Herramientas de consulta DNS

Ping

- Ping no es una herramienta de diagnósitico DNS pero nos permite realizar resoluciones simples:

Comando:

```
ping example.com
```

Salida:

```
PING example.com (93.184.216.34) 56(84) bytes of data.
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=1 ttl=56 time=108 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=2 ttl=56 time=108 ms
^C
--- example.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 107.842/108.002/108.162/0.160 ms
```

Nslookup

- Nslookup es un programa para realizar consultas DNS. Se trata de una herramienta de diagnóstico que podemos utilizar para verificar si un servidor está resolviendo correctamente los nombres.
- Está disponible en Windows, Linux y MacOSX.

1. Encontrar un registro A de un dominio

Comando:

```
nslookup example.com
```

Salida:

```
root@ubuntu2004:~# nslookup example.com
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
Name:   example.com
Address: 93.184.216.34
Name:   example.com
Address: 2606:2800:220:1:248:1893:25c8:1946
```

2. Obtener los registros NS de un dominio

Comando:

```
nslookup -type=ns example.com
```

Salida:

```
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
example.com nameserver = a.iana-servers.net.
example.com nameserver = b.iana-servers.net.

Authoritative answers can be found from:
```

3. Obtener el registro SOA de un dominio

Comando:

```
nslookup -type=soa google.com
```

Salida:

```
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
google.com
    origin = ns1.google.com
    mail addr = dns-admin.google.com
    serial = 489786024
    refresh = 900
    retry = 900
    expire = 1800
    minimum = 60

Authoritative answers can be found from:
```

4. Obtener los registros MX responsables del intercambio de emails

Comando:

```
nslookup -type=mx google.com
```

Salida:

```
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
google.com  mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:
```

5. Obtener todos los Registros de Recursos de un dominio

Comando:

```
nslookup -type=any twitter.com
```

Salida:

```
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
Name:   twitter.com
Address: 104.244.42.1
twitter.com nameserver = a.r06.twtrdns.net.
twitter.com nameserver = b.r06.twtrdns.net.
twitter.com nameserver = c.r06.twtrdns.net.
twitter.com nameserver = d.r06.twtrdns.net.
twitter.com nameserver = d01-01.ns.twtrdns.net.
twitter.com nameserver = d01-02.ns.twtrdns.net.
twitter.com nameserver = ns1.p34.dynect.net.
twitter.com nameserver = ns2.p34.dynect.net.
twitter.com nameserver = ns3.p34.dynect.net.
twitter.com nameserver = ns4.p34.dynect.net.
twitter.com
    origin = ns1.p26.dynect.net
    mail addr = zone-admin.dyndns.com
    serial = 2007176709
    refresh = 3600
    retry = 600
    expire = 604800
    minimum = 60
twitter.com mail exchanger = 10 aspmx.l.google.com.
twitter.com mail exchanger = 20 alt1.aspmx.l.google.com.
```

```
twitter.com mail exchanger = 20 alt2.aspmx.l.google.com.
twitter.com mail exchanger = 30 aspmx2.googlemail.com.
twitter.com mail exchanger = 30 aspmx3.googlemail.com.
twitter.com text = "0a8c0fc6-bfa5-4ea7-b09b-87f2989022d6"
twitter.com text = "MS=BEE202D20C326867290BDEFA2DDDF4594B5D6860"
twitter.com text = "adobe-idp-site-
verification=a2ff8fc40c434d1d6f02f68b0b1a683e400572ab8c1f2c180c71c3d985b92
70a"
twitter.com text = "apple-domain-verification=zd1iHoEO9LILEQIq"
twitter.com text = "atlassian-domain-
verification=CCYSIJhsAnbjYWrbdw5r//aHNsYnzgv7Z6Gwz4TkAv5OYdZt3Lm/ycLxT2tmf
m/n"
twitter.com text = "bj6sbt5xqs9hw9jrfvz7hplrg0l680sb"
twitter.com text = "canva-site-verification=lMnZ3wMh7c1uqZqa-cxZTg"
twitter.com text = "google-site-
verification=TNhAkfLUeIbzzzSgPNxS5aEkKMf3aUcpPmCK1_kmIvU"
twitter.com text = "google-site-
verification=h6dJIv0HXjLOkGAotLAWEzvoi9SxqP4vjpx98vrCvvQ"
twitter.com text = "loom-site-
verification=638c6bc173b9458997f64d305bf42499"
twitter.com text = "miro-
verification=6e1ca9ad6d0c2cd2e4186141265f23ed618cfe37"
twitter.com text = "mixpanel-domain-verify=164dda91-31f4-41e8-a816-
0f59b38fea30"
twitter.com text = "traction-guest=6882b04e-4188-4ff9-8bb4-bff5a3d358e6"
twitter.com text = "traction-guest=a4d0248d-fe01-4222-8fcc-33f68323e667"
twitter.com text = "v=spf1 ip4:199.16.156.0/22 ip4:199.59.148.0/22
ip4:8.25.194.0/23 ip4:8.25.196.0/23 ip4:204.92.114.203
ip4:204.92.114.204/31 ip4:54.156.255.69 include:_spf.google.com
include:_thirdparty.twitter.com include:spf.smtp2go.com -all"
twitter.com text = "wrike-
verification=MjU4MTA5MjoyN2UzNDc1MjU3MDZiZTY4NjBiNzliNDQ2OTUwNWY3NmM5NDgyM
TBlYzFkNTcwYTE2YWNmZDdkNTY2ZmE4Yzlh"

Authoritative answers can be found from:
```

