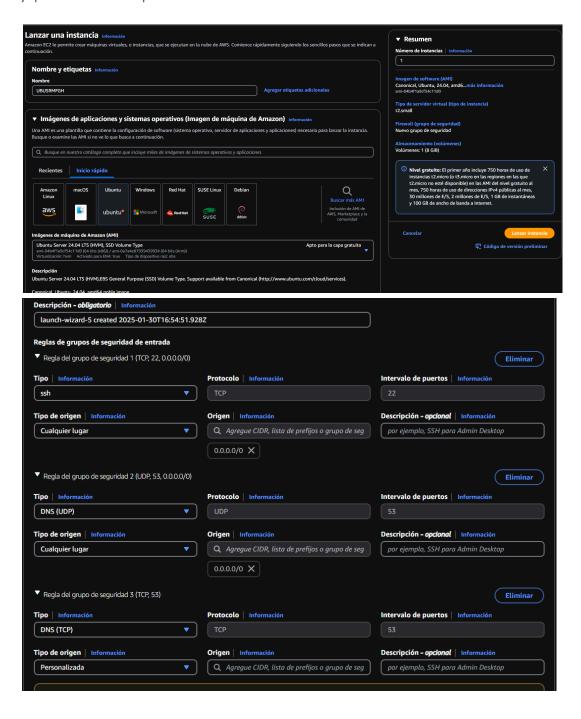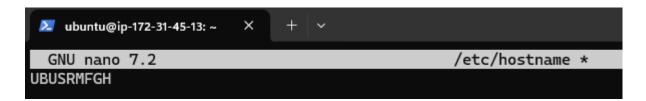# Práctica A3.P2: Servicio DNS en Linux

En esta práctica vamos a realizar la instalación y configuración del servicio DNS en un servidor Ubuntu según las instrucciones presentadas.

Nuestro servidor Ubuntu será una instancia EC2 que tendrá como nombre **UBUSRXXX**. Será accesible desde internet por medio de la dirección IP pública de la VPC de AWS. No es necesario vincularle una IP elástica. Se recomienda utilizar una EC2 tipo *small* con 2GB de RAM. Es interesante que ejecutéis *ip -a* en la instancia y que analicéis la respuesta. Debes modificar el *hostname* a **UBUSRXXX**

```
ubuntu@ip-172-31-45-13: ~          X    +   v

PS C:\Users\Manuel\Downloads> ssh -i labsuser1.pem ubuntu@ec2-54-209-248-192.compute-1.amazonaws.com
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1021-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu Jan 30 17:00:33 UTC 2025

  System load:  0.11              Processes:             107
  Usage of /:   24.9% of 6.71GB   Users logged in:       0
  Memory usage: 10%               IPv4 address for enX0: 172.31.45.13
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
ubuntu@ip-172-31-45-13: ~          X    +   v

  GNU nano 7.2                                                /etc/hostname *
UBUSRMFGH
```

```
ubuntu@ip-172-31-45-13: ~          X    +   v

  GNU nano 7.2                                      /etc/hosts *
127.0.0.1 UBUSRMFGH

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

```
Last login: Thu Jan 30 17:00:36 2025 from 213.194.149.107
ubuntu@UBUSRMFGH:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 0e:1e:25:4a:b3:c1 brd ff:ff:ff:ff:ff:ff
    inet 172.31.45.13/20 metric 100 brd 172.31.47.255 scope global dynamic enX0
       valid_lft 3579sec preferred_lft 3579sec
    inet6 fe80::c1e:25ff:fe4a:b3c1/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@UBUSRMFGH:~$
```

Se pide realizar:

1) Instala el servicio BIND y comprueba el correcto funcionamiento. Configura el servicio como servidor cache y establece como reenviadores los servidores 8.8.8.8 y 1.1.1.1 *(0,5 ptos.)*

```
ubuntu@UBUSRMFGH:~$ sudo apt install bind9 bind9utils bind9-doc -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bind9-utils dns-root-data
Suggested packages:
  bind-doc
The following NEW packages will be installed:
  bind9 bind9-doc bind9-utils bind9utils dns-root-data
0 upgraded, 5 newly installed, 0 to remove and 12 not upgraded.
Need to get 3673 kB of archives.
```

```
>_  ubuntu@UBUSRMFGH: ~        ×    +  ∨

  GNU nano 7.2                          /etc/bind/named.conf.options *
options {
        directory "/var/cache/bind";

