PRÁCTICA 4

Configuración del servidor DNS BIND en Linux.

Configuración del servidor como primario (maestro) para una zona de resolución directa y una zona de resolución inversa.

Para montar el servidor DNS hemos utilizado una máquina con Ubuntu Server y el paquete BIND. BIND (Berkeley Internet Name Domain, anteriormente: Berkeley Internet Name Daemon) es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un estándar de facto.

Configura el servidor BIND de **ServidorDNSXX**

- El servidor sólo servirá a la red local (no sirve a equipos de Internet).
- Actuará como maestro y tendrá autoridad sobre el dominio **dawXX.net.**
    - El servidor DNS maestro del dominio será ServidorDNS.dawXX.net (es decir el equipo donde está instalado en servidor DNS) (registro NS).
    - Los nombres de los equipos serán los representados en el esquema de la red (clientelinuxXX, servidorlinuxXX, Desarrollow7XX…)
    - Se configurarán los siguientes alias (registros CNAME)
        - ns1.dawXX.net será un alias de ServidorDNSXX.dawXX.net.
        - www.dawXX.net será un alias de servidorlinuxXX.dawXX.local.
        - ftp.dawXX.net será un alias de Servidorw2008XX.dawXX.net.
    - El tiempo en cache de las respuestas negativas de la zona será de 1 semana.
- Actuará como maestro y tendrá autoridad sobre la zona de resolución inversa de la red 192.168.0.0/24
    - El servidor DNS maestro del dominio será servidordnsXX.dawXX.net (es decir, el equipo donde está instalado en servidor DNS) (registro NS)
    - Las direcciones IP de los equipos se corresponderán con las representadas en el esquema de la red (registro PTR).
    - El tiempo en cache de las respuestas negativas de la zona será de 1 semana.

Configura los equipos de la red para que usen el servidor DNS instalado en ServidordnsXX y añadan el sufijo dawXX.net a los nombres de dominio no FQDN.

Instalación de BIND

Para instalar BIND simplemente escribimos el siguiente comando:

- sudo apt install bind9

Configuración de los archivos de BIND

Los archivos de configuración que tendremos que **modificar en el servidor DNS** son los siguientes:

- /etc/bind/named.conf
- /etc/bind/named.conf.options
- **/etc/bind/named.conf.local**
- **/etc/bind/db.dawXX.net**
- **/etc/bind/db.192.168.0**

En todos los ordenadores de la red, tendrá que quedar modificado el archivo **/run/systemd/resolve/resolv.conf**.

1. Configuración del dominio de búsqueda en el servidor DNS

En el equipo que será servidor DNS, accede a **/etc/netplan/00-installer-config.yaml** e introduce en el apartado Dominios de búsqueda tu dominio, por ejemplo "daw01.net". Aplica los cambios. Consulta el fichero **/run/systemd/resolve/resolv.conf**. Observa que se ha creado una directiva **search** para definir el dominio configurado.

```
  GNU nano 4.8                  /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      dhcp4: no
      addresses: [192.168.0.15/24]
      gateway4: 192.168.0.1
      nameservers:
        addresses: [192.168.0.15]
        search: [daw01.net]
  version: 2
```

2. Configuración de la zona de resolución directa e inversa

El archivo **named.conf** en realidad no es necesario que lo modifiquemos. Este archivo almacena la configuración de las diferentes zonas generadas por defecto en el momento de la instalación.

Para modificar el archivo **/etc/bind/named.conf.local** podemos utilizar cualquier editor de textos, como nano o vi.

sudo nano /etc/bind/named.conf.local

Una vez abierto tendremos que poner lo siguiente (lo que hay tras el carácter # son comentarios).

#Esta es la definición de la zona.

zone dawXX.net { < ---------- CUIDADO: Sin punto al final
type master;
file "/etc/bind/db.dawXX.net";
};

#Aquí definimos la zona de resolución inversa.

zone 0.168.192.in-addr.arpa { < ---------- CUIDADO: Sin punto al final
type master;
file "/etc/bind/db.192.168.0″;
};

A continuación modificamos el fichero **/etc/bind/named.conf.options**. En este fichero especificaremos aquellos servidores DNS de Internet que resolverán los nombres de dominio que nuestro servidor DNS local no pueda resolver. (NO HACER)

options {
directory "/var/cache/bind";

forwarders {
212.142.144.66;
212.142.144.98;
};

};

Después tendremos que crear el fichero de definición de zona **/etc/bind/db.dawXX.net**. En este fichero es donde pondremos todos los nombres de máquinas y direcciones IP que conocerá nuestro servidor DNS (además de un registro IN SOA y un IN NS).

