

云解析服务

# 产品介绍

文档版本 01  
发布日期 2024-04-30



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

---

# 目录

---

<b>1 什么是云解析服务?</b>	<b>1</b>
<b>2 公网域名解析</b>	<b>3</b>
<b>3 内网域名解析</b>	<b>6</b>
<b>4 反向解析</b>	<b>9</b>
<b>5 智能线路解析</b>	<b>10</b>
<b>6 功能总览</b>	<b>11</b>
<b>7 约束与限制</b>	<b>14</b>
<b>8 安全</b>	<b>16</b>
8.1 责任共担	16
8.2 身份认证与访问控制	17
8.3 审计与日志	17
8.4 服务韧性	17
8.5 监控安全风险	18
8.6 认证证书	18
<b>9 权限管理</b>	<b>20</b>
<b>10 与其他服务的关系</b>	<b>23</b>
<b>11 基本概念</b>	<b>25</b>
11.1 域名格式与级别	25
11.2 记录集及类型	25
11.3 区域和可用区	27
11.4 项目	29
<b>12 修订记录</b>	<b>30</b>

# 1 什么是云解析服务?

云解析服务（Domain Name Service, DNS）提供高可用、高扩展的DNS服务，把人们常用的域名（如www.example.com）转换成用于计算机连接的IP地址（如192.1.2.3）。云解析服务可以让您直接在浏览器中输入域名，访问网站或Web应用程序。

云解析服务默认开通，并且可以免费使用。

## 基本功能

云解析服务为您提供以下解析服务类型：

- **公网域名解析**  
云解析服务将公网域名与IP地址相关联，为您提供基于Internet网络的域名解析服务，实现通过域名直接访问网站或者Web应用程序。
- **内网域名解析**  
云解析服务将在VPC内生效的内网域名与私网IP地址相关联，为华为云上资源提供VPC内的域名解析服务。
- **反向解析**  
云解析服务支持通过IP地址反向获取该IP地址指向的域名，通常用于自建邮件服务器的场景，是提高邮箱IP和域名信誉度的必要设置。
- **智能线路解析**  
云解析服务支持按运营商、地域等不同访问者IP的来源和类型，对同一域名的访问请求作出不同的解析响应，指向不同服务器的IP地址。解决跨运营商或者跨地域访问慢的难题，提高解析效率。

## 产品优势

云解析服务具有以下优势：

- **高性能**  
云解析服务采用自研的新一代高性能解析加速服务，单节点支持千万级并发，为您提供高效稳定的解析服务。
- **轻松访问云上资源**  
云解析服务支持为云服务器创建内网域名，既支持云服务器之间通过内网域名互相访问，也支持云服务器通过内网DNS访问云上资源，无需经过Internet，访问时延小，性能高。

您可以参考[为云服务器配置内网域名](#)为您的云服务器创建域名。

- 平滑切换无感知  
支持将使用中的网站域名迁移至华为云云解析服务进行解析。在域名转入时，我们可以提前创建域名，并设置解析记录，使您网站的DNS服务实现平滑切换，用户访问体验不中断。
- 核心数据安全隔离  
对于保存核心数据的云服务器，不绑定弹性IP，使用内网DNS为其提供域名解析服务，这样，既保证了核心数据的安全性，又实现了对核心数据的访问。

## 如何使用云解析服务

云解析服务提供了Web化的服务管理平台，即管理控制台和基于HTTPS请求的API管理方式。

- 控制台方式  
用户可直接登录管理控制台访问云解析服务。
  - 如果用户已注册账户，可直接登录管理控制台，从主页选择“网络 > 云解析服务”。
  - 如果未注册，请参见[入门指引](#)中的“注册华为云”。通过管理控制台上的简单配置，可以快速的让DNS服务开始提供域名解析工作。
- API方式  
如果用户需要将云解析服务集成到第三方系统，用于二次开发，请使用API方式访问云解析服务，具体操作请参见《[云解析服务API参考](#)》。

# 2 公网域名解析

## 什么是公网域名解析

公网域名解析是基于Internet网络的域名解析过程，可以把人们常用的域名（如www.example.com）转换成用于计算机连接的IP地址（如1.2.3.4）。公网域名解析支持通过直接在浏览器中输入域名，访问网站或Web应用程序。