6. Consultar a un servidor DNS particular

Comando:

```
nslookup wikipedia.org 8.8.8.8
```

Salida:

```
Server:     8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
```

```
Name:   wikipedia.org
Address: 185.15.58.224
Name:   wikipedia.org
Address: 2a02:ec80:600:ed1a::1
```

7. Realizar una consulta inversa

Así podremos saber si una IP está relacionada con un dominio.

Comando:

```
nslookup 185.15.58.224
```

Salida:

```
224.58.15.185.in-addr.arpa  name = text-lb.drmrs.wikimedia.org.

Authoritative answers can be found from:
```

8. Buscar un Registro de Recurso PTR

Tendremos que voltear la IP y añadirla al dominio in-addr.arpa.

Comando:

```
nslookup -type=ptr 224.58.15.185.in-addr.arpa
```

Salida:

```
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
224.58.15.185.in-addr.arpa  name = text-lb.drmrs.wikimedia.org.

Authoritative answers can be found from:
```

9. Cambiar el intervalo de timeout para una respuesta

Así podemos dar más tiempo a un servidor para responder, o ver qué servidores responden en el límite de tiempo que fijemos.

Comando:

```
nslookup -timeout=20 twitter.com
```

Salida:

```
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
Name:   twitter.com
Address: 104.244.42.1
```

10. Activar el modo de debug

Activando el modo *debug* podremos obtener información más detallada de las consultas y las respuestas.

Comando:

```
nslookup -debug facebook.com
```

Salida:

```
Server:     127.0.0.53
Address:    127.0.0.53#53

------------
    QUESTIONS:
    facebook.com, type = A, class = IN
    ANSWERS:
    ->  facebook.com
    internet address = 157.240.246.35
    ttl = 200
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   facebook.com
Address: 157.240.246.35
------------
    QUESTIONS:
    facebook.com, type = AAAA, class = IN
    ANSWERS:
    ->  facebook.com
    has AAAA address 2a03:2880:f104:83:face:b00c:0:25de
    ttl = 300
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
```

```
------------
Name:   facebook.com
Address: 2a03:2880:f104:83:face:b00c:0:25de
```

10. Seleccionar un puerto para la consulta

Comando:

```
nslookup -port=3053 wikipedia.org
```

Nslookup en modo interactivo

La herramienta nslookup cuenta con un **modo interactivo** para realizar consultas.

Para iniciar el modo interactivo escribimos:

```
nslookup
```

Por defecto las búsquedas se llevan a cabo sobre el registro A del dominio. Si queremos obtener registros diferentes, debemos especificarlo:

- set type=A, para buscar registros A.
- set type=PTR, para buscar registros reversos.
- set type=MX, para buscar los registros Mail Exchange del correo.
- set type=TXT, para buscar registros de texto como SPF o DKIM.
- set type=CNAME, para buscar alias del dominio.
- set type=any, para cualquier registro.

