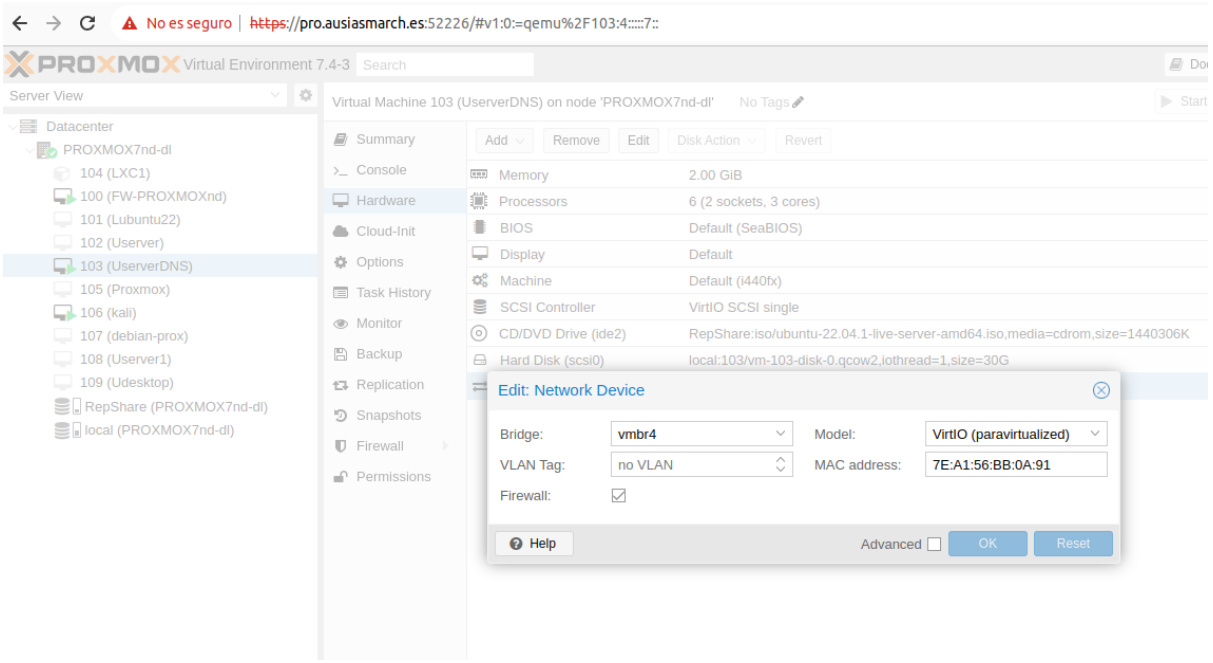
# Práctica DNS Maestro

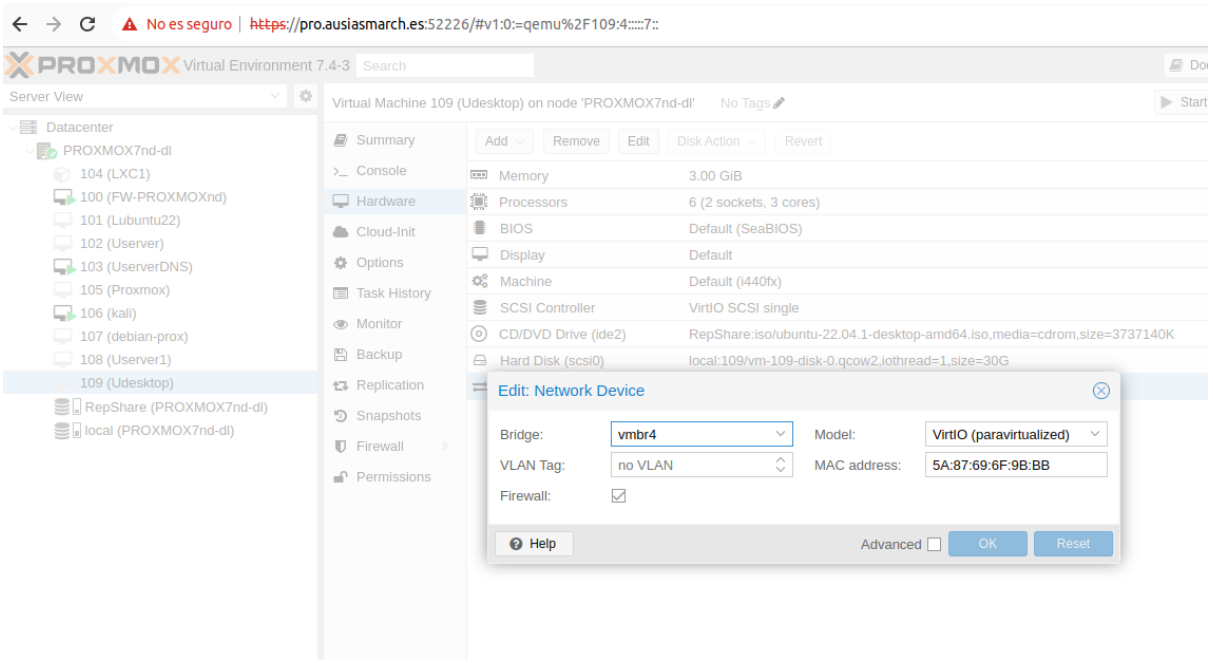
Trabajo realizado por: David López Saorin