        // 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;
                1.1.1.1;
         };

        allow-query { any; };

        dnssec-validation auto;

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

```
ubuntu@UBUSRMFGH:~$ sudo nano /etc/bind/named.conf.options
ubuntu@UBUSRMFGH:~$ sudo systemctl restart bind9
ubuntu@UBUSRMFGH:~$
```

2) Haz una consulta desde tu equipo de clase al servidor DNS con el programa *nslookup* a la máquina *www.google.es* y comprueba que funciona correctamente el servicio DNS. Repite la consulta con el programa dig desde un linux. *(0,5 ptos.)*

```
PS C:\Users\Manuel> nslookup www.google.es 54.209.248.192
Servidor:  ec2-54-209-248-192.compute-1.amazonaws.com
Address:   54.209.248.192

Respuesta no autoritativa:
Nombre:  www.google.es
Addresses:  2607:f8b0:4004:c07::5e
            172.253.62.94

PS C:\Users\Manuel>
```

```
ubuntu@ip-172-31-82-232:~$ dig @54.209.248.192 www.google.es

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> @54.209.248.192 www.google.es
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31782
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: af88e7a3e539c9d801000000679bb39d76868ff74c20b8d5 (good)
;; QUESTION SECTION:
;www.google.es.                 IN      A

;; ANSWER SECTION:
www.google.es.          179     IN      A       172.253.62.94

;; Query time: 1 msec
;; SERVER: 54.209.248.192#53(54.209.248.192) (UDP)
;; WHEN: Thu Jan 30 17:15:09 UTC 2025
;; MSG SIZE  rcvd: 86

ubuntu@ip-172-31-82-232:~$
```

3) Vamos a hacer que el servidor actúe como maestro de la zona *ubuxxx.local*: *(2,5 ptos.)*

```
ubuntu@UBUSRMFGH: ~          ✕     +   ∨

 GNU nano 7.2                              /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 "ubumfgh.local" {
            type master;
            file "/etc/bind/db.ubumfgh.local";
    };
```

a) Añade dos registros de tipo **A** (Host) para los equipos **ser1.ubuxxx.local**, **ser2.ubuxxx.local** y cuatro más para **pc1.ubuxxx.local** al **pc4.ubuxxx.local.** Pon IPs ficticias dentro de tu subnet de AWS. Comprueba que se pueden resolver esos nombres con nslookup o con dig

```
ubuntu@UBUSRMFGH: ~          ✕     +   ∨

 GNU nano 7.2                              /etc/bind/db.ubumfgh.local *
; BIND data file for ubumfgh.local
$TTL 604800
@   IN  SOA  ubuserv.ubumfgh.local. administrador.master.net. (
        10          ; Serial
        1200        ; Refresh
        2400        ; Retry
        86400       ; Expire
        10800       ; Negative Cache TTL (3 horas)
)

; Servidor DNS maestro
@       IN  NS  ubuserv.ubumfgh.local.

; Registros A (Hosts)
ubuserv IN  A   172.31.45.13
ser1    IN  A   172.31.32.10
ser2    IN  A   172.31.32.11
pc1     IN  A   172.31.32.100
pc2     IN  A   172.31.32.101
pc3     IN  A   172.31.32.102
pc4     IN  A   172.31.32.103
```

```
ubuntu@UBUSRMFGH:~$ sudo systemctl daemon-reload
ubuntu@UBUSRMFGH:~$ sudo systemctl restart bind9
ubuntu@UBUSRMFGH:~$
```

```
ubuntu@UBUSRMFGH:~$ named-checkconf
ubuntu@UBUSRMFGH:~$ sudo named-checkzone ubumfgh.local /etc/bind/db.ubumfgh.local
zone ubumfgh.local/IN: loaded serial 10
OK
ubuntu@UBUSRMFGH:~$
```

```
ubuntu@UBUSRMFGH:~$ sudo systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-01-30 17:34:56 UTC; 1min 17s ago
       Docs: man:named(8)
   Main PID: 7701 (named)
     Status: "running"
      Tasks: 5 (limit: 2338)
     Memory: 5.3M (peak: 5.5M)
        CPU: 29ms
     CGroup: /system.slice/named.service
             └─7701 /usr/sbin/named -f -u bind
```