Podemos especificar el servidor:

```
server 8.8.8.8
```

Activar el debug:

```
set debug
```

Pedir unos registros de recursos concretos:

```
set type=mx
```

Para más información sobre las opciones del comando **nslookup** se puede leer el manual:

```
man nslookup
```

Dig

- Dig es una herramienta del ISC y está creada para reemplazar a nslookup.
- No está disponible en Windows, pero se puede instalar.

Interpretación de la respuesta

Si por ejemplo escribimos:

```
dig google.com
```

Obtenemos:

```
; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27551
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.            IN  A

;; ANSWER SECTION:
google.com.     185 IN  A   142.250.184.174

;; Query time: 19 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Nov 21 07:26:11 EST 2022
;; MSG SIZE  rcvd: 55
```

Donde:

```
; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
```

Son la versión y las opciones que se han establecido para la consulta.

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27551
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

Son detalles de información de la respuesta del servidor DNS. Esta parte puede desactivar se añadiendo **+[no]comments**, pero al hacerlo se desactivarán las cabeceras de información.

```
dig google.com +nocomments
```

Esta parte:

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
```

Tiene que ver con "Extended mechanisms for DNS" (EDNS).

Un mensaje DNS consiste en las siguientes 5 secciones:

1. Header
2. Question
3. Answer
4. Authority
5. Additional

Pero a finales de los años 1990 se quiso extender la funcionalidad de DNS, pero tal como estaba construido, no se podían añadir nuevas secciones. EDNS es parte de la seccion Additional.

Más información: Extension Mechanisms for DNS

```
;; QUESTION SECTION:
;google.com.            IN  A
```

Esta parte es la consulta que hemos realizado.

```
;; ANSWER SECTION:
google.com.     185 IN  A   142.250.184.174
```

Es la respuesta a la consulta que hemos realizado.

```
;; Query time: 19 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Nov 21 07:32:21 EST 2022
;; MSG SIZE  rcvd: 55
```

El bloque final incluye estadísticas relacionadas con la consulta, que pueden desactivarse con la opción **+[no]stats**.

```
dig google.com +nostats
```

1. Consulta básica de los registros A

Comando:

```
dig google.com
```

Salida:

```
; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55093
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.            IN  A

;; ANSWER SECTION:
google.com.     22  IN  A   142.250.200.78

;; Query time: 19 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Nov 21 07:40:18 EST 2022
;; MSG SIZE  rcvd: 55
```

2. Consulta a un servidor específico

Le consultamos al servidor 8.8.8.8 por google.com. Hay que tener en cuenta que nuestra red debe de permitir consultas a servidores externos en el puerto 53, porque si no, la consulta fallará.

Comando:

```
dig @8.8.8.8 google.com
```

Salida:

```
; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 635
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.            IN  A

;; ANSWER SECTION:
google.com.     170 IN  A   142.250.178.174

;; Query time: 19 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Nov 21 07:44:55 EST 2022
;; MSG SIZE  rcvd: 55
```

3. Consulta de un RR particular

Comando:

```
dig google.com MX
```

Salida:

```
; <<>> DiG 9.16.1-Ubuntu <<>> google.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6261
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.            IN  MX

;; ANSWER SECTION:
google.com.     266 IN  MX  10 smtp.google.com.

;; Query time: 19 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Nov 21 07:46:05 EST 2022
;; MSG SIZE  rcvd: 60
```

4. Resolución inversa

Comando:

```
dig -x 142.250.184.163
```

Salida:

```
; <<>> DiG 9.16.1-Ubuntu <<>> -x 142.250.184.163
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26680
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;163.184.250.142.in-addr.arpa.  IN  PTR

;; ANSWER SECTION:
163.184.250.142.in-addr.arpa. 7188 IN   PTR mad07s23-in-f3.1e100.net.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Nov 21 07:48:27 EST 2022
;; MSG SIZE  rcvd: 95
```

5. Trazar la consulta DNS

Con la opción **+trace** podemos observar cómo se lleva a cabo la consulta. Primero se consulta un servidor raíz, luego se consulta un servidor ".com" y por último, los servidores de Google. Finalmente los servidores de Google, devuelven la respuesta.

Comando:

```
dig google.com +trace
```

Salida:

```
; <<>> DiG 9.16.1-Ubuntu <<>> google.com +trace
;; global options: +cmd
.           30811   IN  NS  a.root-servers.net.
.           30811   IN  NS  b.root-servers.net.
.           30811   IN  NS  c.root-servers.net.
```

