vhDNS 系统使用手册

一 系统概述

1 系统介绍

vhDNS 系统是一套成熟稳定的 DNS 解析系统，可使用 WEB 界面在线操作管理，支持域名定向解析或自定义解析，支持递归转发，条件转发等复杂应用或网络结构，可对请求查询流量实时统计与汇总，实现对网络的便捷管理与精准管理。可应用于内网，局域名，企业网，区域网，校园网等各种应用场景。一键安装，快速部署，简便易用。合适于任何有自架 DNS 或网关 DNS 应用需求的用户！

为满足不同用户的应用与功能需求，可提供定制化功能开发。

2 系统架构

vhDNS 采用多机分布式主从系统架构，可将主控与应用实现分离，支持集群与规模部署，可无限扩展应用节点。主控负责数据管理与操作，节点（被控）负责解析或转发等服务。在安装部署完成后，所有的管理操作，只需在主控后台上操作即可，数据会自动，实时同步到所有的节点。

主控与节点相互独立，节点与节点也是相互独立，即主控停止或发生故障，不会影响节点的正常使用和解析服务；任何一个节点故障，也不会影响到其它节点的正常使用与服务

二 安装部署

1 硬件配置与系统环境

系统安装环境（云服务器主机或物理机均可）

系统要求：全新安装的纯净系统或最小化安装，CentOS 7.X 最佳

内存要求：最低 512MB，推荐 1024MB 以上，比如 4G，8G，16G

硬盘要求：10G 以上，推荐 50G 起

其它说明：如在已有环境应用的系统上安装，可手工安装或联系我们安装

2 主控安装

主控是指管理后台同时也包括解析服务(主控安装时默认也安装了节点服务，在多机或大流量用户，可以考虑停止主控的节点应用，使主控与节点均在各自独立的机器上使用)

用 SSH 软件登录远程终端服务器，执行下边的命令

cd /tmp

yum install -y wget

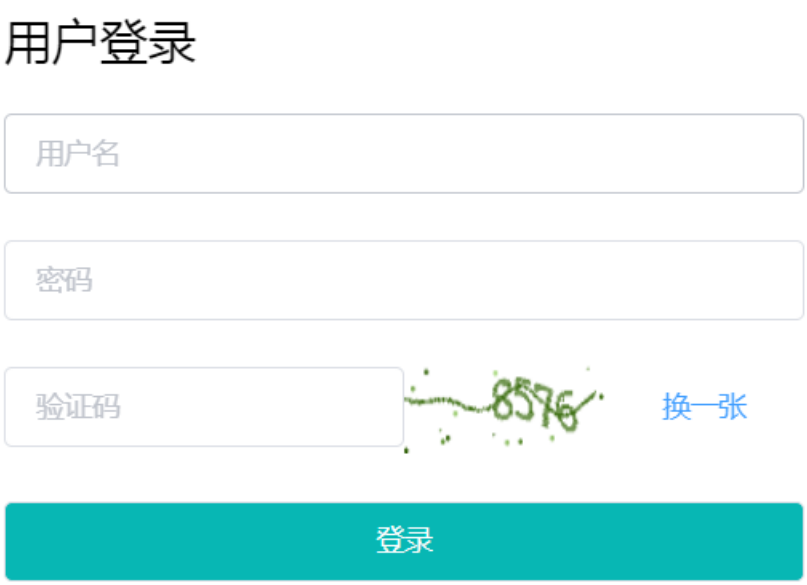
wget http://dl.wdlinux.cn/files/vhdns/install_vha.sh

