

Configuración DNS

David Aparicio Sir

Despliegue de Aplicaciones Web

Grado Superior Desarrollo de aplicaciones Web

IES Los Sauces



Sumario

Instalar bind9.....	3
Cambiar DNS del servidor.....	3
Editar fichero /etc/bind/named-conf.local.....	4
Comprobamos con sudo named-checkconf.....	5
Crear base de datos para almacenar los registros de los recursos.....	5
Creamos fichero resolución directa.....	5
Una vez hecho comprobamos que esté correcto con sudo named-checkzone nombre de la zona nombre del fichero.....	5
Creamos Zona Inversa.....	6
Reiniciamos el servicio.....	7
Abrimos el puerto 53.....	8
Comprobamos que el servicio dns funcione.....	9
Configuramos en la maquina local el dns.....	10
Comprobamos desde Windows 10 que funcione correctamente.....	11
Comprobamos los sitios activos de apache2 en el servidor.....	11
Comprobamos que funcione el dns en Chrome.....	11

Instalar bind9

Lo primero que tenemos que hacer es instalar bind 9

```
miadmin@das-used:~$ sudo apt install bind9
[sudo] password for miadmin:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  openjdk-11-jdk-headless
Utilice «sudo apt autoremove» para eliminarlo.
Se instalarán los siguientes paquetes adicionales:
  bind9-utils dns-root-data
Paquetes sugeridos:
  bind-doc resolvconf
Se instalarán los siguientes paquetes NUEVOS:
  bind9 bind9-utils dns-root-data
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 48 no actualizados.
Se necesita descargar 406 kB de archivos.
Se utilizarán 1.556 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [Y/n]
```

Comprobamos que esté instalado

```
miadmin@das-used:~$ sudo service bind9 status
named.service - BIND Domain Name Server
Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2022-12-13 11:39:42 UTC; 18s ago
Docs: man:named(8)
Process: 1827 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
Main PID: 1828 (named)
Tasks: 3 (limit: 2238)
Memory: 7.0M
CPU: 38ms
CGroup: /system.slice/named.service
└─1828 /usr/sbin/named -u bind

fic 13 11:39:42 das-used named[1828]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
fic 13 11:39:42 das-used named[1828]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
fic 13 11:39:42 das-used named[1828]: network unreachable resolving './DNSKEY/IN': 2001:dc3::35#53
fic 13 11:39:42 das-used named[1828]: network unreachable resolving './NS/IN': 2001:dc3::35#53
fic 13 11:39:42 das-used named[1828]: network unreachable resolving './DNSKEY/IN': 2001:500:1::53#53
fic 13 11:39:42 das-used named[1828]: network unreachable resolving './NS/IN': 2001:500:1::53#53
fic 13 11:39:42 das-used named[1828]: network unreachable resolving './DNSKEY/IN': 2001:500:200::b#53
fic 13 11:39:42 das-used named[1828]: network unreachable resolving './NS/IN': 2001:500:200::b#53
fic 13 11:39:42 das-used named[1828]: managed-keys-zone: Initializing automatic trust anchor management for :
fic 13 11:39:42 das-used named[1828]: resolver priming query complete: success
```

Cambiar DNS del servidor

Cambiamos el DNS para que el principal sea la maquina actual

```

GNU nano 6.2 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses:
        - 192.168.3.208/24
      routes:
        - to: default
          via: 192.168.3.1
      nameservers:
        addresses: [192.168.3.208]
        search: [david.local]

```

Aplicamos los cambios con `sudo netplan apply`

Editar fichero `/etc/bind/named.conf.local`

En este fichero crearemos las 2 zonas del servicio DNS

Crear zona de resolución directa (IP->nombre)

Crear zona resolución inversa(nombre->IP)

```

GNU nano 6.2 /etc/bind/named.conf.local *
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in yo
// organization
//include "/etc/bind/zones.rfc1918";

zone "david.local" {
    type master;
    file "/etc/bind/db.david.local";
};

zone "3.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.3.168.192.in-addr.arpa";
};

```

Comprobamos con sudo named-checkconf

```
miadmin@das-used:~$ sudo named-checkconf
miadmin@das-used:~$
```

Si no sale nada el fichero está correcto

Crear base de datos para almacenar los registros de los recursos

Creamos fichero resolución directa

```
GNU nano 6.2 /etc/bind/db.david.local
;
; BIND data for david.local
;
$TTL      604800
@          IN SOA  das-used.david.local. root.localhost. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        3600 )     ; Negative Cache TTL
;
@          IN      NS      das-used.david.local.
; Registros Host
@          IN      A       192.168.3.208
das-used   IN      A       192.168.3.208

; Registros Alias

daw201    IN      CNAME    das-used.david.local.
daw202    IN      CNAME    das-used.david.local.
daw203    IN      CNAME    das-used.david.local.
daw204    IN      CNAME    das-used.david.local.

www.daw201 IN      CNAME    das-used.david.local.
www.daw202 IN      CNAME    das-used.david.local.
www.daw203 IN      CNAME    das-used.david.local.
www.daw204 IN      CNAME    das-used.david.local.
```

