

Práctica 9 DNS

Guillermo Marcos García

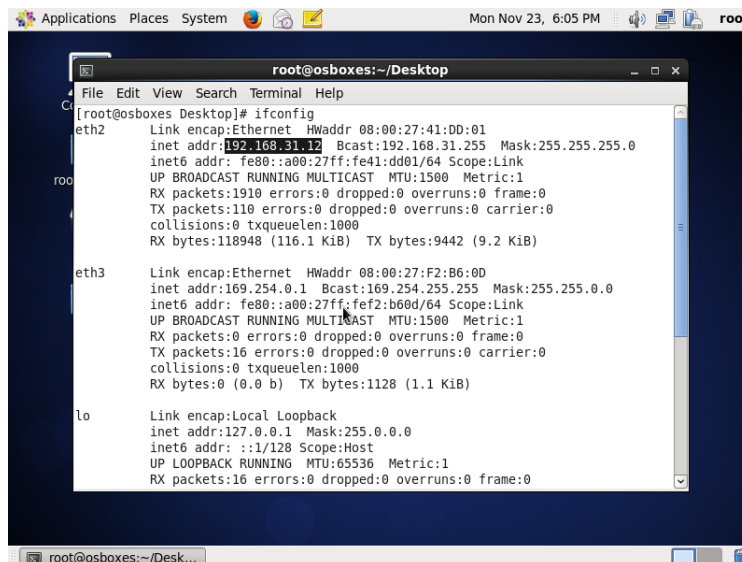
1. ¿Para que sirve esta zona? ¿Qué incluye el fichero named.ca?

La sección options define opciones de configuración globales para el servidor y opciones por defecto para otras secciones del fichero de configuración. Algunas de las que se utilizan normalmente son allow-query, directory o listen-on.

Por otro lado, el fichero named.ca se encarga de guardar los registros DNS (de tipo NS, A, CNAME, MX, etc) para esa zona o dominio.

2. Comprueba que la configuración de red se ha cambiado y la IP del servidor DNS es la del tuyo.

Veamos mediante el comando ifconfig cual es la IP de nuestro servidor:

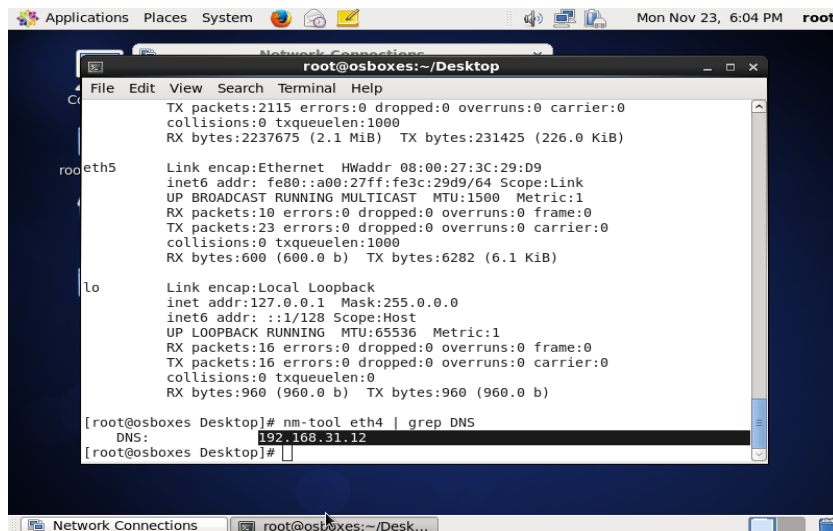


```
root@osboxes: ~/Desktop
File Edit View Search Terminal Help
[root@osboxes Desktop]# ifconfig
eth2      Link encap:Ethernet  HWaddr 08:00:27:41:DD:01
          inet addr:192.168.31.12  Bcast:192.168.31.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe41:dd01/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1910 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:118948 (116.1 KiB)  TX bytes:9442 (9.2 KiB)

eth3      Link encap:Ethernet  HWaddr 08:00:27:F2:B6:0D
          inet addr:169.254.0.1  Bcast:169.254.255.255  Mask:255.255.0.0
          inet6 addr: fe80::a00:27ff:fe41:b60d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:1128 (1.1 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
```

