

ALIBABA CLOUD

Alibaba Cloud

云解析 PrivateZone
用户指南

文档版本：20201124

 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 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.解析器 (Resolver)	05
------------------	----

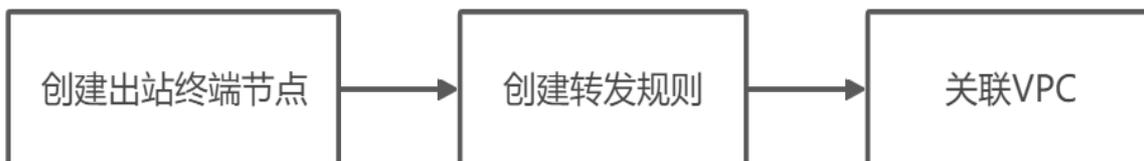
1.解析器 (Resolver)

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。

试用说明

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 PrivateZone 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。

创建出站终端节点
✕

*** 终端节点名称:**

Test

*** 出站VPC ?**

华北2 (北京) / 华北2-vpc-tl ▼

创建出站终端节点之后, 无法更改此值

*** 选择安全组 ?**

[Blank] ▼

创建出站终端节点之后, 无法更改此值

出站流量源IP地址 (为了保证高可用, 至少添加2个, 最多可添加6个) ?

选择可用区	选择vswitch	选择子网	IP地址	
华北 2 可用区... ▼	vsw-2zesd263... ▼	172.17.240.0/20 ▼	172.17.240.x	⊖
华北 2 可用区... ▼	vsw-2zesd263... ▼	172.17.240.0/20 ▼	172.17.240.y	⊖

+ 新增一行

执行此操作时, 如果角色不存在 PrivateZone会创建一个服务关联角色

角色名称: AliyunServiceRoleForPvtz

角色权限策略: AliyunServiceRolePolicyForPvtz

权限说明: 创建终端节点需要访问ECS、VPC产品的云服务资源, PrivateZone使用此角色获取ECS/VPC的访问权限。 [PrivateZone服务关联角色说明](#)

取消

确认

- 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) 目前新品试用期间仅开放北京区域节点，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。

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。

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。

执行此操作时，如果角色不存在 PrivateZone会创建一个服务关联角色

角色名称: AliyunServiceRoleForPvtz
 角色权限策略: AliyunServiceRolePolicyForPvtz
 权限说明: 创建终端节点需要访问ECS、VPC产品的云服务资源，PrivateZone使用此角色获取ECS/VPC的访问权限。[PrivateZone服务关联角色说明](#)

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。

云解析DNS / PrivateZone / 解析器

PrivateZone 全局流量管理GTM 新用户0元试用1个月

新品上线，PrivateZone 解析器 同时开放100个免费试用名额，领完为止。试用期限截止至2020年9月30日，试用到期后正式计费。 [查看详情](#)

公告：使用PrivateZone，搭建云上内网DNS服务，请先参考快速入门。

创建出站终端节点 > 创建转发规则 > 关联VPC

PrivateZone 解析器 请求量统计

创建出站终端节点

终端节点ID/终端节点名称	出站VPC (ID/地域/名称)	出站流量源IP地址	转发规则	状态	最后修改时间 (UTC+8)	操作
hra0e	华北2 (北京) /	192.168.3.123 192.168.6.123		正常	2020-08-18 10:39:52	修改 删除
hra0d	华北2 (北京) /	172.16.0.16 172.16.0.17		正常	2020-08-18 10:35:05	修改 删除
hra0c	华北2 (北京) /	172.16.0.172 172.16.0.173		创建失败	2020-08-18 09:47:33	修改 删除

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。

编辑出站终端节点
✕

*** 终端节点名称:**

Test

出站VPC ?

[Redacted]

创建出站终端节点之后，无法更改此值

*** 选择安全组** ?

[Redacted] ▾

创建出站终端节点之后，无法更改此值

出站流量源IP地址 (为了保证高可用，至少添加2个，最多可添加6个) ?

选择可用区	选择vswitch	选择子网	IP地址
华北 2 可用区... ▾	vsw-2zesd263... ▾	172.17.240.0/20 ▾	172.17.240.23 ⊖
华北 2 可用区... ▾	vsw-2zesd263... ▾	172.17.240.0/20 ▾	172.17.240.24 ⊖

+ 新增一行

执行此操作时，如果角色不存在 PrivateZone会创建一个服务关联角色

角色名称: AliyunServiceRoleForPvtz

角色权限策略: AliyunServiceRolePolicyForPvtz

权限说明: 创建终端节点需要访问ECS、VPC产品的云服务资源，PrivateZone使用此角色获取ECS/VPC的访问权限。 [PrivateZone服务关联角色说明](#)

取消
确认

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。

□	hra0lx Test	[Redacted] 华北2 (北京) / 华北2-vpc	172.17.240.23 172.17.240.24	TestInternetDomain forDel TestInternetDomain2	修改中	2020-08-18 17:42:13	修改 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。

