

Práctica: Configuración Ubuntu Server como DNS.

Bind es el estándar de facto para servidores DNS. Es una herramienta de software libre y se distribuye con la mayoría de plataformas Unix y Linux, donde también se le conoce con el sobrenombre de **named** (name daemon). Bind9 es la versión recomendada para usarse y es la que emplearemos.

1. Primero actualizar Ubuntu Server:

```
$ sudo apt update
```

```
$ sudo apt upgrade
```

2. Para instalar el servidor DNS en Ubuntu Server, usaremos los repositorios oficiales. Por ello, podremos instalarlo como cualquier paquete en Ubuntu:

```
$ sudo apt-get install bind9 bind9-utils
```

3. Para permitir el tráfico hay que abrir el Firewall (ufw)

```
$ sudo ufw status (mira el estado, si está inactivo hay que activarlo para bind)
```

```
$ sudo ufw allow bind9
```

```
$ sudo systemctl status bind9 (mira si el servicio ya está activo)
```

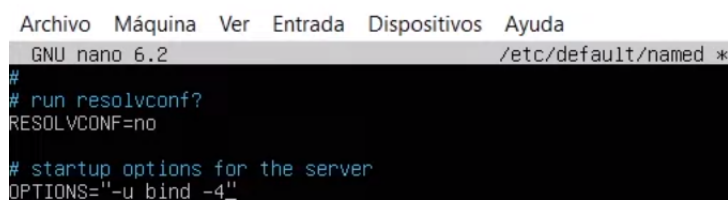
Configuración del servidor

Puesto que en clase sólo vamos a utilizar IPv4, vamos a decírselo a Bind, en su archivo general de configuración. Este archivo **named** se encuentra en el directorio:

`/etc/default`

Y para indicarle que sólo use IPv4, debemos modificar la línea siguiente:

```
OPTIONS = "-u bind -4"
```



```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 6.2 /etc/default/named *
#
# run resolvconf?
RESOLVCONF=no
# startup options for the server
OPTIONS="-u bind -4_
```

El archivo de configuración principal **named.conf** de Bind está en el directorio:

`/etc/bind`

Si lo consultamos veremos lo siguiente:

```
// 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";
~
```

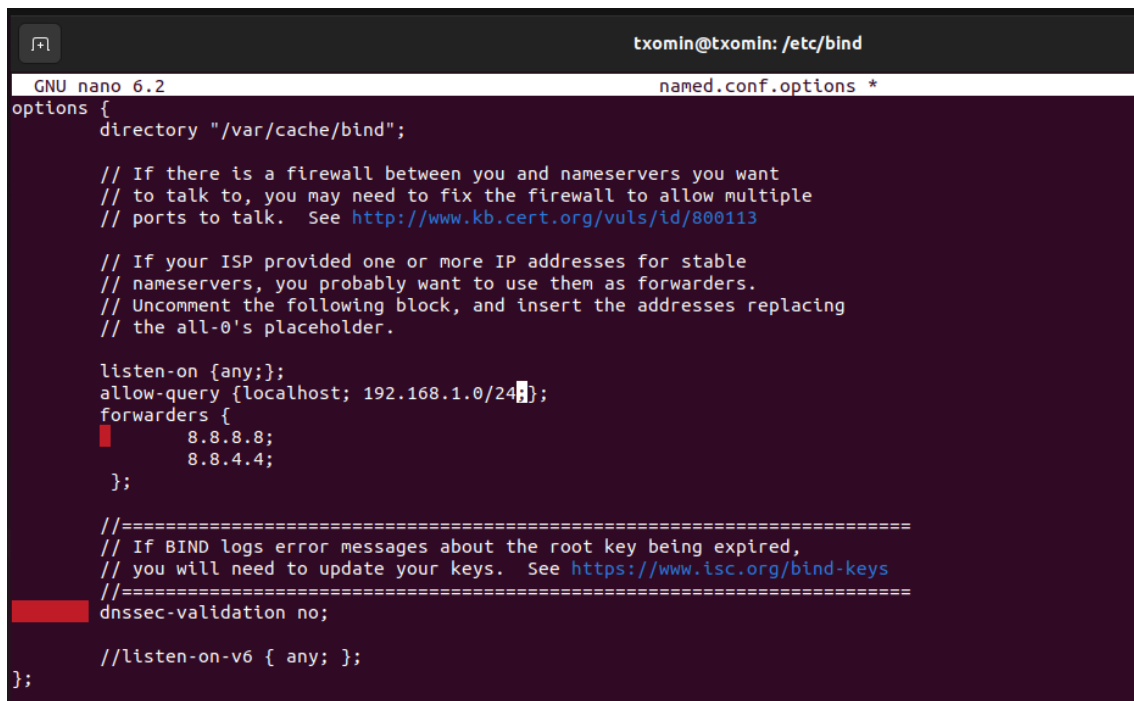
Este archivo sirve simplemente para aglutinar o agrupar a los archivos de configuración que usaremos. Estos 3 includes hacen referencia a los 3 diferentes archivos donde deberemos realizar la verdadera configuración, ubicados en el mismo directorio.

configuración *named.conf.options*

Es una buena práctica que hagáis siempre una copia de seguridad de un archivo de configuración cada vez que vayáis a realizar algún cambio:

```
$sudo cp /etc/bind/named.conf.options /etc/bind/named.conf.options.backup
```

Ahora editaremos el archivo *named.conf.options* e incluiremos los siguientes contenidos:



```
txomin@txomin: /etc/bind
GNU nano 6.2 named.conf.options *
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; 192.168.1.0/24;};
    forwarders {
        8.8.8.8;
        8.8.4.4;
    };

    //=====
    // 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 { any; };
};
```

Si nos fijamos el servidor por defecto ya viene configurado para ser un DNS caché. El directorio donde se cachearán o guardarán las zonas es */var/cache/bind*.

