



RESOLUTORES DE NOMBRES EN SERVIDORES DNS



ENERO DE 2022
DESPREGAMENTO DE APLICACIONES WEB
Rodríguez Jácome, David

En esta actividad haremos una prueba de instalación, configuración y prueba de funcionamiento de servidores DNS para resolver los nombres de un dominio en concreto mediante el servicio BIND9. Detallaremos los pasos en tres máquinas: Ubuntu servidor maestro, Ubuntu servidor esclavo, y Windows 10 cliente.

1. Creo una nueva red NAT con nombre RedPracticaDNS en la aplicación VirtualBox y añado esa red a las máquinas virtuales que voy a usar.

Establezco la red NAT 192.168.0.0/24.

2. Creo dos máquinas virtuales, y usaré una como DNS maestro y otra como esclavo.
3. Para cada máquina actualizo los repositorios e instalo BIND9.
4. Actualizo los repositorios.

```
sudo apt-get update
```

```
sudo apt-get upgrade
```

5. Instalo BIND9.

```
sudo apt-get install bind9
```

```
sudo apt-get install bind9-doc dnsutils resolvconf ufw python-ply-doc
```

6. Instalo net-tools.

```
sudo apt install net-tools
```

7. Compruebo las instalaciones.

```
ps -ef | grep named
```

```
sudo service bind9 status
```

8. Servidor DNS maestro.

8.1. Edito la configuración de red de mi servidor en un archivo .yaml del directorio etc con su IP.

```
01-network-manager-all.yaml x
netplan > 01-network-manager-all.yaml
1  # Let NetworkManager manage all devices on this system
2  network:
3    version: 2
4    renderer: NetworkManager
5    ethernets:
6      enp0s3:
7        dhcp4: no
8        addresses: [192.168.0.10/24]
9        gateway4: 192.168.0.1
10       nameservers:
11         addresses: [192.168.0.10]
```

Aplico la configuración de red: sudo netplan apply.

8.2. Habilito un forwarder en el archivo named.conf.options del directorio bind.

```
named.conf.options x
bind > named.conf.options
1  options {
2    directory "/var/cache/bind";
3
4    // If there is a firewall between you and nameservers you want
5    // to talk to, you may need to fix the firewall to allow multiple
6    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113
7
8    // If your ISP provided one or more IP addresses for stable
9    // nameservers, you probably want to use them as forwarders.
10   // Uncomment the following block, and insert the addresses replacing
11   // the all-0's placeholder.
12
13   // forwarders {
14   // 0.0.0.0;
15   // };
16
17   forwarders {
18     //DNS publico de google
19     8.8.8.8;
20     8.8.4.4;
21   };
22
23   //=====
24   // If BIND logs error messages about the root key being expired,
25   // you will need to update your keys.  See https://www.isc.org/bind-keys
26   //=====
27   dnssec-validation auto;
28
29   listen-on-v6 { any; };
30 };
31
```

8.3. Creo la zona del dominio david.lalin.org con resolución directa e inversa en el archivo named.conf.local del directorio bind.

```
named.conf.local x
bind > named.conf.local
1 //
2 // Do any local configuration here
3 //
4 // Consider adding the 1918 zones here, if they are not used in your
5 // organization
6
7 // include "/etc/bind/zones.rfc1918";
8
9 //Definición de la zona de resolución directa. El nombre del dominio es david.lalin.org
10 //El archivo de definición de la zona es /etc/bind/db.david.lalin.org
11
12 zone "david.lalin.org"{
13 type master;
14 file "/etc/bind/db.david.lalin.org";
15 allow-update { none; };
16 allow-transfer {192.168.0.11;};
17 also-notify {192.168.0.11;};
18 };
19
20 //Definición de la zona de resolución inversa. 0.168.192
21 //El archivo de definición de la zona es /etc/bind/ri.192.168.0
22
23 zone "0.168.192.in-addr.arpa" {
24 type master;
25 file "/etc/bind/ri.192.168.0";
26 allow-update { none; };
27 allow-transfer {192.168.0.11;};
28 also-notify {192.168.0.11;};
29 };
```

