Aitor Pascual Jiménez
Despligue de aplicaciones
2º Daw

Práctica: Configuración Ubuntu Server como DNS.

Tras instalar bind9 junto a sus utilidades, habilitamos el tráfico del servicio en el cortafuegos.

```
vboxuser@ubuntu-despliegue:~$ sudo ufw allow bind9
Reglas actualizadas
Reglas actualizadas (v6)
```

Comprobamos que funciona correctamente.

```
vboxuser@ubuntu-despliegue:/etc/default$ sudo systemctl restart ufw
vboxuser@ubuntu-despliegue:/etc/default$ sudo systemctl status ufw
● ufw.service - Uncomplicated firewall
     Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled)
     Active: active (exited) since Fri 2024-10-04 10:05:26 CEST; 22s ago
       Docs: man:ufw(8)
    Process: 4033 ExecStart=/lib/ufw/ufw-init start quiet (code=exited, status=0/SUCCESS)
   Main PID: 4033 (code=exited, status=0/SUCCESS)
        CPU: 5ms

oct. 04 10:05:26 ubuntu-despliegue systemd[1]: Starting Uncomplicated firewall...
oct. 04 10:05:26 ubuntu-despliegue systemd[1]: Finished Uncomplicated firewall.
```

Para forzar que nuestro DNS solo use ipv4.

```
vboxuser@ubuntu-despliegue:/etc/default$ ls -la named  Listamos los permisos de named
-rw-r--r-- 1 root root 86 oct.   4 10:09 named
vboxuser@ubuntu-despliegue:/etc/default$ sudo chmod 777 named Cambiamos temporalmente los permisos
vboxuser@ubuntu-despliegue:/etc/default$ sudo vim named  Editamos el archivo para añadir -4 y
vboxuser@ubuntu-despliegue:/etc/default$ cat n            forzar que solo use ipv4
named                networkd-dispatcher
vboxuser@ubuntu-despliegue:/etc/default$ cat named
#
# run resolvconf?
RESOLVCONF=no

# startup options for the server
OPTIONS="-u bind -4"
vboxuser@ubuntu-despliegue:/etc/default$ sudo chmod 644 named Restablecemos los permisos
```

Si nos vamos a /etc/bind/named.conf vemos que el propio archivo nos manda a tomar viento y realizar las configuraciones en otros 3 archivos.

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

Aitor Pascual Jiménez
Despligue de aplicaciones
2º Daw

Si nos vamos a ver al archivo .options (después de hacer su copia de seguridad), vemos que nos encontramos una configuración muy escasa por defecto.

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        listen-on-v6 { any; };
};
```

Podemos encontrar todas las opciones de configuración en la wiki de debian.

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        listen-on {
                any;
        };
        allow-query {
                localhost;
                172.16.3.0/24;
        };
        forwarders {
                8.8.8.8;
        };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation no;
        listen-on-v6 {
                none;
        };
};
```

Interfaces de red por las que escuchamos

Permitimos consultas de:
En este caso de nosotros y de todo el que se encuentre en este rango de red

En caso de no tener respuesta, preguntamos a este DNS (perteneciente a google)

No hacemos validaciones con el protocolo dnssec (Corremos el riesgo de que suplanten nuestro DNS)

Deshabilitamos la escucha en ipv6

Como funciona dnssec link.

Aitor Pascual Jiménez
Despligue de aplicaciones
2º Daw

Si checkeamos la configuración con named-checkconf y no recibimos ningún output es que todo está correcto.

```
vboxuser@ubuntu-despliegue:/etc/bind$ sudo named-checkconf
vboxuser@ubuntu-despliegue:/etc/bind$
```

Para cambiar la ip dinámica y dejarla estática en esta versión de ubuntu, debemos entrar en el directorio /etc/netplan donde encontraremos un fichero con extensión yaml que debemos editar.

