

PRÁCTICA. INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR DNS

INTRODUCCIÓN

En esta práctica, vamos a **instalar y configurar un servidor DNS en Linux Ubuntu**. El servidor deberá dar servicio al resto de equipos conectados en la misma red local.

Para esta práctica, debes usar las máquinas virtuales indicadas al inicio de curso. Recuerda que deben tener el direccionamiento correcto. En concreto, para el servidor DNS usaremos la dirección 10.10.5.30/24 (máquina virtual 'server').

Se recomienda guardar una copia de la máquina virtual una vez finalizada la práctica.

Antes de empezar, debes conocer los ficheros que vamos a usar para configurar el servicio DNS:

- **/etc/bind/named.conf.options:** Se utiliza para configurar diferentes parámetros generales del servicio DNS.
- **/etc/bind/named.conf.local:** Se usa para crear las distintas zonas DNS que existirán en el servidor DNS. Se debe crear al menos una zona. Para esa zona se definirá tanto la resolución directa como la inversa.
- **/etc/bind/zones/db.xxxx:** Es el archivo donde se describen todos los registros de recursos (RR) asociados a una zona. 'db.xxxx' es el nombre de la zona que se haya dado en el archivo de configuración named.conf.local. 'db.xxxx' es un ejemplo: deberás darle el nombre correspondiente a tu zona

PARTE 1. CONFIGURACIÓN DEL SERVIDOR DNS EN UBUNTU

En esta primera parte de la práctica, solo debe estar encendida la máquina del servidor. Se configurará un servidor DNS maestro (primario). El dominio será "NOMBRE.com" (*obligatorio: debes indicar tu nombre en NOMBRE*). En la práctica guiada el dominio usado es prueba.com, pero debes modificarlo.

PASO 1. Actualizar los repositorios y paquetes del sistema.

Primero, asegúrate de que tu sistema esté completamente actualizado. Ejecuta los siguientes comandos desde la terminal:

```
sudo apt update && sudo apt upgrade
```

PASO 2. Instala Bind9 en Ubuntu Server 25.04.

```
sudo apt install bind9 bind9utils bind9-doc
```

PASO 3. Ve al archivo de configuración de **netplan** y modifica algunos parámetros de red, específicamente los **servidores DNS**.

```
GNU nano 8.3 /etc/netplan/50-cloud-init.yaml
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      addresses:
        - "10.10.5.30/24"
      nameservers:
        addresses:
          - 127.0.0.1
          - 8.8.8.8
      search: [prueba.com]
```

PASO 4. Aplica los cambios en netplan:

```
>> sudo netplan apply
```

PASO 5. Ejecuta este comando para permitir el servicio DNS a través del firewall:

```
>> sudo ufw allow bind9
>> sudo ufw status
```

PASO 6. Configura el archivo 'named.conf.options' con los siguientes parámetros:

```
GNU nano 8.3 /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; 10.10.5.0/24;};

    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; };
};
```

* **PREGUNTA:** Explica el significado de cada uno de los parámetros incluidos en el archivo anterior (directory, listen-on port, allow-query y forwarders).

PASO 7. Después, tienes que configurar el archivo de zona local. Edita el archivo “/etc/bind/named.conf.local” para definir una zona directa y una zona inversa para tu dominio local (modifica el nombre del dominio por el indicado al principio de la práctica):

```
GNU nano 8.3 /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 "prueba.com" IN {
    type master;
    file "/etc/bind/zonas/db.prueba.com";
};

zone "5.10.10.in-addr.arpa"{
    type master;
    file "/etc/bind/zonas/db.5.10.10";
};
```

*** PREGUNTA:** Explica la diferencia entre resolución directa y resolución inversa.

PASO 8. Comprueba que la sintaxis del archivo es correcta:

```
sudo named-checkconf /etc/bind/named.conf.local
```

PASO 9. Crea una nueva carpeta para almacenar los archivos de zona llamada 'zonas':