Manuel Fernando Gómez Hernández

```
ubuntu@ip-172-31-82-232:~$ nslookup ser1.ubumfgh.local 172.31.45.13
Server:         172.31.45.13
Address:        172.31.45.13#53

Name:   ser1.ubumfgh.local
Address: 172.31.32.10

ubuntu@ip-172-31-82-232:~$ nslookup pc1.ubumfgh.local 172.31.45.13
Server:         172.31.45.13
Address:        172.31.45.13#53

Name:   pc1.ubumfgh.local
Address: 172.31.32.100

ubuntu@ip-172-31-82-232:~$ nslookup ser2.ubumfgh.local 172.31.45.13
Server:         172.31.45.13
Address:        172.31.45.13#53

Name:   ser2.ubumfgh.local
Address: 172.31.32.11

ubuntu@ip-172-31-82-232:~$ nslookup pc2.ubumfgh.local 172.31.45.13
Server:         172.31.45.13
Address:        172.31.45.13#53

Name:   pc2.ubumfgh.local
Address: 172.31.32.101

ubuntu@ip-172-31-82-232:~$ nslookup pc3.ubumfgh.local 172.31.45.13
Server:         172.31.45.13
Address:        172.31.45.13#53

Name:   pc3.ubumfgh.local
Address: 172.31.32.102

ubuntu@ip-172-31-82-232:~$ nslookup pc4.ubumfgh.local 172.31.45.13
Server:         172.31.45.13
Address:        172.31.45.13#53

Name:   pc4.ubumfgh.local
Address: 172.31.32.103

ubuntu@ip-172-31-82-232:~$ |
```

```
ubuntu@ip-172-31-82-232:~$ dig ser1.ubumfgh.local @172.31.45.13

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> ser1.ubumfgh.local @172.31.45.13
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2176
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c6dcba551705a4b901000000679bbf568d833b40c37eb7f0 (good)
;; QUESTION SECTION:
;ser1.ubumfgh.local.            IN      A

;; ANSWER SECTION:
ser1.ubumfgh.local.     604800  IN      A       172.31.32.10

;; Query time: 3 msec
;; SERVER: 172.31.45.13#53(172.31.45.13) (UDP)
;; WHEN: Thu Jan 30 18:05:10 UTC 2025
;; MSG SIZE  rcvd: 91

ubuntu@ip-172-31-82-232:~$ dig pc1.ubumfgh.local @172.31.45.13

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> pc1.ubumfgh.local @172.31.45.13
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27568
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: eccb0af3f3f9832201000000679bbf5c00fe45cf7cc0535c (good)
;; QUESTION SECTION:
;pc1.ubumfgh.local.             IN      A

;; ANSWER SECTION:
pc1.ubumfgh.local.      604800  IN      A       172.31.32.100

;; Query time: 2 msec
;; SERVER: 172.31.45.13#53(172.31.45.13) (UDP)
;; WHEN: Thu Jan 30 18:05:16 UTC 2025
;; MSG SIZE  rcvd: 90
```

b) Crea un RR de tipo **CNAME** para **ser1.ubuxxx.local** llamado **www.ubuxxx.local**

c) Crea un RR de tipo **CNAME** para **ser2.ubuxxx.local** llamado **smtp.ubuxxx.local**

```
; Alias (CNAME)
www      IN  CNAME ser1
smtp     IN  CNAME ser2
```

d) Comprueba que los **CNAME** anteriores se pueden resolver desde tu PC anfitrión

```
ubuntu@ip-172-31-82-232:~$ nslookup www.ubumfgh.local 172.31.45.13
Server:         172.31.45.13
Address:        172.31.45.13#53

www.ubumfgh.local       canonical name = ser1.ubumfgh.local.
Name:   ser1.ubumfgh.local
Address: 172.31.32.10

ubuntu@ip-172-31-82-232:~$ nslookup smtp.ubumfgh.local 172.31.45.13
Server:         172.31.45.13
Address:        172.31.45.13#53

smtp.ubumfgh.local      canonical name = ser2.ubumfgh.local.
Name:   ser2.ubumfgh.local
Address: 172.31.32.11
```

e) Añade un RR de tipo **MX** que nos indique que el servidor de correo para el dominio de correo **ubuxxx.local** es la máquina **smtp.ubuxxx.local**.

```
; Servidor de correo (MTA)
@       IN  MX  10 ser2
```