8.4. Copio un archivo llamado db.local en el directorio bind y lo renombro a bd.david.lalin.org; luego establezco IPs necesarias para ordenadores, servidor, web de la organización y servidor de correo.

```
david@david-VirtualBox: ~  
david@david-VirtualBox:~$ cp /etc/bind/db.local /etc/bind/db.david.lalin.org
```

```
db.david.lalin.org x  
bind > db.david.lalin.org  
1 ;Definición de la resolución directa  
2 ; BIND data file for local loopback interface  
3 ;  
4 $TTL 604800  
5 @ IN SOA david.lalin.org. admin.david.lalin.org (  
6 2 ; Serial  
7 604800 ; Refresh  
8 86400 ; Retry  
9 2419200 ; Expire  
10 604800 ) ; Negative Cache TTL  
11 ;  
12 @ IN NS serverdns.  
13 serverdns IN A 192.168.0.10  
14 servidorPR1 IN A 192.168.0.20  
15 equipo1 IN A 192.168.0.100  
16 equipo2 IN A 192.168.0.101  
17 equipo3 IN A 192.168.0.102  
18 www.david.lalin.org IN CNAME servidorPR1  
19 ftp IN CNAME servidorPR1  
20 @ IN MX 0 mail.  
21 mail IN A 192.168.1.50
```

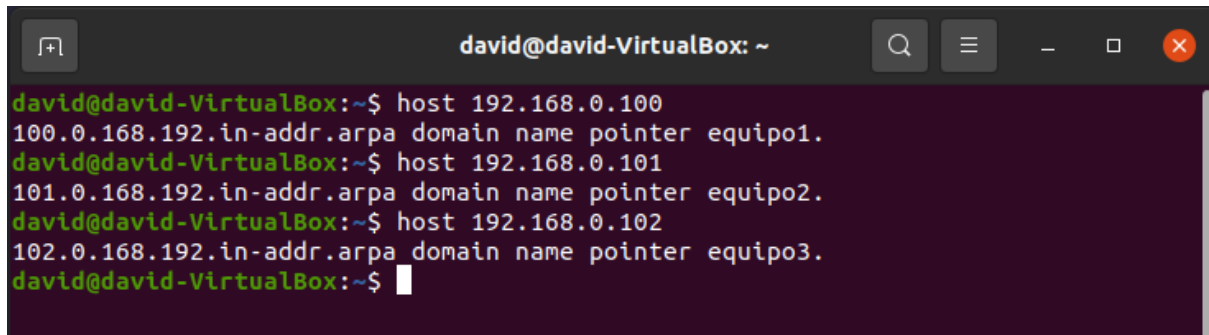
8.5. Hago una prueba de resolución directa en el servidor maestro.

```
david@david-VirtualBox: ~  
david@david-VirtualBox:~$ nslookup equipo1.david.lalin.org  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
Name:   equipo1.david.lalin.org  
Address: 192.168.0.100  
  
david@david-VirtualBox:~$ nslookup equipo2.david.lalin.org  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
Name:   equipo2.david.lalin.org  
Address: 192.168.0.101  
  
david@david-VirtualBox:~$ nslookup equipo3.david.lalin.org  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
Name:   equipo3.david.lalin.org  
Address: 192.168.0.102  
  
david@david-VirtualBox:~$ nslookup serverdns.david.lalin.org  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
Name:   serverdns.david.lalin.org  
Address: 192.168.0.10  
  
david@david-VirtualBox:~$ nslookup servidorPR1.david.lalin.org  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
Name:   servidorPR1.david.lalin.org  
Address: 192.168.0.20  
  
david@david-VirtualBox:~$ nslookup mail.david.lalin.org  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
Name:   mail.david.lalin.org  
Address: 192.168.0.50
```

