Cristina Moure Feijoó 2ºDAW

P3.2 – Configuración de DNS Bind

Primero debemos hacer un sudo apt-get update para actualizar los repositorios.

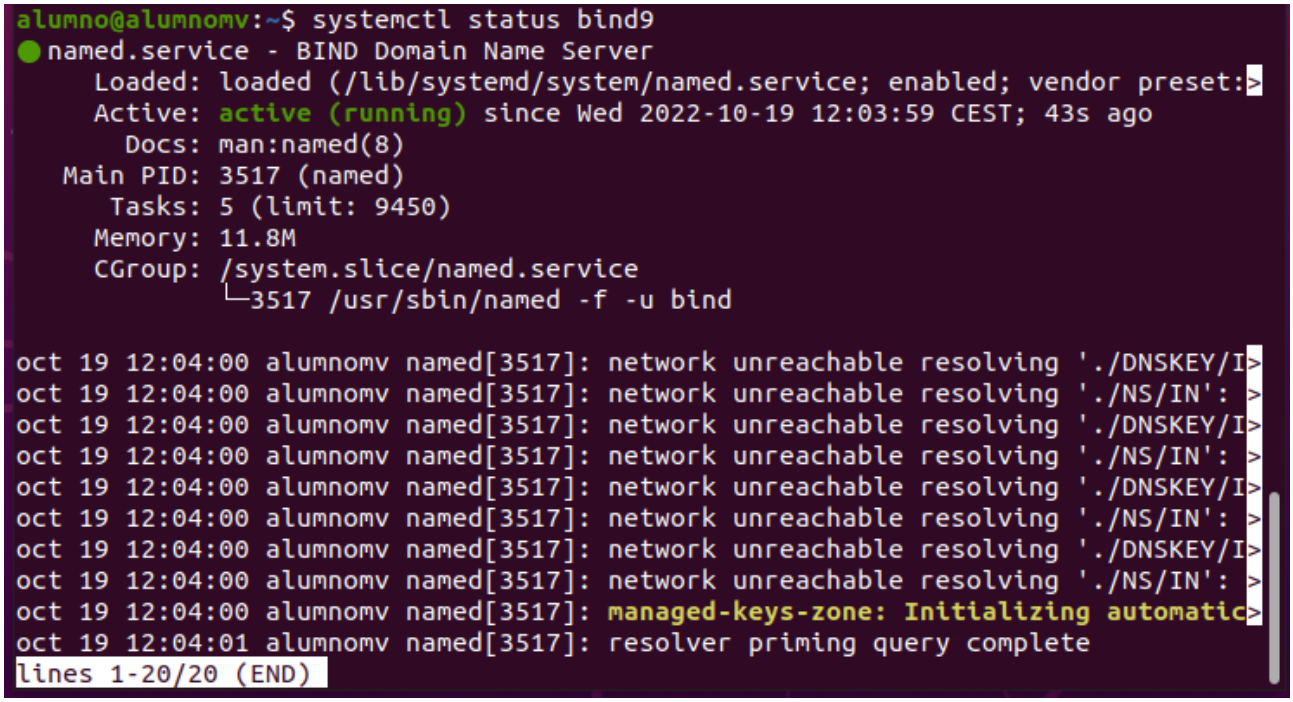
```
alumno@alumnomv:~$ sudo apt-get update
Des:1 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Obj:2 http://es.archive.ubuntu.com/ubuntu focal InRelease
Des:3 http://es.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Des:4 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [1.81
8 kB]
Des:5 http://es.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [2.1
91 kB]
Des:7 http://security.ubuntu.com/ubuntu focal-security/main i386 Packages [514 k
B]
Des:8 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [300
kB]
```

A continuación ejecutamos el siguiente comando para instalar bind9:

```
alumno@alumnomv:~$ sudo apt install bind9
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  bind9-dnsutils bind9-libs bind9-utils python3-ply
Paquetes sugeridos:
  bind-doc resolvconf python-ply-doc
Se instalarán los siguientes paquetes NUEVOS:
  bind9 bind9-utils python3-ply
Se actualizarán los siguientes paquetes:
  bind9-dnsutils bind9-libs
2 actualizados, 3 nuevos se instalarán, 0 para eliminar y 107 no actualizados.
Se necesita descargar 1.647 kB/1.694 kB de archivos.
Se utilizarán 1.909 kB de espacio de disco adicional después de esta operación
¿Desea continuar? [S/n] s
```

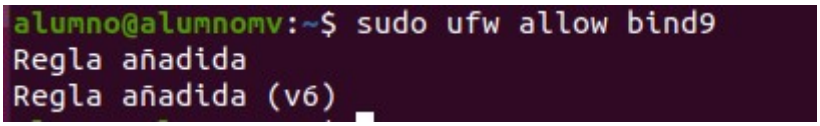
Esperamos a que se complete la instalación.

