

Uso del Nslookup para la administración de servidores DNS

Introducción

DNS traduce nombres de hosts a direcciones IP, cumple así un rol crítico en la infraestructura de la Internet. En esta práctica, veremos el lado cliente de DNS.

Recuerde que el rol del cliente DNS es relativamente simple – un cliente envía una consulta de un nombre de un host (máquina) a su servidor DNS, y recibe una *respuesta* de retorno. Por ejemplo, cuando intentamos abrir una página web, introducimos el nombre del host como primera parte de la dirección web. El navegador tiene que averiguar cuál es la dirección IP de la máquina antes de acceder.

“Bajo la superficie” ocurren muchas cosas invisibles para los clientes DNS, tales como las comunicaciones que tienen lugar entre los servidores DNS de la jerarquía para resolver, ya sea recursivamente o iterativamente, la consulta del cliente DNS. Sin embargo, desde el punto de vista del cliente DNS, el protocolo es bastante simple – una consulta es formulada al servidor DNS local y se recibe una respuesta desde ese servidor.

Comando nslookup

Antes de comenzar es recomendable que se comprenda muy bien la teoría o que al menos se tenga presente para entender bien lo que hacemos.

https://es.wikipedia.org/wiki/Domain_Name_System

Haremos uso intensivo de la herramienta *nslookup*, la cual está actualmente disponible para la mayoría de las plataformas Linux/Unix y Microsoft.

Tenéis un manual de uso en la plataforma Windows en la dirección

<https://support.microsoft.com/kb/200525/es> Para ejecutar *nslookup* en Linux/Unix, solo escribimos el comando *nslookup* en la línea de comandos. Para ejecutarlo en Windows, abra consola y escriba *nslookup* en la línea de comandos

En su modo de operación más básico, la herramienta *nslookup* permite a los hosts que ejecutan la herramienta, interrogar cualquier servidor DNS especificado acerca de un registro DNS. El servidor DNS interrogado puede ser un servidor:

- DNS raíz, un servidor
- DNS de dominio de alto nivel (TLD)
- un servidor DNS con autoridad sobre el dominio preguntado (mantiene el dominio)
- un servidor DNS intermedio que nos dará una respuesta no autoritativa y que posiblemente mantiene el registro en Cache durante un tiempo llamado TTL porque en otro momento ya se le realizó esa pregunta.

Para lograr esta tarea, *nslookup* envía una consulta DNS al servidor DNS especificado, recibe una respuesta DNS desde el servidor DNS especificado, y muestra el resultado.

Considere el primer comando:

```
C:\Documents and Settings\Jose Antonio>nslookup www.mit.edu
Servidor: 250.Red-80-58-61.staticIP.rima-tde.net
Address: 80.58.61.250

DNS request timed out.
  timeout was 2 seconds.
Respuesta no autoritativa:
Nombre: www.mit.edu
Address: 18.9.22.169

C:\Documents and Settings\Jose Antonio>
```

mi servidor DNS

Respuesta que viene de DNS
Cache y no del servidor DNS
que mantiene el dominio

dirección de la máquina

En palabras, este comando está diciendo “*envíeme la dirección IP del host www.mit.edu(FQDN)*”. Como puede verse, la respuesta a este comando tiene dos partes de información:

- El nombre y dirección IP del servidor DNS que provee la respuesta
- La respuesta propiamente dicha, la cual es el nombre del host y la dirección IP de www.mit.edu.

Aunque la respuesta viene del servidor DNS de tu proveedor de Internet (en mi caso telefónica), es posible que este servidor DNS haya contactado con otros servidores DNS para obtener la respuesta si no la mantiene en cache por otra consulta que tuvo

Como podemos ver en la descripción del protocolo en la wikipedia Como podemos ver en la descripción del protocolo en la wikipedia http://es.wikipedia.org/wiki/Domain_Name_System en el apartado de *tipos de registros del DNS*, que son en realidad lo que vamos a guardar en la base de datos del servidor DNS, tenemos un tipo de registro que es NS (name Server) y que identifican los servidores DNS que mantienen el dominio y que serán servidores con Autoridad. De estos servidores tenemos:

- Servidor Primario (maestro): Es el servidor principal que mantiene el dominio y en el que se realizarán las modificaciones.
- Servidores Secundarios (esclavos): Mantiene una copia de la base de datos del DNS y que servirá para ayudar al anterior a balancear la carga.

