eltallerdelbit.com

dig | Linux (Resolución DNS)

15-18 minutos

Dig es un comando de Linux que nos permite realizar consultas DNS.

Los comandos *nslookup* y *host* son de la misma familia (aunque nslookup está en desuso).

Las siglas de dig significan *Domain Information Groper* (algo así como "*tanteador*" de información de Dominio)

Definición de **dig** desde la página de *man dig* (manual del comando dig en Linux):

dig (domain information groper) is a flexible tool for interrogating DNS name servers.

DIG es una herramienta flexible que muestra los resultados de forma clara. Es parte del paquete **Bind** (Berkeley Internet Name Domain). Otras herramientas de búsqueda DNS no suelen tener tantas funcionalidades como dig.

1. dig sin argumentos

dig a secas, realiza una consulta de los servidores NS raíz

```
root@debian:/etc# dig

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR,
id: 5298
;; flags: qr rd ra; QUERY: 1, ANSWER: 13,
AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                  IN    NS
```

```
;; ANSWER SECTION:
.            254899    IN    NS    k.root-
servers.net.
.            254899    IN    NS    a.root-
servers.net.
.            254899    IN    NS    j.root-
servers.net.
.            254899    IN    NS    b.root-
servers.net.
.            254899    IN    NS    e.root-
servers.net.
.            254899    IN    NS    h.root-
servers.net.
.            254899    IN    NS    c.root-
servers.net.
.            254899    IN    NS    g.root-
servers.net.
.            254899    IN    NS    m.root-
servers.net.
.            254899    IN    NS    d.root-
servers.net.
.            254899    IN    NS    i.root-
servers.net.
.            254899    IN    NS    f.root-
servers.net.
.            254899    IN    NS    l.root-
servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.    79533    IN    A
198.41.0.4
g.root-servers.net.    94186    IN    A
```

```
192.112.36.4

;; Query time: 3 msec
;; SERVER: 192.168.130.202#53(192.168.130.202)
;; WHEN: Tue Jun 06 12:45:15 CEST 2017
;; MSG SIZE  rcvd: 271
```

A continuación podemos ver que la consulta ***dig*** muestra los servidores raíz.

Podemos comprobar los servidores raíz desde este enlace y desde root-servers.org.

2. El uso más normal de *dig*: *dig dominio* como argumento

```
ej: dig google.com
```

Con este tipo de consulta, dig mostrará el registro A

```
root@debian:/etc# dig google.com

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR,
id: 21115
;; flags: qr rd ra; QUERY: 1, ANSWER: 1,
AUTHORITY: 13, ADDITIONAL: 16

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.            IN    A

;; ANSWER SECTION:
google.com.        103    IN    A
216.58.201.142

;; AUTHORITY SECTION:
com.            171958    IN    NS    f.gtld-
servers.net.
com.            171958    IN    NS    j.gtld-
servers.net.
com.            171958    IN    NS    c.gtld-
servers.net.
com.            171958    IN    NS    a.gtld-
servers.net.
com.            171958    IN    NS    h.gtld-
servers.net.
com.            171958    IN    NS    i.gtld-
servers.net.
```

```
com.            171958    IN    NS    e.gtld-
servers.net.
com.            171958    IN    NS    k.gtld-
servers.net.
com.            171958    IN    NS    b.gtld-
servers.net.
com.            171958    IN    NS    l.gtld-
servers.net.
com.            171958    IN    NS    d.gtld-
servers.net.
com.            171958    IN    NS    m.gtld-
servers.net.
com.            171958    IN    NS    g.gtld-
servers.net.

;; ADDITIONAL SECTION:
a.gtld-servers.net.    171958    IN    A
192.5.6.30
a.gtld-servers.net.    171958    IN    AAAA
2001:503:a83e::2:30
b.gtld-servers.net.    171958    IN    A
192.33.14.30
b.gtld-servers.net.    171958    IN    AAAA
2001:503:231d::2:30
c.gtld-servers.net.    171958    IN    A
192.26.92.30
d.gtld-servers.net.    171958    IN    A
192.31.80.30
e.gtld-servers.net.    171958    IN    A
192.12.94.30
f.gtld-servers.net.    171958    IN    A
192.35.51.30
g.gtld-servers.net.    171958    IN    A
```

```
192.42.93.30
h.gtld-servers.net.    171958    IN    A
192.54.112.30
i.gtld-servers.net.    171958    IN    A
192.43.172.30
j.gtld-servers.net.    171958    IN    A
192.48.79.30
k.gtld-servers.net.    171958    IN    A
192.52.178.30
l.gtld-servers.net.    171958    IN    A
192.41.162.30
m.gtld-servers.net.    171958    IN    A
192.55.83.30

;; Query time: 7 msec
;; SERVER: 192.168.130.202#53(192.168.130.202)
;; WHEN: Tue Jun 06 12:55:16 CEST 2017
;; MSG SIZE  rcvd: 543
```

Consulta: *dig dominio*

Será la sección *ANSWER SECTION* la que mostrará la info que precisamos.