```
.           30811   IN  NS  d.root-servers.net.
.           30811   IN  NS  e.root-servers.net.
.           30811   IN  NS  f.root-servers.net.
.           30811   IN  NS  g.root-servers.net.
.           30811   IN  NS  h.root-servers.net.
.           30811   IN  NS  i.root-servers.net.
.           30811   IN  NS  j.root-servers.net.
.           30811   IN  NS  k.root-servers.net.
.           30811   IN  NS  l.root-servers.net.
.           30811   IN  NS  m.root-servers.net.
;; Received 262 bytes from 127.0.0.53#53(127.0.0.53) in 24 ms

com.            172800  IN  NS  b.gtld-servers.net.
com.            172800  IN  NS  c.gtld-servers.net.
com.            172800  IN  NS  l.gtld-servers.net.
com.            172800  IN  NS  i.gtld-servers.net.
com.            172800  IN  NS  a.gtld-servers.net.
com.            172800  IN  NS  k.gtld-servers.net.
com.            172800  IN  NS  j.gtld-servers.net.
com.            172800  IN  NS  d.gtld-servers.net.
com.            172800  IN  NS  h.gtld-servers.net.
com.            172800  IN  NS  f.gtld-servers.net.
com.            172800  IN  NS  e.gtld-servers.net.
com.            172800  IN  NS  m.gtld-servers.net.
com.            172800  IN  NS  g.gtld-servers.net.
com.            86400   IN  DS  30909 8 2
E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CF C41A5766
com.            86400   IN  RRSIG   DS 8 1 86400 20221204050000
20221121040000 18733 .
yvIf0dp0+F5Mgp5KHWB48b/K+EePKMqy7XRJfcBKMb3BEOEyNp960igH
t4/AQC4FaNz5V8ij/dYWOgiBKW9QiYkEzTTBomocvnD4kX61QXxSjEZt
ejYqnWxcevLom/occKG2+DCDTxsFppMsKwg022erqY7exPGUOWK2J6TU
uM17dGaPoNk1nXTkLM61QjU+RM79ZGwzXWJ+hH4HKfpsIwqNMKCWu17r
m/a6GqccNghanNPdiO8SVqOYUUVQM1SP+SC4DI0gfJJRQx+E+G/Cib5a
3S+PGfaD2lj3Oxzq/Ro/jjFbfn2pgZQhwrnw356bqmbyRwWGk3lFjP+b 7VjQmw==
;; Received 1170 bytes from 202.12.27.33#53(m.root-servers.net) in 48 ms

google.com.     172800  IN  NS  ns2.google.com.
google.com.     172800  IN  NS  ns1.google.com.
google.com.     172800  IN  NS  ns3.google.com.
google.com.     172800  IN  NS  ns4.google.com.
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN NSEC3 1 1 0 -
CK0Q2D6NI4I7EQH8NA30NS61O48UL8G5 NS SOA RRSIG DNSKEY NSEC3PARAM
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN RRSIG NSEC3 8 2 86400
20221127052428 20221120041428 53929 com.
SnVmAcktp+1bTm0p0l8zbWAgAsmntjN5RgRngxHv37sANfXnkOyXkcor
jUYCXrf2r5KNli9HUQoWb+VHXXrG6hoSy+S/YvQXy8BPN3ilr8NypcT7
W0h07JhVZYz4h4JXJvgvFCyFIBEo3/GOfDUT+7UfRKlrTJiio3vOVmY6
ga8Ia/D3UVkcHl5HbLqjI10ipBFOYQ1SWlour/8bv3vqgQ==
S84BKCIBC38P58340AKVNFN5KR9O59QC.com. 86400 IN NSEC3 1 1 0 -
S84BUO64GQCVN69RJFUO6LVC7FSLUNJ5 NS DS RRSIG
S84BKCIBC38P58340AKVNFN5KR9O59QC.com. 86400 IN RRSIG NSEC3 8 2 86400
20221128061416 20221121050416 53929 com.
DTbFbBAs8M00SNnhSBjNip5cbvI02YrQqO2plJmHzyXO8oelbFOW1+0/
```