Comprobamos que bind9 está funcionando ya con **systemctl status bind9**:



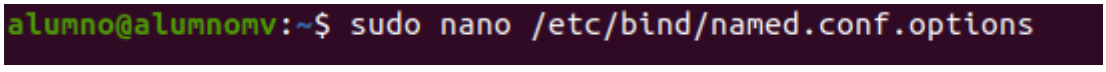
```
alumno@alumnomv:~$ systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset:>
     Active: active (running) since Wed 2022-10-19 12:03:59 CEST; 43s ago
       Docs: man:named(8)
   Main PID: 3517 (named)
      Tasks: 5 (limit: 9450)
     Memory: 11.8M
     CGroup: /system.slice/named.service
             └─3517 /usr/sbin/named -f -u bind

oct 19 12:04:00 alumnomv named[3517]: network unreachable resolving './DNSKEY/I>
oct 19 12:04:00 alumnomv named[3517]: network unreachable resolving './NS/IN': >
oct 19 12:04:00 alumnomv named[3517]: network unreachable resolving './DNSKEY/I>
oct 19 12:04:00 alumnomv named[3517]: network unreachable resolving './NS/IN': >
oct 19 12:04:00 alumnomv named[3517]: network unreachable resolving './DNSKEY/I>
oct 19 12:04:00 alumnomv named[3517]: network unreachable resolving './NS/IN': >
oct 19 12:04:00 alumnomv named[3517]: network unreachable resolving './DNSKEY/I>
oct 19 12:04:00 alumnomv named[3517]: network unreachable resolving './NS/IN': >
oct 19 12:04:00 alumnomv named[3517]: managed-keys-zone: Initializing automatic>
oct 19 12:04:01 alumnomv named[3517]: resolver priming query complete
lines 1-20/20 (END)
```

Vamos a permitir en el firewall el acceso al puerto y el protocolo que usa bind9 para que no nos de problemas:



```
alumno@alumnomv:~$ sudo ufw allow bind9
Regla añadida
Regla añadida (v6)
```

Ahora vamos a ejecutar el siguiente comando para entrar en el fichero de configuración mínima:



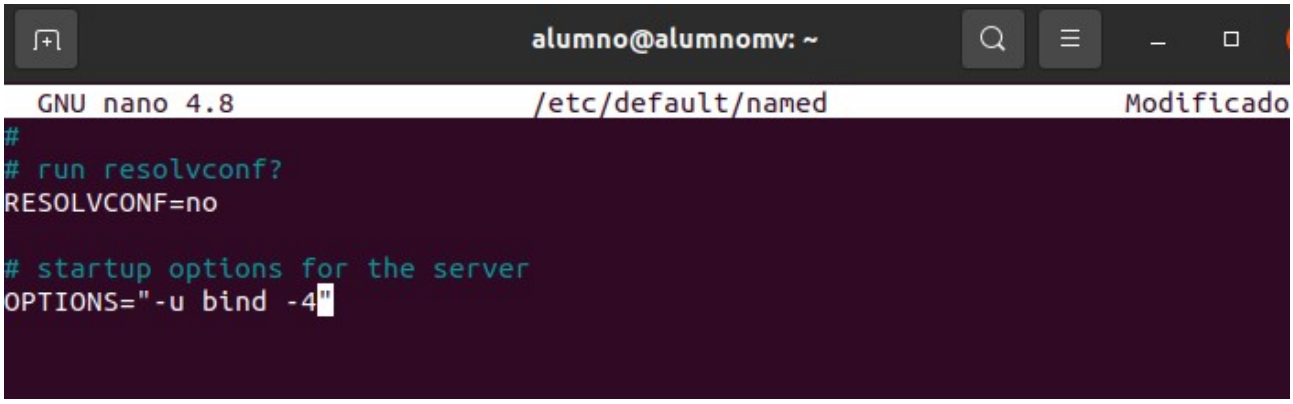
```
alumno@alumnomv:~$ sudo nano /etc/bind/named.conf.options
```