Tras configurar el cliente vemos que la IP del servidor DNS de la interface eth4 coincide con la IP del servidor DNS:



```
TX packets:2115 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2237675 (2.1 MiB) TX bytes:231425 (226.0 KiB)

eth5:
Link encap:Ethernet HWaddr 08:00:27:3C:29:D9
inet6 addr: fe80::a00:27ff:fe3c:29d9/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:10 errors:0 dropped:0 overruns:0 frame:0
TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:600 (600.0 b) TX bytes:6282 (6.1 KiB)

lo:
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:16 errors:0 dropped:0 overruns:0 frame:0
TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:960 (960.0 b) TX bytes:960 (960.0 b)

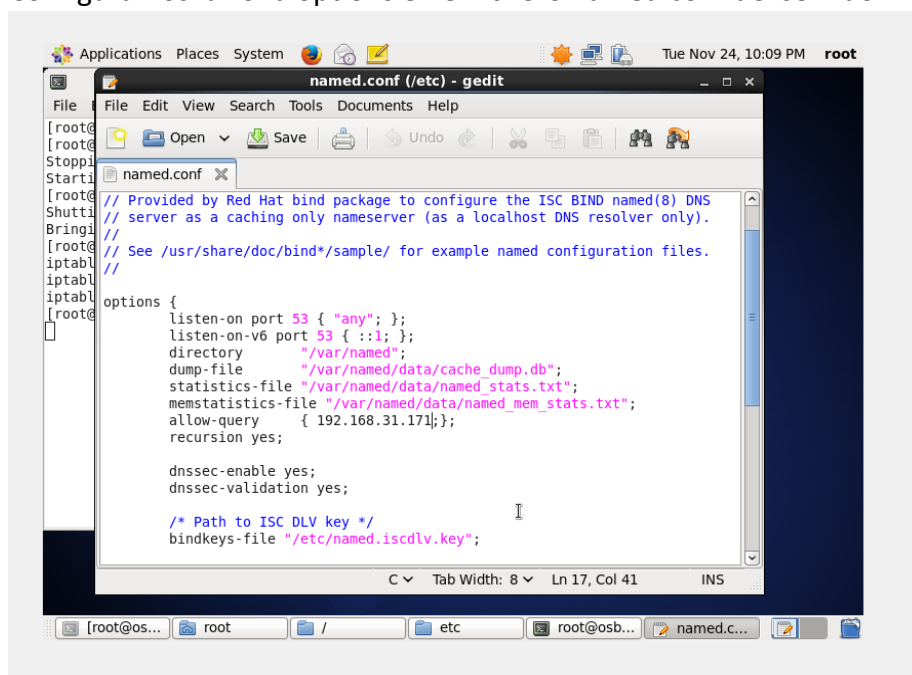
[root@osboxes Desktop]# nm-tool eth4 | grep DNS
DNS: 192.168.31.12
[root@osboxes Desktop]#
```

3. ¿Para que sirve la utilidad rndc? Indica algunos de los comandos que permite.

Permite administrar localmente o a distancia el demonio named gracias a las declaraciones de las líneas de comandos. Uno de los comandos que permite es refresh, que refresca la base de datos del servidor de nombres.

4. Configurar un equipo como servidor de nombres de dominio para la red a la que pertenece el propio equipo (la del laboratorio o la que tengamos virtualizada). Tienes que configurar adecuadamente la sección options y tener la zona "." Configura un equipo cliente para que utilice tu servidor DNS y comprueba que funciona.