云解析服务为您的网站、邮箱服务器等提供公网域名解析服务。

## 实现通过域名访问网站

公网域名解析可以应用于网站搭建场景。如果您想要搭建一个网站，并且使其可以通过Internet被访问，需要完成以下环节的工作：

1. 通过域名注册商注册域名
2. 搭建网站

您可以选择通过华为云或者其他云平台搭建您的网站。

3. 解析域名

您可以选择华为云的云解析服务为您的网站域名提供DNS解析服务。要实现这一点，您需要在云解析服务中创建公网域名，并添加域名到弹性公网IP的解析记录。

[配置网站解析](#)指导您完成域名解析。

之后，您就可以通过在浏览器输入域名访问您的网站，其过程如[图2-1](#)所示。

图 2-1 访问网站示意图



- “阶段一”表示云解析服务的公网域名解析过程。
- “阶段二”表示公网域名解析成功后，用户通过域名访问网站服务器的过程。

公网域名解析过程与域名的分层结构有关，下面详细介绍域名分层结构及域名解析过程。

## 域名分层结构

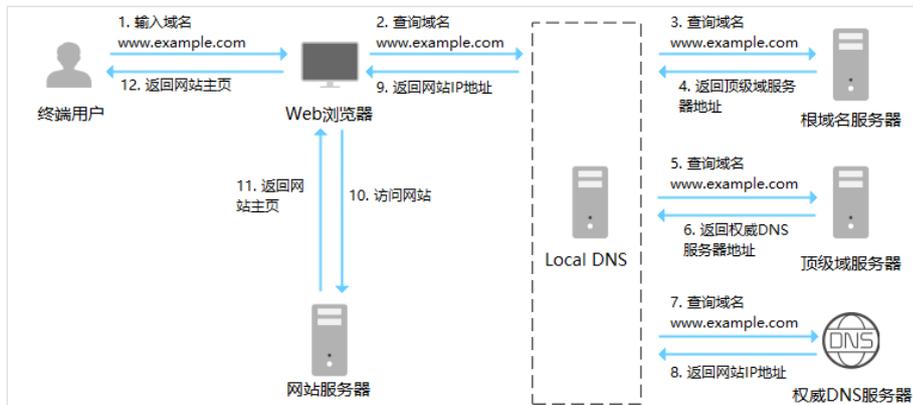
域名解析过程是一种分层的递归查询过程，这是由域名的分层结构决定的。下面以 example.com 为例介绍域名的组成和级别。

- 根域 (.)  
根域即“.”，是最高级别的域名。  
域名在DNS系统中的完整格式为“example.com.”。当我们在浏览器中输入域名时，通常会省略最后的“.”，输入“example.com”，DNS系统会默认将域名转换为完整格式。  
“.”对应根域名服务器，是最高级别的DNS服务器，保存顶级域DNS服务器地址。
- 顶级域 (.com)  
顶级域根据域名后缀进行区分，主要包括两大类：
  - 通用顶级域，如.com，.net，.org，.top等。
  - 国家顶级域，如.cn，.uk，.de等。顶级域对应顶级域名服务器，保存顶级域对应二级域DNS服务器地址。例如，.com顶级域对应的顶级域名服务器保存后缀为.com的二级域名的DNS服务器地址。
- 二级域 (example.com)  
二级域是顶级域的子域，对应权威DNS服务器，为域名提供权威域名解析服务。例如，您在域名服务商处购买域名example.com，并设置域名的DNS服务器地址，实际上就是将域名example.com提供权威解析服务的DNS服务器地址告知.com顶级域的过程。  
如果您选择华为云的云解析服务解析域名，则云解析服务作为权威DNS服务器，为您提供域名的权威DNS服务。

## 域名解析过程

通过域名www.example.com访问网站的域名解析过程如图2-2所示。

图 2-2 域名解析过程



1. 用户通过Web浏览器输入网站域名www.example.com。
2. Web浏览器将对域名www.example.com的查询请求路由到Local DNS。  
Local DNS缓存域名解析数据，并提供递归查询功能。Local DNS通常是Internet服务商提供的DNS。
3. Local DNS在缓存中没有查询到域名的解析记录，将对域名www.example.com的查询请求路由到根域名服务器。
4. 因域名后缀为.com，根域名服务器向Local DNS返回.com顶级域服务器的地址。
5. Local DNS将对域名www.example.com的查询请求路由到.com顶级域服务器。
6. .com顶级域服务器向Local DNS返回为域名example.com提供权威解析服务的权威DNS服务器地址。
7. Local DNS将对域名www.example.com的查询请求路由到权威DNS服务器。  
如果域名www.example.com的DNS服务器设置为[华为云DNS服务器地址](#)，则云解析服务作为权威DNS服务器为域名提供权威的解析记录。
8. 权威DNS服务器向Local DNS返回域名对应的网站IP地址。
9. Local DNS向Web浏览器返回网站IP地址。
10. Web浏览器通过网站IP地址访问网站服务器。
11. 网站服务器向Web浏览器返回网站主页。
12. 终端用户从Web浏览器获取网站主页，对网站的访问成功。

云解析服务支持为域名提供公网域名解析服务，相关操作请参考：[配置网站解析](#)

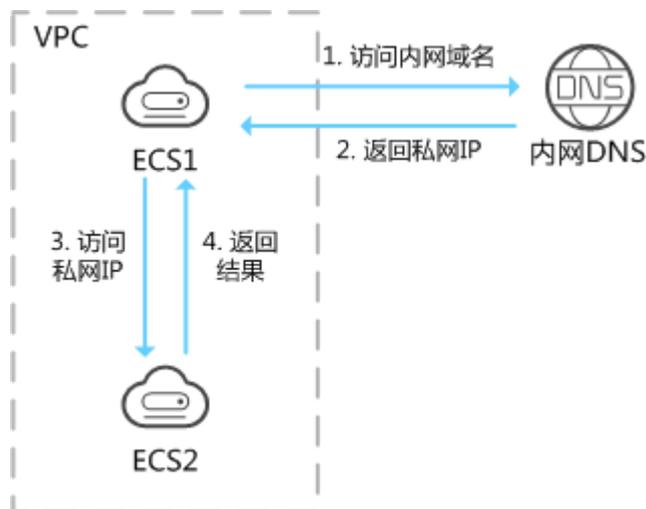
# 3 内网域名解析

## 什么是内网域名解析

内网域名解析是基于VPC网络的域名解析过程，通过华为云内网DNS把域名（如ecs.com）转换成私网IP地址（192.168.1.1）。内网域名解析实现云服务器在VPC内直接通过内网域名互相访问。同时，还支持不经公网，直接通过内网DNS访问云上服务，如OBS、SMN等。

云解析服务的内网DNS为华为云服务提供基于VPC网络的域名解析服务，解析过程如图3-1所示。

图 3-1 内网域名解析过程



当VPC内云服务器访问内网域名时，内网DNS直接对内网域名进行解析，向云服务器返回对应被访问的云服务器的私网IP地址。

云解析服务提供的VPC内的内网域名解析服务，具有以下特点：

- 支持基于VPC任意定制内网域名，灵活自由。
- 一个域名可以关联多个VPC，方便统一管理部署。
- 提供VPC子网专用的内网DNS，直接响应内网域名，以及OBS、SMN等云服务的解析请求，快速高效，有效防护劫持。