f) Resuelve los registros de tipo **MX** para el dominio de correo **ubuxxx.local** usando los comandos *nslookup* y *dig*

```
ubuntu@ip-172-31-82-232:~$ nslookup -type=mx ubumfgh.local 172.31.45
.13
Server:         172.31.45.13
Address:        172.31.45.13#53

ubumfgh.local   mail exchanger = 10 ser2.ubumfgh.local.
```

```
ubuntu@ip-172-31-82-232:~$ dig mx ubumfgh.local @172.31.45.13

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> mx ubumfgh.local @172.31.45.13
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56613
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d7cbc3a0b72d93cc01000000679bc2a3ef5476b8e889b87a (good)
;; QUESTION SECTION:
;ubumfgh.local.                  IN      MX

;; ANSWER SECTION:
ubumfgh.local.          604800  IN      MX      10 ser2.ubumfgh.local.

;; ADDITIONAL SECTION:
ser2.ubumfgh.local.     604800  IN      A       172.31.32.11

;; Query time: 2 msec
;; SERVER: 172.31.45.13#53(172.31.45.13) (UDP)
;; WHEN: Thu Jan 30 18:19:15 UTC 2025
;; MSG SIZE  rcvd: 107
```

g) Resuelve los registros de tipo **NS** para la zona **ubuxxx.local** usando los comandos *nslookup y dig* desde tu PC anfitrión

```
ubuntu@ip-172-31-82-232:~$ nslookup -type=ns ubumfgh.local 172.31.45
.13
Server:         172.31.45.13
Address:        172.31.45.13#53

ubumfgh.local   nameserver = ubuserv.ubumfgh.local.
```

```
^Cubuntu@ip-172-31-82-232:~$ dig ns ubumfgh.local @172.31.45.13

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> ns ubumfgh.local @172.31.45.13
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49960
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ac86972084d466f401000000679bc3246850be588c54c92d (good)
;; QUESTION SECTION:
;ubumfgh.local.                    IN      NS

;; ANSWER SECTION:
ubumfgh.local.          604800  IN      NS      ubuserv.ubumfgh.local.

;; ADDITIONAL SECTION:
ubuserv.ubumfgh.local.  604800  IN      A       192.168.1.111

;; Query time: 2 msec
;; SERVER: 172.31.45.13#53(172.31.45.13) (UDP)
;; WHEN: Thu Jan 30 18:21:24 UTC 2025
;; MSG SIZE  rcvd: 108
```

4) Crea una zona inversa (*Reverse Lookup Zone*) para la red de AWS que se usa en la zona directa *ubuxxx.local* (en mi caso era la 172.31.0.0/16) *(2 ptos)*

  a) La zona inversa **31.172.in-addr.arpa** (o la que te corresponda)

```
ubuntu@UBUSRMFGH: ~        ×      +   v

GNU nano 7.2                          /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 "ubumfgh.local" {
                type master;
                file "/etc/bind/db.ubumfgh.local";
        };

zone "31.172.in-addr.arpa" {
  type master;
  file "/etc/bind/db.172.31";
};
```

b) Añade los registros **SOA**, **NS** y los **PTR** correspondientes a todos los registros de tipo **A** de la zona directa (deberían ser 7)

```
>_  ubuntu@UBUSRMFGH: ~        ×      +   ∨

   GNU nano 7.2                            /etc/bind/db.172.31 *
; Fichero db.172.31

$TTL 1D

@  IN  SOA ubusrmfgh.ubumfgh.local. administrador.master.net. (
     10             ; Serial
     1200           ; Refresh
     2400           ; Retry
     86400          ; Expire
     10800          ; Negative Cache TTL (3 horas)
)

; Servidores DNS del dominio
@  IN  NS  ubusrmfgh.ubumfgh.local.

; Registros PTR para la red 172.31.x.x
13.45 IN PTR ubusrmfgh.ubumfgh.local.
10.32.31.172.in-addr.arpa.    IN PTR ser1.ubumfgh.local.
11.32.31.172.in-addr.arpa.    IN PTR ser2.ubumfgh.local.
100.32.31.172.in-addr.arpa.   IN PTR pc1.ubumfgh.local.
101.32.31.172.in-addr.arpa.   IN PTR pc2.ubumfgh.local.
102.32.31.172.in-addr.arpa.   IN PTR pc3.ubumfgh.local.
103.32.31.172.in-addr.arpa.   IN PTR pc4.ubumfgh.local.
```

