

# PRÁCTICA 5.1: Servicio DNS en LINUX usando bind9

Alejandro Priego Izquierdo

## 1. Tipos de servicio DNS.

### 1.1. Explica si has montado un servicio DNS maestro, caché o esclavo.

El servicio DNS montado funciona como maestro ya que apuntaremos a varias Ips para diferentes servicios y será en el único lugar donde aparezca esta referencia.

### 1.2. Explica esta frase: “El servicio Bind no sustituye a servidores DNS como los que podemos usar de Google (8.8.8.8), Cloudflare (1.1.1.1) u otros, sino que se complementa con ellos”

Se refiere a que los servicios como Google o Cloudflare que almacenan de forma masiva las resoluciones DNS correspondientes a millones de Ips, las cuales se actualizaon constantemente. Esto sería ineficiente e inutil guardarlo de forma local, ya que la mejora de rendimiento sería mínima. Entonces, nuestro servicio Bind nos servirá para redireccionar a las personas de nuestra red a servicios o aplicaciones locales dentro de nuestra red.

### 1.3. Busca en tu sistema el archivo /etc/hosts y explica que tiene en común con un servicio de resolución de nombres.

Este archivo nos permite establecer una serie de “alias” a diferentes direcciones IP. Esto solo afectará al sistema de forma local.

## 2. Instalar y configurar el servicio DNS en Ubuntu Server.

### 2.1. Instalar un servidor DNS en Ubuntu Server usando bind9.

- Comprueba si tienes el servicio instalado:

```
apriego@priegoDAWServer:~$ dpkg -l bind9
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name           Version           Architecture Description
+++-----+-----+-----+-----+
ii bind9           1:9.18.18-0ubuntu0.22.04.1 amd64        Internet Domain Name Server
```

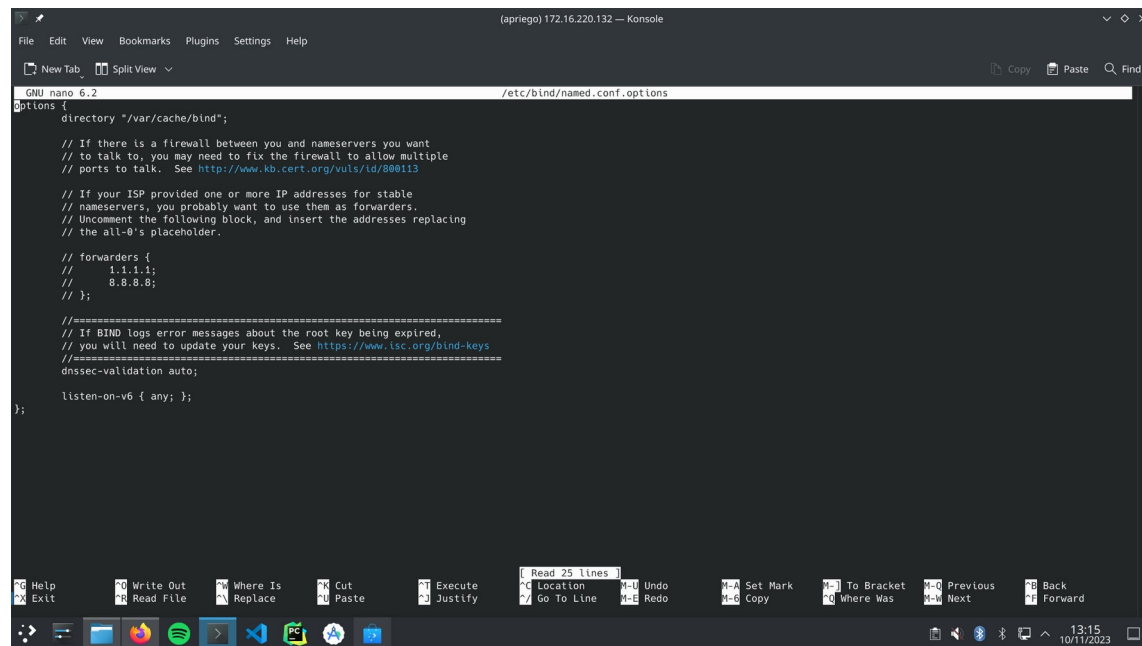
-Comprueba el estado del servicio. Debe estar activo:

```
apriego@priegoDAWServer:~$ systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-11-23 07:45:59 UTC; 28min ago
     Docs: man:named(8)
  Process: 865 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 921 (named)
    Tasks: 4 (limit: 2178)
   Memory: 10.5M
      CPU: 272ms
   CGroup: /system.slice/named.service
           └─921 /usr/sbin/named -u bind

Nov 23 07:46:03 priegoDAWServer named[921]: network unreachable resolving './NS/IN': 2001:500:2::c#53
Nov 23 07:46:03 priegoDAWServer named[921]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
Nov 23 07:46:03 priegoDAWServer named[921]: network unreachable resolving './NS/IN': 2001:dc3::35#53
Nov 23 07:46:03 priegoDAWServer named[921]: network unreachable resolving './NS/IN': 2001:500:1::53#53
Nov 23 07:46:03 priegoDAWServer named[921]: network unreachable resolving './NS/IN': 2001:7fe::53#53
Nov 23 07:46:03 priegoDAWServer named[921]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
Nov 23 07:46:03 priegoDAWServer named[921]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
Nov 23 07:46:03 priegoDAWServer named[921]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Nov 23 07:46:03 priegoDAWServer named[921]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
Nov 23 07:46:03 priegoDAWServer named[921]: resolver priming query complete: success
```

