Administración de plataformas I

Montaje de un DNS con Bind9

Profesor:
Ing. Nicolás Javier Salazar Echeverry
nicolas.salazar1@u.icesi.edu.co

Facultad de Ingeniería, Diseño y Ciencias Aplicadas
10 de abril de 2025

Índice

1. Introducción

Esta guía es un paso a paso para el montaje de un servidor DNS con bind9 en un ubuntu server 24.04 LTS, los archivos de configuración y comandos de esta guía deberían ser usados con permisos de superusuario.

El resumen de la implementación de esta guía se muestra en la figura 1

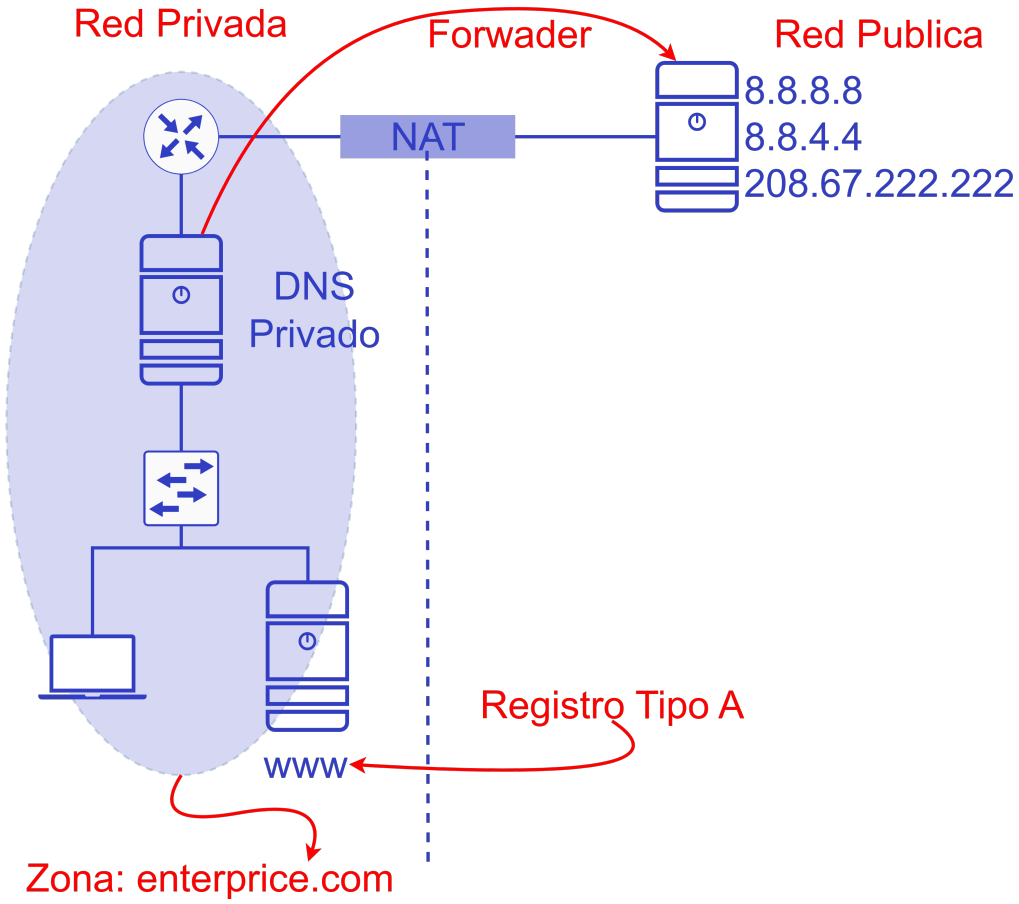

Figura 1: Interacción entre el DNS privado y el DNS de Forwarding

2. Configuración inicial del DNS

Instalación del software: `sudo apt install bind9 bind9-utils`, los archivos de configuración se encuentran en `/etc/bind/`

```
$ vim named.conf.options

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

        forwarders {
                8.8.8.8;
                8.8.4.4;
        };

        dnssec-validation auto;

        listen-on port 53 {
                127.0.0.1;
                192.168.56.10;
        };

        listen-on-v6 port 53 { ::1; };

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

acl "trusted-hosts" {
        localhost;
        localnets;
        192.168.56.10;
        192.168.56.0/24;
};
```