Configuramos la zona options en el fichero named.conf del servidor:

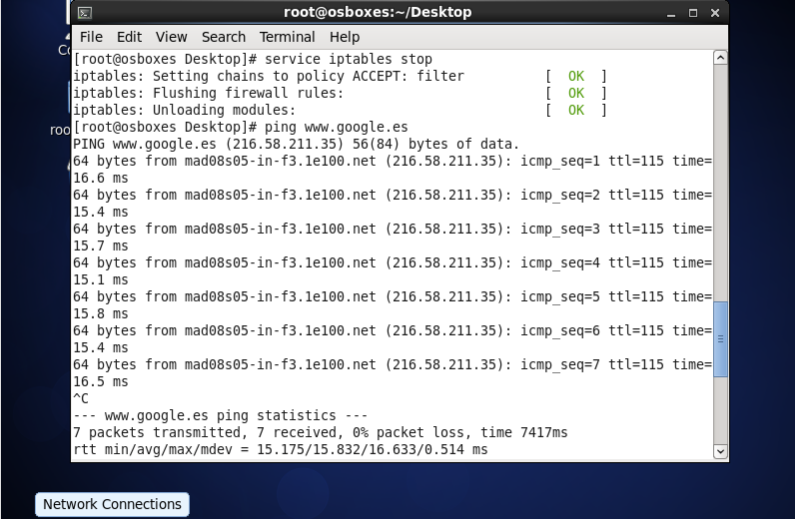


```
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
options {
    listen-on port 53 { "any"; };
    listen-on-v6 port 53 { ::1; };
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query { 192.168.31.171; };
    recursion yes;

    dnssec-enable yes;
    dnssec-validation yes;

    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.iscdlv.key";
}
```

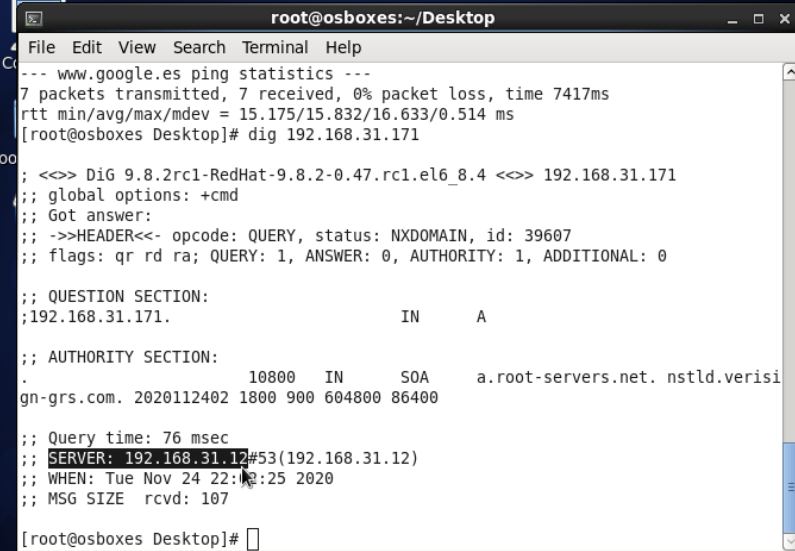
Ahora realizamos el ping a www.google.es desde el cliente:



```
root@osboxes:~/Desktop
File Edit View Search Terminal Help
[root@osboxes Desktop]# service iptables stop
iptables: Setting chains to policy ACCEPT: filter [ OK ]
iptables: Flushing firewall rules: [ OK ]
iptables: Unloading modules: [ OK ]
[root@osboxes Desktop]# ping www.google.es
PING www.google.es (216.58.211.35) 56(84) bytes of data.
64 bytes from mad08s05-in-f3.1e100.net (216.58.211.35): icmp_seq=1 ttl=115 time=16.6 ms
64 bytes from mad08s05-in-f3.1e100.net (216.58.211.35): icmp_seq=2 ttl=115 time=15.4 ms
64 bytes from mad08s05-in-f3.1e100.net (216.58.211.35): icmp_seq=3 ttl=115 time=15.7 ms
64 bytes from mad08s05-in-f3.1e100.net (216.58.211.35): icmp_seq=4 ttl=115 time=15.1 ms
64 bytes from mad08s05-in-f3.1e100.net (216.58.211.35): icmp_seq=5 ttl=115 time=15.8 ms
64 bytes from mad08s05-in-f3.1e100.net (216.58.211.35): icmp_seq=6 ttl=115 time=15.4 ms
64 bytes from mad08s05-in-f3.1e100.net (216.58.211.35): icmp_seq=7 ttl=115 time=16.5 ms
^C
--- www.google.es ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 7417ms
rtt min/avg/max/mdev = 15.175/15.832/16.633/0.514 ms

Network Connections
root@osboxes:~/Desk...
```