## Configuración del sistema:

### Server:




### Cliente:




Para empezar, yo usaré un ubuntu server que se utilizará como servidor DNS en proxmox con una configuración de red personalizada en la interfaz vmbr4 (para que haga de red interna) junto a un cliente ubuntu desktop que está también en la interfaz vmbr4 y más tarde configuraré la red para que conecte con el DNS del server.

## Actualización del sistema y instalación de paquetes necesarios:

```
david@userver:~$ 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 99 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 (1:9.18.12-0ubuntu0.22.04.3).
bind9-utils ya está en su versión más reciente (1:9.18.12-0ubuntu0.22.04.3).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 99 no actualizados.
```

Primero que nada, bajarse los últimos paquetes del sistema con “sudo apt update” para instalar la última versión de bind9 con “sudo apt install bind9 bind9-utils -y”.

```
david@userver:~$ systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2023-10-26 10:00:20 UTC; 1min 38s ago
       Docs: man:named(8)
    Process: 1741 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 1742 (named)
      Tasks: 14 (limit: 2219)
     Memory: 8.9M
        CPU: 107ms
     CGroup: /system.slice/named.service
             └─1742 /usr/sbin/named -u bind

oct 26 10:00:20 userver systemd[1]: Started BIND Domain Name Server.
oct 26 10:00:20 userver named[1742]: network unreachable resolving './DNSKEY/IN': 2001:500:a8::e#53
oct 26 10:00:20 userver named[1742]: running
oct 26 10:00:20 userver named[1742]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
oct 26 10:00:20 userver named[1742]: network unreachable resolving './DNSKEY/IN': 2001:7fd::1#53
oct 26 10:00:20 userver named[1742]: network unreachable resolving './NS/IN': 2001:7fd::1#53
oct 26 10:00:20 userver named[1742]: network unreachable resolving './DNSKEY/IN': 2001:500:2::c#53
oct 26 10:00:20 userver named[1742]: network unreachable resolving './NS/IN': 2001:500:2::c#53
oct 26 10:00:20 userver named[1742]: managed-keys-zone: Initializing automatic trust anchor management for zone '.'; DNSKEY ID 20326 is now trusted, waiving th
oct 26 10:00:20 userver named[1742]: resolver priming query complete: success
```

Ahora, una breve verificación del proceso bind9, donde se puede ver que el proceso está activo pero hay unas líneas abajo que indican que faltan ciertos archivos que se configuran en este pdf más adelante.

## Configuración del archivo “/etc/bind/named.conf.options”:

```
david@userver:~$ cat /etc/bind/named.conf.options
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.

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

En este archivo configuro los reenviadores, de manera que si hay una petición a un DNS que el servidor no conoce se lo pregunte al DNS introducido que en este caso es 8.8.8.8 (Google).
Además, configuro las peticiones de la red 192.168.210.0/24 (En la que estoy), como no tengo DNS secundario, cambio el campo “dnssec-validation” a “no” y por último quito las peticiones que sean de IPv6.

```
david@userver:~$ cat /etc/default/named
#
# run resolvconf?
RESOLVCONF=no

# startup options for the server
OPTIONS="-u bind -4"
```

En el archivo que se encuentra en “/etc/default/named” le establezco que bind utilice el modo IPv4 con el parámetro “-4” ya que solo voy a trabajar con IPs v4.