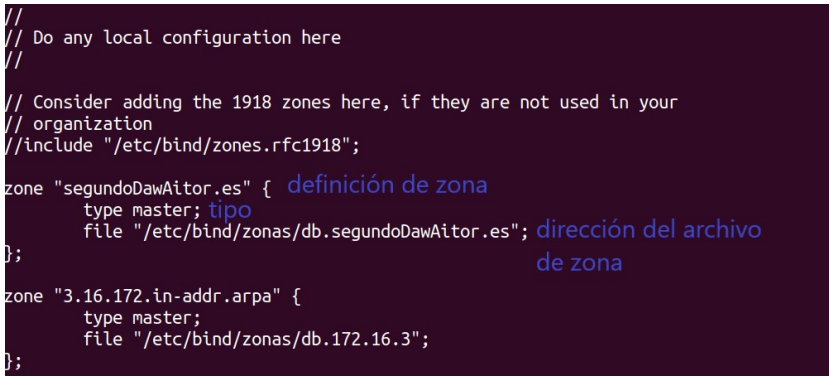
Este es el archivo antes de la edición.

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
```

Así nos debe quedar.

Hacemos “sudo netplan try” y “sudo netplan apply” para aplicar la configuración.

Para crear nuestras zonas, primero deberemos editar el archivo de configuración que se encuentra en “/etc/bind/named.conf.local” (después de hacer su copia de seguridad).



La resolución inversa tiene que tener esa sintaxis, al revés y sin el último octeto.

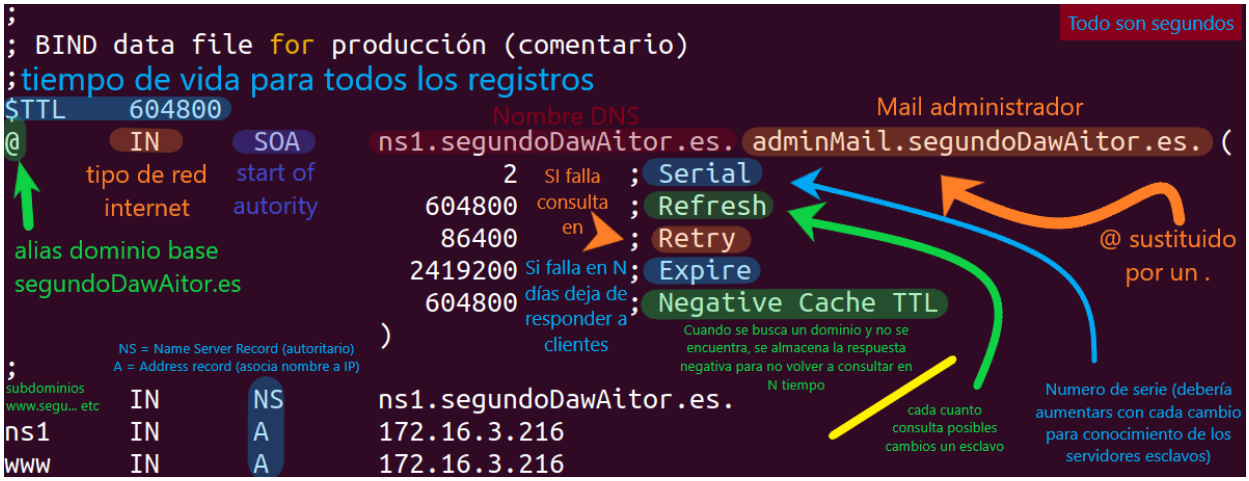
Aitor Pascual Jiménez
Despligue de aplicaciones
2º Daw

```
vboxuser@ubuntu-despliegue:/etc/bind/zonas$ sudo named-checkconf
vboxuser@ubuntu-despliegue:/etc/bind/zonas$
```

Comprobamos que el archivo esté bien.Seguidamente, creamos los archivos en las rutas que hemos especificado.

```
vboxuser@ubuntu-despliegue:/etc/bind$ sudo mkdir zonas
[sudo] contraseña para vboxuser:
vboxuser@ubuntu-despliegue:/etc/bind$ cd zonas/
vboxuser@ubuntu-despliegue:/etc/bind/zonas$ ls
vboxuser@ubuntu-despliegue:/etc/bind/zonas$ sudo touch db.segundoDawAitor.es db.172.16.3
vboxuser@ubuntu-despliegue:/etc/bind/zonas$ ls
db.172.16.3  db.segundoDawAitor.es
```

En los ficheros de zona debemos usar esta sintaxis.




