

Sumario

Actividad 1.....2

Configuración de un servidor maestro.....3

Actividad 2.....5

 Ejercicio 1.....5

 Ejercicio 2.....5

Actividad 1.

Instala el servidor Bind9, edita el fichero `/etc/bind/named.conf.options` y configura como servidor de reenvío el servidor DNS abierto de google (ip -> 8.8.8.8), para las zonas que no administre nuestro servidor:

```
forwarders {  
    8.8.8.8;  
};
```

Comprueba que tu DNS está funcionando como caché. Para ello, realiza resoluciones de nombres de dominio de Internet con el comando `dig`, y comprueba el tiempo que tardan. ¿Qué debe ocurrir si nuestro DNS está funcionando como caché?

```
laura@laura-VirtualBox:~/Escritorio$ sudo apt install bind9 bind9-doc dnsutils
```

```
laura@laura-VirtualBox: /etc/bind
laura@laura-VirtualBox: /etc/bind 80x24
GNU nano 6.2 named.conf.options *
tions {
    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 {
        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
    //=====
```

```
laura@laura-VirtualBox: /etc/bind 80x40
laura@laura-VirtualBox: /etc/bind$ dig www.google.com

; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 31957
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.                0      IN      A      216.58.215.164

;; Query time: 27 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Feb 08 19:54:34 CET 2023
;; MSG SIZE rcvd: 59

laura@laura-VirtualBox: /etc/bind$ dig www.google.com

; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 60957
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.                0      IN      A      216.58.215.164

;; Query time: 11 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Feb 08 19:54:37 CET 2023
;; MSG SIZE rcvd: 59
```

El tiempo de query es de 27ms en la primera llamada y de 11ms en la segunda. Esto es debido a que tenemos la caché activada.

Configuración de un servidor maestro

Hemos creado el fichero db.ddaw.lan y usado el comando named-checkzone para añadirlo.

```
laura@laura-VirtualBox: /etc/bind
laura@laura-VirtualBox: /etc/bind 80x40
GNU nano 6.2 db.ddaw.lan
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns1.ddaw.lan. admin.ddaw.lan. (
                        1      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       ns1.ddaw.lan.
@         IN      NS       ns2.ddaw.lan.
ns1       IN      A        172.16.211.2
ns2       IN      A        172.16.211.3
www       IN      A        172.16.211.1
@         IN      MX       1 mail.ddaw.lan.
mail      IN      A        172.16.211.10

laura@laura-VirtualBox:/etc/bind$ sudo named-checkzone ddaw.lan /etc/bind/db.ddaw.lan
zone ddaw.lan/IN: loaded serial 1
OK
```

Comprobamos si el servidor de nombres es capaz de proporcionarnos la ip de los registros que acabamos de configurar con dig

```
laura@laura-VirtualBox:/etc/bind$ dig @127.0.0.1 www.ddaw.lan

;<<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> @127.0.0.1 www.ddaw.lan
; (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50783
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 1232
; COOKIE: cc71d1a0b6df884d0100000063e3f3b38eb0da993cad53e6 (good)
; QUESTION SECTION:
; www.ddaw.lan.                IN      A

; ANSWER SECTION:
www.ddaw.lan.                604800  IN      A      172.16.211.1

; Query time: 0 msec
; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
; WHEN: Wed Feb 08 20:10:43 CET 2023
; MSG SIZE rcvd: 85
```

En efecto, es correcto.

Para configurar la resolución inversa tendremos que dar de alta una nueva zona en el archivo `named.conf.local` dentro del dominio especial `in-addr.arpa` y que corresponde a la red `172.16.211.0/24`

```
GNU nano 6.2 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 "ddaw.lan" in { //La zona es ddaw.lan
    type master; //Este servidor será primario para la zona
    file "/etc/bind/db.ddaw.lan"; //fichero de registros de zona
};
zone "211.16.172.in-addr.arpa" in {
    type master;
    file "/etc/bind/db.211.16.172
};
```

Creamos el fichero `db.211.16.172` y damos de alta los registros de recursos que necesitamos.

```
laura@laura-VirtualBox: /etc/bind
laura@laura-VirtualBox: /etc/bind 80x40
GNU nano 6.2 db.211.16.172 *
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns1.ddaw.lan. admin.ddaw.lan. (
                        1      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       ns1.ddaw.lan.
@         IN      NS       ns2.ddaw.lan.
1         IN      PTR      www.ddaw.lan.
10        IN      PTR      mail.ddaw.lan.
2         IN      PTR      ns1.ddaw.lan.
3         IN      PTR      ns2.ddaw.lan.
```

Actividad 2

Ejercicio 1

Investiga la funcionalidad que proporcionan las zonas de búsqueda inversa. Cita un ejemplo de aplicación y/o servicio que haga uso de ellas, y para qué lo utiliza. (0.5 puntos)

Las zonas de búsqueda inversa son un componente importante de la resolución de nombres en internet. En lugar de asociar un nombre de dominio a una IP, una zona de búsqueda inversa hace lo contrario: asocia una dirección IP con un nombre de Host. Esto se suele hacer para los correos electrónicos, cuando se envía un correo los servidores necesitan convertir la dirección IP del destinatario en un nombre de host legible para humanos.

Ejercicio 2

Para revisar que los archivos están bien configurados puedes ayudarte de los comandos `named-checkconf` y `named-checkzone`. Busca información sobre como se utilizan y la función que realiza cada uno de ellos.

```
laura@laura-VirtualBox:/etc/bind$ sudo named-checkzone ddaw.lan /etc/bind/db.127
zone ddaw.lan/IN: loaded serial 1
OK
```

`Named-checkconf` es un comando que se utiliza para verificar la sintaxis de un archivo de configuración de BIND.

`Named-checkzone` es un comando que se utiliza para verificar la integridad de un archivo de zona DNS.