```
9NpUgEX4f8ZfXQbRdYSHqoR4dzO6AjaCf7Vco6EcGaENrQMubo9Xc29y
Rs2gubTisxk0ps9Ax0s6kDOQDXSkAUGFiHoSr2fDA7cop1EDLEOG1Fjo
LxzMozVrOZC373Svm/xmS33/Dh7PYLi8IuhTCVKUZDgtYA==
;; Received 836 bytes from 192.55.83.30#53(m.gtld-servers.net) in 60 ms

google.com.     300 IN  A   142.250.200.110
;; Received 55 bytes from 216.239.36.10#53(ns3.google.com) in 40 ms
```

6. Respuestas cortas

A veces nos insteresará obtener una respuesta corta sin tanta información *verbose*. Esto se consigue con la opción **+short**.

Comando:

```
dig google.com +sort
```

Salida:

```
142.250.184.174
```

7. Consultas desde ficheros

Es posible que queramos realizar consultas desde direcciones que tengamos almacenadas en un fichero:

Fichero:

```
www.facebook.com
www.google.com
www.twitter.com
www.microsoft.com
```

Comando:

```
dig -f query.txt +short
```

Salida:

```
star-mini.c10r.facebook.com.
157.240.246.35
142.250.201.68
twitter.com.
```

```
104.244.42.65
www.microsoft.com-c-3.edgekey.net.
www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net.
e13678.dscb.akamaiedge.net.
92.123.57.133
```

8. Consultas a un servidor DNS en un puerto específico

El puerto por defecto de DNS es el 53, pero es posible que configuremos un servidor en otro puerto.

Comando:

```
dig @8.8.8.8 -p <puerto> <host>
```

9. IPv4 e IPv6

Por defecto dig trabaja con direcciones IPv4, pero podemos especificar si queremos utilizar IPv4 con la opción **-4** o IPv6 con la opción **-6**.

Comando:

```
dig -6 @2001:4860:4860::8888 google.com A
```

Salida:

```
; <<>> DiG 9.3.6-P1-RedHat-9.3.6-25.P1.el5_11.8 <<>> @2001:4860:4860::8888
google.com A
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40588
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.            IN  A

;; ANSWER SECTION:
google.com.     294 IN  A   66.102.1.113
google.com.     294 IN  A   66.102.1.101
google.com.     294 IN  A   66.102.1.138
google.com.     294 IN  A   66.102.1.100
google.com.     294 IN  A   66.102.1.139
google.com.     294 IN  A   66.102.1.102

;; Query time: 6 msec
;; SERVER: 2001:4860:4860::8888#53(2001:4860:4860::8888)
```

```
;; WHEN: Tue Sep  6 13:21:10 2016
;; MSG SIZE  rcvd: 124
```

Para que esto funcione, debes tener configurado correctamente la red IPv6.

10. Pedir todos los RR con ANY

Comando:

```
dig google.com ANY
```

Salida:

```
; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.3 <<>> google.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16952
;; flags: qr rd ra; QUERY: 1, ANSWER: 12, AUTHORITY: 0, ADDITIONAL: 11

;; QUESTION SECTION:
;google.com.                    IN      ANY

;; ANSWER SECTION:
google.com.             5       IN      A       216.58.220.110
google.com.             5       IN      NS      ns4.google.com.
google.com.             5       IN      NS      ns3.google.com.
google.com.             5       IN      NS      ns1.google.com.
google.com.             5       IN      NS      ns2.google.com.
google.com.             5       IN      MX      50
alt4.aspmx.l.google.com.
google.com.             5       IN      MX      20
alt1.aspmx.l.google.com.
google.com.             5       IN      MX      30
alt2.aspmx.l.google.com.
google.com.             5       IN      MX      10 aspmx.l.google.com.
google.com.             5       IN      MX      40
alt3.aspmx.l.google.com.
google.com.             5       IN      TXT     "v=spf1
include:_spf.google.com ~all"
google.com.             5       IN      AAAA    2404:6800:4006:801::200e

;; ADDITIONAL SECTION:
ns4.google.com.         5       IN      A       216.239.38.10
ns3.google.com.         5       IN      A       216.239.36.10
ns1.google.com.         5       IN      A       216.239.32.10
ns2.google.com.         5       IN      A       216.239.34.10
alt4.aspmx.l.google.com. 5      IN      A       173.194.219.27
alt4.aspmx.l.google.com. 5      IN      AAAA    2607:f8b0:4002:c03::1a
alt1.aspmx.l.google.com. 5      IN      A       74.125.198.27
```

