eltallerdelbit.com

Comando nslookup | Opciones

5-6 minutos

---

nslookup es "*name server lookup*" (búsqueda de servidores de nombre), y es una herramienta que puede realizar diversos tipos de consultas a servidores de nombres DNS.

Podemos realizar **consultas directas** (nslookup *nombredominio.com*) o consultas reversas (nslookup *IP*).

Respuesta Autoritativa (*Authoritative Answer*) y respuesta no Autoritativa (*Non-Authoritative Answer*)

En las consultas DNS veremos frecentemente estos dos términos.

- *Authoritative Answer* significa que la respuesta DNS se ha producido desde el servidor DNS que tiene todo el archivo de información disponible para esa zona.
- *Non Authoritative Answer* significa que la respuesta DNS se ha producido desde un servidor DNS que tiene en caché una copia de las consultas realizadas para esa zona, al servidor que tiene la Autoridad para responder (el que tiene el archivo de zona). Por esto veremos muy a menudo la

respuesta desde servidores que son *Non Authoritative*.

nslookup en Linux

1. nslookup sin argumentos

Muestra el servidor que realiza la consulta

```
Server: 192.168.130.202
```

que en este caso resulta ser un servidor DNS local (aquí podría aparecer el router de nuestra casa contestando a las consultas DNS).

Y después muestra un servidor DNS (No es el DNS principal, es un DNS no autoritario o *Non Authoritative*) del dominio consultado, que responde a nuestra consulta DNS:

```
Non-Authoritative Answer:

Name: google.es

Address: 216.58.201.131
```

2. nslookup realizando consultas sobre el tipo de registro del que deseamos info.

Con el argumento: *-type=*

- **2.1 -type=any –> muestra todos los registros NS disponibles del dominio.**

es decir:

```
nslookup -type=any google.es
```

Vemos que muestra respuesta de servidores *Non-Authoritative* y de servidores *Authoritative*:

- **2.2 -type=ns –> muestra todos los registros NS disponibles del dominio y una lista de los servidores *Authoritative* de nombre si es que están disponibles (normalmente estarán ocultos y no aparecerán, solo aparecerán los *Non-authoritative*).**

- **2.3 -type=mx –> muestra todos los registros MX (mail) del dominio.**

```
nslookup -type=mx unizar.es
```

Vemos que los registros MX de unizar son:

```
Non-authoritative answer:

mx01.puc.rediris.es

mx02.puc.rediris.es
```

- **2.4 -type=soa –> muestra todos los registros** SOA (Start of Authority) **del dominio.**

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

  Mostrará el servidor con autoridad para responder sobre ese dominio. También mostrará los parámetros del registro *SOA*: el TTL (tiempo de respuesta), *refresh*, *retry*, *expire*, *minimum* …

3. nslookup reverso (reverse nslookup)

Podemos realizar una consulta dns inversa utilizando la IP como un argumento para el comando nslookup; y nos mostrará los datos de resolución inversa de la zona

4. nslookup utilizando un servidor específico

En lugar de utilizar los servidores DNS por defecto para la consulta, podemos especificar qué servidor deseamos que resuelva la consulta.

5. nslookup en modo debug

El modo debug de nslookup muestra info sobre los paquetes durante la consulta dns.

6. nslookup en modo interactivo

El modo interactivo nos permite efectuar consultas como las mencionadas hasta ahora, pero de un modo diferente, introduciendo los comandos uno por uno.

Por ej:

```
nslookup
```

y se abrirá la terminal de nslookup para comenzar a introducir comandos:

```
>
```

entonces podemos introducir el nombre de dominio que queremos consultar:

```
google.es
```

y nos mostrará la respuesta.

Otro comando que podemos introducir en modo interactivo, es el de type= , que nos permite elegir qué tipo de registros deseamos que nos muestre la consulta.

lo haremos así:

```
>set type=ns

>google.es
```

Y obtendremos en este caso la consulta de los registros ns del dominio google.es :

7. nslookup en Windows

Básicamente el comando funciona de forma parecida, aunque con alguna pequeña diferencia en los comandos respecto a los utilizados en Linux.

- nslookup directo

- nslookup reverso

- nslookup modo interactivo

  Si ejecutamos simplemente el comando nslookup, lo primero que mostrará es el servidor DNS predeterminado y su IP, y se abrirá el modo interactivo de nslookup:

Después nos permite comenzar a teclear parámetros para ejecutar diversos tipos de consultas DNS, que veremos a continuación.

- Siguiendo con lo anterior, vamos a realizar una consulta con nslookup, y utilizando después algunos parámetros:

  nslookup
  server 8.8.8.8 (le decimos qué servidor queremos que conteste)

  set q=MX (queremos averiguar los registros MX)

  google.es (le decimos de qué NS queremos saber la info)

- Otra opción es la de hacer una consulta con nslookup sobre el tipo de registro DNS del que deseamos info.

  ```
  nslookup -type=ns unizar.es
  ```

Acabamos de hacer un interesante repaso al **comando nslookup**, sus opciones y funcionamiento, tanto en Linux como en Windows. Realmente el comando nslookup ha sido relegado a un segundo plano, sobre todo en Linux (donde ha sido desplazado por el comando *dig*), pero aún así viene bien conocer su funcionamiento. Para más info sobre nslookup, podemos consultar el artículo de Microsoft sobre nslookup