3. Configuración de la zona

3.1. Definición de la zona:

```
$ vim plataformas.tel.dns

$TTL 604800     ; Time To Live time a record
                ; is allowed to be cached (7 days)

; Start Of Authority ->
; Administrative information
@       IN      SOA     ns1.plataformas.tel. njse22.plataformas
   .tel. (
        1       ; Serial Number
        86400   ; DNS Secondary Refresh Interval
        7200    ; DNS Secondary Retry Interval
        57600   ; DNS Secondary Expire Interval
        3600    ; Domain Cache TTL
)
@       IN      NS      ns1.plataformas.tel.    ; NS record
ns1     IN      A       192.168.56.10           ; A record
web1    IN      A       192.168.56.101          ;
www     IN      CNAME   we1.plataformas.tel.    ; CNAME record
```

```
$ vim named.conf.local

zone "plataformas.tel" IN {
        type master;
        file "/etc/bind/plataformas.tel.dns";
};
```

3.2. Zona Reverse (IPv4 e IPv6)

3.2.1. IPv4

```
$ vim 56.168.192.in-addr.arpa.dns

$TTL 604800
```

```
@       IN  SOA     ns1.plataformas.tel njse22.plataformas.tel.
    (
        1 1d 2h 4w 1h
)
@       IN  NS  ns1.plataformas.tel.
101     IN  PTR web1.plataformas.tel.
```

```
$ vim named.conf.local

zone "plataformas.tel" IN {
    type master;
    file "/etc/bind/plataformas.tel.dns";
};

zone "56.168.192.in-addr.arpa." IN {
    type master;
    file "/etc/bind/56.168.192.in-addr.arpa.dns";
};
```

3.2.2. IPv6: (ejemplo 2001:1234:0::/48)

```
$ vim 0.0.0.0.4.3.2.1.1.0.0.2.ip6.arpa.arpa.dns

$TTL 604800

@       IN  SOA     dns1.plataformas.tel njse22.plataformas.tel
   . (
        1 1d 2h 4w 1h
)
@       IN  NS  dns1.plataformas.tel.
1.0.0.0.d.c.b.a
   .0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.3.2.1.1.0.0.2.ip6.arpa.
     IN  PTR web1.plataformas.tel.
```

4. Domain Name System Security Extensions (DNSSEC)

Crear la ZSK (Zone Signing Key); firma de cada uno de los records (o registros) de la zona

NOTA: ECDSA256 es un alias del algoritmo *ECDSAP256SHA256* definido en DNS Security Algorithm Numbers

```
$ dnssec-keygen -a ECDSA256 plataformas.tel
Generating key pair.
Kplataformas.tel.+013+14835
$ ls  K*
Kplataformas.tel.+013+14835.key
Kplataformas.tel.+013+14835.private
```

Crear la KSK (Key Signed Key)

```
$  dnssec-keygen -a ECDSA256 -f KSK -n ZONE plataformas.tel
Generating key pair.
Kplataformas.tel.+013+36682
$ ls -la K*
Kplataformas.tel.+013+14835.key     # ZSK public
Kplataformas.tel.+013+14835.private # ZSK private
Kplataformas.tel.+013+36682.key     # KSK public
Kplataformas.tel.+013+36682.private # KSK private
```

Agregar las llaves públicas a la zona:

```
$ vim  plataformas.tel.dns
$TTL 604800
$INCLUDE "/etc/bind/Kplataformas.tel.+013+14835.key"
$INCLUDE "/etc/bind/Kplataformas.tel.+013+36682.key"

@       IN      SOA     dns1.plataformas.tel. njse22.
   plataformas.tel. (
        2       ; serial
        86400   ;
        7200    ;
        57600   ;
        3600    ;
```

```
)
@       IN      NS      dns1.plataformas.tel.
dns1    IN      A       192.168.56.10
web1    IN      A       192.168.56.101
www     IN      CNAME   web1.plataformas.tel.
```

Firmas la zona con las llaves:

```
$ dnssec-signzone -o plataformas.tel -N INCREMENT -t
   plataformas.tel.dns
Verifying the zone using the following algorithms:
- ECDSAP256SHA256
Zone fully signed:
Algorithm: ECDSAP256SHA256: KSKs: 1 active, 0 stand-by, 0
   revoked
                            ZSKs: 1 active, 0 stand-by, 0
   revoked
plataformas.tel.dns.signed
Signatures generated:                       11
Signatures retained:                         0
Signatures dropped:                          0
Signatures successfully verified:            0
Signatures unsuccessfully verified:          0
Signing time in seconds:                 0.011
Signatures per second:                 916.743
Runtime in seconds:                      0.019
```