c) Resuelve los registros **PTR** usando *nslookup* y *dig*

```
ubuntu@UBUSRMFGH:~$ sudo nano /etc/bind/db.172.31
ubuntu@UBUSRMFGH:~$ sudo systemctl restart bind9
ubuntu@UBUSRMFGH:~$
```

```
ubuntu@ip-172-31-82-232:~$ nslookup 172.31.32.10 54.209.248.192
10.32.31.172.in-addr.arpa        name = ser1.ubumfgh.local.

ubuntu@ip-172-31-82-232:~$ nslookup 172.31.32.11 54.209.248.192
11.32.31.172.in-addr.arpa        name = ser2.ubumfgh.local.

ubuntu@ip-172-31-82-232:~$ nslookup 172.31.32.100 54.209.248.192
100.32.31.172.in-addr.arpa        name = pc1.ubumfgh.local.

ubuntu@ip-172-31-82-232:~$ nslookup 172.31.32.101 54.209.248.192
101.32.31.172.in-addr.arpa        name = pc2.ubumfgh.local.

ubuntu@ip-172-31-82-232:~$ nslookup 172.31.32.102 54.209.248.192
102.32.31.172.in-addr.arpa        name = pc3.ubumfgh.local.

ubuntu@ip-172-31-82-232:~$ nslookup 172.31.32.103 54.209.248.192
103.32.31.172.in-addr.arpa        name = pc4.ubumfgh.local.
```

```
ubuntu@ip-172-31-82-232:~$ dig -x 172.31.32.10 @54.209.248.192

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> -x 172.31.32.10 @54.209.248.192
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55967
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: cb9af46c548d9153010000000679bc88fcf68dde9a8d0c786 (good)
;; QUESTION SECTION:
;10.32.31.172.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
10.32.31.172.in-addr.arpa. 86400 IN     PTR     ser1.ubumfgh.local.

;; Query time: 1 msec
;; SERVER: 54.209.248.192#53(54.209.248.192) (UDP)
;; WHEN: Thu Jan 30 18:44:31 UTC 2025
;; MSG SIZE  rcvd: 114

ubuntu@ip-172-31-82-232:~$ dig -x 172.31.32.100 @54.209.248.192

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> -x 172.31.32.100 @54.209.248.192
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14653
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d7786efb52e0515e010000000679bc893b6942edd012b89a0 (good)
;; QUESTION SECTION:
;100.32.31.172.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
100.32.31.172.in-addr.arpa. 86400 IN    PTR     pc1.ubumfgh.local.

;; Query time: 1 msec
;; SERVER: 54.209.248.192#53(54.209.248.192) (UDP)
;; WHEN: Thu Jan 30 18:44:35 UTC 2025
;; MSG SIZE  rcvd: 114

ubuntu@ip-172-31-82-232:~$
```

5) Automatizar mediante Ansible una nueva instancia de AWS de nombre DNSAnsibleXXX de manera que quede tal y como se pide en esta práctica. Tened en cuenta que igual tenéis que tocar los ficheros de configuración al cambiar la ip de la instancia en la subnet de AWS. *(2 ptos.)*

```
ubuntu@ip-172-31-19-245:~$ mkdir -p ./ansible/playbooks
ubuntu@ip-172-31-19-245:~$ cd ./ansible/playbooks
ubuntu@ip-172-31-19-245:~/ansible/playbooks$ |
```

```
ubuntu@ip-172-31-19-245: ~/        X    +   ∨

  GNU nano 7.2                                    ./dns_setup.yml
---
- name: Configurar servidor DNS
  hosts: all
  become: yes

  tasks:
    - name: Instalar paquetes de BIND
      apt:
        name: "{{ item }}"
        state: present
      loop:
        - bind9
        - bind9utils
        - bind9-doc

    - name: Configurar named.conf.options
      template:
        src: templates/named.conf.options.j2
        dest: /etc/bind/named.conf.options
      notify:
        - Reiniciar BIND

    - name: Configurar named.conf.local
      template:
        src: templates/named.conf.local.j2
        dest: /etc/bind/named.conf.local
      notify:
        - Reiniciar BIND

    - name: Crear archivo de zona directa
      template:
        src: templates/db.ubumfgh.local.j2
        dest: /etc/bind/db.ubumfgh.local
      notify:
        - Reiniciar BIND

    - name: Crear archivo de zona inversa
      template:
        src: templates/db.31.172.j2
        dest: /etc/bind/db.31.172
      notify:
        - Reiniciar BIND

  handlers:
    - name: Reiniciar BIND
      service:
        name: bind9
```

