

COMANDOS NSLOOKUP, HOST Y DIG

NSLOOKUP (Name System Lookup o Name Server Lookup)

- a) ¿Cuál es el Servidor predeterminado en qué se realizan las consultas de nombres?
- b) Establecer como Servidor para realizar las consultas Google (8.8.8.8)
- c) Realizar las consultas necesarias para obtener la información de los dominios oracle.com, cisco.com, madrid.org. y educa.madrid.org.
- d) Usar el comando adecuado para que nslookup nos devuelva toda la información relativa al nombre www.madrid.org. consultando al servidor DNS olimpia.madrid.org.
- e) El comando set type nos permite consultar los diferentes tipos de registro de una base de datos de DNS. Consultar en la documentación del comando los diferentes valores que puede tomar. Realizar la consulta directamente al servidor DNS que corresponde al dominio y de esa forma extraer más información. Utilizar los comandos set type y server
- f) Obtener el nombre canónico del dominio www.madrid.org

DIG (Domain Information Groper)

- a) Determinar la dirección IP de la máquina www.it.uc3m.es
- b) Obtener el nombre y dirección IP de servidores de nombres autoritarios (primarios y secundarios) para las zonas lab.it.uc3m.es, it.uc3m.es y uc3m.es
- c) Obtener la IP asociada al dominio www.it.uc3m.es preguntándose al dns 1.1.1.1
- d) Obtener la IP asociada al dominio www.it.uc3m.es preguntándose al dns local de la máquina en la que estás haciendo la práctica.
- e) Obtener la IP asociada al dominio www.it.uc3m.es preguntándose al dns directamente a cualquiera de los servidores primarios del dominio uc3m.es
- f) Determinar el nombre de dominio asociado a la IP 130.206.13.20

HOST

- a) La información referente al registro de recurso CNAME para www.google.es.
- b) La información referente al registro de recurso CNAME para www.elpais.com.
- c) El servidor de nombres autorizado de la zona it.uc3m.es
- d) Las máquinas encargadas de la entrega del correo en el dominio it.uc3m.es
- e) El registro de recurso que relaciona una dirección IP con el dominio lab.it.uc3m.es

NSLOOKUP (Name System Lookup o Name Server Lookup)

Herramienta que nos permite obtener información, relacionada con el dominio o el host, en una red mediante la consulta a un servidor de nombres (DNS). Nos permite diagnosticar los posibles problemas de configuración que pudieran haber surgido en el DNS, detectando si está resolviendo correctamente los nombres y las IP.

El comando nslookup permite dos formas de uso:

a) **Modo normal o no interactivo**, al igual que en los otros comandos en la consola, se introduce el comando, a continuación, las opciones y se oprime Enter, la sintaxis es:

nslookup [-opcion] [host] [servidor]

Donde host es la dirección IP o nombre de dominio a consultar, servidor es la IP del servidor en el cual se hará la consulta.

Si queremos el listado completo de opciones únicamente tendremos que utilizar el parámetro `/?` o `/help`

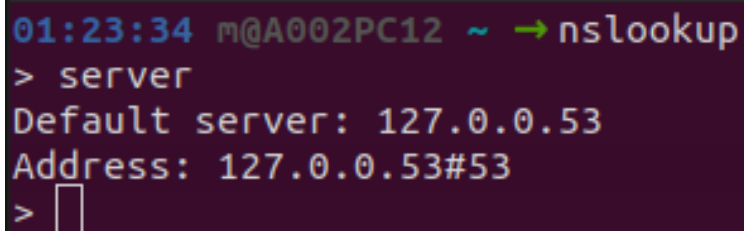
b) **Modo interactivo**, se hace la consulta en tiempo real y de manera consecutiva en líneas diferentes, mostrará un carácter `>` antes de cada comando introducido.

Para iniciar el modo interactivo solo escribe: nslookup y aparecerá el prompt del sistema

a) ¿Cuál es el Servidor predeterminado en qué se realizan las consultas de nombres?

Cuando ejecutas 'nslookup' sin parámetros, el comando utiliza el servidor DNS configurado por defecto en el sistema. Normalmente, este servidor es el que está configurado por el proveedor de Internet o el que se haya establecido en las configuraciones de red.