Verificar con `less plataformas.tel.dns.signed`, luego deberá actualizar el archivo al que apunta la zona:

```
$ vim  named.conf.local
zone "plataformas.tel" IN {
        type master;
        file "/etc/bind/plataformas.tel.dns.signed";
};
```

NOTA: hay un archivo particular que no es estrictamente necesario para DNSs privados, pero si lo cuando se desea exponer el servicio con algún proveedor (como AWS o Hover, por ejemplo) este archivo tiene la KSK Hash.

```
$cat dsset-plataformas.tel.
```

```
plataformas.tel.        IN DS 36682 13 2 75535
   A0EB62526FE9609622E4D7F831E2143657B11F007016F023044
   85659027
```

5. Transaction Signatures (TSIG)

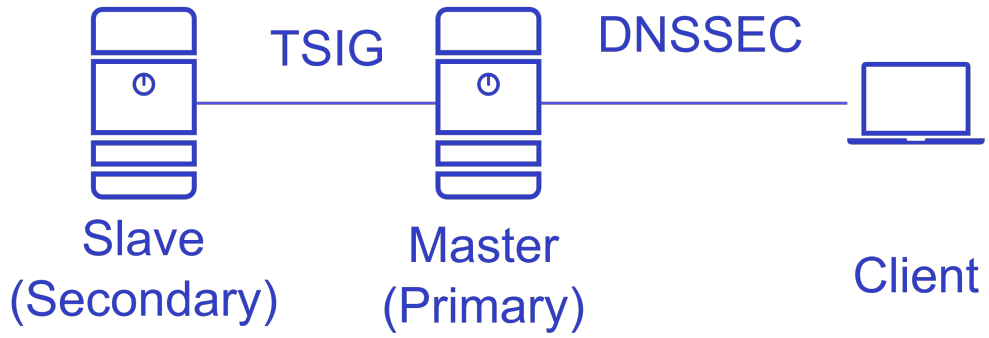

Figura 2: *Arquitectura en DNSs seguros*

Para esta configuración, es necesario tener un **DNS primario (o master)** y un **DNS secundario (o slave)**

En el DNS **primario (o master)** hay que generar la llave de para habilitar la replicación, y esa llave la agregamos a las configuraciones de nuestro servidor DNS

```
$ tsig-keygen ns1-ns2. | sudo tee -a /etc/bind/named.conf.local
```

Además, es necesario que especifiquemos a qué servidores se les va a replicar la zona:

```
server 192.168.56.11 {
        keys {
                ns1-ns2. ;
        };
};
```

Además hay que especificarlo en el parámetro de `allow-transfers` del archivo `named.conf.options`. En el DNS **secundario (o slave)** debemos agregar las configuraciones necesarias para definir que es un secundario

```
zone "plataformas.tel" {
        type slave;
        masters { 192.168.56.10 key ns1-ns2. };
        file "plataformas.tel.dns.signed";
};
```

Luego debemos especificar las llaves que usaremos para *TSIG*:

```
key "ns1-ns2." {
        algorithm hmac-sha256;
        secret "<HMAC SHA256 KEY>";
};

server 192.168.56.10 {
        keys {
                ns1-ns2. ;
        };
};
```

6. APÉNDICE

6.1. Resumen de algunos comando

- `nslookup`: comando para diagnosticar a servidores DNS, multiplataforma
- `dig`: comando para diagnosticar a servidores DNS. Normalmente, solo está disponible en plataformas compatibles con BIND, soporta más utilidades de `nslookup`
- `rndc`: Herramienta de mantenimiento remoto para BIND.
- `rndc-confgen`: Utilidad para generar claves y archivos rndc.conf para su uso con la utilidad `rndc` incluyendo una por defecto.

- `nsupdate` : Utilidad para actualizar dinámicamente los archivos de zona.
- `named-checkconf` : Utilidad para comprobar la sintaxis del archivo named.conf.
- `named-checkzone` : Utilidad para verificar los archivos de zona.
- `dnssec-signzone` : Utilidad para firmar criptográficamente zonas para su uso con DNSSEC.
- `dnssec-keygen` : Utilidad para generar claves usadas en varias transacciones DNS seguras.
- `tsig-keygen` : Utilidad para generar claves usadas entre transacciones de los servidores DNS

6.2. Ejemplos de algunos comandos

```
$ dig @<dns-server> <name-record> <necord-type> +flag
```

```
$ rndc status
```

```
$ rndc reconfig
```

```
$ rndc tsig-list
```

```
$ rndc reload zone.com
```

```
$ rndc retransfer zone.com
```