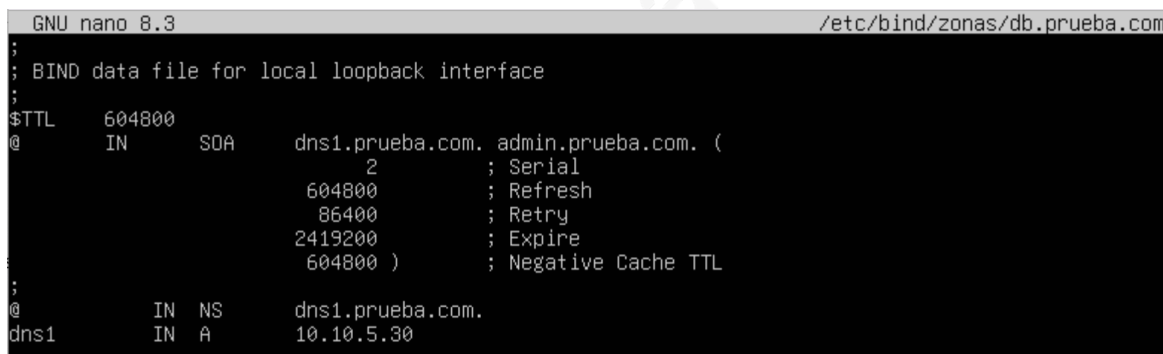
```
sudo mkdir /etc/bind/zonas
```

PASO 10. Configura el archivo de zona directa "db.prueba.com" (**debes poner tu nombre**) con todos los registros de recursos (RR) de la zona.

Primero, hacemos una copia del archivo predefinido 'db.local' en nuestro archivo de zona 'db.prueba.com'.

→ `cp /etc/bind/db.local /etc/bind/zonas/db.prueba.com`

Después, editamos nuestro archivo para modificar las opciones necesarias.



```
GNU nano 8.3 /etc/bind/zonas/db.prueba.com
; BIND data file for local loopback interface
$TTL 604800
@ IN SOA dns1.prueba.com. admin.prueba.com. (
    2 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS dns1.prueba.com.
dns1 IN A 10.10.5.30
```

*** PREGUNTA:** ¿Qué se está configurando dentro de este archivo?

*** PREGUNTA:** Explica para qué sirve cada uno de los registros de recursos (RR) incluidos en el archivo.

*** PREGUNTA:** ¿Se podrían definir otros registros de recursos (RR) en el archivo? Indica cuáles.

PASO 11. Configura el archivo de zona inversa con todos los registros de recursos (RR) de la zona:

Primero, hacemos una copia del archivo predefinido 'db.127' en nuestro archivo de zona 'db.5.10.10'.

➔ `cp /etc/bind/db.127 /etc/bind/zonas/db.5.10.10`

Después, editamos nuestro archivo para modificar las opciones necesarias.

```
GNU nano 8.3 /etc/bind/zonas/db.5.10.10
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      dns1.prueba.com. admin.prueba.com. (
                        1      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
30        IN      NS       dns1.prueba.com.
30        IN      PTR      dns1.prueba.com.
```

* **PREGUNTA:** ¿Qué se está configurando dentro de este archivo?

* **PREGUNTA:** ¿En el archivo de zona inversa se han configurado los mismos RR que en el archivo de zona directa?

PASO 12. Verifica que los archivos de zona, tanto el de la zona directa como el de la zona inversa, sean correctos:

```
>> sudo named-checkzone prueba.com /etc/bind/zonas/db.prueba.com
>> sudo named-checkzone 5.10.10.in-addr.arpa /etc/bind/zonas/db.5.10.10
```

PASO 13. Finalmente, cada vez que realices cambios en la configuración, debes reiniciar el servicio DNS para que los cambios tengan efecto. Además, debes comprobar el estado del servicio:

```
>> sudo systemctl restart bind9
>> sudo systemctl status bind9
```

PARTE 2. CONFIGURACIÓN DEL CLIENTE DNS EN UBUNTU

En esta segunda parte de la práctica, debes encender la máquina cliente con Linux Ubuntu.

Configura los parámetros de red en el archivo netplan, como se muestra a continuación:

```
GNU nano 8.3 /etc/netplan/50-cloud-init.yaml
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      dhcp4: false
      addresses:
        - 10.10.5.50/24
      nameservers:
        addresses:
          - 10.10.5.30
      search:
        [prueba.com]
```

Recuerda aplicar los cambios con “sudo netplan apply”.

En esta última parte de la práctica, debes tener encendida la máquina cliente y también el servidor DNS.

En este caso, vamos a realizar consultas desde el cliente a nuestro servidor DNS local sobre el dominio definido en nuestro servidor. Debemos comprobar que el servidor DNS responde correctamente al cliente en todas sus consultas. Para ello, vamos a probar las diferentes herramientas DNS. Debes probar **dig**, **host** y **nslookup**. El uso de estas herramientas está explicado en el documento ‘**Herramientas DNS**’ de Aules.

Aquí os pongo un ejemplo de prueba con la herramienta nslookup:

```
profesora@profesora-Clienteprivado:~$ nslookup dns1.prueba.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   dns1.prueba.com
Address: 10.10.5.30
```