sh install_vha.sh

如无错误提示，便已顺利安装完成后

使用浏览器打开 http://ip:8088

即可登录后台，如下



主控后台即管理后台，默认使用 8088 端口（可修改为其它端口或使用 nginx 代理转发）

默认密码可查看 /root/admin_pw.txt 文件

3 节点安装

节点指解析转发的服务程序或机器，一般只需要在新加机器或独立机

器时安装使用，主控默认已安装一个节点服务

用 SSH 软件登录远程终端服务器，执行下边的命令

cd /tmp

yum install -y wget

wget http://dl.wdlinux.cn/files/vhdns/install_vhd.sh

sh install_vhd.sh

如无错误提示，便可顺便安装完成

可登录管理后台，将该机器添加到节点列表里

如下

输入相应的 IP 地址和名称，确定就完成了

节点添加后，系统会自动将所有数据自动同步节点里，此后再不用操作节点。所有的管理操作都在主控后台上完成操作

4 软件卸载

只要删除/opt/vhdns 目录即可，如 rm –fr /opt/vhdns

5 流量统计(ES 组件安装)

ES 组件主要用于实时流量统计与汇总功能，如果不开启该功能可不安装(默认未安装或未启用)；该组件对硬件要求高些，建议使用 4 核/8 核，8G/16G 内存以上

安装方法如下

cd /tmp

wget http://dl.wdlinux.cn/files/vhdns/install_es.sh

sh install_es.sh

如无错误提示便已顺利安装完成

该组件只需在主控上安装即可，同时需要开放 9200 端口（可针对节点开放）

三 功能说明

一） 解析管理

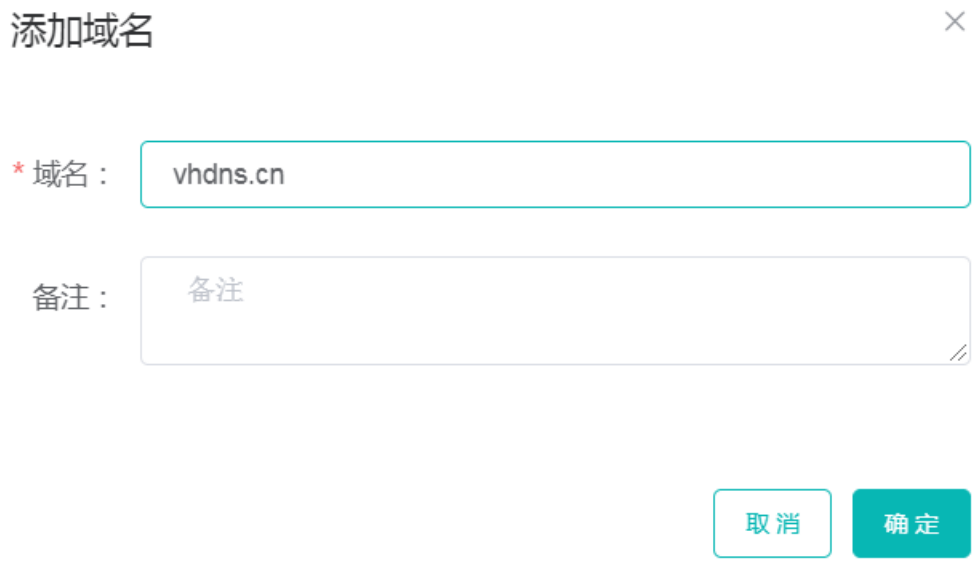
1 域名解析

可以根据域名或针对域名，进行设置定向解析，即设置指定的域名或二级域名解析到指定的 IP 地址，这对于部分复杂网络应用或功能调戏时，是非常有用或灵活应用的。此定向解析，只对设置指定的二级域名有效，对于非设置的域名或二级域名，则仍然是使用转发递归，实现正常的解析请求和访问。

