

PRÁCTICA 3:

Servidor DNS BIND en Linux. Instalación, configuración como solo caché y configuración para que reenvíe consultas recursivas.

Instala y configura un servidor DNS *BIND* en ServidorDNSXX para que actúe como solo *cache* y responda a consultas recursivas. Posteriormente configúralo para que reenvíe las consultas recursivas al servidor DNS del centro liberando de tráfico a la red.

1. Instalación

- 1.1. Inicia una sesión en ServidorDNSXX con un usuario con privilegios de administrador.
- 1.2. Abre un terminal del Linux desktop llamado ServidorDNSXX e instala el servidor *BIND* (también puedes utilizar el centro de software de *Ubuntu* el gestor de paquetes *Synaptic*).

```
sudo apt-get update
sudo apt install bind9
```

- 1.3. Comprueba que el servidor (proceso *named*) se ha iniciado al terminar la instalación

```
ps -ef | grep named           o bien

udo service bind9 status      (pulsas CTRL+C para salir)
```

- 1.4. Comprueba que el servidor está a la escucha en los puertos 53 TCP y UDP.

```
sudo netstat -tln
```

- 1.5. En *Ubuntu* los ficheros de configuración de *BIND* se guardan por defecto en el `/etc/bind`. Accede a ese directorio y consulta los ficheros de configuración para analizarlos.

■ `/etc/bind/named.conf`

- Fichero de configuración principal.
- No se suele modificar.
- Almacena la configuración de las diferentes zonas generadas por defecto en el momento de la instalación.
- Incluye los ficheros (mediante la directiva ***include***):
 - o `/etc/bind/named.conf.options`
 - o `/etc/bind/named.conf.local`
 - o `/etc/bind/named.conf.default-zones`

■ `/etc/bind/named.conf.options`

- Configuración de opciones generales de funcionamiento del servidor.

■ `/etc/bind/named.conf.local`

- Fichero de configuración de zonas.
- Se declaran las zonas de resolución directa y de resolución inversa del servidor.

■ `/etc/bind/named.conf.default-zones`

- Contienen la declaración de las zonas por defecto que tiene creadas BIND.

■ Ficheros de zonas

- Ficheros que definen los registros de recursos de cada zona.

- Son referenciados desde las declaraciones de zonas en **/etc/bind/named.conf.local**.
- Al instalar el servidor se crean un conjunto de archivos de zonas por defecto
 - o **/etc/bind/db.local**: Resolución directa del bucle local.
 - o **/etc/bind/db.127**: Resolución inversa del bucle local.
 - o **/etc/bind/db.0**: Resolución inversa *broadcast*.
 - o **/etc/bind/db.255**: Resolución inversa *broadcast*.

1.6. Haz una copia de seguridad de los ficheros de configuración que se modificarán en esta y sucesivas prácticas (**/etc/bind/named.conf.options** y **/etc/bind/named.conf.local**).

2. Configuración del servidor como solo *cache*

Por defecto el servidor está configurado como solo *cache* (no es autorizado para ninguna zona) que responde a consultas recursivas (tiene la recursividad activada).

- 2.1. Cambia en el fichero **/etc/netplan/00-installer-config.yaml** la IP del nameserver por tu propia IP, que sería 192.168.0.15
- 2.2. Aplica el cambio.
- 2.3. Comprueba que el cambio está presente en el archivo **/run/systemd/resolve/resolv.conf**
- 2.4. Inicia sesión en *ClienteLinuxXX*.
- 2.5. Configura el cliente DNS *ClienteLinuxXX* para que utilice el servidor DNS instalado en la máquina local (192.168.0.15) y comprueba que en el archivo **/run/systemd/resolve/resolv.conf** está presente el cambio.
- 2.6. Usa el comando *nslookup* para resolver un nombre.
- 2.7. Usa el comando *dig* para preguntar por un nombre de dominio diferente al usado en el punto 2.6. Comprueba el tiempo de respuesta.
- 2.8. Vuelve a usar el comando *dig* para preguntar por el mismo nombre de dominio. Comprueba que el tiempo de respuesta es mucho menor porque el servidor ha consultado su *cache*.
- 2.9. Ejecuta sucesivas veces el mismo comando y observa como el campo TTL de los registros de recursos de la respuesta decrementa.
- 2.10. Vuelve al equipo *ServidorDNSXX*.

3. Configuración del servidor para que reenvíe consultas a reenviadores (*forwarders*)

- 3.1. Edita el fichero de configuración **named.conf.options** y configura como reenviador el servidor DNS del centro eliminando el comentario de la directiva **forwarders** dejándolo de esta forma:

```
forwarders {
    212.142.144.66;
    212.142.144.98;
};
```

- 3.2. Reinicia el servidor para que tengan efecto los cambios realizados.

```
sudo service bind9 restart
```

- 3.3. Comprueba el fichero de logs del sistema (**/var/log/syslog**) y verifica que no se han producido fallos al arrancar el servidor.

