9 Guía Servidor DNS

MATERIAL

- Los contenidos de la unidad y esta guía
- Máquinas Virtuales Ubuntu 22.04 Desktop (1 limpia + 1 Servidor Web).
- Virtualbox
- Ordenador con S.O. Windows 10.
- Navegador para comprobar la realización de la tarea.
- Procesador de textos para elaborar la documentación y los archivos de la tarea.
- Acceso a Internet.

9.1 Instalación Servidor DNS – BIND

1. Realizar la instalación del Servidor DNS BIND y habilitar el servicio bind9 para que se permita el acceso a él desde el firewall de Ubuntu

   En esta actividad instalaremos el Servidor DNS Bind para resolver los nombres de red con un dominio **nombre_del_alumno.net** en una máquina Ubuntu 22.04 LTS, dentro de una red privada que crearemos poniendo la tarjeta de red del servidor DNS en adaptador puente.

   Para instalar en Servidor DNS emplearemos los paquetes de los repositorios del sistema.

   El primer paso será actualizar los repositorios.

   Actualizamos las listas de paquetes y sus versiones.

   #apt get update

   Realizamos la actualización de los paquetes.

   #apt get upgrade

Para instalar el paquete bind9.

#sudo apt-get install -y bind9

```
informatica@informatica-VirtualBox:~$ sudo apt install -y bind9
[sudo] contraseña para informatica:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  libfprint-2-tod1 libllvm10 linux-headers-5.4.0-54
  linux-headers-5.4.0-54-generic linux-image-5.4.0-54-generic
```

Una vez descargado e instalado el Bind y sus dependencias se crea un nuevo servicio en Ubuntu 22.04. El servicio es bind9 o bind9.service.

De igual modo que hemos realizado hasta ahora podemos ver su estado, parar el servicio, recargarlo o reiniciarlo. Comprobamos que está activo:

#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 Sat 2022-01-08 10:00:27 WET; 2min 55s ago
       Docs: man:named(8)
   Main PID: 36327 (named)
      Tasks: 8 (limit: 2299)
     Memory: 18.9M
     CGroup: /system.slice/named.service
             └─36327 /usr/sbin/named -f -u bind

ene 08 10:00:28 informatica-VirtualBox named[36327]: network unreachable resolving './DNSKEY/IN': 2001:503:ba3e::2:30#53
ene 08 10:00:28 informatica-VirtualBox named[36327]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
ene 08 10:00:28 informatica-VirtualBox named[36327]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0d#53
ene 08 10:00:28 informatica-VirtualBox named[36327]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
ene 08 10:00:28 informatica-VirtualBox named[36327]: network unreachable resolving './DNSKEY/IN': 2001:500:200::b#53
ene 08 10:00:28 informatica-VirtualBox named[36327]: network unreachable resolving './NS/IN': 2001:500:200::b#53
ene 08 10:00:28 informatica-VirtualBox named[36327]: network unreachable resolving './DNSKEY/IN': 2001:7fe::53#53
ene 08 10:00:28 informatica-VirtualBox named[36327]: network unreachable resolving './NS/IN': 2001:7fe::53#53
ene 08 10:00:28 informatica-VirtualBox named[36327]: managed-keys-zone: Initializing automatic trust anchor management for zone '.'; DNSKEY I
ene 08 10:00:28 informatica-VirtualBox named[36327]: resolver priming query complete
```

En la anterior captura vemos que nos aparecen una serie de advertencias de resolución irrecuperable de red. Al tratarse de una red local es normal que nos muestre esos errores. En los siguientes párrafos lo solucionaremos.

Configuramos el firewall de Ubuntu 22.04 para permitir el acceso al DNS Bind.

#sudo ufw allow bind9