Y por último comprobamos con el comando dig que estamos accediendo a través del servidor DNS:



```
root@osboxes:~/Desktop
File Edit View Search Terminal Help
--- www.google.es ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 7417ms
rtt min/avg/max/mdev = 15.175/15.832/16.633/0.514 ms
[root@osboxes Desktop]# dig 192.168.31.171

;<>> Dig 9.8.2rc1-RedHat-9.8.2-0.47.rc1.el6_8.4 <>> 192.168.31.171
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 39607
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;192.168.31.171. IN A

;; AUTHORITY SECTION:
. 10800 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2020112402 1800 900 604800 86400

;; Query time: 76 msec
;; SERVER: 192.168.31.12#53(192.168.31.12)
;; WHEN: Tue Nov 24 22:13:25 2020
;; MSG SIZE rcvd: 107

[root@osboxes Desktop]#
```

5. Tu servidor DNS va a ser servidor DNS autoritativo y maestro, para el dominio uniTierraMedia.com. Crea en named.conf la zona para ello y el fichero de zona correspondiente.

Mostramos la configuración del fichero named.conf:

```
zone "." IN {
    type hint;
    file "named.ca";
};

zone "uniTierraMedia.com." IN {
    type master;
    file "uniTierraMedia.com.zone";
};
```

Ahora vemos el archivo uniTierraMedia.com.zone:



```
$TTL 86400
@ IN SOA dns1.uniTierraMedia.com. paco.uniTierraMedia.com. (
20301120;
86400;
3600;
604800;
10800
)

IN NS dns1.uniTierraMedia.com.
dns1 IN A 192.168.31.12
eq16 IN A 192.168.31.171
www IN CNAME eq16
```

Comprobamos realizando los ping:

Ping a dns1.uniTierraMedia.com

```
PING dns1.uniTierraMedia.com (192.168.31.12) 56(84) bytes of data.
64 bytes from 192.168.31.12: icmp_seq=1 ttl=64 time=0.559 ms
64 bytes from 192.168.31.12: icmp_seq=2 ttl=64 time=0.780 ms
64 bytes from 192.168.31.12: icmp_seq=3 ttl=64 time=0.397 ms
64 bytes from 192.168.31.12: icmp_seq=4 ttl=64 time=0.950 ms
64 bytes from 192.168.31.12: icmp_seq=5 ttl=64 time=0.843 ms
64 bytes from 192.168.31.12: icmp_seq=6 ttl=64 time=0.663 ms
64 bytes from 192.168.31.12: icmp_seq=7 ttl=64 time=0.517 ms
64 bytes from 192.168.31.12: icmp_seq=8 ttl=64 time=0.885 ms
^C
--- dns1.uniTierraMedia.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 8203ms
```

Ping a uniTierraMedia.com

```
[root@osboxes Desktop]# ping www.uniTierraMedia.com
PING eq16.uniTierraMedia.com (192.168.31.171) 56(84) bytes of data.
64 bytes from 192.168.31.171: icmp_seq=1 ttl=64 time=0.009 ms
64 bytes from 192.168.31.171: icmp_seq=2 ttl=64 time=0.038 ms
64 bytes from 192.168.31.171: icmp_seq=3 ttl=64 time=0.025 ms
64 bytes from 192.168.31.171: icmp_seq=4 ttl=64 time=0.038 ms
64 bytes from 192.168.31.171: icmp_seq=5 ttl=64 time=0.041 ms
64 bytes from 192.168.31.171: icmp_seq=6 ttl=64 time=0.019 ms
64 bytes from 192.168.31.171: icmp_seq=7 ttl=64 time=0.040 ms
^C
--- eq16.uniTierraMedia.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6705ms
```