4. Otras consideraciones

- 4.1. Para ver cual es el servidor DNS que estamos utilizando en nuestro propio equipo poner:

`sudo systemd-resolve --status`

```
Link 2 (ens33)
    Current Scopes: DNS
DefaultRoute setting: yes
    LLMNR setting: yes
MulticastDNS setting: no
    DNSOverTLS setting: no
    DNSSEC setting: no
    DNSSEC supported: no
    DNS Servers: 192.168.0.15
lines 8-43/43 (END)
```

4.2 Para ver la cache

`sudo systemd-resolve --statistics`

```
servidordns01@servidordns01:~$ sudo systemd-resolve --statistics
DNSSEC supported by current servers: no

Transactions
Current Transactions: 0
Total Transactions: 33

Cache
Current Cache Size: 3
Cache Hits: 0
Cache Misses: 3

DNSSEC Verdicts
Secure: 0
Insecure: 0
Bogus: 0
Indeterminate: 0
```

4.3 Para borrar la cache

`sudo systemd-resolve --flush-caches`

```
servidordns01@servidordns01:~$ sudo systemd-resolve --flush-caches
servidordns01@servidordns01:~$ sudo systemd-resolve --statistics
DNSSEC supported by current servers: no

Transactions
Current Transactions: 0
Total Transactions: 33

Cache
Current Cache Size: 0
Cache Hits: 0
Cache Misses: 3

DNSSEC Verdicts
Secure: 0
Insecure: 0
Bogus: 0
Indeterminate: 0
```

Cliente DNS BIND en Linux. Configuración

a) Editando ficheros de configuración

1. Inicia una sesión en ClienteLinuxXX.
2. Consulta el contenido del fichero **/etc/nsswitch.conf**. En este fichero se define el orden que usa el *resolv* a la hora de buscar información sobre nombres de dominio. El servicio DNS se identifica con la palabra *hosts* al principio de la línea. Observa que el orden definido es, en primer lugar, **files** (se busca en el fichero **/etc/hosts**) y en segundo lugar **mdns4** (se busca en los servidores DNS definidos en el fichero **/run/systemd/resolve/resolv.conf**).

3. Edita el fichero **/run/systemd/resolve/resolv.conf**

Este fichero consta de un conjunto de directivas a los que se les puede asociar valores

<atributo> <valor1> <valor2> <valorN>

El atributo más importante es **nameserver** que permite especificar las direcciones IP de los servidores DNS que consultará el *resolv*. Se consultan en el orden que aparecen definidos. Otros atributos muy utilizados son **domain** seguida del nombre del dominio al que pertenece el equipo y el que se añadirá a las búsquedas de nombres no cualificados (este nombre de dominio deberá ser el mismo que el indicado en el archivo */etc/defaultdomain*) y **search** seguida de uno o varios dominios separados por espacios que especifica la lista de dominios en las búsquedas de nombres no cualificados (es decir, cuando la consulta especifica un nombre de equipo pero ningún nombre de dominio) Las opciones **search** y **domain** son mutuamente excluyentes y no deben aparecer a la vez. Si hay más de una instancia de estas palabras clave, la última instancia gana.

4. Usa la directiva **nameserver** para configurar como servidor DNS preferido el servidor DNS instalado y como secundario el servidor DNS *cache* de *Google* (8.8.8.8).

nameserver 172.16.10.XX5

nameserver 8.8.8.8

Nota: si se utiliza una distribución de Linux que ofrezca herramienta gráfica para configurar los servidores DNS, como por ejemplo Ubuntu Desktop, se recomienda editar el fichero manualmente.

5. Haz un ping a **www.google.es** y verifica que resuelve el nombre correctamente.
6. Haz un ping a **ClienteLinuxXX.dawXX.net** y comprueba que el servidor no es capaz de resolver el nombre DNS.
7. Edita el fichero **/etc/hosts** en el cliente y añade una entrada para el nombre ClienteLinuxXX.dawXX.net asociado con la IP 172.16.10.XX9 siendo esta la IP del ClienteLinuxXX.
8. Haz un ping a ClienteLinuxXX.dawXX.net y comprueba que en esta ocasión si se resuelve el nombre porque el cliente DNS ha mirado en primer lugar en el archivo **/etc/hosts**.
9. Edita el fichero **/etc/hosts** y borra la entrada para el nombre ClienteLinux.dawXX.net creada anteriormente.

10. Edita el fichero **/run/systemd/resolve/resolv.conf** y borra la entrada para el servidor secundario DNS

Nota: Normalmente el archivo **/etc/hosts** siempre contiene por defecto la línea correspondiente al equipo local *localhost*. Cada línea de este archivo especifica una dirección IP y su correspondiente nombre de equipo. El archivo **/etc/hosts** se ha utilizado tradicionalmente para resolver direcciones en pequeñas redes y conseguir un acceso rápido a través de los nombres de los equipos. Sin embargo en redes grandes o con dominios más complejos, es imposible realizar una gestión eficaz de este modo.

b) Usando herramientas gráficas

1. Inicia una sesión en ClienteLinuxXX con un usuario con privilegios de administración.
2. Accede al icono de red -> Cableado conectado -> Configuración de red cableada -> Icono dentado de netplan-ens33-> accede a las propiedades TCP/IP versión 4 del adaptador de red y observa que existe un campo en el que es posible definir uno o varios servidores DNS separados por comas. También se pueden definir los dominios de búsqueda.
3. Introduce como servidor DNS preferido el servidor DNS del centro.
4. Aplica los cambios. Desactiva y activa la conexión de red para que los cambios tengan efecto.
5. Abre un terminal y consulta el fichero **/run/systemd/resolve/resolv.conf** Observa que ha creado una directiva **nameserver**, para el servidor DNS configurado.
6. Haz un ping a www.google.es y verifica que se resuelve el nombre correctamente.