```
informatica@informatica-VirtualBox:~$ sudo ufw allow bind9
Reglas actualizadas
Reglas actualizadas (v6)
```

9.2 Configurar Servidor y Clientes DNS - BIND

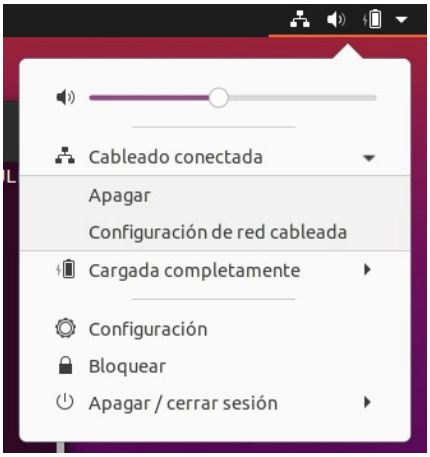
2. Configurar los clientes de red para usar el servicio DNS Bind de Ubuntu 22.04

   Para que los clientes hagan uso del Servidor DNS que estamos instalando se puede hacer introduciendo en el DHCP del router que envíe como servidor de nombres (DNS) la dirección IP del servidor que estamos configurando. De este modo de manera automática los equipos clientes tomarían la IP de nuestro servidor.

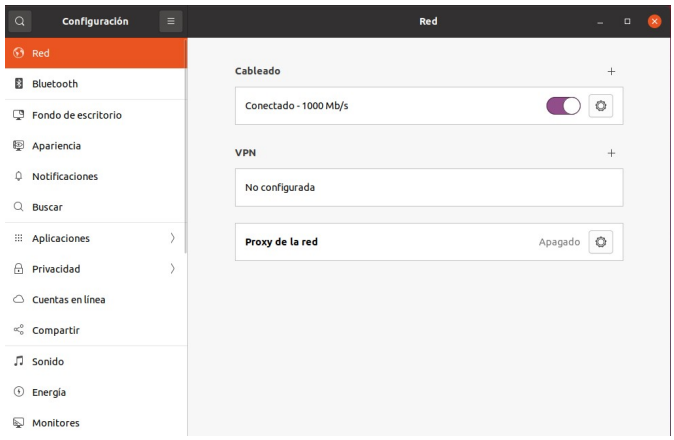
   Contamos con la posibilidad si no tenemos acceso a la configuración DHCP del router de asignar de manera manual la IP del Servidor DNS, pudiendo dejar el direccionamiento DHCP de manera automática y asignando de manera manual las DNS.

   Para hacer la configuración de la DNS en el cliente en Ubuntu lo conseguimos por medio del Netplan, editando el archivo de configuración de la interfaz de red o también de manera gráfica.

   Esta configuración la realizamos de manera gráfica. Accedemos en la parte superior pulsando sobre el icono de red.

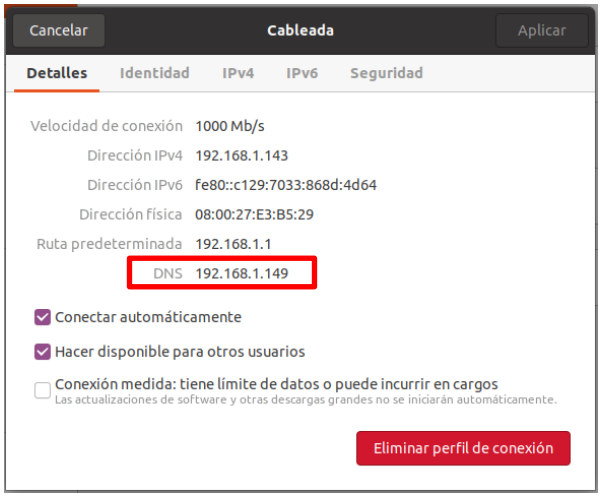


Seleccionamos “Configuración de red cableada” y accedemos a la siguiente pantalla, en la que debemos pulsar sobre la rueda dentada.



En la ventana que se nos abre, seleccionamos la pestaña de IPv4 y en la parte de DNS, desplazamos el botón de automático para apagarlo y ponemos la IP de nuestro Servidor en el casillero, pulsamos en Aplicar.

Para que la nueva configuración sea operativa en la ventana de la rueda dentada deslizamos el botón para apagar la conexión de red y la volvemos a deslizar para encenderla. Si pulsamos en la rueda dentada debemos de tener configurada la IP de nuestro Servidor de DNS.



3. Configurar el Servidor DNS Bind en Ubuntu 22.04 LTS para el dominio **nombre_del_alumno.net**, donde debe personlizar cada alumno el nombre del dominio con su nombre.

   Los archivos para realizar la configuración del Servidor DNS se encuentran en la ruta /etc/bind/.

   El archivo principal es **named.conf** que se limita a cargar las configuraciones de los archivos **named.conf.options**, **named.conf.local** y **named.conf.default-zones**.

   En nuestro caso sólo vamos a trabajar con el protocolo IPv4, por lo que vamos a configurarlo en el archivo /etc/default/named.

   #sudo nano /etc/default/named

   Lo editamos añadiendo el parámetro -4, quedando:

```
  GNU nano 4.8                    /etc/default/named
#
# run resolvconf?
RESOLVCONF=no

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

   Guardamos, cerramos y recargamos el servicio.

   #sudo systemctl reload bind9

Desactivamos el DNSSEC, al trabajar con un Servidor DNS local, no funcionará la capa de seguridad DNSSEC. Para desactivarla editamos el archivo named.conf.options.