Podemos averiguar que servidores DNS mantienen un dominio con

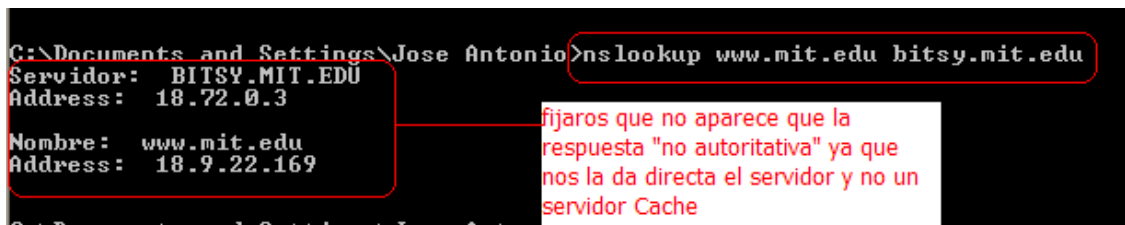
```
C:\Documents and Settings\Jose Antonio>nslookup -type=NS mit.edu
Servidor: 250.Red-80-58-61.staticIP.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
mit.edu nameserver = BITSY.mit.edu
mit.edu nameserver = W20NS.mit.edu
mit.edu nameserver = STRAWB.mit.edu

BITSY.mit.edu internet address = 18.72.0.3
```

Apartado 1:

El registro SOA nos indica información importante de la zona de dominio. Averigua mediante nslookup para el dominio mit.edu cual es el registro SOA teniendo en cuenta que la opción -type le indicamos que registro queremos ver. Veamos un tercer comando.



```
C:\Documents and Settings\Jose Antonio>nslookup www.mit.edu bitsy.mit.edu
Servidor:  BITSY.MIT.EDU
Address:  18.72.0.3

Nombre:   www.mit.edu
Address:  18.9.22.169
```

fijaros que no aparece que la respuesta "no autoritativa" ya que nos la da directa el servidor y no un servidor Cache

Fijaros que el servidor que mantiene mit.edu es entre otros bitsy.mit.edu. Por defecto, nslookup utiliza nuestro servidor DNS configurado (podemos averiguar cual es mediante ipconfig /all), pero podemos obligar a que nslookup utilice el servidor DNS que queramos. En concreto vamos a preguntar al servidor bitsy.mit.edu.

Apartado 2:

Google ofrece un servidor DNS con dirección 8.8.8.8. Pregunta a este servidor la dirección de www.iesperemaria.com.

Apartado 3:

Averigua cuales son los servidores DNS que mantienen www.iesperemaria.com y pregunta por la dirección directamente al DNS que mantiene la zona de dominios para que te de una respuesta Autoritativa

Como indica la teoría, todo nombre de dominio se lee de derecha a izquierda y empieza por un punto. El punto indica la raíz, así como en el árbol de directorios de los sistema Linux comienza por la raíz y se representa por "/" en los dominios se representa por "." aunque no se suele escribir. De esta manera, un nombre real o FQDN sería www.iesperemaria.com. (acabado en punto)

El dominio raíz es mantenido actualmente por 13 superservidores DNS y todo servidor DNS tiene configurado cuales son alguno o todos estos servidores para poder realizar una consulta y conseguir averiguar cual es el servidor DNS final que mantiene un cierto dominio.

Podemos averiguar cuales son estos servidores raíz con nslookup

```

C:\>nslookup -type=ns .
Servidor: 250.Red-80-58-61.staticIP.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
(root) nameserver = M.ROOT-SERVERS.NET
(root) nameserver = K.ROOT-SERVERS.NET
(root) nameserver = F.ROOT-SERVERS.NET
(root) nameserver = H.ROOT-SERVERS.NET
(root) nameserver = L.ROOT-SERVERS.NET
(root) nameserver = J.ROOT-SERVERS.NET
(root) nameserver = G.ROOT-SERVERS.NET
(root) nameserver = A.ROOT-SERVERS.NET
(root) nameserver = B.ROOT-SERVERS.NET
(root) nameserver = I.ROOT-SERVERS.NET
(root) nameserver = D.ROOT-SERVERS.NET
(root) nameserver = G.ROOT-SERVERS.NET
(root) nameserver = E.ROOT-SERVERS.NET

M.ROOT-SERVERS.NET internet address = 202.12.27.33
M.ROOT-SERVERS.NET AAAA IPv6 address = 2001:dc3::35
K.ROOT-SERVERS.NET internet address = 193.0.14.129
K.ROOT-SERVERS.NET AAAA IPv6 address = 2001:7fd::1
F.ROOT-SERVERS.NET internet address = 192.5.5.241
H.ROOT-SERVERS.NET internet address = 128.63.2.53
L.ROOT-SERVERS.NET internet address = 199.7.83.42
J.ROOT-SERVERS.NET internet address = 192.58.128.30
G.ROOT-SERVERS.NET internet address = 192.33.4.12
A.ROOT-SERVERS.NET internet address = 198.41.0.4
A.ROOT-SERVERS.NET AAAA IPv6 address = 2001:503:ba3e::2:30
B.ROOT-SERVERS.NET internet address = 192.228.79.201
I.ROOT-SERVERS.NET internet address = 192.36.148.17
D.ROOT-SERVERS.NET internet address = 128.8.10.90
G.ROOT-SERVERS.NET internet address = 192.112.36.4

