC共享DNS解析数据，来实现业务间能实时调用。本文章将讲解如何实现云上PrivateZone访问云下DNS解析数据的方法。



解决方案

实现云上访问云下资源，可以通过3种解决方案实现。本文则主要为您详细说明方案一：通过解析器实现云上访问云下资源 的操作步骤和验证方法。

（一）通过解析器实现云上访问云下资源

1.通过SAG/专线/VPN等连接方式，将云上VPC与传统数据中心互联。本示例采用IPsec-VPN隧道方式。

（二）通过修改云上服务器的LocalDns实现云上访问云下资源

1.通过SAG/专线/VPN等连接方式，将云上VPC与传统数据中心互联。本示例采用IPsec-VPN隧道方式。

2.通过修改云上服务器的LocalDns，客户端发起直接向线下自建DNS服务器发起解析请求。

[centos]# vim /etc/resolv.conf

```
#根据线下自建DNS实际IP修改下方nameserver
nameserver 2.2.XX.XX
nameserver 3.3.XX.XX
```

（三）通过辅助DNS实现云上访问云下资源

1.通过SAG/专线/VPN等连接方式，将云上VPC与传统数据中心互联。本示例采用IPsec-VPN隧道方式。

2.辅助DNS。通过辅助DNS将线下自建DNS的解析同步至云上进行解析。

> 注意
>
> 自建DNS建议使用Bind，目前辅助DNS对Windows DNS Server不提供完整支持。

通过解析器实现云上访问云下资源

什么是解析器？

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。

资源准备

1.使用阿里云服务器模拟线下IDC，然后通过Bind搭建自建DNS服务。

2.阿里云VPC侧VPN网关产品服务

3.云解析PrivateZone产品服务

参考链接：

- 建立VPC到本地数据中心的连接
- strongSwan配置

操作步骤

步骤一：创建VPN网关

完成以下操作，创建VPN网关。

1. 登录专有网络管理控制台 。
2. 在左侧导航栏，单击**VPN > VPN网关**。
3. 在**VPN网关**页面，单击**创建VPN网关**。
4. 在购买页面，根据以下信息配置VPN网关，然后单击**立即购买**完成支付。
5. 返回VPN网关页面，查看创建的VPN网关。本示例VPC公网IP为：x.x.x.217

刚创建好的VPN网关的状态是准备中，约两分钟左右会变成正常状态。正常状态表明VPN网关完成了初始化，可以正常使用了。

步骤二：创建用户网关

完成以下操作，创建用户网关。

1. 在左侧导航栏，单击**VPN > 用户网关**。
2. 选择用户网关的地域。
3. 在**用户网关**页面，单击**创建用户网关**。
4. 在**创建用户网关**页面，根据以下信息配置用户网关，然后单击**确定**。
   - **名称**：输入用户网关的名称。
   - **IP地址**：输入VPC要连接的本地数据中心网关设备的公网IP。本示例模拟自建IDC的IP为：x.x.x.44
   - **描述**：输入用户网关的描述信息。

步骤三：创建IPsec连接

完成以下操作，创建IPsec连接。

1. 在左侧导航栏，单击**VPN > IPsec连接**。
2. 选择创建IPsec连接的地域。
3. 在**IPsec连接**页面，单击**创建IPsec连接**。
4. 在**创建IPsec连接**页面，根据以下信息配置IPsec连接，然后单击**确定**。
   - **名称**：输入IPsec连接的名称。
   - **VPN网关**： 选择已创建的VPN网关。
   - **用户网关**：选择要连接的用户网关。
   - **本端网段**：输入已选VPN网关所属VPC的网段。本示例为：172.25.0.0/16
   - **对端网段**：输入本地数据中心的网段。本示例为：172.28.0.0/16
   - **立即生效**：选择是否立即生效。
     - **是**：配置完成后立即进行协商。
     - **否**：当有流量进入时进行协商。
   - **预共享密钥**：输入共享密钥，该值必须与本地网关设备的预共享密钥一致。其他选项使用默认配置。
   - 高级配置：
     - IKE配置：
       - 加密算法：根据实际场景进行选择。本示例为：3des。
       - 认证算法：根据实际场景进行选择。本示例为：md5
     - IPsec配置：
       - 加密算法：根据实际场景进行选择。本示例为：3des。
       - 认证算法：根据实际场景进行选择。本示例为：md5。
       - DH分组：根据实际场景进行选择。本示例为：disabled。

步骤四：在本地网关设备中加载VPN配置

完成以下操作，在本地网关设备中加载VPN配置。

1. 在左侧导航栏，单击**VPN > IPsec连接**。
2. 选择IPsec连接的地域。
3. 在**IPsec连接**页面，找到目标IPsec连接，然后单击**操作**列下的**下载对端配置**。