主要有如下两个设置方式

A 一般操作

先添加域名，或进入域名的子域名记录列表进行操作，如下



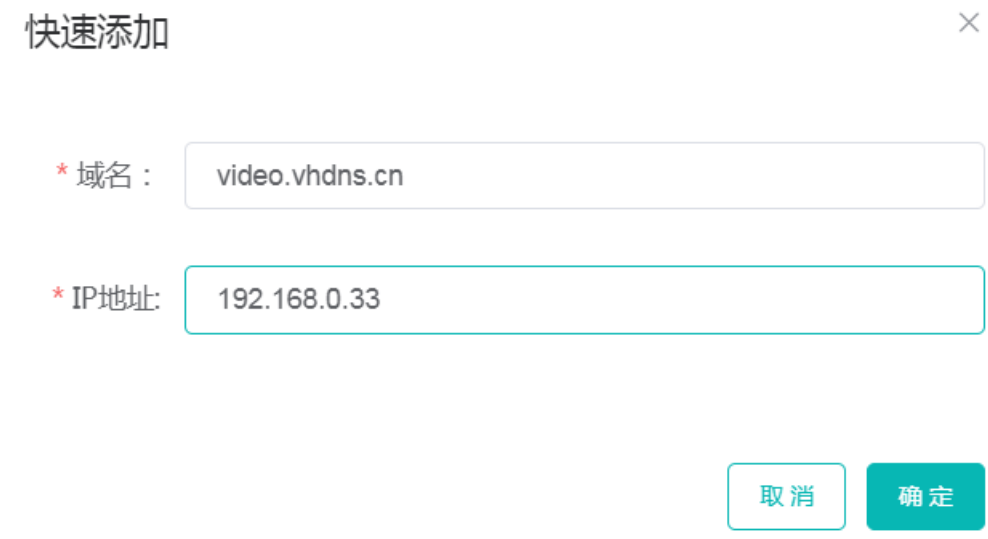
然后进入域名的二级域名或子域名列表，进行操作与设置，如下

这样便可设置相应的二级域名

对于多级域名，操作方式类似，可先创建相应的域名，再进行子域名记录添加操作

B 快速添加

直接输入相应的二级域名，如下图



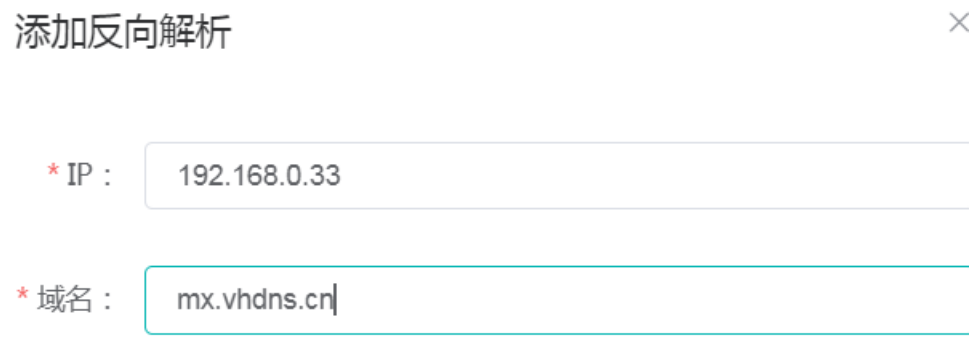
添加后如下图

即可完成

对于快速添加，只对二级域名有效，对于三级或是多级域名，请使用普通方式添加操作

2 反向解析

反向解析是根据 IP 地址来查询域名，一般在邮件记录里会比较常用到，如下

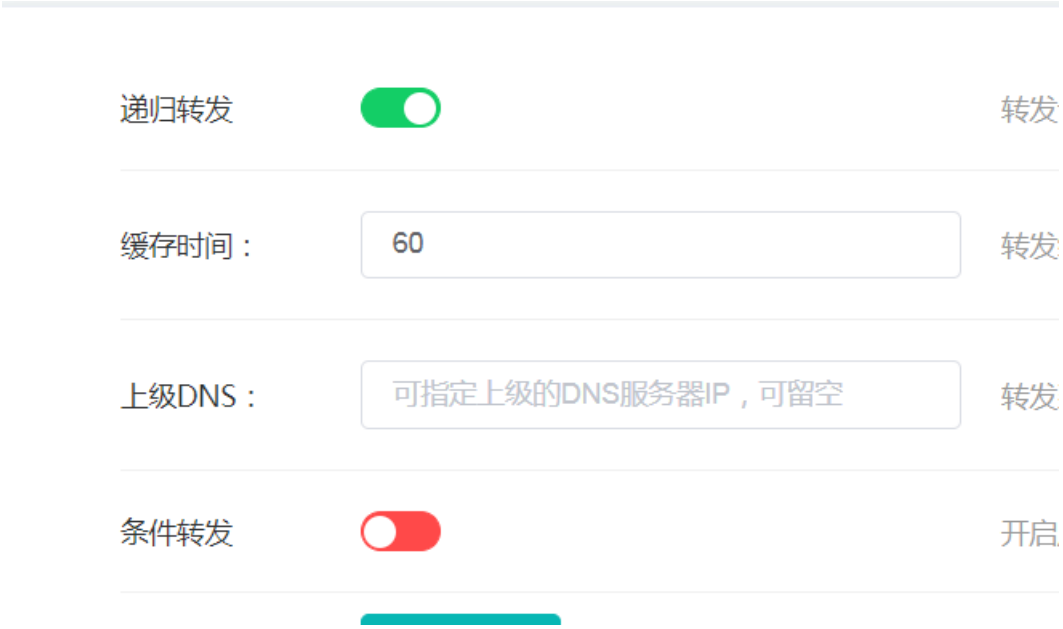


添加后如下