#sudo nano /etc/bind/named.conf.options

Buscamos en el archivo dnssec con Ctrl+W, comentamos la línea existente y añadimos:

```
#dnssec-validation auto;

dnssec-validation no;
```

Quedando:

```
        #dnssec-validation auto;
        dnssec-validation no;
        listen-on-v6 { any; };
};
```

Guardamos, cerramos y recargamos la configuración del servidor DNS.

#sudo systemctl reload bind9

Si comprobamos el estado del servicio veremos que ya no nos aparece los mensajes de advertencia.

```
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2022-01-09 09:06:32 WET; 2h 21min ago
       Docs: man:named(8)
    Process: 4645 ExecReload=/usr/sbin/rndc reload (code=exited, status=0/SUCCESS)
   Main PID: 734 (named)
      Tasks: 8 (limit: 2299)
     Memory: 34.8M
     CGroup: /system.slice/named.service
             └─734 /usr/sbin/named -f -u bind

ene 09 11:27:58 informatica-VirtualBox named[734]: automatic empty zone: HOME.ARPA
ene 09 11:27:58 informatica-VirtualBox named[734]: none:100: 'max-cache-size 90%' - setting to 1782MB (out of 1980MB)
ene 09 11:27:58 informatica-VirtualBox named[734]: configuring command channel from '/etc/bind/rndc.key'
ene 09 11:27:58 informatica-VirtualBox named[734]: configuring command channel from '/etc/bind/rndc.key'
ene 09 11:27:58 informatica-VirtualBox named[734]: reloading configuration succeeded
ene 09 11:27:58 informatica-VirtualBox named[734]: reloading zones succeeded
ene 09 11:27:58 informatica-VirtualBox rndc[4645]: server reload successful
ene 09 11:27:58 informatica-VirtualBox systemd[1]: Reloaded BIND Domain Name Server.
ene 09 11:27:58 informatica-VirtualBox named[734]: all zones loaded
ene 09 11:27:58 informatica-VirtualBox named[734]: running
```

Resolución de nombres de Internet (fordwardind)

Para permitir que además de resolver los nombres de la red local se puedan resolver los nombres de Internet, tenemos que habilitar la recursión. En este caso tenemos que editar nuevamente el archivo anterior, named.conf.options.

#sudo nano /etc/bind/named.conf.options

En el bloque **options**, descomentamos el bloque forwarders y añadiremos las direcciones de los servidores DNS que pueden resolver nombres de Internet.

Configurar zona o dominios

Creamos un archivo de zona para el dominio, normalmente se utiliza el dominio como parte del nombre del archivo, lo que permite facilitar la configuración. En este caso vamos a crear el archivo de zona para el dominio de red local **nombre_del_alumno.net**. En las siguientes capturas yo he empleado en nombre_del_alumno, cristobal, cada alumno que emplee su nombre.

Vamos a aprovechar la estructura de uno de los archivos de zona para crear el nuestro p.e. db.empty, para lo que haremos una copia con el nombre de nuestra zona.

#sudo cp /etc/bind/db.empty /etc/bind/db.nombre_del_alumno.net

Una vez efectuada la copia procedemos a editarlo.

#sudo nano /etc/bind/db.nombre_del_alumno.net

```
  GNU nano 4.8                                          /etc/bind/db.cristobal.net
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    1D
@       IN      SOA     ns.cristobal.net. root.cristobal.net. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL

;Registros NS (Servidores de nombres)

        IN      NS      ns.cristobal.net.

;Registros A

ns.cristobal.net.       IN      A       192.168.1.149
```

Donde debemos de personalizar el nombre de archivo y el dominio con el nombre de cada alumno. Además de poner la IP de nuestro servidor DNS.

Esta configuración inicial se encarga de definir el dominio y el servidor DNS que lo gestiona, que en este caso es nuestro servidor Ubuntu 22.04.

Se ha incluido un registro SOA, un registro NS y un registro A.

En la línea que comienza por @, el registro SOA o «Start of Authority», indicamos cuál es el servidor de nombres del dominio y la dirección de correo electrónico del administrador, especificada sin el carácter @, es decir, root@nombre_del_alumno.net se indica como root.localnet.net. Puedes utilizar el nombre que quieras para tu servidor DNS, pero los cambios deben ser consistentes.

Como prueba vamos a sustituir el nombre del servidor ns por dns1, enlazándola a la misma cuenta de correo del administrador.

Es importante no olvidar los puntos al final de cada nombre de máquina.

La línea etiquetada como ‘serial‘ recoge un número que deberá incrementarse manualmente cada vez que editemos este archivo, ya sea para modificar nombres o añadir nuevos.