Manuel Fernando Gómez Hernández

```
ubuntu@ip-172-31-19-245: ~/    X     +   v

  GNU nano 7.2                                  ./named.conf.options.j2 *
options {
    directory "/var/cache/bind";

    forwarders {
        8.8.8.8;
        1.1.1.1;
    };

    allow-query { any; };

    dnssec-validation auto;

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

```
ubuntu@ip-172-31-19-245: ~/    X     +   v

  GNU nano 7.2                                  ./named.cong.local.j2 *
//
// Do any local configuration here
//

zone "ubumfgh.local" {
    type master;
    file "/etc/bind/db.ubumfgh.local";
};

//| Zona inversa para la red 172.31.0.0/16
zone "31.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.31.172";
};
```

Manuel Fernando Gómez Hernández

```
ubuntu@ip-172-31-19-245: ~/      X      +    ∨

  GNU nano 7.2                                ./db.ubumfgh.local.j2 *
;
; BIND data file for ubumfgh.local
;
$TTL    604800
@ IN SOA ubusrmfgh.ubumfgh.local. administrador.master.net. (
    10              ; Serial
    1200            ; Refresh
    2400            ; Retry
    86400           ; Expire
    10800           ; Negative Cache TTL (3 horas)
)

; Servidores DNS del dominio
@   IN   NS   ubusrmfgh.ubumfgh.local.

; Registros A para los hosts
ubusrmfgh-ansible|   IN   A    172.31.45.13
ser1          IN   A    172.31.32.10
ser2          IN   A    172.31.32.11
pc1           IN   A    172.31.32.100
pc2           IN   A    172.31.32.101
pc3           IN   A    172.31.32.102
pc4           IN   A    172.31.32.103

; Alias (CNAME)
www           IN   CNAME    ser1
smtp          IN   CNAME    ser2

; Servidores de correo (MTA)
@             IN   MX 10    ser2
```

```
ubuntu@ip-172-31-19-245: ~/          X        +    v

 GNU nano 7.2                                    ./db.31.172.j2 *
// db.31.172.j2

$TTL 1D
@    IN   SOA ubusrmfgh.ubumfgh.local. administrador.master.net. (
         10 ; Serial
         1200        ; Refresh
         2400        ; Retry
         86400       ; Expire
         10800       ; Negative Cache TTL
      )

      ; Servidores DNS del dominio
      @    IN   NS   ubusrmfgh.ubumfgh.local.

      ; Registros PTR para las IPs de la red 172.31.x.x
      13.45     IN PTR ubusrmfgh.ubumfgh.local.
      10.31.172.in-addr.arpa.          IN PTR ser1.ubumfgh.local.
      11.31.172.in-addr.arpa.          IN PTR ser2.ubumfgh.local.
      100.31.172.in-addr.arpa.         IN PTR pc1.ubumfgh.local.
      101.31.172.in-addr.arpa.         IN PTR pc2.ubumfgh.local.
      102.31.172.in-addr.arpa.         IN PTR pc3.ubumfgh.local.
      103.31.172.in-addr.arpa.         IN PTR pc4.ubumfgh.local.
```
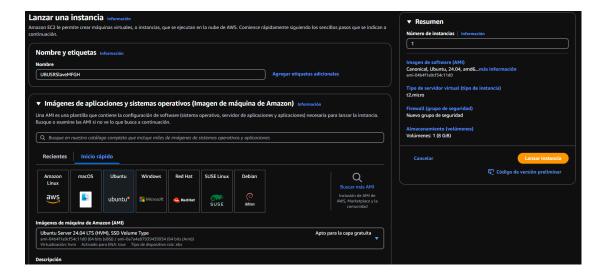
```
ubuntu@ip-172-31-19-245:~/ansible/playbooks/templates$ cd ../
ubuntu@ip-172-31-19-245:~/ansible/playbooks$ nano hosts.ini
```

```
ubuntu@ip-172-31-19-245: ~/          X        +    v

 GNU nano 7.2                                    hosts.ini *
[localhost]
127.0.0.1 ansible_connection=local
```

```
ubuntu@ip-172-31-19-245:~/ansible/playbooks$ ansible-playbook -i hosts.ini dns_setup.yml

PLAY [Configurar servidor DNS] ***************************************************************************************

TASK [Gathering Facts] **********************************************************************************************
ok: [127.0.0.1]

