ALIBABA CLOUD

阿里云

专有云DNS

产品简介

文档版本：20200917

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.基本概念

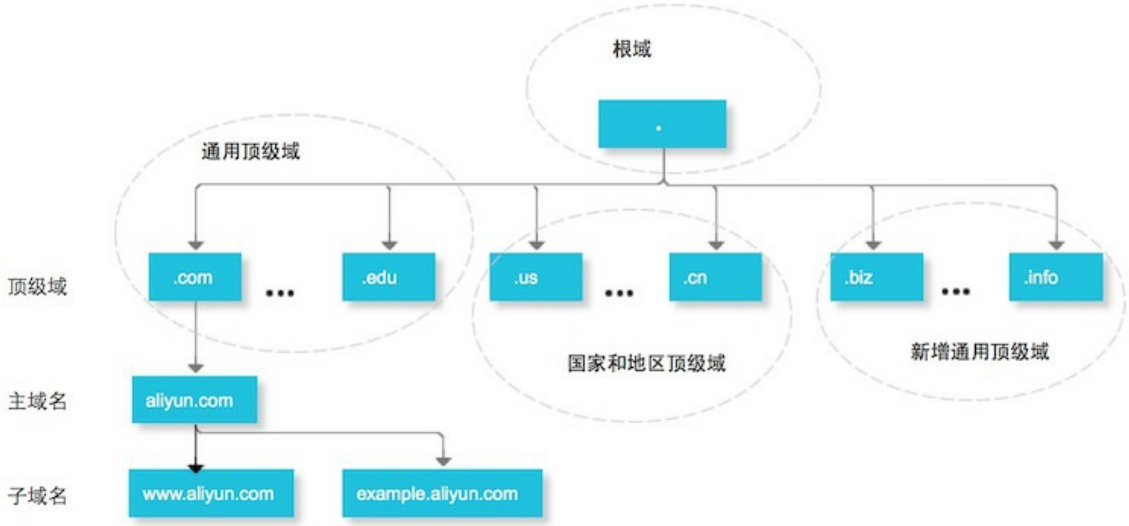
DNS 是域名系统 (Domain Name System) 的缩写，是因特网的一项核心服务，它作为可以将域名和IP地址相互映射的一个分布式数据库，能够使人更方便的访问互联网，而不用去记住能够被机器直接读取的IP数串。

DNS概念

DNS 是域名系统 (Domain Name System) 的缩写，是因特网的一项核心服务，它作为可以将域名和IP地址相互映射的一个分布式数据库，能够使人更方便的访问互联网，而不用去记住能够被机器直接读取的IP数串。

域名的分层结构

由于因特网的用户数量较多，所以因特网在命名时采用的是层次树状结构的命名方法。任何一个连接在因特网上的主机或路由器，都有一个唯一的层次结构的名字，即域名(domain name)。这里，“域”(domain)是名字空间中一个可被管理的划分。从语法上讲，每一个域名都是有标号(label)序列组成，而各标号之间用点(小数点)隔开。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。关于域名层次结构如下图：



举例：

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

DNS的分层结构

域名是分层结构，域名DNS服务器也是对应的层级结构。有了域名结构，还需要有域名DNS服务器去解析域名，且是需要由遍及全世界的域名DNS服务器去解析，域名DNS服务器实际上就是装有域名系统的主机。域名解析过程涉及4个DNS服务器，分别如下：

分类	作用
根DNS服务器	英文：Root nameserver。本地域名服务器在本地查询不到解析结果时，则第一步会向它进行查询，并获取顶级域名服务器的IP地址。
顶级域名服务器	英文：Tld nameserver。负责管理在该顶级域名服务器下注册的二级域名，例 如“www.example.com”，.com则是顶级域名服务器，在向它查询时，可以返回二级域 名“example.com”所在的权威域名服务器地址
权威域名服务器	英文：authoritative nameserver。在特定区域内具有唯一性，负责维护该区域内的域名与IP地址之间的对应关系，例如云解析DNS。
本地域名服务器	英文：DNS resolver或Local DNS。本地域名服务器是响应来自客户端的递归请求，并最终跟踪直到获取到解析结果的DNS服务器。例如用户本机自动分配的DNS、运营商ISP分配的DNS、谷歌/114公共DNS等

注释：

> *1. 每个层的域名上都有自己的域名服务器，最顶层的是根域名服务器*
>
> *2. 每一级域名服务器都知道下级域名服务器的IP地址，以便于一级一级向下查询*

DNS解析过程

DNS查询的结果通常会在本地域名服务器中进行缓存，如果本地域名服务器中有缓存的情况下，则会跳过如下DNS查询步骤，很快返回解析结果。下面的示例则概述了本地域名服务器没有缓存的情况下，DNS查询所需的8个步骤：