Y editamos el fichero de esta forma (la segunda IP en acl internals la adaptamos según la que tenga nuestro equipo en el cual vamos a crear el servidor):

Ahora vamos a obligarle a usar únicamente Ipv4, para ello vamos a editar el siguiente fichero:

```
alumno@alumnomv:~$ sudo nano /etc/default/named
```

Modificamos el fichero añadiendo -4 al final:



Comprobamos la configuración de bind9:

```
alumno@alumnomv:~$ sudo named-checkconf
```

Hacemos un reinicio de bind9 y comprobamos el status para ver si hay errores:

```
alumno@alumnomv:~$ sudo systemctl restart bind9
alumno@alumnomv:~$ systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset:>
     Active: active (running) since Wed 2022-10-19 12:26:22 CEST; 8s ago
       Docs: man:named(8)
   Main PID: 4973 (named)
      Tasks: 5 (limit: 9450)
     Memory: 10.9M
     CGroup: /system.slice/named.service
             └─4973 /usr/sbin/named -f -u bind -4

oct 19 12:26:22 alumnomv named[4973]: command channel listening on 127.0.0.1#953
oct 19 12:26:22 alumnomv named[4973]: managed-keys-zone: loaded serial 2
oct 19 12:26:22 alumnomv named[4973]: zone 0.in-addr.arpa/IN: loaded serial 1
oct 19 12:26:22 alumnomv named[4973]: zone 127.in-addr.arpa/IN: loaded serial 1
oct 19 12:26:22 alumnomv named[4973]: zone 255.in-addr.arpa/IN: loaded serial 1
oct 19 12:26:22 alumnomv named[4973]: zone localhost/IN: loaded serial 2
oct 19 12:26:22 alumnomv named[4973]: all zones loaded
oct 19 12:26:22 alumnomv named[4973]: running
oct 19 12:26:22 alumnomv named[4973]: managed-keys-zone: Key 20326 for zone . i>
oct 19 12:26:22 alumnomv named[4973]: resolver priming query complete
lines 1-20/20 (END)
```

Ahora vamos a editar el siguiente fichero para crear la zona directa e inversa:

```
alumno@alumnomv:~$ sudo nano /etc/bind/named.conf.local
```

Para crear la zona directa escribimos zone “nombre-zona”, añadimos el tipo (master porque será maestro) y allow-transfer internals porque solo permitiremos que el servidor sirva a la red virtual y no a equipos externos. Hacemos lo mismo con la zona inversa pero poniendo los 3 primeros octetos de la IP al revés y añadiendo in-addr-arpa.

Creamos también los archivos de zona “db.daw213.iesldv.com” y “db.10.33.13” porque no existen.

```
  GNU nano 4.8                 /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization

zone "daw213.iesldv.com." {
        type master;
        file "/etc/bind/zonas/db.daw213.iesldv.com";
        allow-transfer { internals; };
};

zone "13.33.10.in-addr.arpa." {
        type master;
        file "/etc/bind/zonas/db.10.33.13";
        allow-transfer { internals; };
};

include "/etc/bind/zones.rfc1918";
```

Ahora vamos a crear el directorio donde guardaremos los archivos de zonas:

```
alumno@alumnomv:~$ sudo mkdir /etc/bind/zonas
```

Y vamos a crear un archivo para la zona directa:

```
alumno@alumnomv:~$ sudo nano /etc/bind/zonas/db.daw213.iesldv.com
```

Ahora los vamos a editar de la siguiente forma:

$TTL será el tiempo de vida.

Añadimos en el registro SOA el servidor principal, el numero de seria (serial), el intervalo de actuación (refresh), el intervalo de reintento (retry), el tiempo de expiración (expire) y el TTL mínimo.