内网域名解析功能可以应用于如下场景：

- [云服务器主机名管理](#)
- [云服务器切换](#)
- [云服务器访问云上资源](#)

## 云服务器主机名管理

您可以根据云服务器的位置、用途、所有者等信息规划主机名，并使用主机名为云服务器添加内网解析记录，便于直观的获取云服务器的信息，更利于管理云服务器。

例如，您在某区域的某个可用区部署了20台ECS，其中10台用于网站A，10台用于网站B，则可以采用以下方式规划主机名和内网域名：

- 网站A: weba01.region1.az1.com~weba10.region1.az1.com
- 网站B: webb01.region1.az1.com~webb10.region1.az1.com

完成上述规划后，可以帮助您快速定位云服务的位置和用途，便于日常管理和维护。

您可以参考[配置内网解析](#)完成云服务器主机名管理的相关操作。

## 云服务器切换

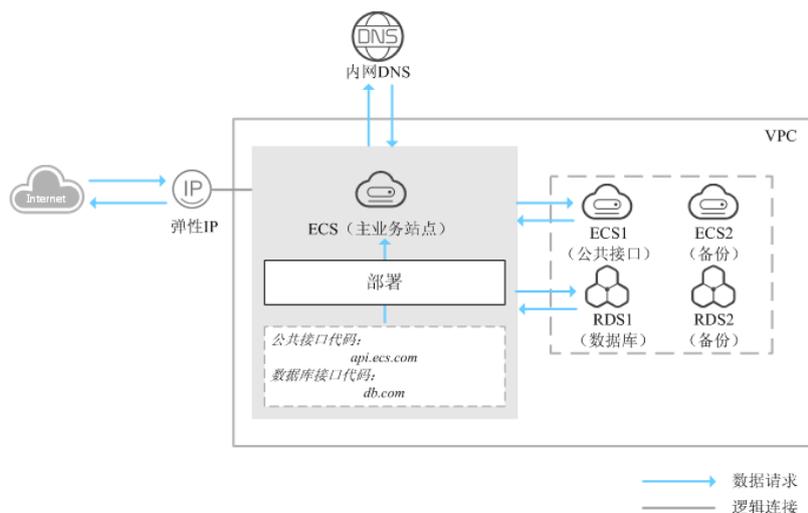
随着互联网用户数量的高速增长，一个网站应用部署在一个服务器上很难经得起高并发的访问，业务拆分到多个服务器分担压力是最基本的方案。

多个服务器可以建立在同一个VPC内，云服务器之间通过私网IP实现互访，私网IP会写入云服务器的内部调用API接口中。此时，存在这样的问题：假如其中一个云服务器发生切换，私网IP也会随之变化，这时就需要修改其他云服务器代码中的API接口，并重新发布变更，维护极其不便。

这时，如果您通过云解析服务为您VPC内的每个云服务器创建一个内网域名，并添加到对应私网IP的解析。这样，云服务器之间可以通过内网域名进行互访。当某个云服务器发生切换时，无需修改云服务器的代码，只需修改对应域名的解析记录即可。

云解析服务作为内网DNS的典型应用场景如[图3-2](#)所示。

图 3-2 为云服务器配置内网域名



在一个VPC内，部署了ECS和RDS。其中：

- ECS：作为主业务站点和业务入口。
- ECS1：作为公共接口。
- RDS1：作为数据库，存储业务数据。
- ECS2和RDS2：作为备份服务器和数据库。

当该网站在运行过程中，因ECS1故障，需要将业务切换到备份的云服务器ECS2时，如果云服务器没有配置内网域名，则需要通过修改主业务节点ECS的代码来重新设置云服务器的内网IP地址。该操作需要中断业务并重新发布网站，耗时耗力。

假如在部署该网站时，我们为云服务器申请了内网域名，且代码中设置的是云服务器的内网域名，则仅需要通过修改内网域名解析记录即可实现云服务器的切换，无需中断业务，也不需要重新发布网站。

您可以参考[为云服务器配置内网域名](#)为您的云服务器规划内网域名信息。

## 云服务器访问云上资源

当您创建云服务器时，可以使用内网DNS进行解析，不经公网直接访问SMN、OBS等云服务。

当您创建云服务器时，

- 如果关联VPC子网的DNS服务器设置为公共DNS，云服务器对云服务的访问需要通过公共DNS在Internet上进行解析。

当云服务器访问OBS、SMN等华为云上服务时，解析过程如[图3-3](#)右侧的“1~10”所示。

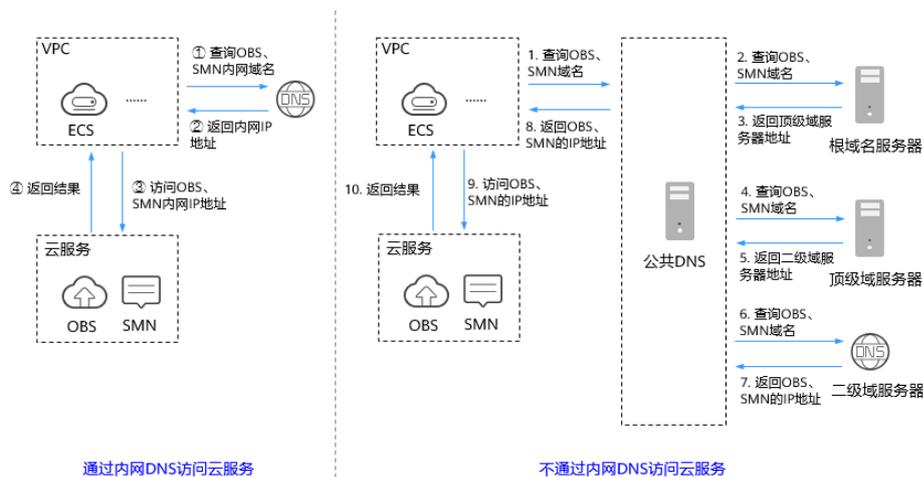
在解析过程中，因需要通过Internet，访问时延大，体验差。

- 如果关联VPC子网的DNS服务器默认为华为云内网DNS，云服务器对云服务的访问直接通过内网DNS进行解析。

当云服务器访问OBS、SMN等华为云上服务时，内网DNS直接返回这些云服务的内网地址，无需通过Internet，访问时延小，性能高，解析过程如[图3-3](#)左侧的“①~④”所示。