二） 转发管理

1 转发设置

如下图



可开启转发递归的功能

可设置结果缓存的时间

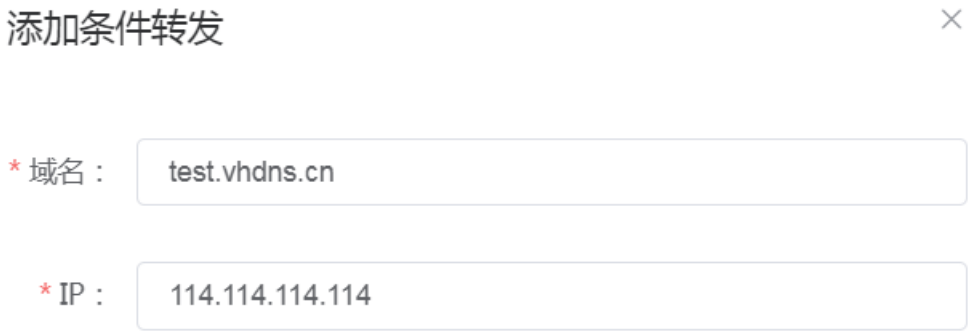
可设置转发指定上级 DNS 的 IP，留空则使用服务器系统的值

可开启条件转发的功能

2 条件转发

条件转发是指可设置指定域名的域名使用指定的 DNS 来进行解析和返回请求结果，此转发不支持顶级域名设置，只支持所设置的域名或二级域名进行转发，其它的仍然是使用默认的转发规则

添加操作如下



三） 节点设备

节点是指实际负责进行解析或递归转发的机器或服务程序，可以独立安装在独立的机器上，默认主控在安装时，也安装了节点服务，在节点列表里显示为 127.0.0.1 的 IP，在实际使用或解析中，则为相应的 IP 地址，因与主机为同一台机器，所以在节点列表里显示为 127.0.0.1 的 IP

