

MANUAL



DNS

DAVID SEGURA TRISTANCHO
2º ASIR 2022/23

¿QUÉ ES DNS?

DNS son las iniciales de Domain Name System (sistema de nombres de dominio) y es una tecnología basada en una base de datos que sirve para resolver nombres en las redes, es decir, para conocer la dirección IP de la máquina donde está alojado el dominio al que queremos acceder. En el siguiente manual, vamos a conocer en profundidad su uso en diferentes sistemas operativos y servidores, hasta llegar a entenderlo de una manera más lógica. Sin más, comencemos.

INSTALACION DE BIND9

Y es que Bind9 es el software que va a hacer de servidor dns. Sin mayores preámbulos, lo instalamos con *sudo apt install bind9*. Una vez instalado, me aseguro de que está activo.

```
usuario@usuario:~$ sudo service bind9 status
• named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-10-11 06:36:11 UTC; 2min 27s ago
     Docs: man:named(8)
   Main PID: 2198 (named)
    Tasks: 5 (limit: 1066)
   Memory: 14.1M
   CGroup: /system.slice/named.service
           └─2198 /usr/sbin/named -f -u bind
```

Accedo a `cd /etc/bind`, hago un `ls` para hacer una primera valoración de los archivos que contiene, los cuales algunos de ellos veremos en profundidad posteriormente. Quiero ver los puertos disponibles, con los que contamos, así que hago uso del siguiente comando.

```
usuario@usuario:/etc/bind$ sudo netstat -natup | grep "name"
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.1:953          0.0.0.0:*               LISTEN
2198/named
tcp        0      0 192.168.128.171:53     0.0.0.0:*               LISTEN
2198/named
tcp        0      0 127.0.0.1:53          0.0.0.0:*               LISTEN
2198/named
tcp6       0      0 :::953                 :::*                    LISTEN
2198/named
tcp6       0      0 fe80::a00:27ff:fe7e::53 :::*                    LISTEN
2198/named
tcp6       0      0 :::53                  :::*                    LISTEN
2198/named
udp        0      0 192.168.128.171:53     0.0.0.0:*               LISTEN
2198/named
udp        0      0 127.0.0.1:53          0.0.0.0:*               LISTEN
2198/named
udp6       0      0 :::53                  :::*                    LISTEN
2198/named
udp6       0      0 fe80::a00:27ff:fe7e::53 :::*                    LISTEN
2198/named
```

Contamos con protocolos tcp y udp, bajo el puerto 53. Por cierto, si no contamos con la herramienta netstat se puede instalar mediante *sudo install net-tools*.

De los archivos que contiene `/etc/bind9`, vamos a quedarnos en esta primera parte con tres trascendentales: `named.conf.default-zones` y `named.conf.local`.

En `named.conf.local` vamos a crear nuestra primera zona, tal y como quedara reflejado en la siguiente imagen:

```
GNU nano 4.8      named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "iespsur.es" {
    type master;
    file "/etc/bind/db.iespsur";
};
```

Hemos modificado el archivo de la zona, dándole el nombre de `/etc/bind/db.iespsur`. Ahora, entramos en dicho archivo y en la sección de NS hacemos las siguientes modificaciones:

```
usuario@usuario: /etc/bind 80x24
GNU nano 4.8      db.iespsur      Modified
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns1.iespsur.es. info.iespsur.es. (
; Serial
        2         ; Refresh
        604800    ; Retry
        86400     ; Expire
        2419200   ; Negative Cache TTL
)
;
@         IN      NS       ns1.iespsur.es.
ns1.iespsur.es. IN      A       192.168.128.171
www       IN      A       192.168.128.152
nas.iespsur.es. IN      A       192.168.128.114
;@        IN      AAAA     ::1
```

Antes de este paso, por cierto, he copiado el archivo `db.local` a `db.iespsur`. Ergo, una vez editado el archivo `db.iespsur` reinicio el sistema.

```
usuario@usuario:/etc/bind$ sudo cp db.local db.iespsur
usuario@usuario:/etc/bind$ sudo nano db.iespsur
usuario@usuario:/etc/bind$ sudo service bind9 restart
usuario@usuario:/etc/bind$
```

Para comprobar los cambios producidos puedo hacerlo mediante dos formas. Una, más tradicional, se realiza mediante el comando `nslookup`, algo más compleja. La segunda, la más actual, se efectúa mediante el comando `dig`. En la siguiente página, vemos dos ejemplos.

```

usuario@usuario:/etc/bind$ dig @192.168.128.171 nas.iespsur.es

; <<>> DiG 9.16.1-Ubuntu <<>> @192.168.128.171 nas.iespsur.es
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17223
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 1cc73e2b0c0e5eb60100000063452275661c98993fd1ddb8 (good)
;; QUESTION SECTION:
;nas.iespsur.es.                IN      A

;; ANSWER SECTION:
nas.iespsur.es.                604800  IN      A      192.168.128.114

;; Query time: 0 msec
;; SERVER: 192.168.128.171#53(192.168.128.171)
;; WHEN: mar oct 11 07:59:49 UTC 2022
;; MSG SIZE rcvd: 87

```

```

usuario@usuario:/etc/bind$ dig @192.168.128.171 ns1.iespsur.es

; <<>> DiG 9.16.1-Ubuntu <<>> @192.168.128.171 ns1.iespsur.es
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47009
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: ca15cdacb3d54b62010000006345223ff2c8f2dd47a1e91b (good)
;; QUESTION SECTION:
;ns1.iespsur.es.                IN      A

;; ANSWER SECTION:
ns1.iespsur.es.                604800  IN      A      192.168.128.171

;; Query time: 15 msec
;; SERVER: 192.168.128.171#53(192.168.128.171)
;; WHEN: mar oct 11 07:58:55 UTC 2022
;; MSG SIZE rcvd: 87

```

Si quiero saber si todas las zonas están cargadas, hago uso del siguiente comando:

```

usuario@usuario:/etc/bind$ sudo cat /var/log/syslog | grep "all zones"
Oct 11 06:36:13 usuario named[2198]: all zones loaded
Oct 11 07:29:16 usuario named[2991]: all zones loaded
Oct 11 07:48:44 usuario named[3227]: all zones loaded
Oct 11 07:50:41 usuario named[3258]: all zones loaded

```

Igualmente, con el siguiente comando, también podemos ver si realmente se han cargado las zonas:

```

usuario@usuario:/etc/bind$ sudo tail -n 50 /var/log/syslog | grep zone
Oct 11 07:50:41 usuario named[3258]: managed-keys-zone: loaded serial 4
Oct 11 07:50:41 usuario named[3258]: zone 0.in-addr.arpa/IN: loaded serial 1
Oct 11 07:50:41 usuario named[3258]: zone 127.in-addr.arpa/IN: loaded serial 1
Oct 11 07:50:41 usuario named[3258]: zone 255.in-addr.arpa/IN: loaded serial 1
Oct 11 07:50:41 usuario named[3258]: zone localhost/IN: loaded serial 2
Oct 11 07:50:41 usuario named[3258]: zone iespsur.es/IN: loaded serial 2
Oct 11 07:50:41 usuario named[3258]: all zones loaded
Oct 11 07:50:41 usuario named[3258]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)

```