Para comprobar el servidor predeterminado deberemos escribir el comando 'nslookup' en nuestro terminal seguido de 'server' y nos saldrá esta información:

A terminal window with a dark purple background. The prompt shows the time 01:23:34, the user m, and the host A002PC12. The command nslookup is entered. The output shows the command 'server' and the result 'Default server: 127.0.0.53' followed by 'Address: 127.0.0.53#53'. A cursor is visible on the line following the output.

```
01:23:34 m@A002PC12 ~ → nslookup
> server
Default server: 127.0.0.53
Address: 127.0.0.53#53
> 
```

“Default Server” será el servidor DNS que se utilizara para consultas.

b) Establecer como Servidor para realizar las consultas Google (8.8.8.8)

Puedes cambiar el servidor DNS con el comando server y a continuación el servidor al que quieres cambiar dentro de la sesión de nslookup. En este caso, configuraremos el DNS de Google (8.8.8.8).

```
01:30:19 m@A002PC12 ~ → nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
>
```

c) Realizar las consultas necesarias para obtener la información de los dominios oracle.com, cisco.com, madrid.org. y educa.madrid.org.

Para consultar cada dominio simplemente escribiremos el nombre de cada dominio manualmente dentro del comando nslookup

```
12:38:39 m@A002PC12 ~ → nslookup
> oracle.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   oracle.com
Address: 138.1.33.162
> cisco.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   cisco.com
Address: 72.163.4.185
Name:   cisco.com
Address: 2001:420:1101:1::185
> madrid.org
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
*** Can't find madrid.org: No answer
> educa.madrid.org
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   educa.madrid.org
Address: 193.146.123.119
>
```

d) Usar el comando adecuado para que nslookup nos devuelva toda la información relativa al nombre www.madrid.org. consultando al servidor DNS olimpia.madrid.org.

Para realizar una consulta específica utilizando un servidor DNS personalizado, primero debes especificar el servidor al que quieres consultar. En este caso, haremos la consulta al servidor olimpia.madrid.org.

Y después realizar la consulta a www.madrid.org como en este ejemplo:

```
12:47:00 m@A002PC12 ~ → nslookup
> server olimpia.madrid.org.
Default server: olimpia.madrid.org.
Address: 213.0.53.140#53
> www.madrid.org
Server:      olimpia.madrid.org.
Address:     213.0.53.140#53

www.madrid.org canonical name = d3omk6xn5p4d3d.cloudfront.net.
** server can't find d3omk6xn5p4d3d.cloudfront.net: REFUSED
> █
```

Esto devolverá toda la información que el servidor olimpia.madrid.org tiene sobre el dominio www.madrid.org.

e) El comando `set type` nos permite consultar los diferentes tipos de registro de una base de datos de DNS. Consultar en la documentación del comando los diferentes valores que puede tomar. Realizar la consulta directamente al servidor DNS que corresponde al dominio y de esa forma extraer más información. Utilizar los comandos `set type` y `server`

El comando `set type` en `nslookup` permite especificar el tipo de registro DNS que deseas consultar. Aquí algunos de los valores más comunes que puedes utilizar con `set type`:

- **A**: Devuelve la dirección IPv4 del dominio.
- **AAAA**: Devuelve la dirección IPv6 del dominio.
- **MX**: Devuelve los registros de intercambio de correo (Mail Exchange).
- **NS**: Devuelve los servidores de nombres responsables del dominio.
- **SOA**: Devuelve el registro de autoridad de origen (Start of Authority).
- **CNAME**: Devuelve el nombre canónico (alias) del dominio.
- **PTR**: Utilizado para la resolución inversa de direcciones IP a nombres de dominio.
- **TXT**: Devuelve los registros TXT (información de texto asociada con el dominio).