```

servidores raíz que
mantienen el inicio del
árbol DNS

Estos servidores saben cuales son los servidores que mantienen los dominios de primer nivel como pueden ser "es.", "com.", "net."....

Por ejemplo, vamos averiguar quienes son los servidores que mantienen el dominio "es."

```

sns-pb.isc.org AAAA IPv6 address = 2001:500:2e::1
C:\>nslookup -type=ns es.
Servidor: 250.Red-80-58-61.staticIP.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
es nameserver = sun.rediris.es
es nameserver = ns3.nic.fr
es nameserver = ns1.cesca.es
es nameserver = sns-pb.isc.org
es nameserver = ns15.communitydns.net
es nameserver = ns-ext.nic.cl
es nameserver = ns1.nic.es
es nameserver = ns1.crn.nic.es
es nameserver = ns2.nic.es

sun.rediris.es internet address = 130.206.1.2
ns3.nic.fr internet address = 192.134.0.49
ns1.cesca.es internet address = 84.88.0.3
sns-pb.isc.org internet address = 192.5.4.1
ns-ext.nic.cl internet address = 200.1.123.14
ns1.nic.es internet address = 194.69.254.1
ns1.crn.nic.es internet address = 195.81.201.11

```

observar que hay que añadir el "."

servidores DNS
que mantienen
"es."

Fijaos en la siguiente consulta en la que preguntamos directamente a un servidor raíz y que nos da una respuesta autoritativa ya que conoce los servidores que mantiene "es."

```
C:\Documents and Settings\Jose Antonio>nslookup -type=ns es. g.root-servers.net
192.in-addr.arpa    nameserver = X.ARIN.NET
192.in-addr.arpa    nameserver = BASIL.ARIN.NET
192.in-addr.arpa    nameserver = Y.ARIN.NET
192.in-addr.arpa    nameserver = Z.ARIN.NET
192.in-addr.arpa    nameserver = HENNA.ARIN.NET
192.in-addr.arpa    nameserver = INDIGO.ARIN.NET
192.in-addr.arpa    nameserver = DILL.ARIN.NET
*** No se puede encontrar el nombre de servidor para la dirección 192.112.36.4:
No information
Servidor: UnKnown
Address: 192.112.36.4

es      nameserver = SUN.REDIRIS.es
es      nameserver = NS1.CESCA.es
es      nameserver = NS3.NIC.FR
es      nameserver = NS1.CRN.NIC.es
es      nameserver = NS-EXT.NIC.CL
es      nameserver = NS1.NIC.es
es      nameserver = SNS-PB.ISC.ORG
NS1.CRN.NIC.es      internet address = 195.81.201.11
NS1.NIC.es          internet address = 194.69.254.1
NS1.CESCA.es        internet address = 84.88.0.3
NS3.NIC.FR           internet address = 192.134.0.49
SUN.REDIRIS.es      internet address = 130.206.1.2
```

uno de los 13
servidores raiz

servidores que
mantienen el dominio
"es."

Apartado 4:

Averigua que servidores mantienen el dominio primario "net".

Apartado 5:

Pregunta que servidores mantienen "com." pero a un servidor que mantenga ese dominio, es decir, que la respuesta sea autoritativa.

Apartado 6:

Averigua cual es el servidor DNS primario de "es.". Recuerda que el registro SOA mantiene la información de la Zona

Los servidores DNS también son capaces de decirnos dada una dirección IP cual es el nombre de la máquina. Este tipo de registros se llaman PTR y se mantienen en las llamadas zonas de resolución inversa. Por ejemplo, podemos averiguar cual es FQDN o nombre de un host con nslookup mediante

```
C:\>nslookup 192.134.0.49
Servidor: 250.Red-80-58-61.staticIP.rima-tde.net
Address: 80.58.61.250

Nombre: ns3.nic.fr
Address: 192.134.0.49
```

Apartado 7:

Averigua el nombre o FQDN de la máquina con ip 130.57.4.24