DNS TOOLS

Descargar PDF

INTRODUCCIÓN

Existen utilidades que permiten consultar a los servidores DNS por la resolución de nombres de dominio, así como obtener los diferentes tipos de registros de sus bases de datos. Las más habituales son:

- **nslookup**
- **dig**
- **host**

INSTALACION

Estas utilidades pertenecen a la suite BIND de ISC. Veamos su proceso de instalación:

Windows

BIND 9.16 es la última versión con soporte para Windows. Podemos acceder al repositorio de BIND y descargarnos la versión para windows en el siguiente enlace BIND 9.16 windows.

Pasos para la instalación:

- 0.Descargar BIND 9.16 windows.
- 1.Descomprimir el archivo BIND9.16.0.x64.zip
- 2.Ejecutar BINDInstall.exe con permisos de administrador.
- 3.Cambiar directorio de instalación a C:\BINDTools
- 4.Marcar solamente la casilla Tools.
- 5.Pulsar el botón instalar.

> **Nota:** La utilidad nslookup también está instalada por defecto en los sistemas windows.
> directorio \windows\system32\

Linux

```
Debian      apt update && apt install dnsutils -y
Alpine      apk update && apk add bind-tools
```

NSLOOKUP

Se puede encontrar información del comando en nslookup man. NSLOOKUP se puede ejecutar de manera interactiva y no-interactiva. Por su utilidad nos centraremos en la no-interactiva. El esquema general del comando es:

```
nslookup [options] [domain-name] [name-server]

options
 -debug             muestra información de depuración
 -port=[port]       utilizar puerto en lugar del 53
 -timeout=[segons]  tiempo en segundos para esperar respuesta
 -type=a            consultar registros A (Address)
 -type=any          consultar todos los registros
 -type=hinfo        consultar registros hardware
 -type=mx           consultar registros mail Exchange
 -type=ns           consultar registros de nombres de servidores.
 -type=ptr          consultar registros pòinter (reverse lookup)
 -type=soa          consultar registros de definición de zona
domain-name         nombre de dominio a consultar.
name-server         servidor dns al que se hace la consulta.
                    Si no se indica utilizará el configurado en el sistema.
```

Algunos ejemplos de uso:

nslookup www.ua.es

```
Servidor:  UnKnown
Address:  192.168.1.1
Respuesta no autoritativa:
Nombre:  www.edu.gva.es
Addresses:  195.77.20.137
            193.145.200.137
```

Nos indica que ha utilizado el servidor configurado por defecto 192.168.1.1 y que ha obtenido como respuesta para el nombre www.edu.gva.es las IPs 195.77.20.137 i 193.145.200.137. Eso es porque hay dos máquinas que pueden responder a este nombre, normalmente se utiliza esta técnica para el balanceado de carga (round robin). Nos indica además que la respuesta es no autoritativa, es decir, que el servidor 192.168.1.1 no define este nombre en su base de datos si no que lo ha obtenido al consultar a otro servidor.

nslookup www.elmundo.es

```
Servidor:  UnKnown
Address:  192.168.1.1
Respuesta no autoritativa:
Nombre:  unidadeditorial.map.fastly.net
Address:  151.101.133.50
Aliases:  www.elmundo.es
```

Nos indica que ha utilizado el servidor configurado por defecto 192.168.1.1 y que ha obtenido como respuesta para el nombre www.elmundo.es la IP 151.101.133.50. Además, nos indica que el nombre real es unidadeditorial.map.fastly.net y que www.elmundo.es se trata de un alias. La respuesta es no autoritativa.

nslookup www.edu.gva.es 1.1.1.1

```
Servidor:  one.one.one.one
Address:  1.1.1.1
Respuesta no autoritativa:
Nombre:  www.edu.gva.es
Addresses:  193.145.200.137
            195.77.20.137
```

Nos indica que ha utilizado el servidor 1.1.1.1 que ha identificado con el nombre one.one.one.one. Ha obtenido como respuesta las IPs 193.145.200.137 i 195.77.20.137 de forma no autoritativa.