您可以参考[怎样切换内网DNS?](#)将云服务器的默认DNS服务器修改为华为云的内网DNS，这样就可以实现通过内网DNS直接访问云服务。

图 3-3 访问云服务



# 4 反向解析

反向解析是指通过IP地址反向获取该IP地址指向的域名，可以应用于自建邮件服务器的场景，是提高邮箱IP和域名信誉度的必要设置。

通常收件服务器在收到邮件时，会通过检测发件方邮箱的IP信誉度和域名信誉度，来判断是否为垃圾邮件。如果收件服务器反向解析发件方IP地址无法获取邮箱域名，则会认为这是由恶意主机发送的垃圾邮件而拒收。因此，搭建邮箱服务器时，建议您为邮箱服务器的IP地址添加到域名的反向解析。

假设要部署ECS作为邮箱服务器，且已经通过云解析服务为ECS的弹性IP添加反向解析记录，此时，反向解析在邮件收发过程中的应用如图4-1所示。

图 4-1 反向解析应用



## 说明

图4-1中仅描述与云解析服务相关的流程，邮件收件方对于发件方IP和域名信誉度的检测，本文不做描述。

如果没有为邮箱服务器添加反向解析记录，则收件方在收到邮件后，无法根据发件方的IP地址反向解析出邮箱域名。收件方会认为这是由恶意主机发送的垃圾邮件而选择拒收。因此，自建邮箱服务器时，为邮箱服务器的IP地址添加反向解析记录是必不可少的步骤。

您可以参考[配置反向解析](#)为您的云服务器配置反向解析。

# 5 智能线路解析

普通的域名解析只为用户返回解析结果，不会考虑访问者IP的来源和类型，这样，所有的访问者都被解析到同样的IP地址上，容易出现由跨运营商或者跨地域访问引起网络体验欠佳。

云解析服务的智能线路解析功能支持按运营商、地域等维度区分访问者IP的来源和类型，对同一域名的访问请求做出不同的解析响应，指向不同服务器的IP地址。

云解析服务还支持按IP网段划分访问者的自定义线路解析，您可以更细粒度的设置解析线路，将访问者路由至不同的网站服务器。

华为云解析服务支持的智能线路解析包括：

- [配置运营商线路解析](#)
- [配置地域线路解析](#)
- [配置自定义线路解析](#)
- [配置权重解析](#)

## 说明

公网域名支持使用智能线路解析功能。内网域名、反向解析不支持使用智能线路解析功能。

# 6 功能总览

表6-1列出了云解析服务的常用功能。

在使用云解析服务之前，建议您先了解云解析服务的**基本概念**，以便更好地理解云解析服务提供的各项功能。

表 6-1 云解析服务常用功能

功能分类	功能名称	功能描述
公网域名解析	公网域名	DNS支持为通过域名注册商注册的域名提供Internet网络的解析服务。DNS提供创建、修改、删除、暂停/启用、查看公网域名详情等基本操作。 详细内容，请参见 <a href="#">公网域名管理简介</a> 。
	域名级别	DNS支持创建的域名级别为主域名以及主域名的一级子域名。 <ul style="list-style-type: none"><li>如果域名后缀为一级（例如.com），支持创建主域名（例如example.com）、子域名（www.example.com）</li><li>如果域名后缀为两级（例如.com.cn），支持创建主域名（例如example.com.cn）、子域名（例如www.example.com.cn）</li></ul>
	记录集	记录集是一组资源记录，用于定义域名的解析类型以及解析值。DNS支持为公网域名添加A、CNAME、MX、AAAA、TXT、SRV、NS以及CAA类型的记录集，还支持修改、删除、查看、暂停以及启用记录集。 详细内容，请参见 <a href="#">记录集管理简介</a> 。
	找回域名	当域名已经被其他租户创建时，DNS支持域名所有者找回域名。 详细内容，请参见 <a href="#">找回域名</a> 。
	泛解析	DNS支持为主域名的所有子域名添加记录集，为所有子域名提供解析服务。 详细内容，请参见 <a href="#">设置域名泛解析</a> 。

