Configuración de un servicio de DNS

Práctica 3 - GIRC

Aarón Escolano Candela

Introducción **2**
Objetivo de la práctica 2
Entorno de instalación 3
Esquema de la VPC 3
Características de las ec2 3
Grupos de seguridad de las máquinas 4
Instalación y configuración **4**
Instalación BIND 4
Configuración BIND9 **4**
Archivos configuración 4
Zonas Forward 6
Aplicar DNS local **7**
Comprobar DNS de la máquina **8**
DNS Local **8**
Referencias **8**

Introducción

Objetivo de la práctica

La práctica consistirá en la configuración y prueba de un servidor de DNS local. Nuestro DNS debe ser capaz de resolver las IP 's de nuestra red local. Los nombres y las direcciones serán las mismas que la práctica anterior de configuración de TCP/IP.

La configuración a realizar debe soportar los siguientes servicios:

1. Se tendrán dos servidores de nombres, uno actuando como maestro y el otro como esclavo.
2. Los servidores atenderán múltiples zonas (sólo dos) mediante resolución directa.
3. Los servidores atenderán múltiples zonas (sólo dos) mediante resolución inversa.
4. Se soportarán vistas. Es decir, ante la misma consulta sobre el router virtual, se devolverán distintas respuestas, dependiendo de si el origen de la consulta es interno a nuestra red o externo. Según la práctica anterior, se considerará la Red-A interna y la Red-B externa.
5. Se soportará distribución de carga Round Robin para el recurso “www.midominio.es” entre tres servidores Web.
6. Se podrá acceder al recurso “atlético.midominio.es” desde un navegador Web
7. Por supuesto, si las consultas no están en nuestra base de datos se redirigirán a otro servidor de nombres.

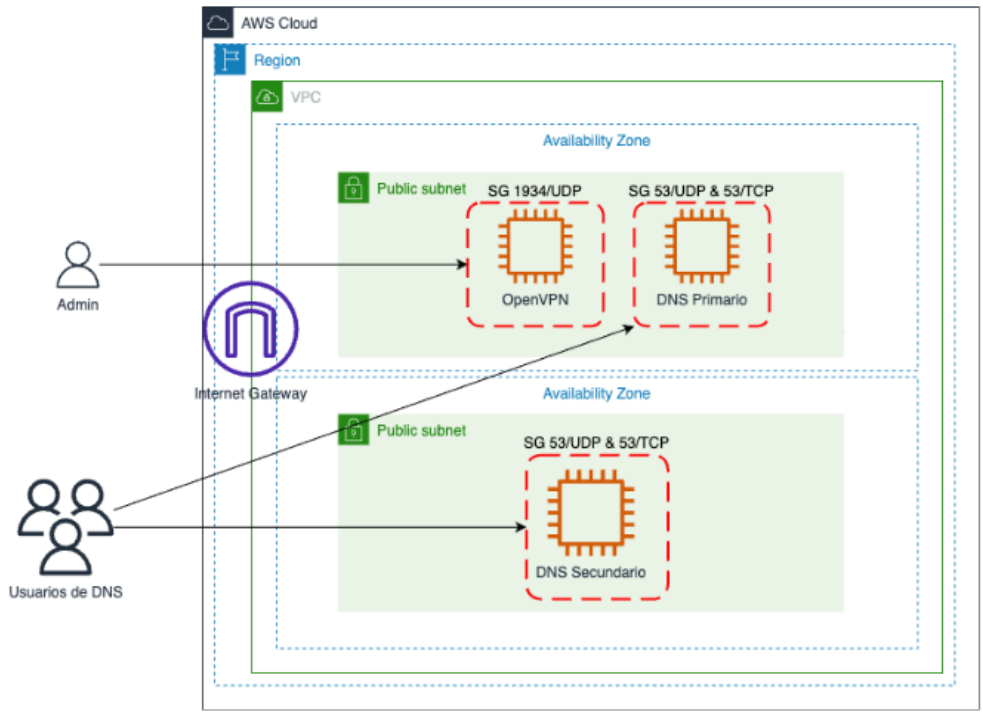
Para probar el funcionamiento de nuestro servicio, disponemos de las herramientas nslookup o dig, con la que probaremos la configuración realizada.