Observa que el registro NS está indentado, ya que si no lo está la configuración no funcionará.

Editamos el archivo db.nombre_del_alumno.net nuevamente, para introducir los cambios indicados.

#sudo nano /etc/bind/db.nombre_del_alumno.net

```
  GNU nano 4.8                                          /etc/bind/db.cristobal.net
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    1D
@       IN      SOA     dns1.cristobal.net. root.cristobal.net. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL

;Registros NS (Servidores de nombres)

        IN      NS      dns1.cristobal.net.

;Registros A

dns1.cristobal.net.     IN      A       192.168.1.149
```

Guardamos y cerramos el archivo.

Realizamos una comprobación para ver si la configuración es correcta. Para ello empleamos el comando **named-checkzone** al que le pasamos como parámetros el dominio que queremos comprobar.

#sudo named-checkzone nombre_del_alumno.net /etc/bind/db.nombre_del_alumno.net

```
informatica@informatica-VirtualBox:/$ sudo named-checkzone cristobal.net /etc/bind/db.cristobal.net
zone cristobal.net/IN: loaded serial 2
OK
```

Una vez que la configuración inicial es correcta, podemos editar el archivo de nuevo y añadir nombres de máquinas de nuestra red y sus correspondientes direcciones IP, mediante registros A adicionales y actualizamos el serial, quedando como se muestra:

```
 GNU nano 4.8                                    /etc/bind/db.cristobal.net
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    1D
@       IN      SOA     dns1.cristobal.net. root.cristobal.net. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL

;Registros NS (Servidores de nombres)

        IN      NS      dns1.cristobal.net.

;Registros A

dns1.cristobal.net.     IN      A       192.168.1.149
router.cristobal.net.   IN      A       192.168.1.1
web.cristobal.net.      IN      A       192.168.1.143
```

Volvemos a comprobar con el named-checkzone.

#sudo named-checkzone nombre_del_alumno.net /etc/bind/db.nombre_del_alumno.net

```
informatica@informatica-VirtualBox:/$ sudo named-checkzone cristobal.net /etc/bind/db.cristobal.net
zone cristobal.net/IN: loaded serial 3
OK
```

Para que esta configuración sea tenida en cuenta por el servicio DNS Bind, será necesario incluirla desde el archivo *named.conf.default-zones*, así que lo editamos.

#sudo nano /etc/bind/named.conf.default-zones

Añadimos el siguiente bloque al final del archivo.

```
zone "cristobal.net" IN {
        type master;
        file "/etc/bind/db.cristobal.net";
};
```

Una vez configurado el servicio, recargamos el servicio.

#sudo systemctl reload bind9

Comprobación funcionamiento

Podemos realizar la comprobación del funcionamiento realizando ping al dominio y subdominios creados desde la máquina cliente.

#ping dns1.nombre_del_alumno.net

```
informatica@informatica-dpl:~$ ping dns1.cristobal.net
PING dns1.cristobal.net (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149 (192.168.1.149): icmp_seq=1 ttl=64 time=0.446 ms
64 bytes from 192.168.1.149 (192.168.1.149): icmp_seq=2 ttl=64 time=1.34 ms
64 bytes from 192.168.1.149 (192.168.1.149): icmp_seq=3 ttl=64 time=1.37 ms
```

#ping web.nombre_del_alumno.net

```
informatica@informatica-dpl:~$ ping web.cristobal.net
PING web.cristobal.net (192.168.1.143) 56(84) bytes of data.
64 bytes from informatica-dpl (192.168.1.143): icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from informatica-dpl (192.168.1.143): icmp_seq=2 ttl=64 time=0.106 ms
```