Agregamos el name-server (NS), los hosts (A) y los alias (CNAME), además del servidor de correo del dominio que en este caso será ubuntu (MX)

```
  GNU nano 4.8          /etc/bind/zonas/db.daw213.iesldv.com
$TTL    1D
@       IN      SOA     daw213.iesldv.com. ubuntu.daw213.iesldv.com. (
        1       ; Serial
        25m     ; Refresh
        15m     ; Retry
        2D      ; Expire
        2h )    ; Negative Cache TTL
;

@               IN      NS      ubuntu.daw213.iesldv.com.
ubuntu          IN      A       10.33.13.2
windows10       IN      A       10.33.13.4
wserver         IN      A       10.33.13.3
ipcop           IN      A       10.33.13.1
dns1            IN      CNAME   wserver.daw213.iesldv.com.
www             IN      CNAME   windows10.daw213.iesldv.com.
crism           IN      CNAME   windows10.daw213.iesldv.com.
ubuntu          IN      MX      10 ubuntu.daw213.iesldv.com.
```

De la misma forma creamos otro archivo para configurar la zona inversa:

```
alumno@alumnomv:~$ sudo nano /etc/bind/zonas/db.10.33.13
```

Y lo configuramos así:

Añadimos lo mismo que en la zona directa con la diferencia de que en este caso solo agregaremos el NS y los punteros (PTR).

```
  GNU nano 4.8              /etc/bind/zonas/db.10.33.13
$TTL    1d ;
@       IN      SOA     daw213.iesldv.com. ubuntu.daw213.iesldv.com. (
                        20210222        ; Serial
                        12h             ; Refresh
                        15m             ; Retry
                        3w              ; Expire
                        2h )    ; Negative Cache TTL
;
@                               IN      NS      ubuntu.daw213.iesldv.com.
1.13.33.10.in-addr.arpa.        IN      PTR     ipcop.daw213.iesldv.com.
2.13.33.10.in-addr.arpa.        IN      PTR     ubuntu.daw213.iesldv.com.
3.13.33.10.in-addr.arpa.        IN      PTR     wserver.daw213.iesldv.com.
4.13.33.10.in-addr.arpa.        IN      PTR     windows10.daw213.iesldv.com.
```

Ahora vamos a reiniciar bind9:

```
alumno@alumnomv:~$ sudo systemctl restart bind9
```

Vamos a comprobar que funciona la zona directa:

```
alumno@alumnomv:~$ sudo named-checkzone daw213.iesldv.com. /etc/bind/zonas/db.da
w213.iesldv.com
zone daw213.iesldv.com/IN: loaded serial 1
OK
```

Y también comprobamos que funciona la zona inversa:

```
alumno@alumnomv:~$ sudo named-checkzone 13.33.10.in-addr.arpa. /etc/bind/zonas/d
b.10.33.13
zone 13.33.10.in-addr.arpa/IN: loaded serial 20210222
OK
```

Ahora vamos a comprobar que todo funciona correctamente utilizando el comando nslookup para la zona directa y host para la inversa:

Con host ponemos primero la IP que queremos comprobar y luego al DNS que le estamos preguntando, que en este caso es nuestra máquina ubuntu.

```
alumno@alumnomv:~$ host 10.33.13.1 10.33.13.2
Using domain server:
Name: 10.33.13.2
Address: 10.33.13.2#53
Aliases:

1.13.33.10.in-addr.arpa domain name pointer ipcop.daw213.iesldv.com.
alumno@alumnomv:~$ host 10.33.13.2 10.33.13.2
Using domain server:
Name: 10.33.13.2
Address: 10.33.13.2#53
Aliases:

2.13.33.10.in-addr.arpa domain name pointer ubuntu.daw213.iesldv.com.
alumno@alumnomv:~$ host 10.33.13.3 10.33.13.2
Using domain server:
Name: 10.33.13.2
Address: 10.33.13.2#53
Aliases:

3.13.33.10.in-addr.arpa domain name pointer wserver.daw213.iesldv.com.
alumno@alumnomv:~$ host 10.33.13.4 10.33.13.2
Using domain server:
Name: 10.33.13.2
Address: 10.33.13.2#53
Aliases:

4.13.33.10.in-addr.arpa domain name pointer windows10.daw213.iesldv.com.
```

Y ahora comprobamos con nslookup pero primero debemos configurar que le pregunte a nuestro DNS, es decir 10.33.13.2