$TTL 604800

//TTL (Time To Live) de respuestas positivas (Registros de recursos de nombres
//resueltos). Es el número de segundos que puede estar el registro en caché antes de ser
//descartado. Definido con $ sirve de modo global a todos los registros de recursos.
//Recomendado 1día o más.

@ IN SOA servidordnsXX.dawXX.net. administrador.dawXX.net. (

//aulaMS2.com. situado delante del IN es el nombre de la Zona y podría sustituirse por
//@. administrador.aulaMS2.com. es el correo de la persona responsable del dominio.

// Obligatorio el espacio en blanco antes del paréntesis. *Las siguientes líneas no es necesario que las modifiquemos*

2020091502 ;Serial
604800 ;Refresh
86400 ;Retry
2419200 ;Expire
604800) ;Negative Cache TTL

;

//TTL de respuestas negativas (Información de que no existen registros de recursos //para un nombre consultado) El máximo recomendado que sea de una semana.

//Ahora definimos los servidores DNS del dominio

@ IN NS servidordnsXX.dawXX.net.

//dawXX.net. situado delante de IN es el nombre de la Zona y podría colocarse @

//Cambia los nombres máquinas y direcciones IP por las de tu red

//Ahora definimos los Hosts del dominio

servidordnsXX IN A 192.168.0.XX5

//Como servidor no termina en "." equivale a ServidorDNSXX.aulaMS2.com

servidorlinuxXX.dawXX.net. IN A 192.168.0.XX6

//Como servidorlinuxXX.dawXX.net. termina en "." no se completa con el nombre de la //Zona

Desarrollow7XX IN A 192.168.0.XX7
ServidorW2008XX IN A 192.168.0.XX8
clientelinuxXX IN A 192.168.0.XX9

//Así para el resto de equipos de la red

//Lo siguiente es un alias. Para que desde el navegador podamos poner //www.dawXX.net en lugar de servidorlinuxXX.dawXX.net

ns1 IN CNAME servidordnsXX

www IN CNAME servidorlinuxXX

ftp IN CNAME servidorlinuxXX

```
  GNU nano 4.8                              /etc/bind/db.daw01.net
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     servidordns01.daw01.net. administrador.daw01.net. (
                     2020091502         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      servidordns01.daw01.net.
servidordns01   IN      A       192.168.0.15
servidorlinux01 IN      A       192.168.0.16
Desarrollow701  IN      A       192.168.0.17
ServidorW200801 IN      A       192.168.0.18
clientelinux01  IN      A       192.168.0.19

ns1             IN      CNAME   servidordns01
www             IN      CNAME   servidorlinux01
ftp             IN      CNAME   servidorlinux01
```

A continuación creamos el archivo de zona de resolución inversa **/etc/bind/db.192.168.0** con el siguiente contenido:

//Cambia dawXX.net por el nombre de tu dominio
//Cambia servidordnsXX por el nombre de tu servidor de nombres.

$TTL 604800

// TTL (Time To Live) . Es el número de segundos que puede estar el registro en caché //antes de ser descartado.

@ IN SOA 0.168.192.in-addr.arpa. administrador.dawXX.net. (

// El @ situado delante de IN equivale al nombre de la Zona 0.168.192.in-addr.arpa

//administrador.aulaMS2.com. es el correo de la persona responsable del dominio.

//Obligatorio el espacio en blanco antes del paréntesis

2020091502 ;Serial
604800 ;Refresh
86400 ;Retry
2419200 ;Expire
604800) ;Negative Cache TTL

;

//Cambia dawXX.net por el nombre de tu dominio
//Cambia servidordnsXX por el nombre de tu servidor de nombres de dominio
//El número que aparece delante de IN PTR es el último octeto de la dirección IP de la //máquina
//192.168.0.XX5 para servidordnsXX, 192.168.0.XX6 para servidorlinuxXX, 192.168.0.XX7 para Desarrollow7XX, 192.168.0.XX8 para ServidorW2008XX….
//Cambia las direcciones IP y nombres por los de tu red

//Ahora definimos los servidores DNS del dominio

@ IN NS servidordnsXX.dawXX.net.