```
david@userver:~$ sudo named-checkconf
david@userver:~$ sudo systemctl restart bind9
david@userver:~$ sudo systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2023-10-26 10:14:54 UTC; 5s ago
       Docs: man:named(8)
    Process: 2774 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 2775 (named)
      Tasks: 8 (limit: 2219)
     Memory: 6.1M
        CPU: 95ms
     CGroup: /system.slice/named.service
             └─2775 /usr/sbin/named -u bind -4

oct 26 10:14:52 userver named[2775]: configuring command channel from '/etc/bind/rndc.key'
oct 26 10:14:52 userver named[2775]: command channel listening on 127.0.0.1#953
oct 26 10:14:54 userver named[2775]: managed-keys-zone: loaded serial 2
oct 26 10:14:54 userver named[2775]: zone 0.in-addr.arpa/IN: loaded serial 1
oct 26 10:14:54 userver named[2775]: zone 127.in-addr.arpa/IN: loaded serial 1
oct 26 10:14:54 userver named[2775]: zone localhost/IN: loaded serial 2
oct 26 10:14:54 userver named[2775]: zone 255.in-addr.arpa/IN: loaded serial 1
oct 26 10:14:54 userver named[2775]: all zones loaded
oct 26 10:14:54 userver named[2775]: running
oct 26 10:14:54 userver systemd[1]: Started BIND Domain Name Server.
```

En este paso vuelvo a verificar mi configuración por si encuentra errores. El comando “sudo named-checkconf” comprueba la sintaxis de un archivo de configuración named. conf. Después “restarteo” el servicio de bind9 y lo compruebo con “status”, y se puede ver que todavía faltan pasos.

## Configuración de fichero de zonas:

QEMU (UserverDNS) - noVNC - Google Chrome

No es seguro | https://pro.ausiasmarch.es:52226/?console=kvm&novnc=1&vmid=103&vmname=UserverDNS&node=PROXMOX

```
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";
};

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

El siguiente paso es configurar el archivo de zonas que está en la ruta “/etc/bind/named.conf.local”. Aquí le digo que la zona david.vid (mi DNS), sea maestro y esté en la ruta “/etc/bind/zones/db.david.vid”, lo mismo con el archivo de zona inversa.

## Configuración de zonas db.david.local y db.210.168.192:

```
david@userver:~$ cat /etc/bind/zones/db.david.vid
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     primary.david.local. root.david.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
                IN      NS      primary.david.local.
primary         IN      A       192.168.210.19
cliente0        IN      A       192.168.210.20
server          IN      CNAME   primary
david@userver:~$ _
```

Aquí, lo que hago es establecer mi SOA primero que es “primary.david.local.”. Le indico mi root, “root.david.local.” y abajo borro las líneas que había por defecto como localhost y establezco mi configuración DNS, mi NS principal “primary.david.local.”, le asigno la IP a “primary”, qué es la mía, y añado cliente0, que será mi ubuntu desktop, y le asigno su IP correspondiente que luego configurare de manera estática, y por último añado un “CNAME”, o sea, un alias que apunte a “primary.david.local”.
Cabe destacar que este archivo es un copia pega del archivo db.local que hay por defecto en la ruta “/etc/bind” y creo una carpeta en la misma ruta que se llama “zones” y ahi pego el archivo db.local y lo renombro como db.david.vid que así lo llame en el archivo “named.conf.local” donde lo configuro como DNS maestro.

```
david@userver:~$ ls /etc/bind/zones/
db.210.168.192  db.david.local
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
;
                IN      NS      primary.david.local.
19              IN      PTR     primary.david.local
```

Este archivo es el de zona inversa, lo único que hago es indicar mi ip (19) y añadir el registro PTR que es un puntero que apunta a “primary.david.local.” para resolverlo de manera inversa.