8.6. Creo el archivo “ri.192.168.0” en el directorio bind y lo edito.

```
ri.192.168.0 x  
bind > ri.192.168.0  
1 ;Resolucion inversa  
2 $TTL 86400  
3 @ IN SOA serverdns.david.lalin.org. admin.david.lalin.org (  
4 2015101500 ; Serial  
5 604800 ; Refresh  
6 86400 ; Retry  
7 2419200 ; Expire  
8 3600 ) ; Negative Cache TTL  
9 ;  
10 @ IN NS serverdns.  
11 10 IN PTR serverdns.  
12 20 IN PTR servidorPR1.  
13 100 IN PTR equipo1.  
14 101 IN PTR equipo2.  
15 102 IN PTR equipo3.  
16 @ IN PTR mail.
```

8.7. Hago una prueba de resolución inversa en el servidor maestro.

A terminal window titled 'david@david-VirtualBox: ~' with standard window controls. It shows three reverse DNS lookup commands and their outputs. The first command is 'host 192.168.0.100', which returns '100.0.168.192.in-addr.arpa domain name pointer equipo1.'. The second is 'host 192.168.0.101', returning '101.0.168.192.in-addr.arpa domain name pointer equipo2.'. The third is 'host 192.168.0.102', returning '102.0.168.192.in-addr.arpa domain name pointer equipo3.'. The prompt returns to 'david@david-VirtualBox:~\$' after each command.

```
david@david-VirtualBox:~$ host 192.168.0.100
100.0.168.192.in-addr.arpa domain name pointer equipo1.
david@david-VirtualBox:~$ host 192.168.0.101
101.0.168.192.in-addr.arpa domain name pointer equipo2.
david@david-VirtualBox:~$ host 192.168.0.102
102.0.168.192.in-addr.arpa domain name pointer equipo3.
david@david-VirtualBox:~$
```

9. Servidor DNS esclavo.

Parte de la configuración del servidor DNS esclavo es similar a la del servidor maestro. Los archivos se encuentran en las mismas ubicaciones en ambas máquinas.

9.1. En el servidor maestro añado los parámetros allow-update, allow-transfer y also-notify.

Este será el único cambio que haremos en el servidor maestro en este punto. El resto de pasos están orientados al servidor esclavo.

A screenshot of a text editor showing the configuration file 'named.conf.local'. The file is opened in a window titled 'named.conf.local x'. The content shows a configuration for a master DNS server for the domain 'david.lalin.org'. It includes comments in Spanish and configuration parameters like 'type master', 'file', 'allow-update { none; }', 'allow-transfer {192.168.0.11;}', and 'also-notify {192.168.0.11;}'. It also defines a reverse lookup zone for '0.168.192.in-addr.arpa'.

```
bind > named.conf.local
1 //
2 // Do any local configuration here
3 //
4 // Consider adding the 1918 zones here, if they are not used in your
5 // organization
6
7 // include "/etc/bind/zones.rfc1918";
8
9 //Definición de la zona de resolución directa. El nombre del dominio es david.lalin.org
10 //El archivo de definición de la zona es /etc/bind/db.david.lalin.org
11
12 zone "david.lalin.org"{
13 type master;
14 file "/etc/bind/db.david.lalin.org";
15 allow-update { none; };
16 allow-transfer {192.168.0.11;};
17 also-notify {192.168.0.11;};
18 };
19
20 //Definición de la zona de resolución inversa. 0.168.192
21 //El archivo de definición de la zona es /etc/bind/ri.192.168.0
22
23 zone "0.168.192.in-addr.arpa" {
24 type master;
25 file "/etc/bind/ri.192.168.0";
26 };
```

9.2. Edito la configuración de red de mi servidor esclavo con su IP correspondiente.

```
01-network-manager-all.yaml x
netplan > 01-network-manager-all.yaml
1  # Let NetworkManager manage all devices on this system
2  network:
3      version: 2
4      renderer: NetworkManager
5      ethernets:
6          enp0s3:
7              dhcp4: no
8              addresses: [192.168.0.11/24]
9              gateway4: 192.168.0.1
10             nameservers:
11                 addresses: [192.168.0.11]
```