功能分类	功能名称	功能描述
	TTL	DNS支持设置解析记录在本地DNS服务器的缓存时间。TTL取值范围：1~2147483647。
	权重	DNS支持通过权重比例返回解析记录。 当域名在同一解析线路中有多条同一类型的解析记录时，可以通过“权重”设置解析记录的响应比例。 详细内容，请参见 <a href="#">配置权重解析</a> 。
	批操作	DNS支持批量删除域名列表中的公网域名。
内网域名解析	内网域名	DNS支持创建在关联VPC内生效的内网域名，并为域名提供内网DNS解析服务。DNS提供创建、修改、删除、查看内网域名等基本操作，还支持关联VPC、解关联VPC功能。 <ul style="list-style-type: none"> <li>内网域名无需注册，可以自由创建。</li> <li>内网域名在关联VPC内唯一。</li> </ul> 详细内容，请参见 <a href="#">内网域名管理简介</a> 。
	关联/解关联VPC	DNS支持为内网域名关联或者解关联VPC。 详细内容，请参见 <a href="#">为内网域名关联VPC</a> 和 <a href="#">为内网域名解关联VPC</a> 。
	记录集	记录集是一组资源记录，用于定义域名的解析类型以及解析值。DNS支持为内网域名添加A、CNAME、MX、AAAA、TXT、PTR以及SRV类型的记录集，还支持修改、删除以及查看记录集。 详细内容，请参见 <a href="#">解析管理简介</a> 。
	泛解析	DNS支持为内网域名的所有子域名添加记录集，为所有子域名提供解析服务。 详细内容，请参见 <a href="#">设置域名泛解析</a> 。
	TTL	DNS支持设置解析记录在本地DNS服务器的缓存时间。TTL取值范围：1~2147483647。
	批操作	DNS支持批量删除域名列表中的内网域名。
	反向解析	反向解析
	TTL	DNS支持设置解析记录在本地DNS服务器的缓存时间。TTL取值范围：1~2147483647。
智能线路解析	运营商线路解析	DNS支持根据访问用户所在运营商网络调度到最佳访问地址。 详细内容，请参见 <a href="#">配置运营商线路解析</a> 。

功能分类	功能名称	功能描述
	地域解析	DNS支持根据访问用户所处地理位置调度到最佳访问地址。 详细内容，请参见 <a href="#">配置地域解析</a> 。
解析记录	全局搜索记录集	DNS支持集中管理公网域名和内网域名记录集。主要包括： <ul style="list-style-type: none"> <li>支持根据记录集状态、记录集类型、域名、记录集的值、记录集ID以及标签等条件搜索公网域名或者内网域名记录集。</li> <li>支持修改、删除、暂停或者启用公网域名的记录集。</li> <li>支持修改、删除内网域名的记录集。</li> </ul> 详细内容，请参见 <a href="#">全局搜索记录集</a> 。
	批操作	DNS支持对公网域名和内网域名记录集的批操作，包括批量导入、批量导出以及批量删除。 详细内容，请参见 <a href="#">批量导入域名解析记录</a> 和 <a href="#">批量导出域名解析记录</a> 。
审计	查看审计日志	通过云审计，您可以记录与云解析服务相关的操作事件，便于日后的查询、审计和回溯。 华为云提供 <a href="#">查看审计日志</a> 功能，支持在云审计服务管理控制台查看或导出最近7天的操作记录。
标签	资源标签	DNS支持为公网域名、内网域名、记录集以及反向解析等资源配置标签，也支持通过标签管理服务的 <a href="#">预定义标签</a> 功能快速将标签与资源进行关联。
配额	配额调整	为防止资源滥用，云平台限制了各类资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少公网域名、内网域名、记录集或者反向解析。 如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。 详细内容，请参见 <a href="#">配额调整</a> 。

# 7 约束与限制

云解析服务的使用约束与限制如表7-1所示。

表 7-1 DNS 约束与限制

资源	默认配额 (个)	如何提升配额
公网域名	50	可以通过 <a href="#">提交工单</a> 提高此限制。
内网域名	50	
记录集	500	
反向解析	50	
自定义线路	50	
每个内网域名关联的VPC的最大个数	无限制	-
每个解析规则关联的VPC的最大个数	无限制	-
VPC内单个ECS解析请求量	2000次/秒	VPC内单IP每秒最高QPS为2000次，每秒请求DNS峰值超过限制阈值后，将面临限速风险。 如果您的业务确实会产生超高的并发解析请求，建议您开启DNS缓存功能，以提升解析效率。
VPC内所有ECS解析总请求量	无限制	-
VPC内单个ECS外部递归解析请求量	600次/秒	VPC内单IP外部递归解析请求阈值为600次/秒，超过限速阈值后，将面临限速风险。 如果您的业务确实会产生超高的并发解析请求，建议您开启DNS缓存功能，以提升解析效率。

资源	默认配额 (个)	如何提升配额
VPC内所有ECS外部递归解析总请求量	5000次/秒	单个VPC内整体外部递归请求阈值为5000次/秒，超过限速阈值后，将面临限速风险。 如果您有特殊诉求访问大量互联网域名等业务场景，请提前 <a href="#">提交工单</a> 联系技术支持沟通解决方案，以免因为限速影响您的业务。

# 8 安全

## 8.1 责任共担

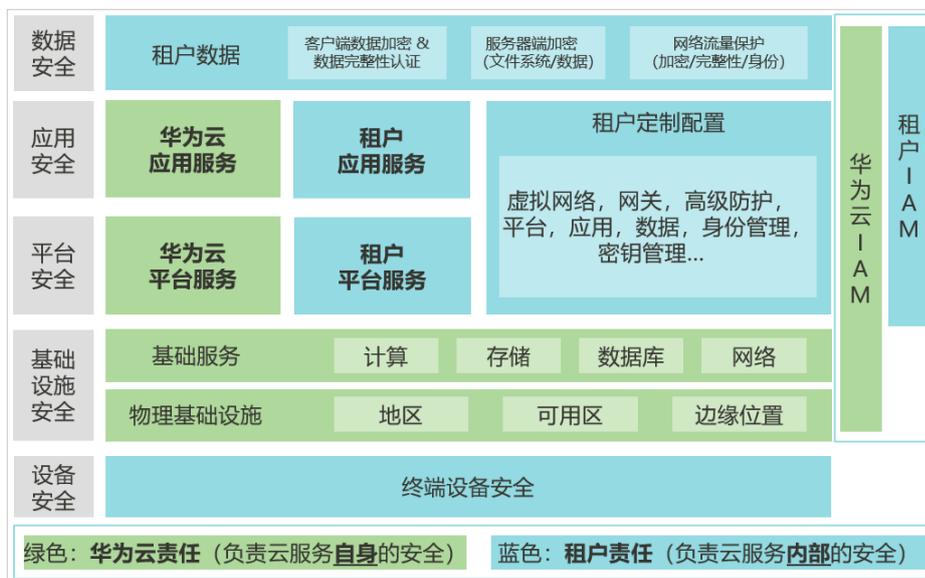
华为云秉承“将对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图8-1所示。