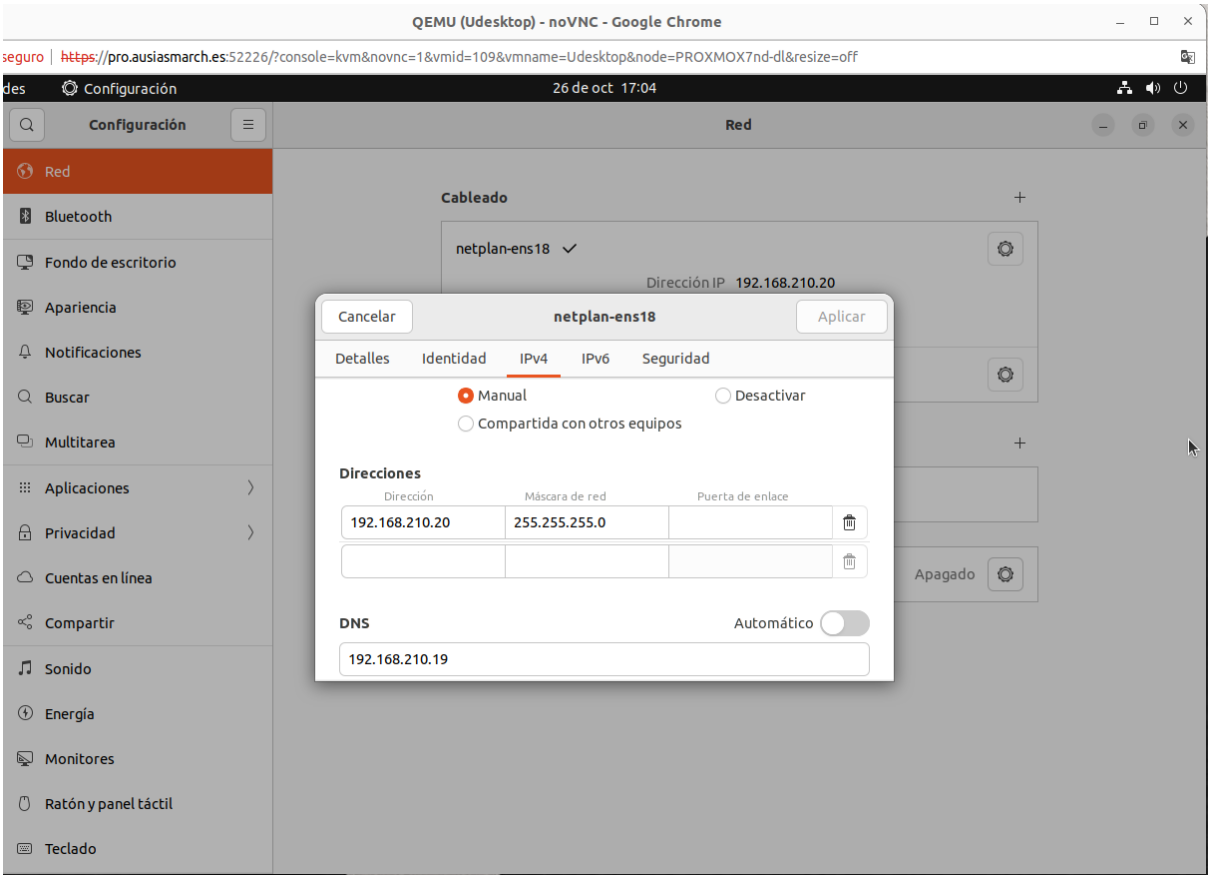
```
david@userver:~$ sudo named-checkconf /etc/bind/named.conf.local
david@userver:~$ sudo named-checkzone david.local /etc/bind/zones/db.david.local
zone david.local/IN: loaded serial 2
OK
david@userver:~$ sudo named-checkzone 210.168.192.in-addr.arpa /etc/bind/zones/db.210.168.192
zone 210.168.192.in-addr.arpa/IN: loaded serial 2
OK
```

Ahora lo que hago es verificar que el formato de los ficheros que he editado estan en buen estado con estos comandos de verificación.