Para realizar una consulta con `set type` y `server` ejecutaremos el comando `nslookup`, con el servidor que queremos utilizar como predeterminado para hacer consultas, y estableceremos el tipo de registro que se quiere consultar de esta manera:

```
12:53:40 m@A002PC12 ~ → nslookup
> set type=MX
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> madrid.org
Server:          8.8.8.8
Address:         8.8.8.8#53

Non-authoritative answer:
madrid.org      mail exchanger = 10 mx1.hc1855-42.eu.iphmx.com.
madrid.org      mail exchanger = 20 mail.madrid.org.
madrid.org      mail exchanger = 10 mx2.hc1855-42.eu.iphmx.com.
```

Esto te devolverá los registros MX asociados al dominio.

f) Obtener el nombre canónico del dominio `www.madrid.org`

Para obtener el nombre canónico (alias) de un dominio, se utiliza el tipo de consulta `CNAME` en `nslookup`.

Es decir, lo que hemos hecho anteriormente, pero estableciendo set type=CNAME

```
12:58:11 m@A002PC12 ~ → nslookup
> set type=CNAME
> www.madrid.org
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
www.madrid.org canonical name = d3omk6xn5p4d3d.cloudfront.net.

Authoritative answers can be found from:
> █
```

DIG (Domain Information Groper)

Comando de gran utilidad para realizar consultas a registros DNS. Se utiliza principalmente para el diagnóstico de Servidores DNS.

Las principales opciones de dig son las siguientes:

dig [@server] [-p port#] [name] [type] [queryopt...]

- **@server:** Especifica el servidor DNS al que enviar la consulta (opcional).
- **-p port:** Cambia el puerto para realizar la consulta (por defecto es el puerto 53).
- **name:** El nombre de dominio que queremos consultar.
- **type:** Tipo de registro DNS a consultar (A, MX, NS, etc.).
- **queryopt:** Otras opciones de consulta, como la recursividad o la iteración.

Consultar el significado de las opciones del comando dig prestando especial atención en la forma en que se pueden resolver las consultas (iterativa vs recursiva). A continuación, responder a las siguientes cuestiones:

- **Consulta recursiva:** El servidor DNS al que se envía la consulta busca la respuesta por sí mismo consultando otros servidores si es necesario. dig realiza consultas recursivas por defecto.

- **Consulta iterativa:** El servidor DNS responde con la mejor respuesta que tiene en su base de datos y, si no tiene la respuesta final, proporciona una lista de servidores a los que consultar.

a) Determinar la dirección IP de la máquina www.it.uc3m.es

Para obtener la dirección IP simplemente se introducirá el comando `dig` seguido del dominio y en la sección ANSWER del resultado podrás ver la IP asociada al dominio.

```

01:17:48 m@A002PC12 ~ → dig www.it.uc3m.es

; <<> DiG 9.16.48-Ubuntu <<> www.it.uc3m.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33817
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.it.uc3m.es.                IN      A

;; ANSWER SECTION:
www.it.uc3m.es.                3228    IN      CNAME   contrabajo.it.uc3m.es.
contrabajo.it.uc3m.es.        7199    IN      A       163.117.139.115

;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Oct 21 13:18:00 CEST 2024
;; MSG SIZE rcvd: 84

```

b) Obtener el nombre y dirección IP de servidores de nombres autoritarios (primarios y secundarios) para las zonas lab.it.uc3m.es, it.uc3m.es y uc3m.es

Para obtener los servidores NS de las zonas deberemos introducir:

-dig lab.it.uc3m.es NS

-di it.uc3m.es NS

-uc3m.es

En la sección AUTHORITY podrás ver los servidores NS

c) Obtener la IP asociada al dominio `www.it.uc3m.es` preguntándoselo al dns `1.1.1.1`

Para realizar una consulta a un servidor DNS específico:

```
01:23:13 m@A002PC12 ~ → dig @1.1.1.1 www.it.uc3m.es

; <<>> DiG 9.16.48-Ubuntu <<>> @1.1.1.1 www.it.uc3m.es
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28053
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.it.uc3m.es.                IN      A

;; ANSWER SECTION:
www.it.uc3m.es.                86500   IN      CNAME   contrabajo.it.uc3m.es.
contrabajo.it.uc3m.es.        86500   IN      A       163.117.139.115

;; Query time: 40 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Mon Oct 21 13:23:34 CEST 2024
;; MSG SIZE rcvd: 84
```

Esto forzará la consulta al servidor DNS establecido.

d) Obtener la IP asociada al dominio `www.it.uc3m.es` preguntándoselo al dns local de la máquina en la que estás haciendo la práctica.