可以安装两台或多台节点服务，以确保解析服务的稳定性和支撑更大的流量

如果主控只做管理用，不做节点用或不作解析用，可以将该节点停用或删除

四） 查询统计

1 查询统计

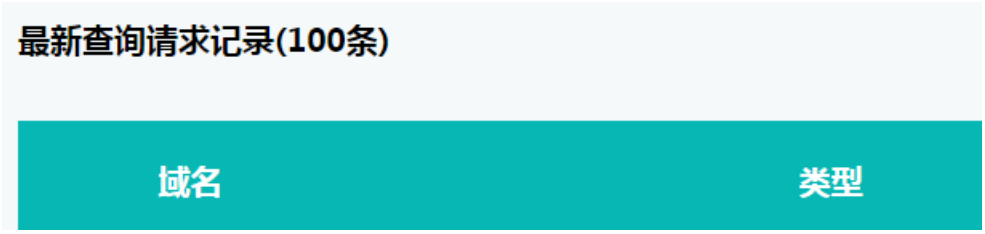
可实时统计或上述时间段时间统计的请求查询日志与记录

2 排行统计

可根据域名或 IP 等进行统计汇总，并按大小排行显示前 30 个数据

如下图

3 最新记录或日志



请求查询的最新记录或日志，显示最新的 100 条记录

五） 系统设置

1 后台设置

可设置该后台显示的名称或访问端口，及安全访问地址

如下图

2 系统设置

可设置后台登录的 cookie 有效时间，默认为 60 分钟

如下

3 修改密码

可修改后台访问的登录密码，如下图

四 常见问题

1 服务启动重启相关

主控后台/管理后台

supervisorctl restart vha //重启，停止，启动

supervisorctl start vha //启动

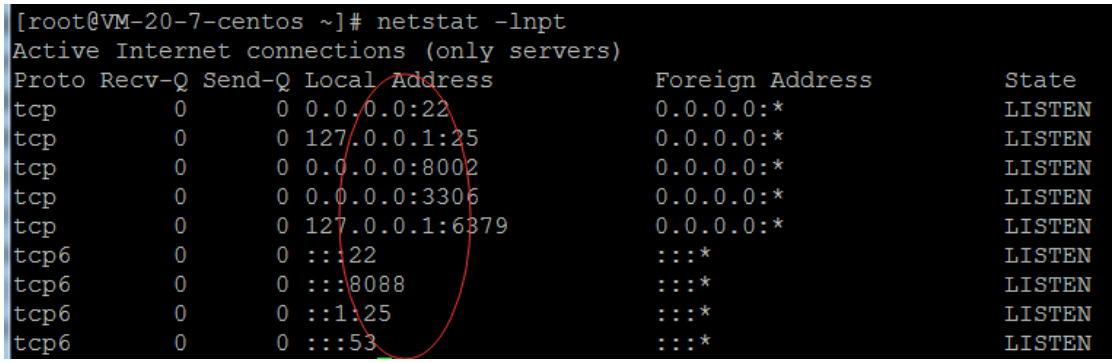
supervisorctl stop vha//停止

管理后台要确保 redis,mysql 服务已安装并启动

可使用 netstat –lnpt 命令查看是否有相关端口 ,如 8088,6379,3306

等端口，如没有则可能是安装出错或未安装完整，或服务未启动

如下



节点设备服务/解析服务

supervisorctl restart vhd //重启

supervisorctl start vhd //启动

supervisorctl stop vhd //停止

可使用 netstat –lnpt 命令查看是否有 8002,53,6379 等端口

2 检查服务器解析是否正常

直接在节点服务器上使用命令进行检查（因为 DNS 有缓存，直接在节点服务器上检查才能确定服务器本身是否正常），在服务器执行如下命令，如

dig @127.0.0.1 www.vhdns.cn

正常情况，会显示如下信息(把 www.vhdns.cn 替换为相应的域名)

```
[root@VM-20-7-centos ~]# dig @127.0.0.1 www.vhdns.cn

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> @127.0.0.1 www.vhdns.cn
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56191
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.vhdns.cn.                  IN      A

;; ANSWER SECTION:
www.vhdns.cn.           3600    IN      A       192.168.0.1
```