Luego comprobamos cada host y los alias.

```
alumno@alumnomv:~$ nslookup
> server 10.33.13.2
Default server: 10.33.13.2
Address: 10.33.13.2#53
> wserver.daw213.iesldv.com.
Server:         10.33.13.2
Address:        10.33.13.2#53

Name:   wserver.daw213.iesldv.com
Address: 10.33.13.3
> ipcop.daw213.iesldv.com.
Server:         10.33.13.2
Address:        10.33.13.2#53

Name:   ipcop.daw213.iesldv.com
Address: 10.33.13.1
> windows10.daw213.iesldv.com.
Server:         10.33.13.2
Address:        10.33.13.2#53

Name:   windows10.daw213.iesldv.com
Address: 10.33.13.4
> ubuntu.daw213.iesldv.com.
Server:         10.33.13.2
Address:        10.33.13.2#53

Name:   ubuntu.daw213.iesldv.com
Address: 10.33.13.2
```

```
> dns1.daw213.iesldv.com.
Server:         10.33.13.2
Address:        10.33.13.2#53

dns1.daw213.iesldv.com  canonical name = wserver.daw213.iesldv.com.
Name:   wserver.daw213.iesldv.com
Address: 10.33.13.3
> www.daw213.iesldv.com.
Server:         10.33.13.2
Address:        10.33.13.2#53

www.daw213.iesldv.com   canonical name = windows10.daw213.iesldv.com.
Name:   windows10.daw213.iesldv.com
Address: 10.33.13.4
> crism.daw213.iesldv.com.
Server:         10.33.13.2
Address:        10.33.13.2#53

crism.daw213.iesldv.com canonical name = windows10.daw213.iesldv.com.
Name:   windows10.daw213.iesldv.com
Address: 10.33.13.4
```

Comprobamos tambien que funciona en windows 10 por ejemplo, aquí comprobamos la zona directa:

```
C:\Users\alumno>nslookup
Servidor predeterminado:  dns.google
Address:  8.8.8.8

> server 10.33.13.2
Servidor predeterminado:  [10.33.13.2]
Address:  10.33.13.2

> wserver.daw213.iesldv.com.
Servidor:  [10.33.13.2]
Address:  10.33.13.2

Nombre:  wserver.daw213.iesldv.com
Address:  10.33.13.3

> ubuntu.daw213.iesldv.com.
Servidor:  [10.33.13.2]
Address:  10.33.13.2

Nombre:  ubuntu.daw213.iesldv.com
Address:  10.33.13.2

> ipcop.daw213.iesldv.com.
Servidor:  [10.33.13.2]
Address:  10.33.13.2

Nombre:  ipcop.daw213.iesldv.com
```

```
> windows10.daw213.iesldv.com.
Servidor:  [10.33.13.2]
Address:  10.33.13.2

Nombre:  windows10.daw213.iesldv.com
Address:  10.33.13.4

> www.daw213.iesldv.com.
Servidor:  [10.33.13.2]
Address:  10.33.13.2

Nombre:  windows10.daw213.iesldv.com
Address:  10.33.13.4
Aliases:  www.daw213.iesldv.com

> dns1.daw213.iesldv.com.
Servidor:  [10.33.13.2]
Address:  10.33.13.2

Nombre:  wserver.daw213.iesldv.com
Address:  10.33.13.3
Aliases:  dns1.daw213.iesldv.com

> crism.daw213.iesldv.com.
Servidor:  [10.33.13.2]
Address:  10.33.13.2

Nombre:  windows10.daw213.iesldv.com
Address:  10.33.13.4
Aliases:  crism.daw213.iesldv.com
```

Y comprobamos la zona inversa:

```
> 10.33.13.1
Servidor:  [10.33.13.2]
Address:  10.33.13.2

Nombre:  ipcop.daw213.iesldv.com
Address:  10.33.13.1

> 10.33.13.2
Servidor:  [10.33.13.2]
Address:  10.33.13.2

Nombre:  ubuntu.daw213.iesldv.com
Address:  10.33.13.2

> 10.33.13.3
Servidor:  [10.33.13.2]
Address:  10.33.13.2

Nombre:  wserver.daw213.iesldv.com
Address:  10.33.13.3

> 10.33.13.4
Servidor:  [10.33.13.2]
Address:  10.33.13.2

Nombre:  windows10.daw213.iesldv.com
Address:  10.33.13.4
```