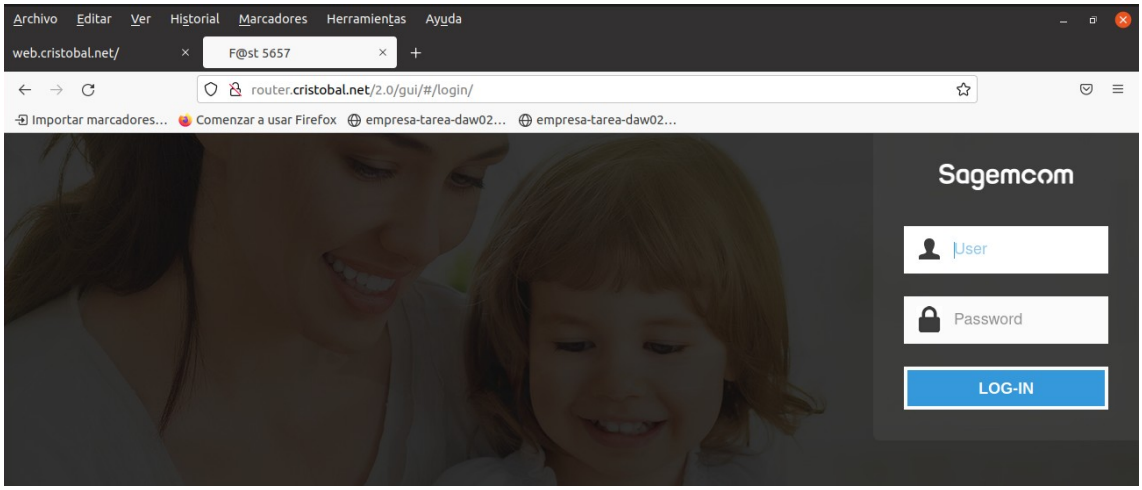
#ping router.nombre_del_alumno.net

```
informatica@informatica-dpl:~$ ping router.cristobal.net
PING router.cristobal.net (192.168.1.1) 56(84) bytes of data.
64 bytes from _gateway (192.168.1.1): icmp_seq=1 ttl=64 time=9.21 ms
64 bytes from _gateway (192.168.1.1): icmp_seq=2 ttl=64 time=1.67 ms
```

También podemos hacer la comprobación vía navegador web.

web.nombre_del_alumno.net

router.nombre_del_alumno.net



4. Configurar el Servidor DNS para que posibilite la resolución inversa de DNS.

   La resolución inversa DNS consiste que dada una IP obtenemos el nombre de dominio.

   Para realizar esto creamos un nuevo archivo de zona correspondiente a nuestra dirección de red.

   Lo primero es hacer una copia para tener un archivo de referencia, vamos tomar el db.nombre_del_alumno.net como referencia.

   #sudo cp /etc/bind/db. nombre_del_alumno.net **/etc/bind/db.1.168.192.net**

   Una vez realizada la copia, procedemos a editar el archivo de zona.

   #sudo nano /etc/bind/db.1.168.192

   Quedando como se muestra.

```
  GNU nano 4.8                  /etc/bind/db.1.168.192
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    1D
@       IN      SOA     dns1.cristobal.net. root.cristobal.net. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL

        IN      NS      dns1.cristobal.net.

;Registros PTR

1       IN      PTR     router.cristobal.net.
143     IN      PTR     web.cristobal.net.
149     IN      PTR     dns1.cristobal.net.
```

El registro SOA ahora indica el dominio o zona a la que corresponde la resolución inversa, también incluye la dirección de correo-e del administrador y los parámetros de número de serie y tiempos.

Recuerda incrementar el número de serie si haces cambios en este archivo.

Para asociar la parte de dirección de máquina de la dirección IP con los nombres DNS usamos registros PTR.

En este ejemplo usamos una red clase C, así que usamos los 3 primeros números (dirección de red) para el nombre del archivo de zona y el cuarto y último número para los registros PTR.

Guardamos los cambios y comprobamos la corrección del archivo con named-checkzone:

#sudo named-checkzone 1.168.192 /etc/bind/db.1.168.192

```
informatica@informatica-VirtualBox:~$ sudo named-checkzone 1.168.192 /etc/bind/d
b.1.168.192
zone 1.168.192/IN: loaded serial 1
OK
```

Ahora introducimos la nueva zona en named.conf.default-zones

#sudo nano /etc/bind/named.conf.default-zones

Añadimos el siguiente bloque al final del archivo.

```
zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.1.168.192";
};
```

Hacemos una comprobación de los archivos de configuración.

#sudo named-checkconf

```
informatica@informatica-VirtualBox:~$ sudo named-checkconf
informatica@informatica-VirtualBox:~$
```

Recargamos el servicio Bind para que se apliquen los cambios realizados.

#sudo systemctl reload bind9

Ahora realizamos la comprobación de que hace la resolución inversa desde el cliente.

#nslookup 192.168.1.1

```
informatica@informatica-dpl:~$ nslookup 192.168.1.1
1.1.168.192.in-addr.arpa        name = router.cristobal.net.

Authoritative answers can be found from:
```

 # nslookup 192.168.1.143

```
informatica@informatica-dpl:~$ nslookup 192.168.1.143
143.1.168.192.in-addr.arpa      name = web.cristobal.net.

Authoritative answers can be found from:
```

#nslookup 192.168.1.149

```
informatica@informatica-dpl:~$ nslookup 192.168.1.149
149.1.168.192.in-addr.arpa      name = dns1.cristobal.net.

Authoritative answers can be found from:
```