能显示相应的结果信息，就说明服务器的解析服务是正常的

此命令可检查任何 IP 节点，只要把 127.0.0.1 替换为相应的 IP 即可

如果没有 dig 命令，先进行安装（使用 yum install –y bind-utils）

3 服务器要开放哪些端口？

主控后台（8088/TCP），如有修改为其它则做相应调整。

如果主控也提供解析服务，则同样需要添加 53 端口

节点服务

53 UDP/TCP，这个是 DNS 服务必须用到的端口

8002/TCP，这个是与主控通讯使用到的端口

9200/TCP，这个是流量统计，只要节点与主控使用的端口

4 数据库默认密码

主控使用的数据库是 mysql，默认安装，数据库文件目录在

/var/lib/mysql 目录下

默认数据库管理密码可查看文件 /root/mysql_pw.txt

5 服务正常也按上述方法检查也正常

如果按上述方法检查过一遍，都正常也没当现什么问题，如有服务端口，有开防火墙等，所有常见问题都检查过，确定没问题，还是不行？那请检查下运行在 53 在端口的是不是我们的节点程序，我们的节点程序名为 vhd，如果不是，请停止其它程序，然后重启机器。重启完后再次检查。（目前发现有用户的机器，有其它程序运行在 53 端口上，导致我们的节点解析服务启动不了，自然不行，所以强烈建议，纯净系统安装，将会减少出错的可能和问题）

6 实时查询小工具 dig?

如果系统没有这个命令，请先安装（yum install –y bind-utils）。

简单实例：

dig @127.0.0.1 vhdns.cn

dig @127.0.0.1 vhdns.cn mx

更详细介绍请看下文：

DNS 查询实用程序 Dig。

语法

dig [@server] [-b address] [-c class] [-f filename] [-k filename] [-n][-p port#] [-t type] [-x addr] [-y name:key] [name] [type] [class] [queryopt...]

dig [-h]

dig [global-queryopt...] [query...]

描述

dig（域信息搜索器）命令是一个用于询问 DNS 域名服务器的灵活的工具。它执行 DNS 搜索 ,显示从受请求的域名服务器返回的答复。多数 DNS 管理员利用 dig 作为 DNS 问题的故障诊断 , 因为它灵活性好、易用、输出清晰。虽然通常情况下 dig 使用命令行参数，但它也可以按批处理模式从文件读取搜索请求。不同于早期版本 ,dig 的 BIND9 实现允许从命令行发出多个查询。除非被告知请求特定域名服务器 ,dig 将尝试 /etc/resolv.conf 中列举的所有服务器。当未指定任何命令行参数或选项时 , dig 将对 “.”（根)执行 NS 查询。

标志

-b address 设置所要询问地址的源 IP 地址。这必须是主机网络接口上的某一合法的地址。

-c class 缺省查询类（IN for internet）由选项 -c 重设。class 可以是任何合法类，比如查询 Hesiod 记录的 HS 类或查询 CHAOSNET 记录的 CH 类。

-f filename 使 dig 在批处理模式下运行，通过从文件 filename

读取一系列搜索请求加以处理。文件包含许多查询；每行一个。文件中的每一项都应该以和使用命令行接口对 dig 的查询相同的方法来组织。

-h 当使用选项 -h 时，显示一个简短的命令行参数和选项摘要。

-k filename 要签署由 dig 发送的 DNS 查询以及对它们使用事务签名（TSIG）的响应，用选项 -k 指定 TSIG 密钥文件。

-n 缺省情况下 ,使用 IP6.ARPA 域和 RFC2874 定义的二进制标号搜索 IPv6 地址。为了使用更早的、使用 IP6.INT 域和 nibble 标签的 RFC1886 方法，指定选项 -n（nibble）。

-p port# 如果需要查询一个非标准的端口号，则使用选项 -p。port# 是 dig 将发送其查询的端口号，而不是标准的 DNS 端口号 53。该选项可用于测试已在非标准端口号上配置成侦听查询的域名服务器。