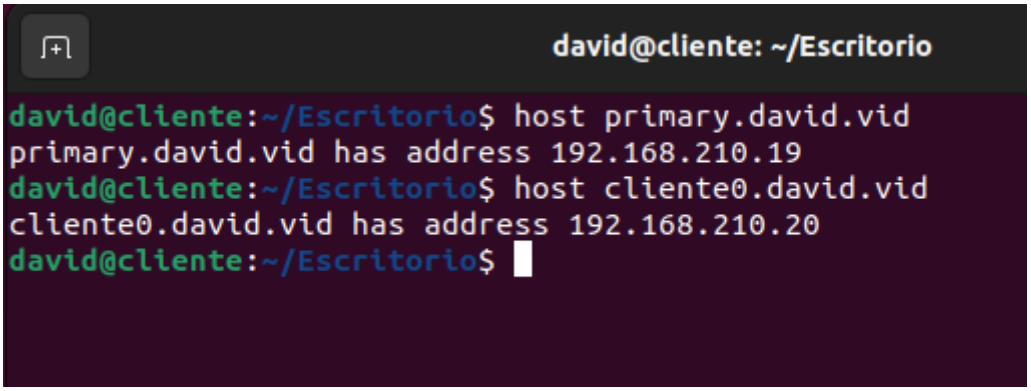
```
david@userver:~$ sudo systemctl restart bind9
david@userver:~$ sudo systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2023-10-26 10:33:46 UTC; 5s ago
       Docs: man:named(8)
    Process: 3215 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 3216 (named)
      Tasks: 8 (limit: 2219)
     Memory: 6.1M
        CPU: 93ms
     CGroup: /system.slice/named.service
             └─3216 /usr/sbin/named -u bind -4

oct 26 10:33:46 userver named[3216]: managed-keys-zone: loaded serial 3
oct 26 10:33:46 userver named[3216]: zone 0.in-addr.arpa/IN: loaded serial 1
oct 26 10:33:46 userver named[3216]: zone 210.168.192.in-addr.arpa/IN: loaded serial 2
oct 26 10:33:46 userver named[3216]: zone 255.in-addr.arpa/IN: loaded serial 1
oct 26 10:33:46 userver named[3216]: zone david.local/IN: loaded serial 2
oct 26 10:33:46 userver named[3216]: zone 127.in-addr.arpa/IN: loaded serial 1
oct 26 10:33:46 userver named[3216]: zone localhost/IN: loaded serial 2
oct 26 10:33:46 userver named[3216]: all zones loaded
oct 26 10:33:46 userver named[3216]: running
oct 26 10:33:46 userver systemd[1]: Started BIND Domain Name Server.
```

Y vuelvo a restartear el servicio de bind9 y muestro el estado del mismo para, como se puede ver, mostrar que se han cargado correctamente las zonas.

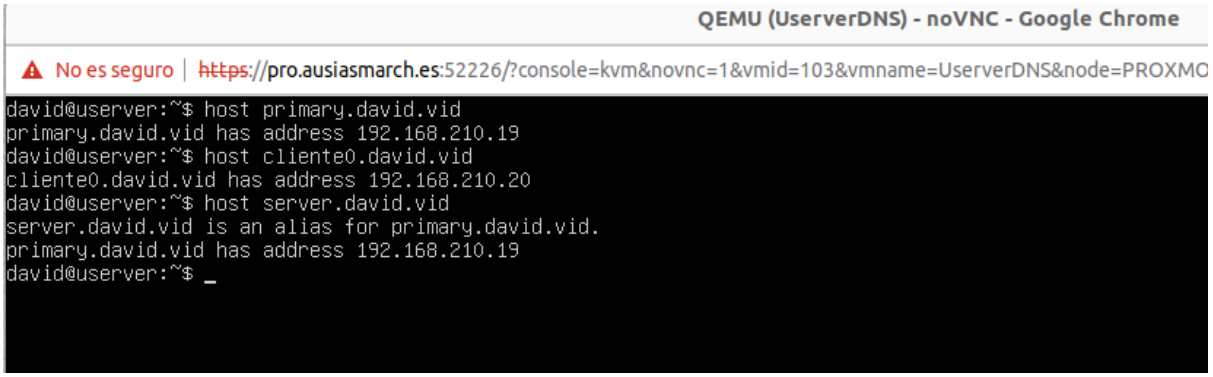
## Configuración y pruebas de cliente-servidor:




En mi cliente ubuntu desktop configuro la red. Como quiero que sea estático, pincho la opcion manual, y le establezco la IP “192.168.210.20” que es la que configuré en el archivo de zona “db.david.vid”, la máscara “/24” y el servidor DNS le digo que sea la IP de mi servidor primario.




Realizo unas pruebas de conexión con host y… Funciona!!




Y por último realizo las pruebas en mi propio servidor y también resuelve las IPs y la inversa!