- **华为云**：负责云服务自身的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务内部的安全，安全地使用云。华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《[华为云安全白皮书](#)》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 8-1 华为云安全责任共担模型



## 8.2 身份认证与访问控制

云解析服务支持通过IAM权限策略进行访问控制。IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。管理员创建IAM用户后，需要将用户加入到一个用户组中，IAM可以对这个组授予DNS所需的权限，组内用户自动继承用户组的所有权限。

详情请参见[权限管理](#)。

## 8.3 审计与日志

云审计服务（Cloud Trace Service, CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务后，CTS可记录DNS的操作事件用于审计。

- CTS的详细介绍和开通配置方法，请参见[CTS快速入门](#)。
- DNS支持审计的操作事件请参见[支持审计的关键操作列表](#)。
- 查看审计日志请参见[查看审计日志](#)。

## 8.4 服务韧性

基于华为在全球ICT基础设施领域积累，华为云DNS累计在全球20+国家/地区部署上百个节点，实现每个Region多AZ多集群容灾，即使部分节点、集群、Region发生故障也不会导致解析中断，极大提高服务可靠性。

华为十多年安全攻防经验及优秀实践，结合华为云自建多地高防机房和运营商骨干网高防清洗中心多重防护，支持T级DDoS防护，可以快速有效应对各类DNS攻击，保护域名解析业务连续性。

自研新一代高性能DPDK解析加速服务，单服务器节点支持千万级并发，服务整体支持亿级并发，为用户提供高性能无限扩展的解析服务。

支持智能解析，可以按运营商、大洲/国家、权重等方式将用户流量调度到不同后端服务器，极大提高客户业务可靠性。

## 8.5 监控安全风险

云监控（Cloud Eye）是面向华为云资源的监控平台，提供了实时监控、及时告警、资源分组、站点监控等能力，使您全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

监控是保持云解析服务可靠性、可用性和性能的重要部分，通过云监控，可以按时间轴查看域名解析流量，错误日志相关情况，动态告警分析潜在风险。

## 8.6 认证证书

### 合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行[申请下载](#)合规资质证书。

图 8-2 合规证书下载

The screenshot shows a webpage titled "合规证书下载" (Compliance Certificate Download). At the top, there is a search bar with the placeholder text "请输入关键字搜索". Below the search bar, there are six cards, each representing a different certification or report. Each card includes a logo, the name of the certification, a brief description, and a "下载" (Download) button.

- BS 10012:2017**: BS 10012为个人信息管理体系提供了一个符合欧盟GDPR原则的最佳实践框架。它概述了组织在收集、存储、处理、保留或处理与个人相关的个人记录时需要考虑的核心需求。保留或处理与个人相关的个人记录时需要考虑的核心需求。
- CSA STAR认证**: CSA STAR认证是由标准研发机构BSI（英国标准协会）和CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
- ISO 20000-1:2018**: ISO 20000是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务提供商可提供有效的IT服务来满足客户和业务的需求。
- SOC 1 类型II 报告 2022.04.01-2023.03.31**: 华为云每年滚动发布两期SOC1报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为2022.04.01-2023.03.31。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 1报告着重于评估与财务报告流程有关的控制，通常使用者为云客户和其独立审计师。
- SOC 1 类型II 报告 2022.10.01-2023.09.30**: 华为云每年滚动发布两期SOC1报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为2022.10.01-2023.09.30。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 1报告着重于评估与财务报告流程有关的控制，通常使用者为云客户和其独立审计师。
- SOC 2 类型II 报告 2022.04.01-2023.03.31**: 华为云每年滚动发布两期SOC2报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为2022.04.01-2023.03.31。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 2报告着重于组织的内部运作与合规，包括安全性、可用性、进程完整性、保密性、隐私性五大控制属性。

## 资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看[资源中心](#)。

图 8-3 资源中心



# 9 权限管理

如果您需要对华为云上创建的DNS资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云账号中给员工创建IAM用户，并授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有DNS的使用权限，但是不希望他们拥有删除DNS资源等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用DNS，但是不允许删除DNS资源的权限，控制他们对DNS资源的使用范围。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用DNS的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

关于IAM的详细介绍，请参见[IAM产品介绍](#)。

## DNS 权限

默认情况下，账号管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

DNS资源包括：

- 公网域名：在创建时不区分物理区域，为全局级服务。
- 内网域名：在创建时通过物理区域划分，为项目级服务。
- 反向解析：在创建时通过物理区域划分，为项目级服务。

上述DNS资源中，公网域名的权限不支持在“全局服务”中设置。因此，DNS资源的权限均需按照项目级服务进行授权。

授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如亚太-曼谷）对应的项目（ap-southeast-2）中设置相关权限，则该权限在所有区域项目中都生效。访问DNS时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对DNS服务，管理员能够控制IAM用户仅能对某一类DNS资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，DNS支持的API授权项请参见[策略及授权项说明](#)。

如表9-1所示，包括了DNS的所有系统权限。

表 9-1 DNS 系统权限

系统角色/策略名称	描述	类别	依赖关系
DNS FullAccess	云解析服务的所有执行权限。	系统策略	无
DNS ReadOnlyAccess	云解析服务只读权限，拥有该权限的用户仅能查看云解析服务资源。	系统策略	无
DNS Administrator	云解析服务的所有执行权限。	系统角色	该角色有依赖，需要在同项目中勾选依赖的角色： <b>Tenant Guest</b> 、 <b>VPC Administrator</b> 。