De esta forma dig mostrará:

- si la resolución ha sido correcta, mostrará status: *NOERROR*
- Mostrará la sección que ha respondido a la interrogación sobre el DNS
- Muestra el tiempo de respuesta de la consulta: *Query time: 8 msec*
- Y el servidor que responde a esa consulta *DNS: SERVER: 192.168.130.202#53* (se trata de un servidor DNS local, configurado como servidor DNS caché con Bind, que ejecuta reenvíos de consultas al servidor DNS primario de la red, el cual le devuelve el resultado de esas consultas y le permite guardarlos

para mostrarlos y guardarlos en caché).

2.1 dig a un dominio, usando como argumento un NS concreto (nameserver)

Es interesante poder utilizar el **comando dig** con otros parámetros y argumentos, como el argumento *NS*, que nos permite realizar una consulta dig de un dominio, pero utilizando un *NS* (*Name Server*) concreto, cuya IP pondremos en la consulta:

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

De esta forma dig consulta los DNS de google.com, al servidor 8.8.8.8

Y vemos cómo el NS que ha respondido a la petición es el server 8.8.8.8

```
root@debian:/etc# dig @8.8.8.8 google.com

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> @8.8.8.8
google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR,
id: 3070
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 3,
AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
google.com.        299    IN    A
216.58.201.142
google.com.        299    IN    A
216.58.201.142
google.com.        299    IN    A
216.58.201.142

;; Query time: 41 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Jun 06 13:06:14 CEST 2017
;; MSG SIZE  rcvd: 87
```

2.2 Con dig también podemos especificar el tipo de registro que deseamos consultar (*ANY*, *A*, *MX*, *NS* …)

Vamos a ver un ejemplo buscando los registros MX (correo).

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

```
root@debian:/etc# dig MX @8.8.8.8 google.es

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> MX
@8.8.8.8 google.es
; (1 server found)
;; global options: +cmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR,
id: 53401
;; flags: qr rd ra; QUERY: 1, ANSWER: 5,
AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
google.es.         599    IN    MX    30
alt2.aspmx.l.google.com.
google.es.         599    IN    MX    10
aspmx.l.google.com.
google.es.         599    IN    MX    50
alt4.aspmx.l.google.com.
google.es.         599    IN    MX    20
alt1.aspmx.l.google.com.
google.es.         599    IN    MX    40
alt3.aspmx.l.google.com.

;; Query time: 35 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Jun 06 13:45:29 CEST 2017
;; MSG SIZE  rcvd: 156
```

2.3 Consultando TODOS los tipos de registros (*ANY*)

Con la opción *ANY* consultaremos TODOS los registros de un dominio.

```
dig ANY google.es
```

```
root@debian:/etc# dig ANY google.es

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> ANY
google.es
;; global options: +cmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR,
id: 4952
;; flags: qr rd ra; QUERY: 1, ANSWER: 13,
AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.es.            IN    ANY

;; ANSWER SECTION:
google.es.        293    IN    AAAA
2a00:1450:4003:807::2003
google.es.        293    IN    TXT    “v=spf1
-all”
google.es.        593    IN    MX    20
alt1.aspmx.l.google.com.
google.es.        593    IN    MX    10
aspmx.l.google.com.
google.es.        593    IN    MX    50
alt4.aspmx.l.google.com.
google.es.        593    IN    MX    40
alt3.aspmx.l.google.com.
google.es.        593    IN    MX    30
alt2.aspmx.l.google.com.
google.es.        53    IN    SOA
ns4.google.com. dns-admin.google.com. 158122735
900 900 1800 60
google.es.        233    IN    A
216.58.210.131
google.es.        72196    IN    NS
ns4.google.com.
google.es.        72196    IN    NS
```

```
ns1.google.com.
google.es.        72196    IN    NS
ns3.google.com.
google.es.        72196    IN    NS
ns2.google.com.

;; AUTHORITY SECTION:
google.es.        72196    IN    NS
ns2.google.com.
google.es.        72196    IN    NS
ns3.google.com.
google.es.        72196    IN    NS
ns4.google.com.
google.es.        72196    IN    NS
ns1.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.        69377    IN    A
216.239.32.10
ns2.google.com.        84802    IN    A
216.239.34.10
ns3.google.com.        170862    IN    A
216.239.36.10
ns4.google.com.        170862    IN    A
216.239.38.10

;; Query time: 8 msec
;; SERVER: 192.168.130.202#53(192.168.130.202)
;; WHEN: Tue Jun 06 14:12:21 CEST 2017
;; MSG SIZE  rcvd: 462
```