```
alt1.aspmx.l.google.com. 5      IN      AAAA    2607:f8b0:400e:c03::1b
alt2.aspmx.l.google.com. 5      IN      A       64.233.182.27
alt2.aspmx.l.google.com. 5      IN      AAAA    2607:f8b0:4003:c05::1a
aspmx.l.google.com.     5       IN      A       64.233.188.27

;; Query time: 28 msec
;; SERVER: 192.168.220.2#53(192.168.220.2)
;; WHEN: Tue Sep 06 09:53:06 AEST 2016
;; MSG SIZE  rcvd: 512
```

Algunos servidores **no soportan esto** y van a denegar la respuesta, como Coudfare.

```
dig cloudfare.com ANY
```

```
; <<>> DiG 9.10.6 <<>> cloudfare.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11217
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cloudfare.com.         IN  ANY

;; ANSWER SECTION:
cloudfare.com.      3789    IN  HINFO   "RFC8482" ""

;; Query time: 69 msec
;; SERVER: 192.168.1.2#53(192.168.1.2)
;; WHEN: Tue Nov 22 00:08:30 CET 2022
;; MSG SIZE  rcvd: 63
```

Algunos servidores autoritativos no responden a las consultas por todos los registros de recursos por temas de política local, seguridad y rendimiento:

- Más información: [RFC8482](https://www.rfc-editor.org/rfc/rfc8482]

Personalizar la salida de dig

Podemos personalizar la salida de dig con diferentes opciones

- Con **+noall++ podemos esconder la mayor parte de la salida.

Comando:

```
dig google.com +noall
```

Salida:

```
; <<>> DiG 9.10.6 <<>> google.com +noall
;; global options: +cmd
```

- Con **+stats** podemos imprimir las estadísticas.

Comando:

```
dig google.com +noall +stats
```

Salida:

```
; <<>> DiG 9.10.6 <<>> google.com +noall +stats
;; global options: +cmd
;; Query time: 88 msec
;; SERVER: 192.168.1.2#53(192.168.1.2)
;; WHEN: Mon Nov 21 19:04:56 CET 2022
;; MSG SIZE  rcvd: 55
```

- Con **+answer** podemos imprimir la respuesta.

Comando:

```
dig google.com +noall +answer
```

Salida:

```
; <<>> DiG 9.10.6 <<>> google.com +noall +answer
;; global options: +cmd
google.com.     174 IN  A   216.58.209.78
```

Ajustes por defecto con el archivo ~/.digrc

Podemos definir ajustes por defecto de las opciones que queremos que dig corra por defecto en el archivo ~/.digrc que siempre se ejecuta con el comando dig.

```
$ cat .digrc
+short
$ dig google.com
216.58.209.78
```

Más información

Para más información, consulta el manual de **dig** con:

```
man dig
```

host

Host es otra herramienta para realizar consultas DNS.

Sintaxis:

```
host [-aCdlnrsTwv] [-c class] [-N ndots] [-R number] [-t type] [-W wait]
[-m flag] [-4] [-6] {name} [server]
```

Opciones:

- -a: Muestra todos los registros de recurso DNS para el hostname dado. Equivalentae a -v -t SOA
- -C: Muestra los registros de recursos SOA y los servidores DNS autorizados.
- -d: Es equivalente a -v.
- -l: Lista todos los hosts en un nombre de dominio usando AXFR.
- -r: Realiza consultas no recursivas. Con esta opción, despeja el bit RD en la consulta. Por lo tanto el servidor DNS que la recibe no intentará resolver el nombre, por lo general, serán referencias a otros servidores DNS.
- -s: Le dice al host que no envíe la consulta al siguiente servidor de nombres si algún servidor responde con una respuesta SERVFAIL.
- -T: Utiliza TCP en vez de UDP para consultas al servidor de nombres. Esto está implícito en consultas que requieran TCP, como las peticiones AXFR.
- -v: Genera salida verbose.
- -t: Se utiliza para seleccionar el tipo de query. Tipo de Query: CNAME,NS,SOA,KEY etc,.
- -W: Especifica cuánto esperar para una respuesta. Cuando se usa la opción -w, el host esperará por siempre una respuesta.
- -4: Obliga al host a usar solo el transporte de consultas IPv4.
- -6: Obliga al host a usar solo el transporte de consultas IPv6.

1. Obtención de la dirección IP

Comando:

```
host pixfans.com
```

Salida:

```
pixfans.com has address 5.39.80.5
pixfans.com mail is handled by 20 ALT1.ASPMX.L.GOOGLE.com.
pixfans.com mail is handled by 10 ASPMX.L.GOOGLE.com.
```

2. Búsqueda inversa

Comando:

```
host 5.39.80.5
```

Respuesta:

```
5.80.39.5.in-addr.arpa domain name pointer ns3033936.ip-5-39-80.eu.
```

Comando:

```
host 1.1.1.1
```

Respuesta:

```
1.1.1.1.in-addr.arpa domain name pointer one.one.one.one.
```

3. Consultar al servidor 1.1.1.1 por los servidores DNS del dominio .es

Comando:

```
host -t NS es 1.1.1.1
```

Salida:

```
    Using domain server:
    Name: 1.1.1.1
    Address: 1.1.1.1#53
```

```
    Aliases:

    es name server a.nic.es.
    es name server f.nic.es.
    es name server g.nic.es.
    es name server h.nic.es.
    es name server ns1.cesca.es.
    es name server ns-es.nic.fr.
    es name server ssdns-tld.nic.cl.
```

Consultar al servidor DNS 8.8.8.8 por el registro de recursos (RR) SOA del dominio .ES

Comando:

```
host -t SOA es 8.8.8.8
```

Salida:

```
    Using domain server:
    Name: 8.8.8.8
    Address: 8.8.8.8#53
    Aliases:

    es has SOA record ns1.nic.es. hostmaster.nic.es. 2020110206 7200 7200
2592000 86400
```

Realizar una consulta ANY a un servidor, preguntando al 8.8.4.4

Comando:

```
host -a pixfans.com 8.8.4.4
```

Salida:

```
    Trying "pixfans.com"
    Using domain server:
    Name: 8.8.4.4
    Address: 8.8.4.4#53
    Aliases:

    ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12972
    ;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 0

    ;; QUESTION SECTION:
```

```
    ;pixfans.com.           IN  ANY

    ;; ANSWER SECTION:
    pixfans.com.        299 IN  SOA ns.dinahosting.com.
hostmaster.pixfans.com. 2018012301 3600 120 1209600 300
    pixfans.com.        299 IN  A   5.39.80.5
    pixfans.com.        299 IN  NS  ns.dinahosting.com.
    pixfans.com.        299 IN  NS  ns2.dinahosting.com.
    pixfans.com.        299 IN  NS  ns4.dinahosting.com.
    pixfans.com.        299 IN  NS  ns3.dinahosting.com.
    pixfans.com.        299 IN  MX  10 ASPMX.L.GOOGLE.com.
    pixfans.com.        299 IN  MX  20 ALT1.ASPMX.L.GOOGLE.com.

    Received 227 bytes from 8.8.4.4#53 in 42 ms
```

Informes de DNS

Existen herramientas online que nos pueden ayudar a diagnosticar problemas con DNS.

- **DNS Checker**
  - Nos permite comprobar si se han propagado nuestros registros DNS.
  - Comprobar la configuración de un sitio.
  - Dispone de una lista de servidores DNS públicos categorizados por país.
- **DNS Spy**
  - Monitoriza, valida y verifica configuraciones DNS.
- Etc.

WHOIS

Whois no es una herramienta de diagnóstico DNS pero sí nos ofrece información sobre el registro del dominio.

Consulta bases de datos que contienen información del usuario, empresa u organización que registra un nombre de dominio o una dirección IP en Internet.

El protocolo whois se encapsula en TCP y sólo especifica el intercambio de peticiones y respuestas, no el formato de los datos a intercambiar, por lo tanto éstas pueden variar.

Ejemplo de whois

Comando:

```
whois gestal.es
```

Respuesta:

```
    % IANA WHOIS server
    % for more information on IANA, visit http://www.iana.org
    % This query returned 1 object

    refer:        whois.nic.es

    domain:       ES

    organisation: Red.es
    address:      Edificio Bronce
    address:      Plaza Manuel Gomez Moreno
    address:      Madrid  28020
    address:      Spain

    contact:      administrative
    name:         David Cierco Jiménez de Parga
    organisation: Red.es
    address:      Edificio Bronce
    address:      Plaza Manuel Gomez Moreno
    address:      Madrid  28020
    address:      Spain
    phone:        +34 91 212 76 24
    fax-no:       +34 91 555 76 64
    e-mail:       esnic-admin@red.es

    contact:      technical
    name:         Juan Antonio Gutierrez Gil
    organisation: Red.es
    address:      Edificio Bronce
    address:      Plaza Manuel Gomez Moreno
    address:      Madrid  28020
    address:      Spain
    phone:        +34 91 212 76 20
    fax-no:       + 34 91 556 88 64
    e-mail:       esnic-tech@red.es

    nserver:      A.NIC.ES 194.69.254.1 2001:67c:21cc:2000:0:0:64:41
    nserver:      F.NIC.ES 130.206.1.7 2001:720:418:caf1:0:0:0:7
    nserver:      G.NIC.ES 2001:500:14:7001:ad:0:0:1 204.61.217.1
    nserver:      H.NIC.ES 194.0.33.53 2001:678:40:0:0:0:0:53
    nserver:      NS-ES.NIC.FR 194.0.9.1 2001:678:c:0:0:0:0:1
    nserver:      NS1.CESCA.ES 2001:40b0:1:1122:ce5c:a000:0:3 84.88.0.3
    nserver:      SSDNS-TLD.NIC.CL 200.7.5.14 2001:1398:276:0:200:7:5:14
    ds-rdata:     29450 8 2
8BEC32A2C9CFE42E393BAF81FFE71B521D3E940612A4590B4763ADC539E4B563
    ds-rdata:     29450 8 1 417BEAFB46ABF3430B75C5C29AEF785D476B60E1
    ds-rdata:     50252 8 2
dd2b515da6dbc0e826006e6ae02864c05825694a84b3e4e0e59918c78c1bc8eb
    ds-rdata:     50252 8 1 9bf0115b43a4ee8f7223fbf5b294d91cdeed2dbe

    whois:        whois.nic.es
```

```
    status:       ACTIVE
    remarks:      Registration information: http://www.nic.es/

    created:      1988-04-14
    changed:      2020-04-05
    source:       IANA

    # whois.nic.es

    Conditions of use for the whois service via port 43 for .es domains

    Access will only be enabled for  IP addresses  authorised  by Red.es.
A maximum of one  IP address per
    user/organisation is permitted.

    Red.es accepts  no responsibility  whatsoever  for  the availability
of access to WHOIS,  which may be
    suspended at any time and without prior warning at the discretion of
the public entity.

    The service will be limited to the data established by Red.es.

    The user  promises  to make use of the service and to  carry out any
action derived  from the aforesaid
    use in accordance with  current applicable  regulations, in particular
with legislation on ".es" domain
    names and personal data protection.

    In particular, the user undertakes not to use  the service  to carry
out abusive  or speculative domain
    name registrations, pursuant to section 5 of the Sixth Additional
Provision of Law 34/2002, of 11 July,
    on Services of the  Information  Society and  Electronic Commerce.
Likewise, the User undertakes not to
    use the service to  obtain data, the possession  of which may
contravene the provisions of Organic Law
    15/1999,  of  13 December,  on Personal Data Protection, and  its
Regulations, or in Law 34/2002, of 11
    July, on Services of the Information Society and Electronic Commerce.

    Failure  to comply with these conditions will result in the immediate
withdrawal of the service and any
    registered domain name which breaches said conditions may be
officially cancelled by Red.es.
    ------------------------------------------------------------------------
--------------------------------

    The IP address used to perform the query  is not authorised  or  has
exceeded the established limit for
    queries.To request access to the service,complete the form located at
https://sede.red.gob.es/sede/whois,
    where you may also consult the service conditions.

    ------------------------------------------------------------------------
```

```
--------------------------------
    More information on each domain may be consulted at www.dominios.es.
```

Por privacidad, muchas veces los datos de los **auténticos propietarios** de los dominios no aparecen. Aparecen los de la compañía en la que se registró el dominio.

Whois desde web

Algunas páginas webs nos permiten realizar consultas whois desde el navegador:

- ICANN WHOIS
- DOMANINTOOLS – Whois Lockup
- DonDominio – Whois

Fuentes

- 10 most used nslookup commands
- Cómo utilizar el comando dig
- 12 dig command examples to query dns in linux