表9-2列出了DNS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 9-2 常用操作与系统权限的关系

操作	DNS FullAccess	DNS ReadOnlyAccess	DNS Administrator
创建公网域名	√	x	√
查看公网域名	√	√	√
修改公网域名	√	x	√
删除公网域名	√	x	√
批量删除公网域名	√	x	√
暂停/启用公网域名	√	x	√

操作	DNS FullAccess	DNS ReadOnlyAccess	DNS Administrator
创建内网域名	√	x	√
查看内网域名	√	√	√
修改内网域名	√	x	√
删除内网域名	√	x	√
批量删除内网域名	√	x	√
为内网域名关联VPC	√	x	√
为内网域名解关联VPC	√	x	√
添加记录集	√	x	√
查看记录集	√	√	√
修改记录集	√	x	√
删除记录集	√	x	√
批量删除记录集	√	x	√
暂停/启用记录集	√	x	√
批量导出解析记录	√	x	√
批量导入解析记录	√	x	√
创建反向解析	√	x	√
查看反向解析	√	√	√
修改反向解析	√	x	√
删除反向解析	√	x	√
批量删除反向解析	√	x	√

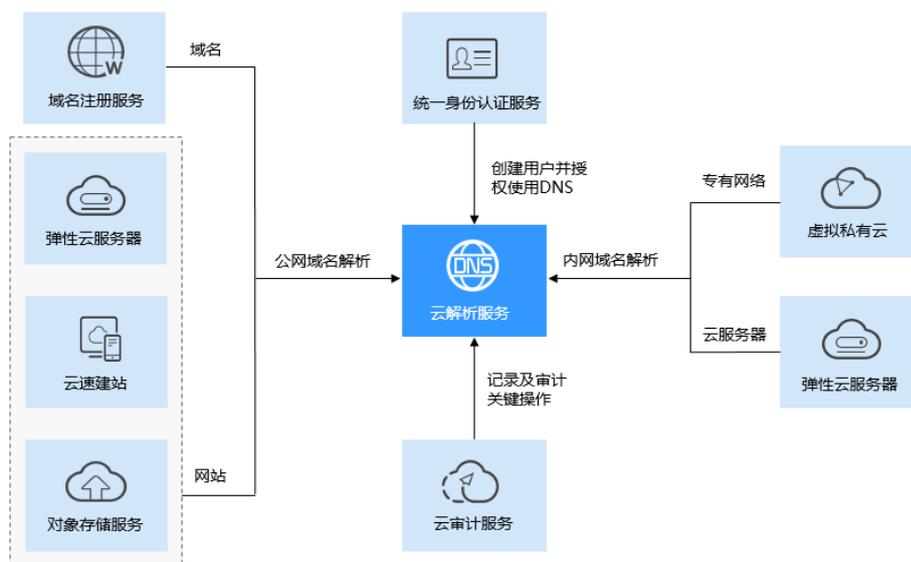
## 相关链接

- [IAM产品介绍](#)
- [创建用户组、用户并授予DNS权限](#)
- [策略支持的授权项](#)

# 10 与其他服务的关系

云解析服务与周边服务的依赖关系如图10-1所示。

图 10-1 云解析服务与其他服务的关系示意图



云解析服务与其他服务的关系如表10-1所示。

表 10-1 与其他服务的关系

相关服务	交互功能	位置
弹性云服务器	为弹性云服务器提供域名解析服务	配置网站解析
虚拟私有云	提供基于VPC网络的域名解析服务	配置内网解析
对象存储服务	托管静态网站，提供域名到存储桶资源的映射	托管静态网站

相关服务	交互功能	位置
云审计服务	记录与云解析服务相关的操作事件	<a href="#">支持审计的关键操作列表</a>

# 11 基本概念

## 11.1 域名格式与级别

域名格式需满足如下要求：

- 域名以点号分隔成多个字符串。
- 单个字符串由各国文字的特定字符集、字母、数字、连字符（-）组成，连字符（-）不得出现在字符串的头部或者尾部。
- 单个字符串长度不超过63个字符。
- 字符串间以点分割，且总长度（包括末尾的点）不超过254个字符。

云解析服务定义域名级别如下：

- 根域名：.。
- 顶级域名：.com，.net，.org，.cn等。
- 二级域名：即顶级域名的子域名，example.com，example.net，example.org等。
- 三级域名：即主域名的子域名，abc.example.com，abc.example.net，abc.example.org等。
- 以此类推，在上一级域名最左侧进行域名级别的拓展，def.abc.example.com，def.abc.example.net，def.abc.example.org等。