## 2.2 Configurar los forwarders de Bind usando servidores DNS públicos.

Lo primero que vamos a hacer es configurar unos servidores DNS de forwarding, es decir, los servidores DNS públicos para reenviar las consultas de cara a Internet. El archivo de configuración que se encarga de esta tarea es «named.conf.options»



```
GNU nano 6.2 /etc/bind/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.

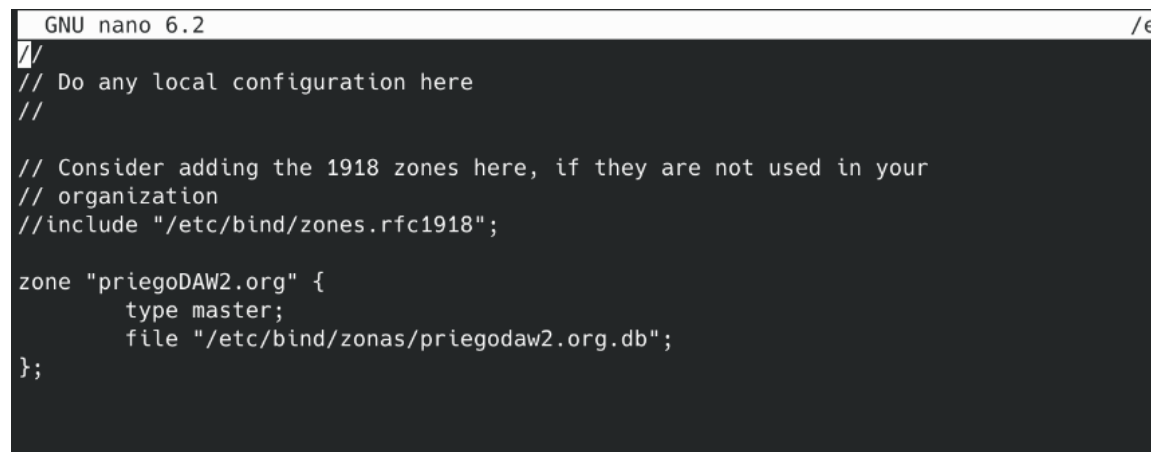
    // forwarders {
    //     1.1.1.1;
    //     8.8.8.8;
    // };

    //=====
    // 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 auto;

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

## 2.3 Configura un DNS maestro creando un dominio ficticio(zona) llamado tuapellidoDAW2.org

A. - Configura el archivo principal /etc/bind/named.conf.local donde se indica los nombres de las zonas de las que este servidor va a tener “autoridad”. Observa que también hay que indicar dónde estarán archivos de configuración de cada zona que se defina.

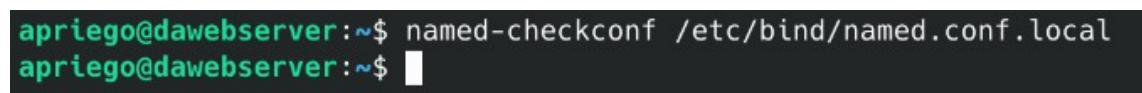