TASK [Instalar paquetes de BIND] ************************************************************************************
ok: [127.0.0.1] => (item=bind9)
ok: [127.0.0.1] => (item=bind9utils)
ok: [127.0.0.1] => (item=bind9-doc)

TASK [Configurar named.conf.options] ********************************************************************************
ok: [127.0.0.1]

TASK [Configurar named.conf.local] **********************************************************************************
changed: [127.0.0.1]

TASK [Crear archivo de zona directa] ********************************************************************************
changed: [127.0.0.1]

TASK [Crear archivo de zona inversa] ********************************************************************************
changed: [127.0.0.1]

RUNNING HANDLER [Reiniciar BIND] ************************************************************************************
changed: [127.0.0.1]

PLAY RECAP **********************************************************************************************************
127.0.0.1                  : ok=7    changed=4    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

ubuntu@ip-172-31-19-245:~/ansible/playbooks$
```

```
ubuntu@ip-172-31-82-232:~$ nslookup pc1.ubumfgh.local 54.209.248.192
Server:         54.209.248.192
Address:        54.209.248.192#53

Name:   pc1.ubumfgh.local
Address: 172.31.32.100

ubuntu@ip-172-31-82-232:~$ dig ser1.ubumfgh.local @54.209.248.192

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> ser1.ubumfgh.local @54.209.248.192
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62168
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 868facbe910d511e01000000679bd34dc16a95444082940c (good)
;; QUESTION SECTION:
;ser1.ubumfgh.local.             IN      A

;; ANSWER SECTION:
ser1.ubumfgh.local.     604800  IN      A       172.31.32.10

;; Query time: 2 msec
;; SERVER: 54.209.248.192#53(54.209.248.192) (UDP)
;; WHEN: Thu Jan 30 19:30:21 UTC 2025
;; MSG SIZE  rcvd: 91

ubuntu@ip-172-31-82-232:~$ dig -x 172.31.32.10 @54.209.248.192

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> -x 172.31.32.10 @54.209.248.192
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29305
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 92f8db9613cba01301000000679bd35f3edbf3652a506952 (good)
;; QUESTION SECTION:
;10.32.31.172.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
10.32.31.172.in-addr.arpa. 86400 IN     PTR     ser1.ubumfgh.local.

;; Query time: 2 msec
;; SERVER: 54.209.248.192#53(54.209.248.192) (UDP)
```

6) Utilizando una nueva instancia de AWS de nombre **UBUSRSlaveXXX** realiza una configuración DNS maestro-esclavo para la zona directa *ubuxxx.local* y su correspondiente zona inversa. Comprueba que se produce la transferencia de zona y que el servidor esclavo responde de forma correcta a las consultas DNS de sus zonas. *(2,5 ptos.)*

Añado esa IP a la configuración del maestro.

```
ubuntu@UBUSRMFGH:~$ sudo nano /etc/bind/named.conf.local
ubuntu@UBUSRMFGH:~$ sudo systemctl restart bind9
ubuntu@UBUSRMFGH:~$ sudo system status bind9
sudo: system: command not found
ubuntu@UBUSRMFGH:~$ sudo systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-01-30 19:42:01 UTC; 10s ago
       Docs: man:named(8)
   Main PID: 8590 (named)
     Status: "running"
      Tasks: 4 (limit: 2338)
     Memory: 5.2M (peak: 5.4M)
        CPU: 32ms
     CGroup: /system.slice/named.service
             └─8590 /usr/sbin/named -f -u bind
```

Instalo bind en el esclavo, y hago lo mismo, pero especificando que soy el maestro, y esta vez, poniendo la IP privada del maestro, asegurandome de especificar que la ip es "masters".

```
ubuntu@ip-172-31-83-38: ~        ×     +    ∨

GNU nano 7.2                    /etc/bind/named.conf.local *
//
// Do any local configuration here
//

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

        zone "ubumfgh.local" {
                type slave;
                file "/etc/bind/db.ubumfgh.local";
                masters { 172.31.45.13; };
        };

zone "31.172.in-addr.arpa" {
  type slave;
  file "/etc/bind/db.172.31";
  masters { 172.31.45.13; };
};
```

```
ubuntu@ip-172-31-83-38: ~        ×     +    ∨

GNU nano 7.2                    /etc/hostname *
UBUSRSlaveMFGH
```

Funcionan las transferencias.

Resolvemos con la IP privada del esclavo.