4. RESOLUCIÓN INVERSA: Resuelve de IP a nombre

Con el parámetro -x podremos realizar la **resolución inversa de un dominio**. Esta resolución inversa nos mostrará por tanto la IP del dominio. Si no añadimos más argumentos, la resolución inversa será del registro A.

ejemplo:

```
dig -x 8.8.8.8
```

```
root@debian:/home/# dig -x 8.8.8.8

; <<>> DiG 9.9.5-9+deb8u11-Debian <<>> -x 8.8.8.8
;; global options: +cmd
```

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR,
id: 23544
;; flags: qr rd ra; QUERY: 1, ANSWER: 1,
AUTHORITY: 13, ADDITIONAL: 14

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;8.8.8.8.in-addr.arpa. IN PTR

;; ANSWER SECTION:
8.8.8.8.in-addr.arpa. 75915 IN PTR google-public-
dns-a.google.com.

;; AUTHORITY SECTION:
. 246702 IN NS i.root-servers.net.
. 246702 IN NS l.root-servers.net.
. 246702 IN NS e.root-servers.net.
. 246702 IN NS f.root-servers.net.
. 246702 IN NS k.root-servers.net.
. 246702 IN NS j.root-servers.net.
. 246702 IN NS h.root-servers.net.
. 246702 IN NS c.root-servers.net.
. 246702 IN NS g.root-servers.net.
. 246702 IN NS a.root-servers.net.
. 246702 IN NS d.root-servers.net.
. 246702 IN NS m.root-servers.net.
. 246702 IN NS b.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net. 83834 IN A 198.41.0.4
b.root-servers.net. 83907 IN A 192.228.79.201
```

```
c.root-servers.net. 83948 IN A 192.33.4.12
d.root-servers.net. 83989 IN A 199.7.91.13
e.root-servers.net. 84030 IN A 192.203.230.10
f.root-servers.net. 84135 IN A 192.5.5.241
g.root-servers.net. 84176 IN A 192.112.36.4
h.root-servers.net. 84217 IN A 198.97.190.53
i.root-servers.net. 84258 IN A 192.36.148.17
j.root-servers.net. 84427 IN A 192.58.128.30
k.root-servers.net. 84468 IN A 193.0.14.129
l.root-servers.net. 84509 IN A 199.7.83.42
m.root-servers.net. 83793 IN A 202.12.27.33

;; Query time: 2 msec
;; SERVER: 192.168.130.202#53(192.168.130.202)
;; WHEN: Thu Jul 13 13:23:23 CEST 2017
;; MSG SIZE rcvd: 512
```

- Vamos a ver también el ejemplo con el dominio *Linkedin.com*, primero resolución directa y luego realizaremos la resolución inversa:

  ```
  dig linkedin.com
  ```

  Ahora realizamos la resolución inversa de la IP que nos ha aparecido:

5. RESOLUCIÓN DE ERRORES DNS: DEBUG DNS (*dig +trace*)

Podemos realizar un rastreo en la ruta de búsqueda DNS con la opción *+ trace*.

Como se muestra a continuación al consultar *google.es* podemos ver lo que realmente sucede:
– Primero se muestran los servidores de nombres raíz ‘.’

– Después se rastrean los **servidores de nombres para el dominio .es** y, finalmente, se devuelven los **servidores de nombres** de *google.es*, seguidos de los **registros DNS** de la misma.