4. 根据本地网关设备的配置要求，将下载的配置添加到本地网关设备中。具体参考：

   strongSwan配置。

5. 本示例采用的是Strongswan搭建IPsec-VPN服务，具体部署过程如下：

   i. 安装Strongswan：yum install strongswan -y

   ii. 配置Strongswan。本示例配置仅供参考。

(1).[centos ~]# vim /etc/strongswan/ipsec.conf

```
# ipsec.conf - strongSwan IPsec configuration file
# basic configuration

config setup
    # strictcrlpolicy=yes
    uniqueids = never

conn %default
        ikelifetime=1440m
        keylife=60m
        rekeymargin=3m
        keyingtries=0
        keyexchange=ikev1   #ike版本
        authby=psk

conn toMyIdc
      left=%defaultroute
      leftid=x.x.x.44    #本地IDC网关公网IP
      leftsubnet=172.28.0.0/16    #本地IDC私有网络地址，如果要确保VPC网段都能通，需要添加整段VPC地址
      right=x.x.x.152      #阿里云VPN网关公网IP
      rightid=x.x.x.152    #阿里云VPN网关公网IP
      rightsubnet=172.17.0.0/16     #阿里云VPN网关关联VPC私有网络地址
      auto=start   #进程主动时立即建立 IPsec 安全连接
      type=tunnel
      ike=3des-md5-modp1024
      esp=3des-md5
```

(2).运行以下命令打开ipsec.secrets配置文件。本示例配置仅供参考。

```
[centos ~]# vi /etc/strongswan/ipsec.secrets
# ipsec.secrets - strongSwan IPsec secrets file
x.x.x.44 x.x.x.152 : PSK 1234567
```

(3)./etc/sysctl.conf系统配置。本示例配置仅供参考。

```
[centos ~]# vim /etc/sysctl.conf

#配置转发，默认是0
net.ipv4.ip_forward = 1
#关闭重定向，防止恶意用户可以使用IP重定向来修改远程主机中的路由表
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0

#使配置生效
[centos ~]# sysctl -p
```

c.启动Strongswan服务

[centos ~]# systemctl start strongswan.service

d.添加路由，本示例直接在界面化添加。

在IDC核心网关上添加到对端172.17.0.0/16的路由，下一跳指向strongswan的IP 172.28.0.7。

步骤五：配置VPN网关路由

完成以下操作，配置VPN网关路由。

1. 在左侧导航栏，单击**VPN > VPN网关**。
2. 选择VPN网关的地域。
3. 在**VPN网关**页面，找到目标VPN网关，单击**实例ID/名称**列下的实例ID。
4. 在**目的路由表**页签，单击**添加路由条目**。
5. 在**添加路由条目**页面，根据以下信息配置目的路由，然后单击**确定**。
   - **目标网段**：输入本地IDC侧的私网网段。本示例为：172.28.0.0/16。
   - **下一跳**：选择IPsec连接实例。
   - **发布到VPC**：选择是否将新添加的路由发布到VPC路由表。本例选择是。
   - **权重**：选择权重值。本例选择100。

步骤六：测试网络访问

登录到阿里云VPC内一台无公网IP的ECS实例，并通过ping命令ping本地数据中心内一台服务器的私网IP地址，验证通信是否正常。

步骤七：搭建自建DNS服务

1.安装Bind：[centos ~]# yum install -y *bind

2.配置named.conf：[centos ~]# vim /etc/named.conf。本示例配置仅供参考。

```
zone "alidns-example.com" IN {
        type master;
        file "alidns-example.com.zone";
        allow-update {127.0.0.1; };
};
```

3.配置alidns-example.com.zone：[centos ~]# vim /var/named/alidns-example.com.zone。本示例配置仅供参考。

```
$TTL 3600
@       IN SOA  172.28.0.7. admin.alidns-example.com. (
                                        8       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      172.28.0.7.
@       IN      A       15.15.15.15
```

4.启动Bind：[centos ~]# systemctl start named.service。

步骤八：解析器（Resolver）配置

具体配置链接可以参考：

解析器（Resolver）

一.创建出站终端节点

完成以下操作，配置出站终端节点。

1.登录云解析控制台>PrivateZone>解析器>出站终端节点>创建出站终端节点。

2.在创建出站终端节点页面，根据以下信息进行配置，然后点击确定。

- 终端节点名称：输入终端节点名称。本示例采用Test。
- 出站VPC：解析器所有出站的DNS查询流量都将由此VPC进行流量转发。本示例选取北京Region下的vpc。
- 选择安全组：安全组里面的规则将应用于出站VPC。本示例进行了TCP/UDP 53端口入站/出站开放。

> **说明**
>
> 目前仅支持选择非托管安全组。托管安全组

- 出站流量源IP地址：选择并填入可用区内子网下的IP地址（非ECS已占用IP地址）。

二、创建转发规则

1.切换到转发规则页面，并根据以下信息进行配置转发规则，然后点击确定。

- 规则名称：输入规则名称。本示例采用Test。
- 规则类型：目前仅可选择“转发至外部DNS系统”。
- 转发Zone：填入您需要转发查询的Zone名称。本示例为：alidns-example.com。
- 出站终端节点：选择已经创建好的出站终端节点。本示例为上一步创建的出站终端节点Test。
- 外部DNS系统的IP地址和端口：线下IDC中自建DNS服务器的IP地址与端口号。本示例为：172.28.0.7:53