9.3. Establezco un forwarder.

```
named.conf.options x
bind > named.conf.options
1  options {
2      directory "/var/cache/bind";
3
4      // If there is a firewall between you and nameservers you want
5      // to talk to, you may need to fix the firewall to allow multiple
6      // ports to talk.  See http://www.kb.cert.org/vuls/id/800113
7
8      // If your ISP provided one or more IP addresses for stable
9      // nameservers, you probably want to use them as forwarders.
10     // Uncomment the following block, and insert the addresses replacing
11     // the all-0's placeholder.
12
13     // forwarders {
14     //  0.0.0.0;
15     // };
16
17     forwarders {
18         //DNS público de google
19         8.8.8.8;
20         8.8.4.4 ;
21     };
22
23     //=====
24     // If BIND logs error messages about the root key being expired,
25     // you will need to update your keys.  See https://www.isc.org/bind-keys
26     //=====
27     dnssec-validation auto;
28
29     listen-on-v6 { any; };
30 };
```

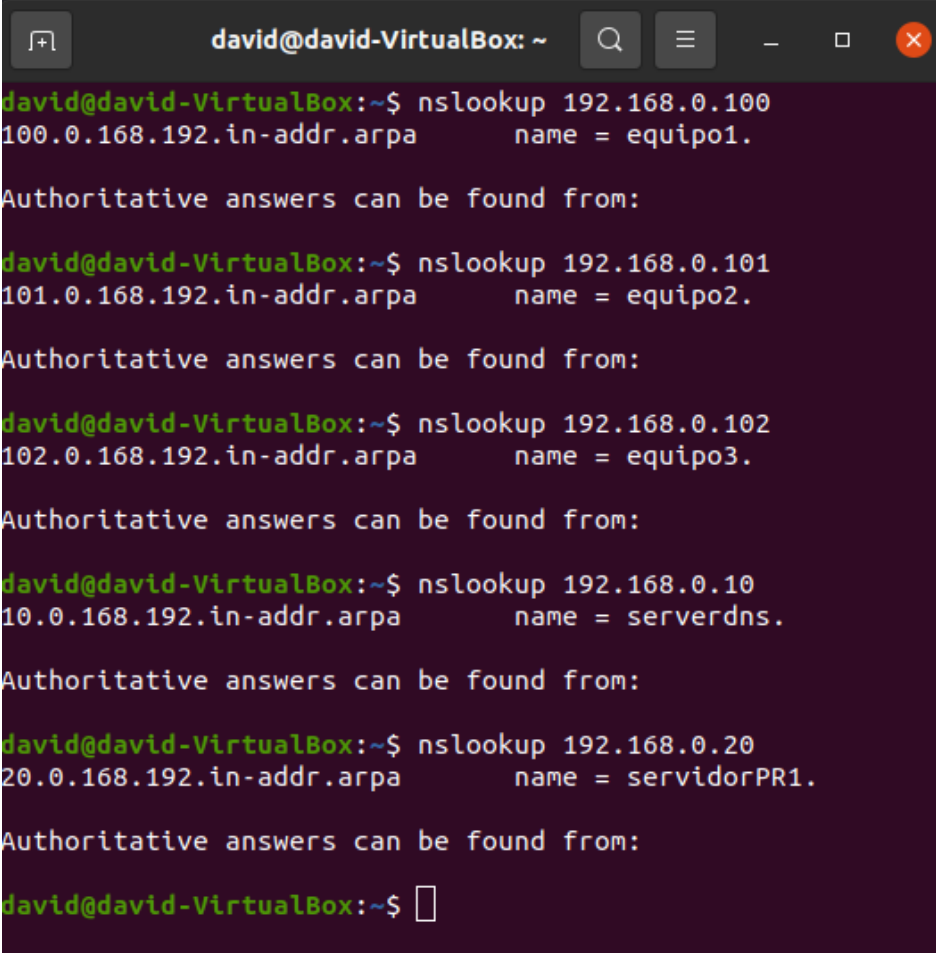

9.4. Configuro la zona de resolución directa y de búsqueda inversa.

```
named.conf.local x
bind > named.conf.local
1 //
2 // Do any local configuration here
3 //
4
5 // Consider adding the 1918 zones here, if they are not used in your
6 // organization
7 //include "/etc/bind/zones.rfc1918";
8
9 zone "david.lalin.org"{
10 type slave;
11 file "/etc/bind/db.david.lalin.org";
12 masters {192.168.0.10;};
13 };
14
15 // Zona de búsqueda inversa para 192.168.1.0/24