```
dig +trace google.es
```

```
root@debian:/etc# dig +trace google.es

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> +trace
```

```
google.es
;; global options: +cmd
.            249366    IN    NS    j.root-
servers.net.
.            249366    IN    NS    i.root-
servers.net.
.            249366    IN    NS    d.root-
servers.net.
.            249366    IN    NS    f.root-
servers.net.
.            249366    IN    NS    l.root-
servers.net.
.            249366    IN    NS    a.root-
servers.net.
.            249366    IN    NS    e.root-
servers.net.
.            249366    IN    NS    b.root-
servers.net.
.            249366    IN    NS    g.root-
servers.net.
.            249366    IN    NS    k.root-
servers.net.
.            249366    IN    NS    c.root-
servers.net.
.            249366    IN    NS    m.root-
servers.net.
.            249366    IN    NS    h.root-
servers.net.
;; Received 271 bytes from
192.168.130.202#53(192.168.130.202) in 70 ms

es.            172800    IN    NS    sns-
pb.isc.org.
```

```
es.             172800    IN    NS    ns3.nic.fr.
es.             172800    IN    NS    f.nic.es.
es.             172800    IN    NS    ns-
ext.nic.cl.
es.             172800    IN    NS    g.nic.es.
es.             172800    IN    NS    a.nic.es.
es.             172800    IN    NS
ns1.cesca.es.
es.             86400    IN    DS    44290 8 1
7711F564D55B41C8CE7DFAF4DD323C5B271F86CD
es.             86400    IN    DS    44290 8 2
562EF35E7065588A7178A4BD0155C8527F029C82AA455DD359C84908
B2A7FE17
es.             86400    IN    RRSIG    DS 8 1
86400 20170619050000 20170606040000 14796 .
Z2dBpJNwru3b15TSXSDBDDvK9oSUW11YEWxBHpY6CMVlWNs66gICRhMv
uFkMqvje0wL+7t7v0lJPhGaLx3L1hybn/3tPhkPGCUClzrnTpOiXGULi
ydvUcB8xCt1FxvxMUJ4NiIxvpJs51xYMIxTLoihJ8s2wXhm+tL8joQ3l
WE42jfBIXfVw6PKCfoHlxgiQ/ZTbUKBSUzTdSMKzhlL1zGFclVXNdNKv
jZgNMRwN7G5cn/4Dv1IAnQMXJ12S/Cr4sIowe5yE
/u7XNB4hHIiDSGeQ
nxAjRpZOFZ0tzCGWnwc8mGMsQoKp2i3My1s5S7poX+Ut/GvOGgVjgOHi
WILoEg==
;; Received 844 bytes from 192.5.5.241#53(f.root-
servers.net) in 71 ms

google.es.        86400    IN    NS
ns2.google.com.
google.es.        86400    IN    NS
ns1.google.com.
vhgig769k8fqo5v5ig9q7a6un45t1hhj.es. 86400 IN
NSEC3 1 1 5 7F6C8C66C2BC205D
VHOEO0370MQNG4CA8NT2VHR8REPI91SU NS SOA RRSIG
```

```
DNSKEY NSEC3PARAM
vhgig769k8fqo5v5ig9q7a6un45t1hhj.es. 86400 IN
RRSIG NSEC3 8 2 86400 20170611025013
20170528075535 61810 es.
kSDEA9hbIoynY757uNfRzHVfdoaFeiGRu5u1Ph79Y1RaqOmnfum5SBc1
HRE+nztM7B4A7jfCa5kPNtjQeLwYR0N8L6hivDveHrqg6d/SQLLGZTHC
nmMgt1PbM0siEStFcntKK9n5JaCSI0tabiwXDKWK1S1WA50WGQvFvPxE
4GQ=
bat3rrbtibfqoh1t1ottbvdk2q30b3am.es. 86400 IN
NSEC3 1 1 5 7F6C8C66C2BC205D
BBAI9G16OK3893I7B3QMCL4TRS6A9ID4 NS DS RRSIG
bat3rrbtibfqoh1t1ottbvdk2q30b3am.es. 86400 IN
RRSIG NSEC3 8 2 86400 20170611152235
20170528195912 61810 es.
DcnxJPHRI7Ztgwbnorn58BWbGhxLd5vpAgut4onDZpZIP/YbmwvJM7/F
HydAkFyGL1WVIlebVVyEMRbdsLxOL0+Ly0JWVnsBk1YLQwckyd3Gg0b\
dQh4K2pq2RpBgfKmkGFCQPAcsJuN4nSWLbDFJb+iAHlIRKCkMUNygFau
l2o=
;; Received 583 bytes from 192.5.4.1#53(sns-
pb.isc.org) in 53 ms

google.es.        300    IN    A
216.58.210.163
;; Received 43 bytes from
216.239.32.10#53(ns1.google.com) in 33 ms
```

Todas estas opciones y argumentos del comando dig nos serán muy útiles para ejecutar diferentes tipos de consultas DNS.

- Otros ejemplos del uso del comando dig
- Cómo usar el comando dig