Si no se especifica un servidor DNS, el comando `dig` usará el servidor DNS local que este configurado en tu máquina. La IP del dominio aparecerá en la sección `ANSWER`

```
01:23:34 m@A002PC12 ~ → dig www.it.uc3m.es

; <<>> DiG 9.16.48-Ubuntu <<>> www.it.uc3m.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2838
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.it.uc3m.es.                IN      A

;; ANSWER SECTION:
www.it.uc3m.es.                2582    IN      CNAME   contrabajo.it.uc3m.es.
contrabajo.it.uc3m.es.        6554    IN      A       163.117.139.115

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Oct 21 13:28:46 CEST 2024
;; MSG SIZE rcvd: 84
```

e) Obtener la IP asociada al dominio www.it.uc3m.es preguntándoselo al dns directamente a cualquiera de los servidores primarios del dominio uc3m.es
Primero deberas encontrar los NS primarios del dominio uc3m.es

```
01:30:12 m@A002PC12 ~ → dig uc3m.es NS

; <<>> DiG 9.16.48-Ubuntu <<>> uc3m.es NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17955
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 65494
;; QUESTION SECTION:
;uc3m.es.                IN      NS

;; ANSWER SECTION:
uc3m.es.                21600   IN      NS      sun.rediris.es.
uc3m.es.                21600   IN      NS      chico.rediris.es.
uc3m.es.                21600   IN      NS      vortex.uc3m.es.
uc3m.es.                21600   IN      NS      saruman.uc3m.es.

;; Query time: 12 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Oct 21 13:30:18 CEST 2024
;; MSG SIZE rcvd: 125
```

Una vez consultados los NS de uc3m.es, realizaremos la consulta a www.it.uc3m.es preguntando directamente a uno de los servidores (Ej: sun.rediris.es.)

```

01:30:18 m@A002PC12 ~ → dig @sun.rediris.es. www.it.uc3m.es

; <<>> DiG 9.16.48-Ubuntu <<>> @sun.rediris.es. www.it.uc3m.es
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11288
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.it.uc3m.es.                IN      A

;; AUTHORITY SECTION:
it.uc3m.es.      86400    IN      NS      varpa.it.uc3m.es.
it.uc3m.es.      86400    IN      NS      tantam.it.uc3m.es.
it.uc3m.es.      86400    IN      NS      vortex.uc3m.es.

;; ADDITIONAL SECTION:
varpa.it.uc3m.es. 86400    IN      A       163.117.139.253
tantam.it.uc3m.es. 86400    IN      A       163.117.139.31
vortex.uc3m.es.   86400    IN      A       163.117.131.31
vortex.uc3m.es.   86400    IN      AAAA    2001:720:410:b131::31

;; Query time: 36 msec
;; SERVER: 199.184.182.1#53(199.184.182.1)
;; WHEN: Mon Oct 21 13:31:57 CEST 2024
;; MSG SIZE rcvd: 181

```

el servidor DNS al que consultaste no permite consultas recursivas. Esto es indicado por la advertencia:

WARNING: recursion requested but not available

El servidor sun.rediris.es solo te proporcionó información de los servidores DNS autoritarios de la zona it.uc3m.es en la sección **AUTHORITY**. Estos servidores son:

- **varpa.it.uc3m.es** (IP: 163.117.139.253)
- **tamtam.it.uc3m.es** (IP: 163.117.139.31)
- **vortex.uc3m.es** (IP: 163.117.131.31)

Así que para consultar la IP de www.it.uc3m.es deberás hacer la consulta desde cualquiera de esos servidores.

f) Determinar el nombre de dominio asociado a la IP 130.206.13.20

Para realizar una consulta inversa y determinar el nombre de dominio asociado a una dirección IP, se utiliza el tipo de registro PTR. Para consultar la IP 130.206.13.20:

dig -x 130.206.13.20

```
01:40:36 m@A002PC12 ~ → dig -x 130.206.13.20

; <<>> DiG 9.16.48-Ubuntu <<>> -x 130.206.13.20
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4180
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
20.13.206.130.in-addr.arpa. 5227 IN      PTR      www.rediris.es.

;; Query time: 108 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Oct 21 13:42:55 CEST 2024
;; MSG SIZE rcvd: 83
```

En la sección **ANSWER** aparecerá el nombre de dominio asociado a esa dirección IP, si existe un registro PTR correspondiente. En este caso www.rediris.es.