16 zone "0.168.192.in-addr.arpa" {
17 type slave;
18 file "ri.192.168.0";
19 masters {192.168.0.10;}; // dirección del servidor primario
20 };
```

9.5. Reinicio el servicio BIND9 y compruebo que funciona la resolución directa.

```
david@david-VirtualBox: ~
david@david-VirtualBox:~$ host equipo1.david.lalin.org
equipo1.david.lalin.org has address 192.168.0.100
david@david-VirtualBox:~$ host equipo2.david.lalin.org
equipo2.david.lalin.org has address 192.168.0.101
david@david-VirtualBox:~$ host equipo3.david.lalin.org
equipo3.david.lalin.org has address 192.168.0.102
david@david-VirtualBox:~$
```

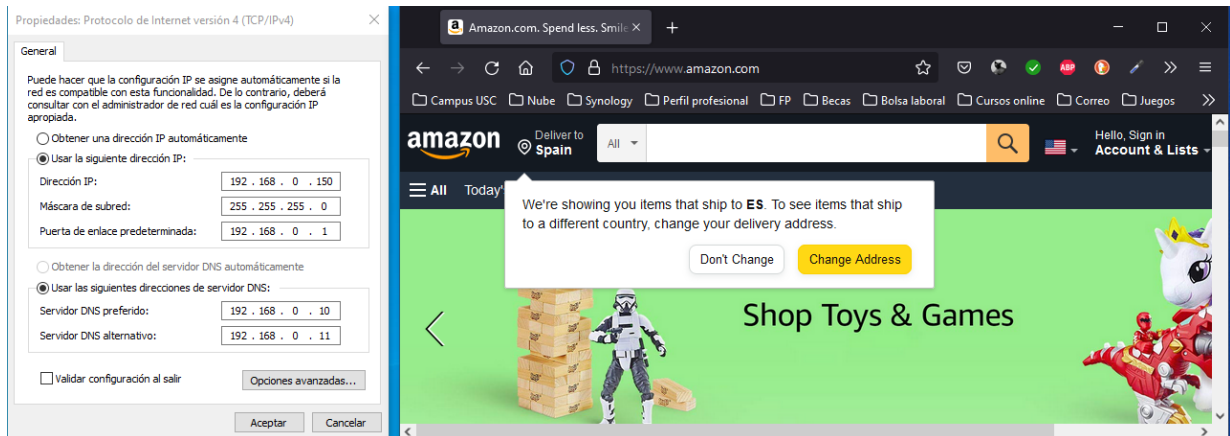
9.6. Verifico la resolución inversa.



```
david@david-VirtualBox: ~  
david@david-VirtualBox:~$ nslookup 192.168.0.100  
100.0.168.192.in-addr.arpa      name = equipo1.  
  
Authoritative answers can be found from:  
  
david@david-VirtualBox:~$ nslookup 192.168.0.101  
101.0.168.192.in-addr.arpa      name = equipo2.  
  
Authoritative answers can be found from:  
  
david@david-VirtualBox:~$ nslookup 192.168.0.102  
102.0.168.192.in-addr.arpa      name = equipo3.  
  
Authoritative answers can be found from:  
  
david@david-VirtualBox:~$ nslookup 192.168.0.10  
10.0.168.192.in-addr.arpa      name = serverdns.  
  
Authoritative answers can be found from:  
  
david@david-VirtualBox:~$ nslookup 192.168.0.20  
20.0.168.192.in-addr.arpa      name = servidorPR1.  
  
Authoritative answers can be found from:  
  
david@david-VirtualBox:~$
```