nslookup –debug www.edu.gva.es 1.1.1.1

```
Respuesta no autoritativa:
------------
Got answer:
HEADER:
opcode = QUERY, id = 1, rcode = NOERROR
header flags:  response, want recursion, recursion avail.
questions = 1,  answers = 1,  authority records = 0,  additional = 0
QUESTIONS:
1.1.1.1.in-addr.arpa, type = PTR, class = IN
ANSWERS:
->  1.1.1.1.in-addr.arpa
name = one.one.one.one
ttl = 1491 (24 mins 51 secs)
------------
Servidor:  one.one.one.one
Address:  1.1.1.1
------------
Got answer:
HEADER:
opcode = QUERY, id = 2, rcode = NOERROR
header flags:  response, want recursion, recursion avail.
questions = 1,  answers = 2,  authority records = 0,  additional = 0
QUESTIONS:n
www.edu.gva.es, type = A, class = IN
ANSWERS:
->  www.edu.gva.es
internet address = 195.77.20.137
ttl = 30 (30 secs)
->  www.edu.gva.es
internet address = 193.145.200.137
ttl = 30 (30 secs)
------------
------------
Got answer:
HEADER:
opcode = QUERY, id = 3, rcode = NOERROR
header flags:  response, want recursion, recursion avail.
questions = 1,  answers = 0,  authority records = 1,  additional = 0
QUESTIONS:
www.edu.gva.es, type = AAAA, class = IN
AUTHORITY RECORDS:
->  www.edu.gva.es
ttl = 86400 (1 day)
primary name server = www.edu.gva.es
responsible mail addr = administrator.www.edu.gva.es
serial  = 998545544
refresh = 28800 (8 hours)
retry   = 7200 (2 hours)
expire  = 604800 (7 days)
default TTL = 86400 (1 day)
------------
Nombre:  www.edu.gva.es
Addresses:  195.77.20.137
            193.145.200.137
```

La primera consulta trata de resolver de manera inversa el nombre del servidor 1.1.1.1 y obtiene como respuesta one.one.one.one. La segunda pregunta es para obtener las IPv4 para el nombre www.edu.gva.es y recibe dos IPs. La tercera pregunta es para obtener las IPv6 del mismo nombre y como respuesta obtiene el registro SOA pero no las IPs por que no están definidas.

DIG

Se puede encontrar información del comando en dig man. El esquema general del comando es:

```
dig [@name-server] [options] [domain-name] [type class] [+queryopt]

@name-server    servidor dns al que se hace la consulta.
                Si no se indica utilizará el configurado en el sistema.
options
 -4                 IPv4
 -6                 IPv6
 -b ip[#port]       ip y puerto origen de la consulta
 -c class           Por defecto IN, también puede ser HS o CH
 -f file            fichero con consultas. Una por línea
 -h                 help
 -i                 consulta inversa
 -k keyfile         Consulta firmada con TSIG.
 -p port            consultar en el puerto y no en el 53.
 -q name            consultar el nombre name.
 -t type            consultar tipo de registro (NS,A,SOA,...)
 -u                 mostrar el tiempo en microsegundos
 -v                 mostrar versión de dig
 -x addr            consulta inversa addr (B1.B2.B3.B4)
 -y [hmac]keyname:secret    Consulta firmada amb TSIG
 -d                 Debug mode
domain-name         nombre de dominio a consultar
type class          Por defecto class IN.
+queryopt           Se pueden consultar en man dig con dig -h
```

Algunos ejemplos de uso.

dig www.edu.gva.es 1.1.1.1

```
; <<>> DiG 9.9.5-W1 <<>> www.ua.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63707
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.ua.es.                     IN      A
;; ANSWER SECTION:
www.ua.es.              78      IN      CNAME   vuala.ua.es.
vuala.ua.es.            2375    IN      A       193.145.235.30
;; Query time: 15 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Feb 05 19:29:08 Hora estßndar romance 2024
;; MSG SIZE  rcvd: 74
```

El servidor configurado por defecto 192.168.1.1 nos da como a respuesta para el nombre www.ua.es dos registros, el primer registro nos dice que www.ua.es es un alias de vuala.ua.es, el segundo registro nos dice que vuala.ua.es tiene la IP 193.145.235.30. La respuesta es no autoritativa (AUTHORITY 0).

dig ua.es ANY

```
; <<>> DiG 9.9.5-W1 <<>> ua.es ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60632
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 7
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;ua.es.                         IN      ANY
;; ANSWER SECTION:
ua.es.                  7193    IN      SOA     aitana.cpd.ua.es. root.aitana.cpd.ua.es. 2024020502 14400 7200 2592000 600
ua.es.                  289     IN      NS      aitana.cpd.ua.es.
ua.es.                  289     IN      NS      sun.rediris.es.
ua.es.                  289     IN      NS      chico.rediris.es.
ua.es.                  289     IN      NS      tabarca.cpd.ua.es.
;; ADDITIONAL SECTION:
sun.rediris.es.         1250    IN      AAAA    2620:171:808::1
chico.rediris.es.       5634    IN      AAAA    2620:10a:80eb::2
sun.rediris.es.         14763   IN      A       199.184.182.1
chico.rediris.es.       2105    IN      A       162.219.54.2
aitana.cpd.ua.es.       755     IN      A       193.145.233.5
tabarca.cpd.ua.es.      6642    IN      A       193.145.233.6
;; Query time: 15 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Feb 05 19:16:29 Hora estßndar romance 2024
;; MSG SIZE  rcvd: 295
```