HOST

Comando que permite realizar búsquedas en DNS. Se utiliza principalmente para convertir nombres en direcciones IP y viceversa.

SINTAXIS BASICA:

host [opciones] [nombre_dominio]

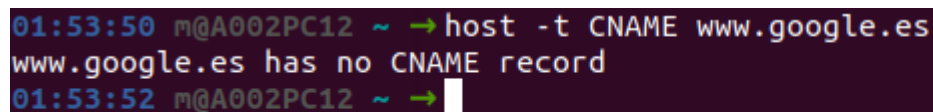
- **nombre_dominio:** El nombre del dominio que deseas consultar.
- **opciones:** Parámetros adicionales para obtener información específica, como CNAME, NS, MX, etc.
 - ALGUNAS OPCIONES UTILES
 - -t [tipo]: Especifica el tipo de registro DNS que deseas consultar (A, CNAME, MX, NS, etc.).
 - -a: Devuelve toda la información sobre el dominio, incluyendo varios tipos de registros.
 - -v: Activa el modo detallado (verbose), que muestra más información sobre la consulta.

Consultar las opciones del comando host y responder a las siguientes cuestiones:

a) La información referente al registro de recurso CNAME para www.google.es.

Para obtener el registro CNAME de www.google.es usaremos el comando:

host -t CNAME www.google.es.



```
01:53:50 m@A002PC12 ~ → host -t CNAME www.google.es
www.google.es has no CNAME record
01:53:52 m@A002PC12 ~ →
```

En este caso, www.google.es no tiene un CNAME.

b) La información referente al registro de recurso CNAME para www.elpais.com.

Host -t CNAME www.elpais.com.

c) El servidor de nombres autorizado de la zona it.uc3m.es

host -t NS it.uc3m.es

d) Las máquinas encargadas de la entrega del correo en el dominio it.uc3m.es

host -t MX it.uc3m.es

```

01:58:27 m@A002PC12 ~ → host -t CNAME www.elpais.com.
www.elpais.com is an alias for prisa-us-eu.map.fastly.net.
01:58:37 m@A002PC12 ~ → host -t NS it.uc3m.es
it.uc3m.es name server vortex.uc3m.es.
it.uc3m.es name server tamtam.it.uc3m.es.
it.uc3m.es name server varpa.it.uc3m.es.
01:58:59 m@A002PC12 ~ → host -t MX it.uc3m.es
it.uc3m.es mail is handled by 10 ASPMX.L.GOOGLE.COM.
it.uc3m.es mail is handled by 20 ALT2.ASPMX.L.GOOGLE.COM.
it.uc3m.es mail is handled by 30 ASPMX2.GOOGLEMAIL.COM.
it.uc3m.es mail is handled by 20 ALT1.ASPMX.L.GOOGLE.COM.
it.uc3m.es mail is handled by 30 ASPMX3.GOOGLEMAIL.COM.
01:59:08 m@A002PC12 ~ →

```

e) El registro de recurso que relaciona una dirección IP con el dominio lab.it.uc3m.es
 Para obtener el nombre de dominio asociado a la IP de lab.it.uc3m.es, necesitas saber la IP correspondiente y luego realizar una consulta inversa.

host lab.it.uc3m.es => Esto te dara la IP asociada

Una vez tengas la IP asociada

host <IP asociada>

```

02:01:26 m@A002PC12 ~ → host lab.it.uc3m.es
lab.it.uc3m.es has address 163.117.144.129
lab.it.uc3m.es has address 163.117.144.200
lab.it.uc3m.es mail is handled by 5 smtp.uc3m.es.
02:01:36 m@A002PC12 ~ → host 163.117.144.129
129.144.117.163.in-addr.arpa domain name pointer lm000.lab.it.uc3m.es.
02:02:09 m@A002PC12 ~ → host 163.117.144.200
200.144.117.163.in-addr.arpa domain name pointer it000.lab.it.uc3m.es.
02:02:15 m@A002PC12 ~ →

```