Entorno de instalación

La práctica estaba planteada para realizarse en un entorno local con tres máquinas virtuales pero para aprovechar el entorno cloud y poder acceder al servidor DNS de una forma más realista desde internet, se ha realizado en el entorno Cloud.

Esquema de la VPC

En esta práctica utilizaremos una VPC con dos subredes públicas, cada una en una zona de disponibilidad diferente. En la primera subred pública instalaremos una máquina ec2 con un host bastión para permitir la configuración externa de las máquinas y el servidor DNS master. En la otra subred instalaremos el DNS esclavo.



Características de las ec2

La AMI utilizada en las dos máquinas es una Ubuntu Server 22.04 LTS (HVM), SSD Volume Type t2.micro.

Grupos de seguridad de las máquinas

La ec2(master) tendrá dos grupos de seguridad:

1. GRUPO 1
    a. 0.0.0.0/0 1934/udp Allow traffic to OpenVPN Server
    b. 0.0.0.0/0 943/tcp Admin Web UI OpenVPN

2. GRUPO 2
    a. From GRUPO 1 22/tcp SSH
    b. 0.0.0.0/0 53/tcp DNS
    c. 0.0.0.0/0 53/udp DNS

La ec2(slave) tendrá un grupo de seguridad:

1. GRUPO 1
    a. From GRUPO 1 22/tcp SSH
    b. 0.0.0.0/0 53/tcp DNS
    c. 0.0.0.0/0 53/udp DNS

Instalación y configuración

Instalación BIND

Los comandos básicos para instalar y iniciar el servicio:

```
sudo apt install bind9

systemctl enable named
systemctl start named
systemctl status named
```

Configuración BIND9

Archivos configuración

Los archivos de configuración se encuentran en la carpeta /etc/bind.

Varios archivos importantes:

- /etc/bind/named.conf.options . En este archivo tendremos que habilitar los forwarders para que nuestro servidor reenvíe las peticiones que no pueda resolver hacia otros servidores DNS.

```
options {
        directory "/var/cache/bind";
        forwarders {
                1.1.1.1;
                8.8.8.8;
        };

        dnssec-validation auto;

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

- /etc/bind/named.conf.local . Este archivo contendrá las zonas de nuestro servidor DNS.

```
view trusted{
        match-clients { 10.1.0.0/20; localhost;};

        zone "aaron.es" {
                type master;
                file "/etc/bind/aaron.es.db";
                allow-transfer {10.1.16.12;};
                also-notify {10.1.16.12;};
        };

        zone "escolano.com" {
                type master;
                file "/etc/bind/escolano.com.db";
                allow-transfer {10.1.16.12;};
                also-notify {10.1.16.12;};
        };

        zone "1.1.192.in-addr.arpa" {
                type master;
                file "/etc/bind/1.1.192.in-addr.arpa.db";
                allow-transfer {10.1.16.12;};
                also-notify {10.1.16.12;};
        };

        zone "1.2.192.in-addr.arpa" {
                type master;
                file "/etc/bind/1.2.192.in-addr.arpa.db";
                allow-transfer {10.1.16.12;};
                also-notify {10.1.16.12;};
        };
};

view guest{
        match-clients{"any";};

        zone "aaron.es" {
                type master;
                file "/etc/bind/aaron.es.db.guest";
                allow-transfer {10.1.16.12;};
                also-notify {10.1.16.12;};
        };

        zone "escolano.com" {
                type master;
                file "/etc/bind/escolano.com.db.guest";
                allow-transfer {10.1.16.12;};
                also-notify {10.1.16.12;};
        };

        zone "1.1.192.in-addr.arpa" {
                type master;
                file "/etc/bind/1.1.192.in-addr.arpa.db.guest";
```