> **注意**
>
> 若您填写的自建DNS服务器为公网IP，且您出站终端节点VPC内ECS无公网IP，请开通
>
> NAT网关 并配置 SNAT功能。

三、关联VPC

1.选择要进行VPC关联的转发规则，点击关联VPC，进行VPC绑定。（需要与出站终端节点的VPC一致）。支持 跨账号关联VPC

步骤九：解析测试

1.登录关联VPC内的任一Ecs进行以下命令测试：

[centos ~]# dig alidns-example.com

2.如何PrivateZone同步至自建DNS

本文主要介绍企业在混合云网络场景下，如何通过PrivateZone实现内网DNS记录的配置，并同步至自建DNS。

业务场景

自建IDC与阿里云VPC通过专线或者VPN进行网络连通。部署在自建IDC和阿里云VPC内的业务均需要通过DNS查询进行业务间调用。因此需要在自建IDC和阿里云VPC共享DNS解析数据，以实现业务间能实时调用。

实现难点

自建IDC和阿里云VPC分别属于两套网络环境。在自建IDC中，客户往往已经使用bind9等开源软件搭建了自身的DNS服务；在阿里云VPC内部，客户会使用PrivateZone服务作为内网DNS解析服务。

自建IDC和PrivateZone的数据共享是混合云内网DNS中的一大痛点。分别管理两套数据不仅给运维工程师带来重复新工作的增加，同时也数据一致性管理的风险。给业务带来不确定性。

本文介绍一种自动DNS同步解决方案，可以自动将客户在PrivateZone控制台配置的解析记录同步至自建IDC服务器上，并生成标准Zone文件，bind9可以加载生效。

解决方案

1. 解析记录管理：解析记录管理通过阿里云PrivateZone控制台完成，PrivateZone提供web控制台UI，管理DNS解析记录十分方便；
2. 解析记录同步：在此我们提供一款轻量级的DNS记录同步工具，通过阿里云账号AK，自动读取PrivateZone的解析记录，并在本地生成Zone文件，点击下载工具，下载后解压缩。
3. 解析记录加载：自建IDC内部DNS软件bind9加载生成的Zone文件。
4. 解析生效测试：使用dig或者ping命令验证是否生效。

详细配置

这里以example.com为例，进行说明。

工具配置介绍：

工具有两部分组成，同步程序 `Zone_file_sync` 和 配置文件 `config.json` 。

1. `config.json` 的配置格式：

```
{
  "accessKeyId": "LCAIF4bcGHrU****",
  "accessKeySecret": "KT4eXSgppowkkPZ5AgSbxNMBHl****",
  "zone": [
    {
      "zoneName": "example.com",
      "zoneId": "298cc343c4387b0745e9b5e24fdej624",
      "filePath": "/var/named/example.com.zone"
    }
  ]
}
```

其中：

- `accessKeyId` 与 `accessKeySecret` 为阿里云账号AK;
- `zoneName` 与 `zoneId` 为PrivateZone控制台显示的Zone名称和Zoneid，请替换为自己的配置;
- `filePath` 为工具生成的Zone文件在自建IDC的DNS服务器上存放的目录，建议为您的bind9的Zone文件存放目录;
- `Zone` 内部是JSON列表，可以配置多个需要同步的Zone，最多一次同步10个Zone;

bind9配置介绍

1. bind9的 `named.conf` 配置：在 `named.conf` 文件中， `example.com` 的配置如下：

```
zone "example.com" IN {
     type master;
     file "example.com.zone";
     allow-update { 127.0.0.1; };
};
```

自动同步配置

在准备好同步工具和bind9后，按照如下命令的顺序，进行执行，同步最新的PrivateZone记录。（这里需要将命令替换为具体实际执行的命令。）

1. 执行更新锁定： `/usr/sbin/rndc freeze host.local` ;
2. 执行同步记录： `./Zone_file_sync -c config.json` ;
3. 执行bind9数据加载： `/usr/sbin/rndc thaw host.local` ;

以上命令，您可以写成shell脚本，并使用linux服务器的crontab功能进行定时执行，以实现自动同步PrivateZone的记录更新功能。

生效测试

使用如下命令进行测试： `dig @localhost 域名` ;

总结：

本文介绍了一种使用自动同步工具的方式，将PrivateZone的解析记录同步至本地自建IDC内部DNS服务器的方式。方便运维工程师搭建混合云DNS解析方案，有效的降低了混合云场景下DNS配置的复杂度，同时能够避免专线或者VPN的故障对自建IDC内部DNS解析的影响。