10. Hago una prueba de conexión a internet desde una máquina cliente Windows.

Para la conexión, editamos la configuración de red asignándole una IP 192.168.0.150, y para DNS las IP de las máquinas maestro y esclavo; comprobamos que tenemos internet en el cliente Windows.



Ahora pararemos los servicios de BIND9 en las máquinas maestro y esclavo para cortar la conexión a internet de la máquina cliente Windows:

- Servidor DNS maestro:

```
david@david-VirtualBox: ~  
david@david-VirtualBox:~$ sudo service bind9 stop  
[sudo] contraseña para david:  
david@david-VirtualBox:~$ sudo service bind9 status  
● named.service - BIND Domain Name Server  
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)  
   Active: inactive (dead) since Tue 2022-02-01 12:36:40 CET; 3s ago  
     Docs: man:named(8)  
  Process: 13644 ExecStart=/usr/sbin/named -f $OPTIONS (code=exited, status=0/SUCCESS)  
  Process: 13816 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)  
    Main PID: 13644 (code=exited, status=0/SUCCESS)  
  
feb 01 12:36:40 david-VirtualBox named[13644]: no longer listening on 127.0.0.1  
feb 01 12:36:40 david-VirtualBox named[13644]: no longer listening on 192.168.0.1  
feb 01 12:36:40 david-VirtualBox named[13644]: no longer listening on ::1#53  
feb 01 12:36:40 david-VirtualBox named[13644]: no longer listening on fe80::a00:  
feb 01 12:36:40 david-VirtualBox named[13644]: shutting down: flushing changes  
feb 01 12:36:40 david-VirtualBox named[13644]: stopping command channel on 127.  
feb 01 12:36:40 david-VirtualBox named[13644]: stopping command channel on ::1#  
feb 01 12:36:40 david-VirtualBox named[13644]: exiting
```

- Servidor DNS esclavo:

```
david@david-VirtualBox: ~  
david@david-VirtualBox:~$ sudo service bind9 stop  
[sudo] contraseña para david:  
david@david-VirtualBox:~$ sudo service bind9 status  
● named.service - BIND Domain Name Server  
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: >  
   Active: inactive (dead) since Tue 2022-02-01 12:36:02 CET; 5s ago  
     Docs: man:named(8)  
   Process: 14046 ExecStart=/usr/sbin/named -f $OPTIONS (code=exited, status=0>  
   Process: 14258 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)  
    Main PID: 14046 (code=exited, status=0/SUCCESS)  
  
Feb 01 12:36:02 david-VirtualBox named[14046]: no longer listening on ::1#53  
Feb 01 12:36:02 david-VirtualBox named[14046]: no longer listening on fe80::a00>  
Feb 01 12:36:02 david-VirtualBox named[14046]: shutting down: flushing changes  
Feb 01 12:36:02 david-VirtualBox named[14046]: stopping command channel on 127.>  
Feb 01 12:36:02 david-VirtualBox named[14046]: stopping command channel on ::1#>  
Feb 01 12:36:02 david-VirtualBox named[14046]: dumping master file: /etc/bind/t>  
Feb 01 12:36:02 david-VirtualBox named[14046]: dumping master file: /etc/bind/t>  
Feb 01 12:36:02 david-VirtualBox named[14046]: exiting
```

- Máquina cliente Windows:

Finalmente, comprobamos que el cliente no puede conectarse a internet dado que ninguno de los dos servidores le ofrece servicio DNS. Sí podría acceder a internet con cualquiera de ambos encendido, pero no con ambos apagados.