```
GNU nano 6.2 /e
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "priegoDAW2.org" {
    type master;
    file "/etc/bind/zonas/priegodaw2.org.db";
};
```

B. Comprueba la sintaxis correcta del fichero con el comando named-checkconf.



```
apriego@dawebserver:~$ named-checkconf /etc/bind/named.conf.local
apriego@dawebserver:~$
```

- C. Crear el archivo de zona directa (en la foto anterior es sanchezromero.db)
- D. Añade registros para cada servicio

```
apriego@priegoDAWServer:~$ cat /etc/bind/priegodaw2.db
;
; BIND reverse data file for local loopback interface
;
$ORIGIN priegoDAW2.org.
$TTL      604800
@         IN      SOA      priegoDAWServer. root. (
                                4          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
; Registro ns
@         IN      NS       priegoDAWServer.
priegoDAWServer IN    A      192.168.131.1
dns       IN      A        192.168.131.1
www       IN      A        192.168.131.1
ftp       IN      A        192.168.131.1
@         IN      AAAA     ::1
```

- E. Comprueba la sintaxis correcta de los ficheros con el comando named-checkzone nombre\_zona fichero\_de\_zona.

```
apriego@priegoDAW2:~$ named-checkzone priegodaw2.org /etc/bind/priegodaw2.org.db
zone priegodaw2.org/IN: loaded serial 3
OK
```

#### 2.4. Configura el archivo /etc/resolv.conf para el servidor.

Este archivo indica a la máquina quien es el servidor DNS en la red. El servidor en tu caso es también el propio servidor DNS por lo que tendrá que aparecer (127.0.0.1)

```
apriego@priegoDAWServer:~$ cat /etc/resolv.conf
search priegoDAW2.org
domain priegoDAW2.org
nameserver 127.0.0.1
```

2.5. Contesta ahora las siguientes preguntas y repasa con ello que todo está configurado en el apartado anterior.

- ¿Qué hay en el fichero /etc/hostname del server?

```
apriego@priegoDAWServer:~$ cat /etc/hostname
priegoDAWServer
```

- ¿Qué has añadido al fichero /etc/bind/named.conf.local?

```
apriego@priegoDAWServer:~$ cat /etc/bind/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 "priegoDAW2.org" {
    type master;
    file "/etc/bind/priegodaw2.db";
};

zone "1.131.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/192.rev";
};
```

- ¿Qué nuevo fichero has creado para la búsqueda directa?  
priegodaw2.db
- ¿Qué orden has usado para comprobar que no hay errores de sintaxis ?  
named-checkconf /ruta/a/fichero
- ¿Qué has añadido al fichero /etc/resolv.conf del servidor? Asegurate que incluyes "search".

```
apriego@priegoDAWServer:/etc/bind$ cat /etc/resolv.conf
search priegoDAW2.org
domain priegoDAW2.org
nameserver 127.0.0.1
```

- ¿Qué has añadido al fichero /etc/resolv.conf del cliente? Asegurate que incluyes "search".