```
                allow-transfer {10.1.16.12;};
                also-notify {10.1.16.12;};
        };
        zone "1.2.192.in-addr.arpa" {
                type master;
                file "/etc/bind/1.1.192.in-addr.arpa.db.guest";
                allow-transfer {10.1.16.12;};
                also-notify {10.1.16.12;};
        };
};
```

Zonas Forward

- aaron.es.db

```
;
; Forward aaron.es
;
$TTL    604800
@       IN      SOA     ns.aaron.es. aaronescolano.gmail.com. (
                        2       ; Serial
                        604800          ; Refresh
                        86400           ; Retry
                        2419200         ; Expire
                        604800 )        ; Negative Cache TTL

@       IN      NS      ns.aaron.es.
@       IN      NS      ns2.aaron.es.

ns      IN      A       10.1.9.40
ns2     IN      A       10.1.16.12

@       IN      A       7.7.7.7

;Load Balancer
www     IN      A       2.2.2.2 ;Server 1
www     IN      A       2.2.2.3 ;Server 2
www     IN      A       2.2.2.4 ;Server 3

xn--atltico-dya   IN      A       8.8.8.8
```

- aaron.es (GUEST)

```
;
; Forward aaron.es for GUEST
;
$TTL    604800
@       IN      SOA     ns.aaron.es. aaronescolano.gmail.com. (
                        2       ; Serial
                        604800          ; Refresh
                        86400           ; Retry
                        2419200         ; Expire
                        604800 )        ; Negative Cache TTL
;
@       IN      NS      ns.aaron.es.
@       IN      NS      ns2.aaron.es.
@       IN      A       8.8.8.8
ns      IN      A       10.1.9.40
ns2     IN      A       10.1.16.12
www     IN      A       2.2.2.2
atletico        IN      A       8.8.8.8
```

- 1.1.192.in-addr.arpa.db

```
;
; Zona inversa 1
;
$TTL    604800
```

```
@       IN      SOA     ns.aaron.es. aaronescolano.gmail.com. (
                        2       ; Serial
                        604800          ; Refresh
                        86400           ; Retry
                        2419200         ; Expire
                        604800 )        ; Negative Cache TTL
;
@       IN      NS      ns.aaron.es.
@       IN      NS      ns2.aaron.es.

1       IN      PTR     aaron.es.
2       IN      PTR     ns.aaron.es.

;Load Balancer
69      IN      PTR     www.aaron.es
70      IN      PTR     www.aaron.es
71      IN      PTR     www.aaron.es
```

Para comprobar que no hemos cometido errores escribiendo en los archivos de configuración podemos ejecutar el siguiente comando:

```
named-checkconf
```

Este otro comando permite detectar errores en archivos de zonas concretas.

```
named-checkzone demotecadmin.net /var/named/demotecadmin.net.db
```

Aplicar DNS local

Para configurar nuestro servidor DNS cómo el que utilizaremos para resolver peticiones DNS, tendremos que configurar el siguiente archivo para añadir el nameservers a nuestra ip.

```
cd /etc/netplan
nano /etc/netplan/50-cloud-init.yaml
```

```
network:
            ethernets:
            eth0:
                        dhcp4: true
                        dhcp6: false
                        match:
                              macaddress: 0e:04:27:b9:f1:df
                        set-name: eth0
                        nameservers:
                              addresses: [10.1.9.40]
            version: 2
```

```
sudo netplan try
sudo netplan apply
```

Otra forma de configurar el dns utilizando network manager
nmcli c modify <name> ipv4.dns "3.89.149.44"
systemctl restart NetworkManager

Para eliminar el cache DNS.
resolvectl flush-caches

Comprobar DNS de la máquina

El archivo **/etc/resolv.conf** nos indica los servidores dns configurados y el comando

```
resolvectl status
```

nos indica los dns configurados y el que se está utilizando en el momento.

DNS Local

cat /etc/hosts

Debug
vi syslog

Referencias

1. Domain Name Service (DNS) | Ubuntu
2. Instalación y configuración del servidor DNS Bind9 en Ubuntu 22.04
3. BIND 9 Administrator Reference Manual