创建转发规则
X

*** 规则名称:**

Test

*** 规则类型:**

转发至外部DNS系统 v

创建转发规则之后，无法更改此值

*** 转发Zone:**

alidns-example.com

创建转发规则之后，无法更改此值

*** 出站终端节点 ?**

Test v

创建转发规则之后，无法更改此值

+ 创建出站终端节点

*** 外部DNS系统的IP地址和端口 ?**

IP地址	端口
172.28.0.7	53

- **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。

<input type="checkbox"/>	hra0li Test	alidns-example.com	hra0lx Test	172.28.0.7:63	已关联	2020-08-11 15:10:45	修改 关联VPC 删除						
规则ID:	hra0li	规则名称:	Test	转发Zone:	alidns-example.com	出站终端节点:	Test(hra0lx)	转发目标IP地址:端口:	172.28.0.7:63	已关联VPC:	China North 2 华北2-vpc	创建时间 (UTC+8):	2020-08-10 16:54:12
最后修改时间 (UTC+8):	2020-08-11 15:10:45												

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。

权威Zone	解析器	请求量统计						
转发规则	创建转发规则							
出站终端节点	<input type="checkbox"/>	规则ID/规则名称	转发Zone	出站终端节点	转发目标IP地址:端口	关联VPC状态	最后修改时间 (UTC+8)	操作
	<input type="checkbox"/>	hra0sh Test	alidns-example.com	hra0lx Test	172.28.0.7:53	未关联	2020-08-18 17:45:35	修改 关联VPC 删除

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。

编辑转发规则 X

* 规则名称:

Test

* 规则类型:

转发至外部DNS系统
▼

创建转发规则之后，无法更改此值

* 转发Zone:

alidns-example.com

创建转发规则之后，无法更改此值

* 出站终端节点 ?

Test
▼

创建转发规则之后，无法更改此值

* 外部DNS系统的IP地址和端口 ?

IP地址	端口
172.28.0.7	53

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 \(取消关联VPC\) >](#)。

出站终端节点	规则ID/规则名称	转发Zone	出站终端节点	转发目标IP地址/端口	关联VPC状态	最后修改时间 (UTC+8)	操作
hra0sh	Test	alidns-example.com	hra0sh Test	172.28.0.7:53	已关联	2020-08-18 17:45:35	修改 关联VPC 删除

- 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 **PrivateZone** 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**。

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。

出站终端节点	规则ID/规则名称	转发Zone	出站终端节点	转发目标IP地址/端口	关联VPC状态	最后修改时间 (UTC+8)	操作
	hra0sh Test	alidns-example.com	hra0lx Test	172.28.0.7:53	未关联	2020-08-18 17:45:35	修改 关联VPC 删除

关联VPC

选择账号:

+ 添加账号

支持跨账号关联VPC

选择VPC ?

地域:

华北2 (北京)

- [模糊名称]
- 华北2-vpc-tl

已关联专有网络:

名称	地域	操作
华北2-vpc-tl	华北2 (北京)	删除

出站终端节点	规则ID/规则名称	转发Zone	出站终端节点	转发目标IP地址/端口	关联VPC状态	最后修改时间 (UTC+8)	操作
	hra0sh Test	alidns-example.com	hra0lx Test	172.28.0.7:53	已关联	2020-08-18 17:45:35	修改 关联VPC 删除

规则ID:	hra0sh	规则名称:	Test
规则类型:	转发至外部DNS系统	转发Zone:	alidns-example.com
出站终端节点:	Test(hra0lx)	转发目标IP地址/端口:	172.28.0.7:53
已关联VPC:	China North 2 (adns-ecs)	创建时间 (UTC+8):	2020-08-18 17:45:35
最后修改时间 (UTC+8):	2020-08-18 17:45:35		

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。

出站终端节点	规则ID/规则名称	转发Zone	出站终端节点	转发目标IP地址/端口	关联VPC状态	最后修改时间 (UTC+8)	操作
	hra0sh Test	alidns-example.com	hra0lx Test	172.28.0.7:53	已关联	2020-08-18 17:45:35	修改 关联VPC 删除

规则ID:	hra0sh	规则名称:	Test
规则类型:	转发至外部DNS系统	转发Zone:	alidns-example.com
出站终端节点:	Test(hra0lx)	转发目标IP地址/端口:	172.28.0.7:53
已关联VPC:	China North 2 (adns-ecs)	创建时间 (UTC+8):	2020-08-18 17:45:35
最后修改时间 (UTC+8):	2020-08-18 17:45:35		

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

X

选择账号:

a*****@aliyun-test.com ▼ [+ 添加账号](#)

选择VPC ?

地域:		已关联专有网络:		
华北2 (北京)	<input type="checkbox"/>	名称	地域	操作
	<input type="checkbox"/>		华北2 (北京)	删除
	<input type="checkbox"/>	华北2-vpc-tl	华北2 (北京)	删除
	<input type="checkbox"/>			
	<input checked="" type="checkbox"/>			
	<input checked="" type="checkbox"/>	华北2-vpc-tl		