```
priegodaw@lubuntuclient:~$ cat /etc/resolv.conf
search priegoDAW2.org
domain priegoDAW2.org
nameserver 192.168.131.1
```

### 3. Comprueba el buen funcionamiento del servicio.

Haz consultas al servidor DNS mediante el comando `host`, `dig` o `nslookup` y comprueba su correcto funcionamiento tanto resolviendo nombres por búsqueda directa como inversa y tanto para máquinas locales como para externas.

#### 3.1. PRUEBAS 1: Resuelve `www.tuapellidoDAW2.org` y `ftp.tuapellidoDAW2.org` \$ `nslookup www.tuapellidoDAW2.org`

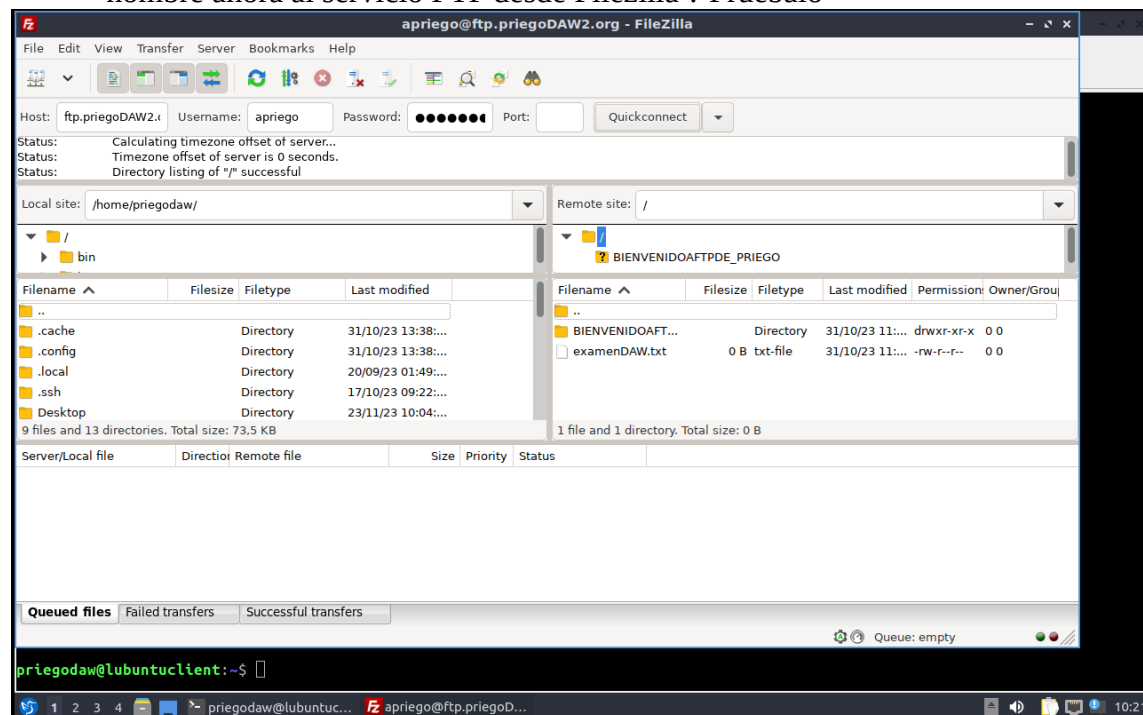
```
apriego@priegoDAWServer:/etc/bind$ nslookup www.priegoDAW2.org
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:   www.priegoDAW2.org
Address: 192.168.131.1

apriego@priegoDAWServer:/etc/bind$ nslookup ftp.priegoDAW2.org
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:   ftp.priegoDAW2.org
Address: 192.168.131.1
```

#### 3.2. PRUEBA 2: Si ya tienes montado el servicio FTP en el server. ¿cómo accederías por nombre ahora al servicio FTP desde Filezilla ? Pruebalo



3.3. PRUEBA 3: resolver "www.xataka.com". ¿Qué mensaje te devuelve el servicio? Captura y Explica lo que significa con tus palabras.

```
apriego@priegoDAWServer:/etc/bind$ nslookup www.xataka.com
Server:          127.0.0.1
Address:         127.0.0.1#53

Non-authoritative answer:
www.xataka.com  canonical name = d2t8dj4tr3q9od.cloudfront.net.
Name:   d2t8dj4tr3q9od.cloudfront.net
Address: 18.154.48.114
Name:   d2t8dj4tr3q9od.cloudfront.net
Address: 18.154.48.68
Name:   d2t8dj4tr3q9od.cloudfront.net
Address: 18.154.48.42
Name:   d2t8dj4tr3q9od.cloudfront.net
Address: 18.154.48.123
```

Vemos que a ese dominio le corresponden esas 4 Ips, en caso de que la primera falle se usaría la segunda y así sucesivamente. Vemos que esto es gestionado por Cloudfront, un servicio de AWS.

3.4. PRUEBA 4: Comprueba ahora que sin indicar el dominio también te resuelve el nombre gracias a la línea 'search' con el dominio por defecto a buscar que metiste en /etc/resolv.conf. Resolver : \$ nslookup ftp