/var/cache/bind

Además, vamos a comentar la línea que pone *listen-on-v6 { any; };* puesto que no vamos a responder a consultas de IPv6. Para comentarla basta añadir al principio de la línea dos barras //. También podría hacerse con una almohadilla pero aparecería resaltado con color

ya que estos comentarios los suele utilizar el administrador para aclarar algún aspecto de la configuración.

Chequeamos que todo esté correcto:

```
$ sudo named-checkconf
```

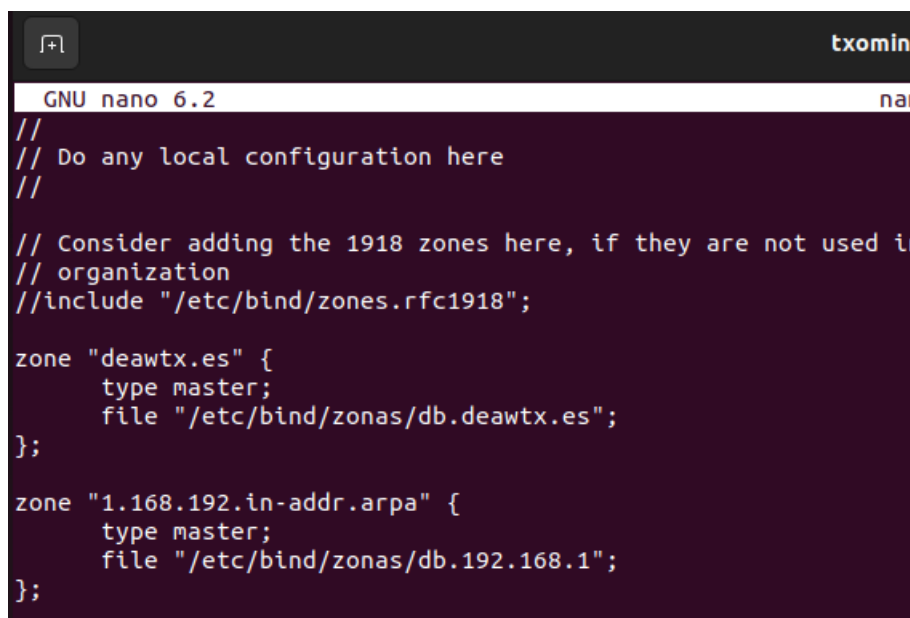
Reinicializamos el servicio bind9

```
$ sudo systemctl restart bind9
```

```
$ sudo systemctl status bind9
```

configuración *named.conf.local* (creación de zonas)

En este archivo configuraremos aspectos relativos a nuestras zonas. Vamos a declarar la zona “deawtx.es” (poned el vuestro propio) y su resolución inversa. Por ahora simplemente indicaremos que el servidor DNS es maestro para esta zona y dónde estarán ubicados los archivos de zona que crearemos más adelante:



```
GNU nano 6.2
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in
// organization
//include "/etc/bind/zones.rfc1918";

zone "deawtx.es" {
    type master;
    file "/etc/bind/zonas/db.deawtx.es";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zonas/db.192.168.1";
};
```

Vamos a crear el archivo de zona de resolución directa justo en el directorio que hemos indicado antes y con el mismo nombre que hemos indicado antes.

```
$ mkdir zonas
```

El contenido será algo así (procurad respetar el formato):

```

txomin@
GNU nano 6.2
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns1.deawtx.es. admin.deawtx.es. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
ns1        IN      NS       ns1.deawtx.es.
www        IN      A        192.168.1.56

```

Recordad que los registros SOA son para detallar aspectos de la zona autoritativa, los NS para indicar los servidores DNS de la zona y los A las IPs respectivas.

Creación del archivo de zona para la resolución inversa

Recordad que deben existir ambos archivos de zona, uno para la resolución directa y otro para la inversa. Vamos pues a crear el archivo de zona inversa.

```

txomin@txo
GNU nano 6.2
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns1.deawtx.es. admin.deawtx.es. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       ns1.deawtx.es.
1         IN      PTR      www.deawtx.es.

```

Comprobación de las configuraciones

Para comprobar la configuración de la zona de resolución directa:

```
$ sudo named-checkzone db.deawtx.es /etc/bind/zonas/db.deawtx.es
```

Y para comprobar la configuración de la zona de resolución inversa:

```
$ sudo named-checkzone 1.168.192 /etc/bind/zonas/db.192.168.1
```

Si todo está bien, devolverá OK. En caso de haber algún error, nos informará de ello.

Reiniciamos el servicio y comprobamos el estado.

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?

Cuestión 3

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

Cuestión 4

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

Cuestión 5

¿Una zona es idéntico a un dominio?

Cuestión 6

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

Cuestión 7

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

Cuestión 8

¿Cuántos servidores raíz existen?

Cuestión 9

¿Qué es una consulta iterativa de referencia?