Práctica DNS Esclavo

Trabajo realizado por: David López Saorin

IP servidor DNS primario: 192.168.210.19
IP servidor DNS secundario: 192.168.210.20
IP cliente: 192.168.210.30

Reconfigurando bind9 DNS maestro:

```
david@userver:~$ cat /etc/bind/named.conf.options
        acl "trusted" {
            192.168.210.19;
            192.168.210.20;
            192.168.210.0/24;
};


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.

        recursion yes;
        allow-recursion { trusted; };
        allow-transfer { none; };

        listen-on { 192.168.210.19; };
        allow-query { localhost; 192.168.210.0/24; };
        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 { any; };
};
```

Para empezar, como en la práctica anterior (DNS primario) no implementé algunas líneas de código estudiadas en clase, así que aprovecho esta práctica para reconfigurar el primario y mejorarlo.

En el archivo "/etc/bind/named.conf.options" añado las líneas de "acl 'trusted'" para especificar las IP y red que son de confianza en nuestro entorno de trabajo, que en este caso son: la IP de mi DNS maestro, la IP del DNS esclavo y la dirección de mi red con su respectiva máscara.

Además, estamos desactivando la transferencia de zona por defecto: Habilitamos consultas recursivas (recursion yes;), Permitimos consultas recursivas de la acl de confianza (allow recursion {trusted;};), Deshabilitamos la zona de transferencia por defecto (allow transfer {none;};) y "Escuchamos" nuestra propia IP (listen-on {192.168.210.19;};).

```
david@userver:~$ cat /etc/bind/zones/db.david.vid
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     primary.david.local. root.david.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
; NS records para name servers
                IN      NS      primary.david.local.
                IN      NS      secondary.david.local.

; A records para name servers
primary         IN      A       192.168.210.19
secondary       IN      A       192.168.210.20
cliente0        IN      A       192.168.210.30

; Alias
server          IN      CNAME   primary
```

En el archivo de zona “/etc/bind/zones/db.david.vid” ordeno los “records” que ya habian antes por secciones con comentarios y añado el registro NS “secondary.david.local.” haciendo referencia a mi DNS secundario que crearé más adelante y el registro A que apunta a su dirección IP (192.168.210.20), además cambio la IP de mi cliente a la “.30”, que configuraré más adelante.

```
david@userver:~$ cat /etc/bind/zones/db.210.168.192
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     primary.david.local. root.david.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
; NS records
                IN      NS      primary.david.local.
                IN      NS      secondary.david.local.
;PTR records
19              IN      PTR     primary.david.local
20              IN      PTR     secondary.david.local
30              IN      PTR     cliente0.david.local
```

En el archivo de zona inversa, de nuevo ordeno los registros anteriores con comentarios y añado el NS de DNS secundario y el registro PTR que apunta a esa IP, y por último vuelvo a configurar el número de host de mi cliente.

```
david@userver:~$ 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 "david.vid" IN {
        type master;
        file "/etc/bind/zones/db.david.vid";
        allow-transfer {192.168.210.20; };
};

zone "210.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/zones/db.210.168.192";
        allow-transfer {192.168.210.20; };
};
```

El último paso de mi DNS maestro es añadir una línea más a cada zona, “allow-transfer {ip_DNS_secundario; };” para indicar a quién va pasar la delegación, o sea, a mi DNS secundario.

Breve aclaración de servidor DNS secundario:

El servidor maestro guarda los archivos de zona con la configuración DNS del dominio y maneja las consultas DNS recursivas o iterativas. Por otro lado, el servidor DNS secundario/esclavo almacena temporalmente registros DNS que son transferidos automáticamente desde el servidor BIND Maestro.

Actualización e instalación de bind9 en nuevo Ubuntu Server:

```
david@userversec:~$ sudo apt update && sudo apt install bind9 bind9-utils -y
Obj:1 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Obj:2 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Se pueden actualizar 204 paquetes. Ejecute «apt list --upgradable» para verlos.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
bind9 ya está en su versión más reciente (1:9.18.18-0ubuntu0.22.04.1).
bind9-utils ya está en su versión más reciente (1:9.18.18-0ubuntu0.22.04.1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 204 no actualizados.
```

En una nueva máquina virtual, con la misma configuración de recursos (mínimo), para que sea el nuevo DNS secundario, actualizo los paquetes del sistema e instalo el bind9 y sus utilidades para comenzar luego la configuración del proceso.

Configuración bind9 DNS esclavo:

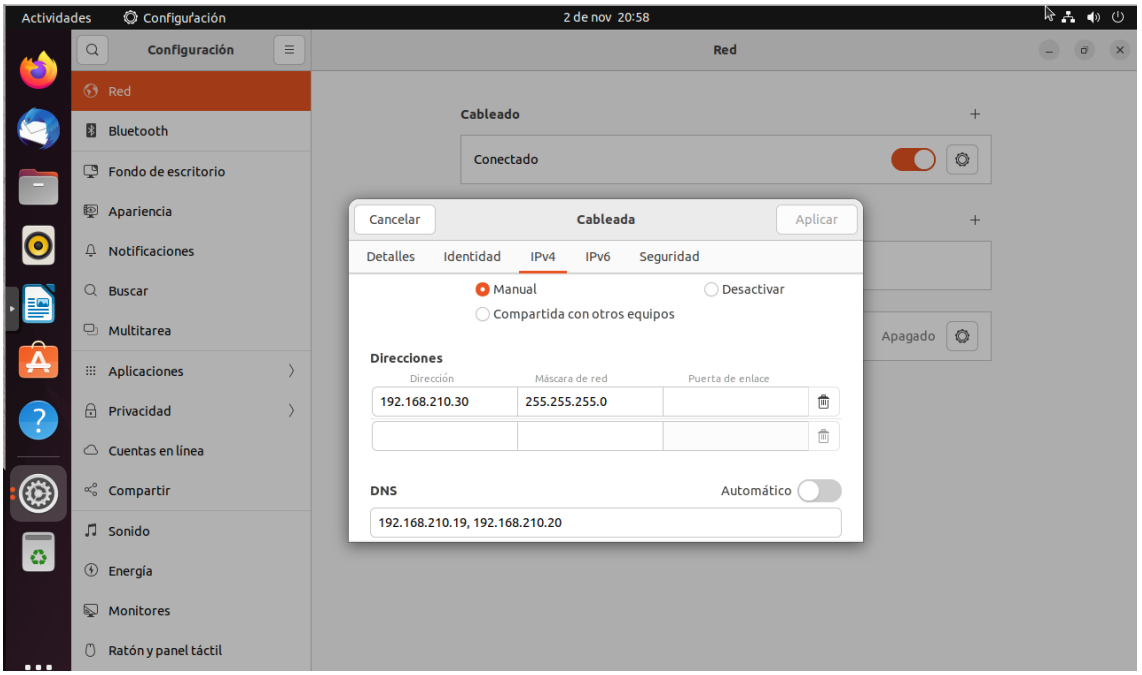
```
david@userversec:~$ cat /etc//bind/named.conf.options
        acl "trusted" {
                192.168.210.19;
                192.168.210.20;
                192.168.210.0/24;
};


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.

        recursion yes;
        allow-recursion { trusted; };
        allow-transfer { none; };

        listen-on { 192.168.210.20; };

        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 auto;

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

La configuración del archivo en “/etc/bind/named.conf.options” es muy similar a la del DNS maestro, la lista de acl de confianza es igual y en el campo de “options” el único parámetro que cambia es el “listen-on {192.168.210.20;};” en el que hay que poner la ip del DNS esclavo.

```
david@userversec:~$ 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 "david.vid" IN {
        type slave;
        file "/etc/bind/zones/db.david.vid";
        masters { 192.168.210.19; };
};

zone "210.168.192.in-addr.arpa" {
        type slave;
        file "/etc/bind/zones/db.192.168.210";
        masters { 192.168.210.19; };
};
```

En este caso, estamos estableciendo las zonas directa e inversa usando el "tipo esclavo" y especificando el servidor DNS Maestro como "192.168.210.19". No hace falta crear un archivo de zona porque los registros y datos DNS se transferirán automáticamente desde el servidor DNS Maestro y se guardarán temporalmente en el servidor DNS secundario/esclavo durante un cierto tiempo.

Reconfiguración del cliente:



Aquí reconfiguro el ubuntu desktop (mi cliente) para que tenga la nueva IP asignada (192.168.210.30) en los servidores DNS, la máscara de red es 255.255.255.0 y como servidores establezco que apunte al primario (192.168.210.19) y al secundario (192.168.210.20).

Verificación de conexión con cliente:

```
david@cliente:~/Escritorio$ host primary.david.vid
primary.david.vid has address 192.168.210.19
david@cliente:~/Escritorio$ host secondary.david.vid
secondary.david.vid has address 192.168.210.20
david@cliente:~/Escritorio$ host cliente0.david.vid
cliente0.david.vid has address 192.168.210.30
david@cliente:~/Escritorio$ dig -x 192.168.210.20

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> -x 192.168.210.20
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45594
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;20.210.168.192.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
20.210.168.192.in-addr.arpa. 604800 IN  PTR     secondary.david.local.210.168.19
2.in-addr.arpa.
```

Con el comando “host” apunto a primary, secondary y cliente0 para probar si resuelven nombres. Y funciona. Además, pruebo con el comando “dig” apuntando a mi secundario y funciona perfectamente.

Verificación de conexión con DNS Esclavo:

```
david@userversec:~$ host primary.david.vid
primary.david.vid has address 192.168.210.19
david@userversec:~$ host secondary.david.vid
secondary.david.vid has address 192.168.210.20
david@userversec:~$ host cliente0.david.vid
cliente0.david.vid has address 192.168.210.30
david@userversec:~$
```

Vuelvo a usar el comando “host” y apunto a primary, secondary (mi localhost) y cliente0 para probar si resuelven nombres. Y funciona

Verificación de conexión con DNS Maestro:

```
david@userver:~$ host primary.david.vid
primary.david.vid has address 192.168.210.19
david@userver:~$ host secondary.david.vid
secondary.david.vid has address 192.168.210.20
david@userver:~$ host cliente0.david.vid
cliente0.david.vid has address 192.168.210.30
david@userver:~$
```

De nuevo uso el comando “host” y apunto a primary (mi localhost), secondary y cliente0 para probar si resuelven nombres. Y funciona.