```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.segundoDawAitor.es. adminMail.segundoDawAitor.es. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800         ; Negative Cache TTL
                        )
;
@       IN      NS      ns1.segundoDawAitor.es.
1       IN      PTR     www.deawtx.es.
```

Comprobamos con named-checkzone

```
vboxuser@ubuntu-despliegue:/etc/bind/zonas$ sudo named-checkzone db.172.16.3 /etc/bind/zonas/db.172.16.3
zone db.172.16.3/IN: loaded serial 2
OK
vboxuser@ubuntu-despliegue:/etc/bind/zonas$ sudo named-checkzone db.segundoDawAitor.es /etc/bind/zonas/db.segundoDawAitor.es
zone db.segundoDawAitor.es/IN: loaded serial 2
OK
```

Aitor Pascual Jiménez
Despligue de aplicaciones
2º Daw

Lanzamos el restart.

```
vboxuser@ubuntu-despliegue:/etc/bind/zonas$ sudo systemctl restart bind9
vboxuser@ubuntu-despliegue:/etc/bind/zonas$ sudo systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-10-14 13:41:45 CEST; 6s ago
```

Probamos que todo esté correcto con nslookup.

```
vboxuser@ubuntu-despliegue:/etc/bind/zonas$ nslookup
> www.segundoDawAitor.es
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.segundoDawAitor.es
Address: 172.16.3.216
> 172.16.3.216
216.3.16.172.in-addr.arpa       name = ubuntu-despliegue.
216.3.16.172.in-addr.arpa       name = ubuntu-despliegue.local.
```

Aitor Pascual Jiménez
Despligue de aplicaciones
2º Daw

CUESTIONARIO

Cuestión 1 ¿Qué pasará si un cliente de una red diferente a la tuya intenta hacer uso de tu DNS de alguna manera, le funcionará?¿Por qué, en qué parte de la configuración puede verse?

- No responderá ya que solo permitimos consultas de nosotros y nuestra red, podemos verlo en el “named.conf.options”.

Cuestión 3 El servidor DNS que acabáis de montar, ¿es autoritativo? ¿Por qué?

- Si, porque no depende de que otro servidor le proporcione las direcciones, si no que las tiene el mismo configuradas.

Cuestión 4 ¿Dónde podemos encontrar la directiva $ORIGIN y para qué sirve?

- Nos la encontramos en los registros de zona, es una constante que añade el nombre de dominio al final de cada nombre que no acabe en punto, si tenemos www, ftp, mail y $ORIGIN vale “miclase.com”, se añadirá al final de cada nombre.

Cuestión 5 ¿Una zona es idéntico a un dominio?

- No, un dominio puede englobar N zonas.

Cuestión 6 ¿Pueden editarse los archivos de zona de un servidor esclavo/secundario?

- No, los archivos que recive de un servidor primario son de solo lectura.

Cuestión 7 ¿Por qué podría querer tener más de un servidor esclavo para una misma zona?

- Para balancear la carga y reducir el tiempo de respuesta al recibir muchas peticiones.
- Por si un servidor falla o está en mantenimiento, no tener que interrumpir el servicio.

Cuestión 8 ¿Cuántos servidores raíz existen?

- Existen 13 servidores raíz (localizados en su mayoría en los Estados Unidos).

Cuestión 9 ¿Qué es una consulta iterativa de referencia?

- El servidor DNS nos dice a que otros servidores podemos preguntarle para obtener una respuesta.

Cuestión 10 En una resolución inversa, ¿a qué nombre se mapearía la dirección IP 172.16.34.56?

- En el caso de existir un dominio en esa IP, nos devolvería su nombre, pero dado que esa IP entra en las privadas de clase B, al estar en el rango entre 172.16.0.0 – 172.31.255.255 y no tenemos ningún dominio en esa IP, nos devolverá non-existain domain.