Se han consultado todos los registros del dominio ua.es

dig www.ua.es +trace +nodnssec

```
; <<>> DiG 9.9.5-W1 <<>> www.ua.es +trace +nodnssec
;;global options: +cmd
.                       16988   IN      NS      a.root-servers.net.
.                       16988   IN      NS      k.root-servers.net.
.                       16988   IN      NS      g.root-servers.net.
.                       16988   IN      NS      b.root-servers.net.
.                       16988   IN      NS      h.root-servers.net.
.                       16988   IN      NS      d.root-servers.net.
.                       16988   IN      NS      c.root-servers.net.
.                       16988   IN      NS      f.root-servers.net.
.                       16988   IN      NS      e.root-servers.net.
.                       16988   IN      NS      i.root-servers.net.
.                       16988   IN      NS      j.root-servers.net.
.                       16988   IN      NS      m.root-servers.net.
.                       16988   IN      NS      l.root-servers.net.
;;Received 823 bytes from 192.168.1.1#53(192.168.1.1) in 16 ms
es.                     172800  IN      NS      a.nic.es.
es.                     172800  IN      NS      c.nic.es.
es.                     172800  IN      NS      g.nic.es.
es.                     172800  IN      NS      h.nic.es.
;;Received 282 bytes from 2001:503:c27::2:30#53(j.root-servers.net) in 62 ms
ua.es.                  86400   IN      NS      tabarca.cpd.ua.es.
ua.es.                  86400   IN      NS      chico.rediris.es.
ua.es.                  86400   IN      NS      sun.rediris.es.
ua.es.                  86400   IN      NS      aitana.cpd.ua.es.
;;Received 258 bytes from 204.61.217.1#53(g.nic.es) in 46 ms
www.ua.es.              600     IN      CNAME   vuala.ua.es.
vuala.ua.es.            7200    IN      A       193.145.235.30
;;Received 74 bytes from 162.219.54.2#53(chico.rediris.es) in 47 ms
```

Se han consultado www.ua.es de manera iterativa sin dnssec activado. Como la consulta es iterativa el servidor 192.168.1.1, configurado por defecto en el sistema, nos proporciona su mejor respuesta que es la lista de servidores raíz. Un servidor raíz (j) nos proporciona la lista de servidores donde se encuentra el domino es. Después un servidor del domini es (g.nic.es) nos da la lista de servidores donde se encuentra el dominio ua.es. Por último, uno de estos servidores, (chico.rediris.es) nos da la respuesta www.ua.es que es un alias del nombre vuala.ua.es con IP 193.145.235.30

dig ua.es –t MX

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40791
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;ua.es.                         IN      MX
;; ANSWER SECTION:
ua.es.                  7200    IN      MX      10 aitana.cpd.ua.es.
;; ADDITIONAL SECTION:
aitana.cpd.ua.es.       7146    IN      A       193.145.233.5
;; Query time: 31 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Feb 05 19:36:28 Hora estßndar romance 2024
;; MSG SIZE  rcvd: 82
```

Se han consultado los registros MX del domino ua.es. Como se puede observar se ha obtenido que los correos usuario@ua.es en realidad son servidos por el servidor de correo aitana.cpd.ua.es cuya IP es la 193.145.233.5.

HOST

Se puede encontrar información del comando en host man. El esquema general del comando es:

```
host  [options] [-c class] [-m flag] [-N ndots] [-R number] [-t type] [-W wait] name [server]

options
 -4                 IPv4
 -6                 IPv6
 -a                 Equivalente a -v -t ANY
 -C                 Comprobar consistencia. Solicita SOA.
 -c clase           Clase IN,HS,CH. Por defecto IN
 -d                 Debug
 -i                 Obsoleto,  sin uso.
 -l                 Listar la zona (NS,PTR,A,AAAA)
 -m flag            Flag record, usage, trace. Se usa junto con -d
 -r                 Consulta no recursiva
 -T                 Usar TCP en lugar de UDP.
 -t type            Tipo de registro
 -v                 Verbose. Equivalente a -d
 -W wait            Tiempo de espera para las consultas. Por defecto 5 sg.

name                nombre de dominio a consultar
server              servidor a consultar. Por defecto el servidor configurado en el sistema.
```

Algunos ejemplos de uso.

host www.ua.es

```
www.ua.es has address 147.156.1.1
```

host -d ua.es

```
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:
Trying "ua.es"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12345
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; QUESTION SECTION:
;;ua.es.                          IN      A
;; ANSWER SECTION:
ua.es.                 3600    IN      A       147.156.1.1
;; Query time: 45 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sat Dec 22 10:00:00 2025
;; MSG SIZE  rcvd: 58
```