```
apriego@priegoDAWServer:/etc/bind$ nslookup www
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:   www.priegoDAW2.org
Address: 192.168.131.1

apriego@priegoDAWServer:/etc/bind$ nslookup ftp
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:   ftp.priegoDAW2.org
Address: 192.168.131.1
```



3.5. Comprueba como el servidor DNS funciona como DNS caché mejorando los tiempos de respuesta en la segunda y posteriores búsquedas de un nombre. P.ej. usa el comando dig para resolver la dirección `www.iesgrancapitan.org` y observa el tiempo que tarda. Repítelo y comprueba cuánto ha mejorado. ¿A qué se debe?

```
apriego@priegoDAWServer:/etc/bind$ dig www.iesgrancapitan.org

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> www.iesgrancapitan.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16063
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 946bab81936e070701000000655f1c24ef6007e391426fdb (good)
;; QUESTION SECTION:
;www.iesgrancapitan.org.                IN      A

;; ANSWER SECTION:
www.iesgrancapitan.org. 6048     IN      A      89.248.100.49

;; Query time: 232 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu Nov 23 09:32:20 UTC 2023
;; MSG SIZE rcvd: 95

apriego@priegoDAWServer:/etc/bind$ dig www.iesgrancapitan.org

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> www.iesgrancapitan.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27351
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: e99113dc141fb17101000000655f1c268a1a55f174500037 (good)
;; QUESTION SECTION:
;www.iesgrancapitan.org.                IN      A

;; ANSWER SECTION:
www.iesgrancapitan.org. 6046     IN      A      89.248.100.49

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu Nov 23 09:32:22 UTC 2023
;; MSG SIZE rcvd: 95
```

El tiempo pasa de 232msec a 0, ya que no necesita consultar a que IP apunta ese dominio.



#### 4. Evitar cambio automático de resolv.conf al cambiar de red y servidor DHCP.

```
apriego@priegoDAWServer:/etc/bind$ sudo systemctl status systemd-resolved.service
[sudo] password for apriego:
○ systemd-resolved.service - Network Name Resolution
   Loaded: loaded (/lib/systemd/system/systemd-resolved.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:systemd-resolved.service(8)
           man:org.freedesktop.resolve1(5)
           https://www.freedesktop.org/wiki/Software/systemd/writing-network-configuration-managers
           https://www.freedesktop.org/wiki/Software/systemd/writing-resolver-clients
```

#### 5. Configuración y prueba de zona inversa.

```
apriego@priegoDAWServer:/etc/bind$ cat ./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 "priegoDAW2.org" {
    type master;
    file "/etc/bind/priegodaw2.db";
};

zone "1.131.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/priegodaw2.rev";
};
```

```

GNU nano 6.2
;
; BIND reverse data file for local loopback interface
;
$ORIGIN 1.131.168.192.in-addr.arpa.
$TTL      604800
@          IN      SOA      priegoDAWServer. root. (
                                1          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@          IN      NS       priegoDAW2.org.
1          IN      PTR      priegoDAW2.org.

```

```

apriego@priegoDAWServer:/etc/bind$ dig -x 192.168.131.1
; <<> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<> -x 192.168.131.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45706
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 03376dcf1864254b01000000655f2029dfaacf053b5f226f (good)
;; QUESTION SECTION:
;1.131.168.192.in-addr.arpa.      IN      PTR

;; AUTHORITY SECTION:
1.131.168.192.in-addr.arpa. 604800 IN      SOA      priegoDAWServer. root. 1 604800 86400 2419200 604800

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu Nov 23 09:49:29 UTC 2023
;; MSG SIZE rcvd: 138

apriego@priegoDAWServer:/etc/bind$

```