Ping a eq16.uniTierraMedia.com

```
[root@osboxes Desktop]# ping eq16.uniTierraMedia.com
PING eq16.uniTierraMedia.com (192.168.31.171) 56(84) bytes of data.
64 bytes from 192.168.31.171: icmp_seq=1 ttl=64 time=0.013 ms
64 bytes from 192.168.31.171: icmp_seq=2 ttl=64 time=0.026 ms
64 bytes from 192.168.31.171: icmp_seq=3 ttl=64 time=0.041 ms
64 bytes from 192.168.31.171: icmp_seq=4 ttl=64 time=0.038 ms
64 bytes from 192.168.31.171: icmp_seq=5 ttl=64 time=0.026 ms
64 bytes from 192.168.31.171: icmp_seq=6 ttl=64 time=0.041 ms
64 bytes from 192.168.31.171: icmp_seq=7 ttl=64 time=0.040 ms
64 bytes from 192.168.31.171: icmp_seq=8 ttl=64 time=0.035 ms
^C
--- eq16.uniTierraMedia.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7724ms
```

6. ¿Con qué comando y argumento visualizas los servidores DNS que está utilizando el sistema?
7. Explica para qué sirve el comando nslookup y su sintaxis general para ejecutar una consulta.

Es un programa utilizado para saber si el DNS está resolviendo correctamente los nombres y las IPs. Funciona tanto en Windows como en UNIX, Un ejemplo de su uso sería nslookup es.wikipedia.org. Estaríamos preguntando quien es es.wikipedia.org y nos devolvería Address: 66.230.200.100. También se podría preguntar quien es 66.230.200.100 con nslookup 66.230.200.100 y este nos devolvería el nombre.

8. Ejecuta el comando nslookup www.usal.es y explica lo que devuelve y quien te está proporcionando esa información.

```

I
[root@osboxes Desktop]# nslookup www.usal.es
Server:          192.168.31.1
Address:         192.168.31.1#53

Non-authoritative answer:
Name:   www.usal.es
Address: 212.128.130.15

[root@osboxes Desktop]#

```

Address nos indica la dirección IP del servidor DNS que estamos usando.

El mensaje “non-authoritative answer “ se indica que el servidor DNS local no puede responder a la consulta por sí solo, sino que ha debido contactar a uno o varios servidores de nombres alternativos.

Nombre nos indica el nombre del dominio que estamos buscando y el último Address nos indica la dirección IP que responde a este dominio.

9. Ejecuta el comando `nslookup-type=NS usal.es` y explica lo que devuelve y quién te está proporcionando esa información.

```

ot[root@osboxes Desktop]# nslookup -type=NS usal.es
Server:          192.168.31.12
Address:         192.168.31.12#53

Non-authoritative answer:
usal.es nameserver = zafiro.usal.es.
usal.es nameserver = topacio.usal.es.
usal.es nameserver = sun.rediris.es.
usal.es nameserver = chico.rediris.es.
usal.es nameserver = agata.usal.es.

Authoritative answers can be found from:
sun.rediris.es  internet address = 199.184.182.1
sun.rediris.es  has AAAA address 2620:171:808::1
agata.usal.es   internet address = 212.128.130.10
chico.rediris.es      internet address = 162.219.54.2
chico.rediris.es      has AAAA address 2620:10a:80eb::2
zafiro.usal.es  internet address = 212.128.130.11
topacio.usal.es internet address = 212.128.130.12

```

10. Ejecuta el comando `nslookup alumni.usal.es topacio.usal.es` y explica lo que devuelve y quién te está proporcionando esa información.

```

[root@osboxes Desktop]# nslookup alumni.usal.es topacio.usal.es
Server:          topacio.usal.es
Address:         212.128.130.12#53

alumni.usal.es  canonical name = ele.usal.es.
Name:   ele.usal.es
Address: 212.128.132.102

```

El primer mensaje server nos indica el nombre del servidor DNS que utilizará la herramienta.

Address nos indica la dirección IP del servidor DNS que estamos usando.

Name nos indica el nombre del dominio que estamos buscando y el último

Address nos indica la dirección IP que responde a este dominio.