//Ahora definimos los Hosts del dominio

XX5 IN PTR servidordnsXX.dawXX.net.

//Como XX5 no termina en "." equivale a XX5.0.168.192.in-addr.arpa

XX6.0.168.192.in-addr.arpa. IN PTR servidorlinuxXX.dawXX.net.

//Como XX6.0.168.192.in-addr.arpa. termina en "." no se completa con el nombre
//de la Zona

XX7 IN PTR Desarrollow7XX.dawXX.net.
XX8 IN PTR ServidorW2008XX.dawXX.net.
XX9 IN PTR clientelinuxXX.dawXX.net.

```
  GNU nano 4.8                              /etc/bind/db.192.168.0
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     0.168.192.in-addr.arpa.  administrador.daw01.net. (
                              2020091502         ; Serial
                                604800         ; Refresh
                                 86400         ; Retry
                               2419200         ; Expire
                                604800 )       ; Negative Cache TTL
;
@       IN      NS      servidordns01.daw01.net.
15      IN      PTR     servidordns01.daw01.net.
16      IN      PTR     servidorlinux01.daw01.net.
17      IN      PTR     Desarrollo701.daw01.net.
18      IN      PTR     ServidorW200801.daw01.net.
19      IN      PTR     clientelinux01.daw01.net.
```

Cuando hayamos creado cada uno de los archivos tendremos que reiniciar BIND con el siguiente comando:

- sudo service bind9 restart

3. Comprobación sintáctica y semántica del servidor DNS

A partir de la versión 9 de BIND se incluye la herramienta software para chequear la sintaxis y semántica de los archivos que describen las zonas. Dicha herramienta es: **named-checkzone**

Para los archivos de zona hay que ejecutar:

- **named-checkzone dawXX.net /etc/bind/db.dawXX.net**

(cambiando dawXX.net por el nombre de tu dominio)

Este comando genera la siguiente salida si todo está correcto:

zone dawXX.net/IN: loaded serial 1 OK

- **named-checkzone 0.168.192.in-addr.arpa /etc/bind/db.192.168.0**

Reinicia el servidor para que se apliquen los cambios realizados.

sudo service bind9 restart

4. Comprobando que el servidor de nombres DNS funciona correctamente

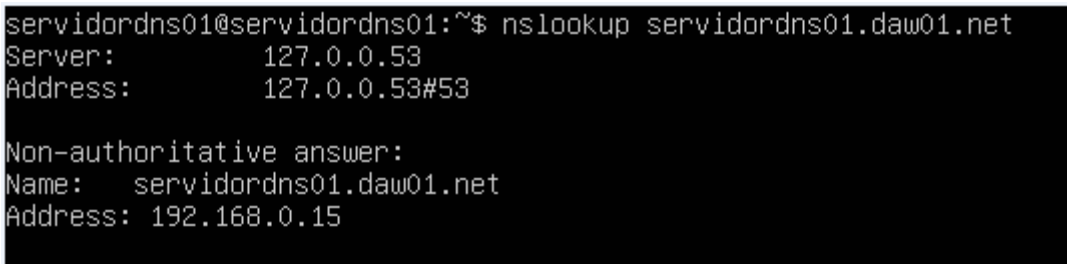
Una vez hayamos reiniciado el servidor DNS debemos comprobar que éste funciona correctamente.

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

Para comprobar que el servidor DNS resuelve consultas directas o inversas sobre la zona creada podemos usar las ordenes nslookup, dig o host.

nslookup servidordnsXX.dawXX.net

Te dirá que equipo resuelve y cuál es la IP de servidordnsXX.dawXX.net



nslookup ftp

En este caso podemos comprobar que al usar un nombre DNS sin puntos, se complete con el sufjo DNS.

```
servidordns01@servidordns01:~$ nslookup ftp
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
ftp.daw01.net   canonical name = servidorlinux01.daw01.net.
Name:   servidorlinux01.daw01.net
Address: 192.168.0.16
```

Para comprobar que nuestro servidor funciona correctamente, también podemos usar:

host servidordnsXX.dawXX.net

(tendrás que cambiar servidor por el nombre de tu servidor y dawXX.net por el nombre de tu dominio). Te dirá su correspondiente IP.

```
servidordns01@servidordns01:~$ host servidordns01.daw01.net
servidordns01.daw01.net has address 192.168.0.15
```