1、用户在Web浏览器中输入“example.com”， 则由本地域名服务器开始进行递归查询。

2、本地域名服务器采用迭代查询的方法，向根域名服务器进行查询。

3、根域名服务器告诉本地域名服务器，下一步应该查询的顶级域名服务器.com TLD的IP地址。

4、本地域名服务器向顶级域名服务器.com TLD进行查询。

5、.com TLD服务器告诉本地域名服务器，下一步查询example.com权威域名服务器的IP地址。

6、本地域名服务器向example.com权威域名服务器发送查询。

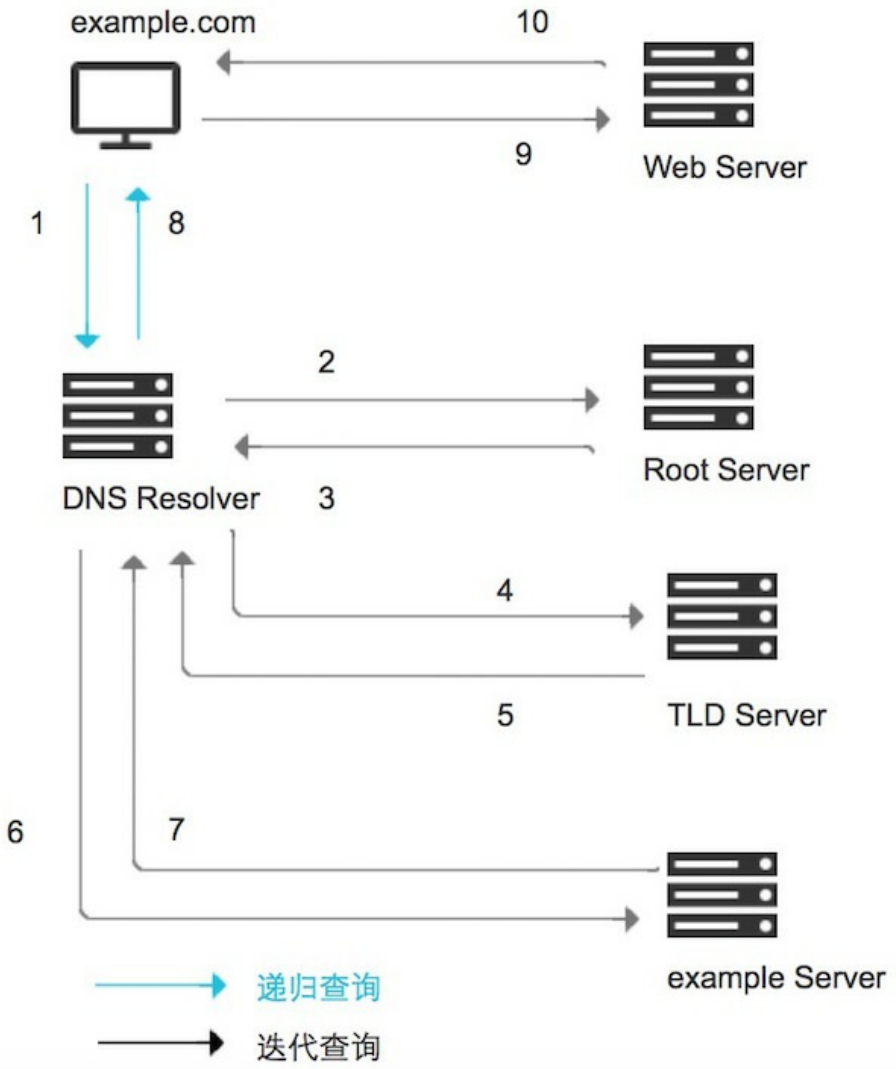
7、example.com权威域名服务器告诉本地域名服务器所查询的主机IP地址。

8、本地域名服务器最后把查询的IP地址响应给web浏览器。

一旦DNS查询的8个步骤返回了example.com的IP地址，浏览器就能够发出对网页的请求：

9、浏览器向IP地址发出HTTP请求

10、该IP处的web服务器返回要在浏览器中呈现的网页



DNS术语

递归查询

是指DNS服务器在收到用户发起的请求时，必须向用户返回一个准确的查询结果。如果DNS服务器本地没有存储与之对应的信息，则该服务器需要询问其他服务器，并将返回的查询结构提交给用户。

迭代查询

是指DNS服务器在收到用户发起的请求时，并不直接回复查询结果，而是告诉另一台DNS服务器的地址，用户再向这台DNS服务器提交请求，这样依次反复，直到返回查询结果。

DNS缓存

DNS缓存是将解析数据存储在靠近发起请求的客户端的位置，也可以说DNS数据是可以缓存在任意位置，最终目的是以此减少递归查询过程，可以更快的让用户获得请求结果。

TTL

英文全称Time To Live ，这个值是告诉本地域名服务器，域名解析结果可缓存的最长时间，缓存时间到期后本地域名服务器则会删除该解析记录的数据，删除之后，如有用户请求域名，则会重新进行递归查询/迭代查询的过程。

IPV4、IPV6双栈技术

双栈英文Dual IP Stack，就是在一个系统中可同时使用IPv6/ IPv4这两个可以并行工作的协议栈

TLD Server

英文全称Top-level domains Server，指顶级域名服务器。

DNS Resolver

指本地域名服务器，它是DNS查找中的第一站，是负责处理发出初始请求的DNS服务器。运营商ISP分配的DNS、谷歌8.8.8.8等都属于DNS Resolver。

Root Server

指根域名服务器，当本地域名服务器在本地查询不到解析结果时，则第一步会向它进行查询，并获取顶级域名服务器的IP地址。

DNS Query Flood Attack

指域名查询攻击，攻击方法是通过操纵大量傀儡机器，发送海量的域名查询请求，当每秒域名查询请求次数超过DNS服务器可承载的能力时，则会造成解析域名超时从而直接影响业务的可用性。

URL转发

英文 Url Forwarding，也可称地址转向，它是通过服务器的特殊设置，将一个域名指向到另外一个已存在的站点

edns-client-subnet

google提交了一份DNS扩展协议，允许DNS resolver传递用户的ip地址给authoritative DNS server.

DNSSEC

域名系统安全扩展（DNS Security Extensions），简称DNSSEC。它是通过数字签名来保证DNS应答报文的真实性和完整性，可有效防止DNS欺骗和缓存污染等攻击，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。