## 11.2 记录集及类型

### 记录集简介

云解析服务的解析记录由各种类型的记录集（Record Set）组成，是指一组资源记录的集合。这些资源记录属于同一域名，用于定义域名支持的解析类型以及解析值。

当您已经在云解析服务中创建完域名，需要对其进行域名级别的拓展或记录域名的详细信息，通过添加记录集来实现。

云解析服务支持的解析记录类型及适用场景如[表11-1](#)所示。

表 11-1 解析记录适用场景说明

记录集类型	适用场景	描述
A	公网域名、内网域名	指定域名对应的IPv4地址，用于将域名解析到IPv4地址。
CNAME	公网域名、内网域名	指定域名的别名，用于将域名解析到另一域名，或者多个域名映射到同一域名上。
MX	公网域名、内网域名	指定域名对应的邮件服务器，用于为邮件域名设置邮箱服务器。
AAAA	公网域名、内网域名	指定域名对应的IPv6地址，用于将域名解析到IPv6地址。
TXT	公网域名、内网域名	用于对域名进行标识和说明，可填写任意的信息。主要用于以下场景： <ul style="list-style-type: none"><li>记录DKIM的公钥，用于反电子邮件欺诈。</li><li>用于记录域名所有者身份信息，用于域名找回。</li></ul>
SRV	公网域名、内网域名	记录了具体某台计算机对外提供哪些服务，供用户查询使用。
NS	公网域名、内网域名	指定域名的权威DNS服务器，用于指定域名由哪个DNS服务器进行解析： <ul style="list-style-type: none"><li>对于公网域名，系统默认创建，支持为域名的子域名手工创建NS记录。</li><li>对于内网域名，系统默认创建，不支持手工创建。</li></ul>
SOA	公网域名、内网域名	指定域名的主权威DNS服务器，系统默认创建，不支持手工创建。
CAA	公网域名	指定为域名颁发HTTPS证书的授权CA机构，用于防止HTTPS证书错误签发。
PTR	公网域名、内网域名	指定IP地址反向解析记录，用于通过私网IP地址反向查询对应的云服务器。

## 记录集示例

记录集在实际解析场景中的应用：

- 网站解析  
A、AAAA类型的记录集，常用于网站解析，通过域名获取对应的IP地址。

图 11-1 网站解析



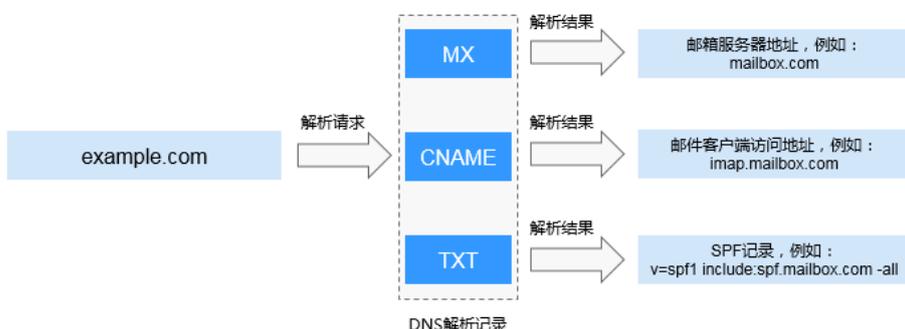
- 内网解析  
A、AAAA类型的记录集常用于内网解析，通过内网域名获取对应的私网IP地址。

图 11-2 内网解析



- 邮箱解析  
MX、CNAME以及TXT类型的记录集常用于邮箱解析。

图 11-3 邮箱解析



- 私网IP反向解析  
PTR记录集常用于通过云服务器的私网IP反向解析对应的内网域名。

图 11-4 私网 IP 反向解析



## 相关链接

添加以及管理记录集的相关操作，请参考[解析管理简介](#)。

## 11.3 区域和可用区

### 什么是区域、可用区？

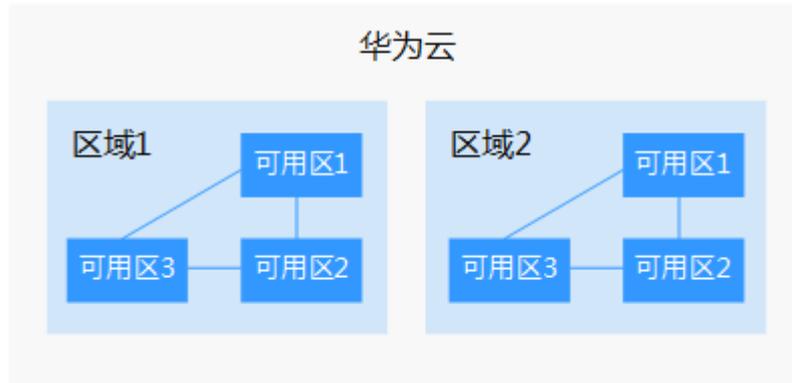
区域和可用区用来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ, Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。

一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图11-5阐明了区域和可用区之间的关系。

图 11-5 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。更多信息请参见[华为云全球站点](#)。

## 如何选择区域？

选择区域时，您需要考虑以下几个因素：

- 地理位置

一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

- 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
- 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
- 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。

### 📖 说明

“拉美-圣地亚哥”区域位于智利。

- 资源的价格

不同区域的资源价格可能有差异，请参见[华为云服务价格详情](#)。

## 如何选择可用区？

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

## 区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅[地区和终端节点](#)。

## 11.4 项目

项目用于将资源（计算资源、存储资源和网络资源等）进行分组和隔离。项目可以是一个部门或者一个项目组。

一个账户中可以创建多个项目。

对于云解析服务，公网域名属于Global级别的资源，而内网域名和反向解析属于区域级别的资源。因此，系统会基于项目实现内网域名、反向解析资源的隔离和管理。在创建、查询、设置内网域名和反向解析前，用户需先指定区域和项目，然后在指定项目下执行相关操作。

# 12 修订记录

发布日期	修订记录
2021-10-30	第七次正式发布。 新增 <a href="#">权限管理</a>
2020-02-12	第六次正式发布。 新增 <a href="#">功能总览</a> 整合操作场景页面，并增加到操作指导的链接，涉及页面： <ul style="list-style-type: none"><li>• <a href="#">公网域名解析</a></li><li>• <a href="#">内网域名解析</a></li><li>• <a href="#">记录集及类型</a></li></ul>
2019-07-02	第五次正式发布。 修改 <a href="#">智能线路解析</a> ，补充运营商线路解析、地域解析的描述。
2019-06-25	第四次正式发布。 新增 <a href="#">区域和可用区</a> ，增加区域和可用区的概念。
2019-03-05	第三次正式发布。 修改 <a href="#">与其他服务的关系</a> ，补充链接。
2019-01-20	第二次正式发布。 补充域名解析的流程以及使用场景。
2018-11-22	第一次正式发布。