-t type 设置查询类型为 type。可以是 BIND9 支持的任意有效查询类型。缺省查询类型是 A ,除非提供 -x 选项来指示一个逆向查询。通过指定 AXFR 的 type 可以请求一个区域传输。当需要增量区域传输（IXFR）时，type 设置为 ixfr=N。增量区域传输将包含自从区域的 SOA 记录中的序列号改为 N 之后对区域所做的更改。

-x addr 逆向查询(将地址映射到名称)可以通过 -x 选项加以简化。addr 是一个以小数点为界的 IPv4 地址或冒号为界的 IPv6 地址。当使用这个选项时，无需提供 name、class 和 type 参数。dig 自动运行类似 11.12.13.10.in-addr.arpa 的域名查询，并分别设置查

询类型和类为 PTR 和 IN。

-y name:key 您可以通过命令行上的 -y 选项指定 TSIG 密钥；name 是 TSIG 密码的名称，key 是实际的密码。密码是 64 位加密字符串，通常由 dnssec-keygen（8）生成。当在多用户系统上使用选项 -y 时应该谨慎，因为密码在 ps（1）的输出或 shell 的历史文件中可能是可见的。当同时使用 dig 和 TSCG 认证时，被查询的名称服务器需要知道密码和解码规则。在 BIND 中，通过提供正确的密码和 named.conf 中的服务器声明实现。

参数

global-queryopt... 全局查询选项（请参阅多个查询）。

查询 查询选项（请参阅查询选项）。

查询选项

dig 提供查询选项号，它影响搜索方式和结果显示。一些在查询请求报头设置或复位标志位，一部分决定显示哪些回复信息，其它的确定超时和重试战略。每个查询选项被带前缀（+）的关键字标识。一些关键字设置或复位一个选项。通常前缀是求反关键字含义的字符串 no。其他关键字分配各选项的值，比如超时时间间隔。它们的格式形如 +keyword=value。查询选项是：

+[no]tcp

查询域名服务器时使用 [不使用] TCP。缺省行为是使用 UDP，除非是 AXFR 或 IXFR 请求，才使用 TCP 连接。

+[no]vc

查询名称服务器时使用 [不使用] TCP。+[no]tcp 的备用语法提供了向下兼容。 vc 代表虚电路。

+[no]ignore

忽略 UDP 响应的中断，而不是用 TCP 重试。缺省情况运行 TCP 重试。

+domain=somename

设定包含单个域 somename 的搜索列表 ,好像被 /etc/resolv.conf 中的域伪指令指定，并且启用搜索列表处理，好像给定了 +search 选项。

+[no]search

使用 [不使用] 搜索列表或 resolv.conf 中的域伪指令（如果有的话）定义的搜索列表。缺省情况不使用搜索列表。

+[no]defname

不建议看作 +[no]search 的同义词。

+[no]aaonly

该选项不做任何事。它用来提供对设置成未实现解析器标志的 dig 的旧版本的兼容性。

+[no]adflag

在查询中设置 [不设置] AD（真实数据）位。目前 AD 位只在响应中有标准含义，而查询中没有，但是出于完整性考虑在查询中这种性能可以设置。

+[no]cdflag

在查询中设置 [不设置] CD（检查禁用）位。它请求服务器不运行响应信息的 DNSSEC 合法性。

+[no]recursive

切换查询中的 RD（要求递归）位设置。在缺省情况下设置该位，也就是说 dig 正常情形下发送递归查询。当使用查询选项 +nssearch 或 +trace 时，递归自动禁用。

+[no]nssearch

这个选项被设置时 ,dig 试图寻找包含待搜名称的网段的权威域名服务器，并显示网段中每台域名服务器的 SOA 记录。

+[no]trace

切换为待查询名称从根名称服务器开始的代理路径跟踪。缺省情况不使用跟踪。一旦启用跟踪，dig 使用迭代查询解析待查询名称。它将按照从根服务器的参照 ,显示来自每台使用解析查询的服务器的应答。