Otra de las herramientas de las que disponemos para hacer consultas sobre un servidor DNS es **dig** (domain information groper**).** Se utiliza para detectar problemas de configuración del servidor.

dig servidordnsXX.dawXX.net

Te dirá su correspondiente IP

```
servidordns01@servidordns01:~$ dig servidordns01.daw01.net

; <<>> DiG 9.16.1-Ubuntu <<>> servidordns01.daw01.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28706
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;servidordns01.daw01.net.       IN      A

;; ANSWER SECTION:
servidordns01.daw01.net. 7152   IN      A       192.168.0.15

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: mar may 26 22:11:46 UTC 2020
;; MSG SIZE  rcvd: 68
```

dig NS dawXX.net

Te dirá cuál es el servidor de nombres del dominio dawXX.net

```
servidordns01@servidordns01:~$ dig  NS daw01.net

; <<>> DiG 9.16.1-Ubuntu <<>> NS daw01.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56107
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;daw01.net.                     IN      NS

;; ANSWER SECTION:
daw01.net.              604800  IN      NS      servidordns01.daw01.net.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: mar may 26 22:13:07 UTC 2020
;; MSG SIZE  rcvd: 66
```

Configuración del cliente DNS BIND en Linux.

En cada uno de los ordenadores de la red habrá que **modificar el fichero /run/systemd/resolve/resolv.conf**. Este fichero tendría el siguiente contenido:

//Cambia 192.168.0.XX5 por la IP de tu servidor de nombres
//Cambia dawXX.net por el nombre de tu dominio
nameserver 192.168.0.XX5
search dawXX.net

El inconveniente que tienes que cuando reinicies pierdes la configuración**.**

Otra solución permanente sería modificar la configuración de la tarjeta de red de cada equipo.

```
  GNU nano 2.9.3     /etc/netplan/01-network-manager-all.yaml

# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
          ens33:
          dhcp4: no
          addresses: [192.168.0.18/24]
          gateway4: 192.168.0.1
          nameservers:
             addresses: [192.168.0.15]
             search: [daw01.net]
```

Rhythmbox

Aplica los cambios y comprueba que se ha modificado el archivo **/run/systemd/resolve/resolv.conf**.

Otra forma de hacerlo sería gráficamente:

1. Acede 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.

2. Introduce como servidor DNS la IP del servidordnsXX que has configurado como servidor maestro.

3. Introduce como dominio de búsqueda dawXX.net

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 modificado la directiva nameserver y se ha añadido la directiva search con el dominio dawXX.net.

```
  GNU nano 2.9.3          /run/systemd/resolve/resolv.conf

# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients directly to
# all known uplink DNS servers. This file lists all configured search domains.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 192.168.0.15
search daw01.net
```

LibreOffice Writer

PRÁCTICA 4

Para comprobar que el servidor DNS resuelve consultas directas o inversas sobre la zona creada podemos usar las ordenes nslookup, dig o host.

dig @192.168.0.15 servidordns01.daw01.net

Le indico que utilice el servidor 192.168.0.15 para darme la IP de servidordns01.daw01.net

```
ubuntu18@maqubuntu18:~$ dig @192.168.0.15 servidordns01.daw01.net

; <<>> DiG 9.11.3-1ubuntu1.12-Ubuntu <<>> @192.168.0.15 servidordns01.daw01.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32563
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2a27a849289b24d6010000005ecd5e72fc72ecd7bada6118 (good)
;; QUESTION SECTION:
;servidordns01.daw01.net.       IN      A

;; ANSWER SECTION:
servidordns01.daw01.net. 604800 IN      A       192.168.0.15

;; Query time: 0 msec
;; SERVER: 192.168.0.15#53(192.168.0.15)
;; WHEN: Tue May 26 20:22:42 CEST 2020
;; MSG SIZE  rcvd: 96
```

dig -x 192.168.0.15

Te dirá nombre y dominio del equipo que tiene esa IP

```
ubuntu18@maqubuntu18:~$ dig -x 192.168.0.15

; <<>> DiG 9.11.3-1ubuntu1.12-Ubuntu <<>> -x 192.168.0.15
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11867
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;15.0.168.192.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
15.0.168.192.in-addr.arpa. 604800 IN    PTR     servidordns01.daw01.net.

;; Query time: 1 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue May 26 20:24:02 CEST 2020
;; MSG SIZE  rcvd: 91
```

ping servidordns01.daw01.net

Comprobamos que hay conexión