+[no]cmd

设定在输出中显示指出 dig 版本及其所用的查询选项的初始注释。缺省情况下显示注释。

+[no]short

提供简要答复。缺省值是以冗长格式显示答复信息。

+[no]identify

当启用 +short 选项时，显示 [或不显示] 提供应答的 IP 地址和端口号。如果请求简短格式应答，缺省情况不显示提供应答的服务器的源地址和端口号。

+[no]comments

切换输出中的注释行显示。缺省值是显示注释。

+[no]stats

该查询选项设定显示统计信息：查询进行时，应答的大小等等。缺省显示查询统计信息。

+[no]qr

显示 [不显示] 发送的查询请求。缺省不显示。

+[no]question

当返回应答时，显示 [不显示] 查询请求的问题部分。缺省作为注释显示问题部分。

+[no]answer

显示 [不显示] 应答的回答部分。缺省显示。

+[no]authority

显示 [不显示] 应答的权限部分。缺省显示。

+[no]additional

显示 [不显示] 应答的附加部分。缺省显示。

+[no]all

设置或清除所有显示标志。

+time=T

为查询设置超时时间为 T 秒。缺省是 5 秒。如果将 T 设置为小于 1 的数，则以 1 秒作为查询超时时间。

+tries=A

设置向服务器发送 UDP 查询请求的重试次数为 A，代替缺省的 3 次。如果把 A 小于或等于 0，则采用 1 为重试次数。

+ndots=D

出于完全考虑，设置必须出现在名称 D 的点数。缺省值是使用在 /etc/resolv.conf 中的 ndots 语句定义的，或者是 1，如果没有 ndots 语句的话。带更少点数的名称被解释为相对名称，并通过搜索列表中的域或文件 /etc/resolv.conf 中的域伪指令进行搜索。

+bufsize=B

设置使用 EDNS0 的 UDP 消息缓冲区大小为 B 字节。缓冲区的最大值和最小值分别为 65535 和 0。超出这个范围的值自动舍入到最近的有效值。

+[no]multiline

以详细的多行格式显示类似 SOA 的记录，并附带可读注释。缺省值是每单个行上显示一条记录，以便于计算机解析 dig 的输出。

多条查询

dig 的 BIND9 支持在命令行上指定多个查询（支持 -f 批处理文件选项的附加功能）。每条查询可以使用自己的标志位、选项和查询选项。

在这种情况下，在上面描述的命令行语法中，每条查询自变量代表一个个别查询。每一条由任意标准选项和标志、待查询名称、可选查询类型和类以及任何适用于该查询的查询选项。

也可以使用对所有查询均有效的查询选项全局集合。全局查询选项必

须位于命令行上第一个名称、类、类型、选项、标志和查询选项的元组之前。任何全局查询选项（除了 +[no]cmd 选项）可以被下面的查询特别选项重设。例如:

dig +qr www.isc.org any -x 127.0.0.1 isc.org ns +noqr 显示 dig 如何从命令行出发进行三个查询：一个针对 www.isc.org 的任意查询、一个 127.0.0.1 的逆向查询，以及一个 isc.org 的 NS 记录查询。应用了 +qr 的全局查询选项，以便 dig 显示进行每条查询的初始查询。最后那个查询有一个本地查询选项 +noqr，表示 dig 在搜索 isc.org 的 NS 记录时不显示初始查询。

示例

一个典型的 dig 调用类似：

dig @server name type 其中：

server

待查询名称服务器的名称或 IP 地址。可以是用点分隔的 IPv4 地址或用冒号分隔的 IPv6 地址。当由主机提供服务器参数时，dig 在查询域名服务器前先解析那个名称。如果没有服务器参数可以提供，dig 参考 /etc/resolv.conf，然后查询列举在那里的域名服务器。显示来自域名服务器的应答。

name

将要查询的资源记录的名称。

type

显示所需的查询类型 - ANY、A、MX、SIG，以及任何有效查询类

型等。如果不提供任何类型参数，dig 将对纪录 A 执行查询。