Una vez hecho comprobamos que esté correcto con `sudo named-checkzone` nombre de la zona nombre del fichero

```
miadmin@das-used:~$ sudo named-checkzone david.local /etc/bind/db.david.local
zone david.local/IN: loaded serial 1
OK
```

Si aparece OK está correcto

Creamos Zona Inversa

Para crear la zona inversa copiamos el archivo que contiene la zona directa

Lo llamaremos `db.xxx.xxx.xxx.in-addr.arpa` siendo las x la direccion ip de la red

```
miadmin@das-used:~$ sudo cp /etc/bind/db.david.local /etc/bind/db.3.168.192.in-addr.arpa
miadmin@das-used:~$ ls /etc/bind
bind.keys          db.local
db.0               named.conf
db.127            named.conf.default-zones
db.255            named.conf.local
db.3.168.192.in-addr.arpa  named.conf.options
db.david.local    rndc.key
db.empty          zones.rfc1918
```

Retiramos todos los registros CNAME

Cambiamos todos los registros a por ptr con la sintaxis host in PTR FQDN

```
GNU nano 6.2 /etc/bind/db.3.168.192.in-addr.arpa
;
; BIND data for 3.168.192.in-addr.arpa
;
$TTL      604800
@          IN SOA  das-used.david.local. root.localhost. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        3600 )     ; Negative Cache TTL
;
@          IN      NS      das-used.david.local.

; Registros Puntero
208        IN      PTR      david.local.
208        IN      PTR      das-used.david.local.
```

Comprobamos

```
miadmin@das-used:~$ sudo named-checkzone 3.168.192.in-addr.arpa /etc/bind/db.3.168.192.in-addr.arpa
zone 3.168.192.in-addr.arpa/IN: loaded serial 1
OK
```

Reiniciamos el servicio

```
miadmin@das-used:~$ sudo service bind9 restart
```

```

miadmin@das-used:~$ sudo service bind9 status
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; v>
   Active: active (running) since Tue 2022-12-13 12:37:32 UTC; 1>
     Docs: man:named(8)
   Process: 2271 ExecStart=/usr/sbin/named $OPTIONS (code=exited,>
 Main PID: 2272 (named)
    Tasks: 3 (limit: 2238)
   Memory: 5.3M
      CPU: 37ms
   CGroup: /system.slice/named.service
           └─2272 /usr/sbin/named -u bind

dic 13 12:37:32 das-used systemd[1]: Started BIND Domain Name Serv>
dic 13 12:37:32 das-used named[2272]: running
dic 13 12:37:32 das-used named[2272]: network unreachable resolvin>
dic 13 12:37:32 das-used named[2272]: network unreachable resolvin>
dic 13 12:37:32 das-used named[2272]: network unreachable resolvin>
dic 13 12:37:32 das-used named[2272]: network unreachable resolvin>
dic 13 12:37:32 das-used named[2272]: network unreachable resolvin>
dic 13 12:37:32 das-used named[2272]: network unreachable resolvin>
dic 13 12:37:32 das-used named[2272]: managed-keys-zone: Key 20326>
dic 13 12:37:32 das-used named[2272]: resolver priming query compl>

```


Abrimos el puerto 53

```
miadmin@das-used:~$ sudo ufw allow 53
```

```
Rule added
```

```
Rule added (v6)
```

```
miadmin@das-used:~$ sudo ufw status
```

```
Status: active
```

To	Action	From
--	-----	----
22	ALLOW	Anywhere
80	ALLOW	Anywhere
9000	ALLOW	Anywhere
9003	ALLOW	Anywhere
8080	ALLOW	Anywhere
81	ALLOW	Anywhere
53	ALLOW	Anywhere
22 (v6)	ALLOW	Anywhere (v6)
80 (v6)	ALLOW	Anywhere (v6)
9000 (v6)	ALLOW	Anywhere (v6)
9003 (v6)	ALLOW	Anywhere (v6)
8080 (v6)	ALLOW	Anywhere (v6)
81 (v6)	ALLOW	Anywhere (v6)
53 (v6)	ALLOW	Anywhere (v6)

Comprobamos que el servicio dns funcione

```
miadmin@das-used:~$ nslookup
> 192.168.3.208
208.3.168.192.in-addr.arpa      name = das-used.david.local.
208.3.168.192.in-addr.arpa      name = david.local.

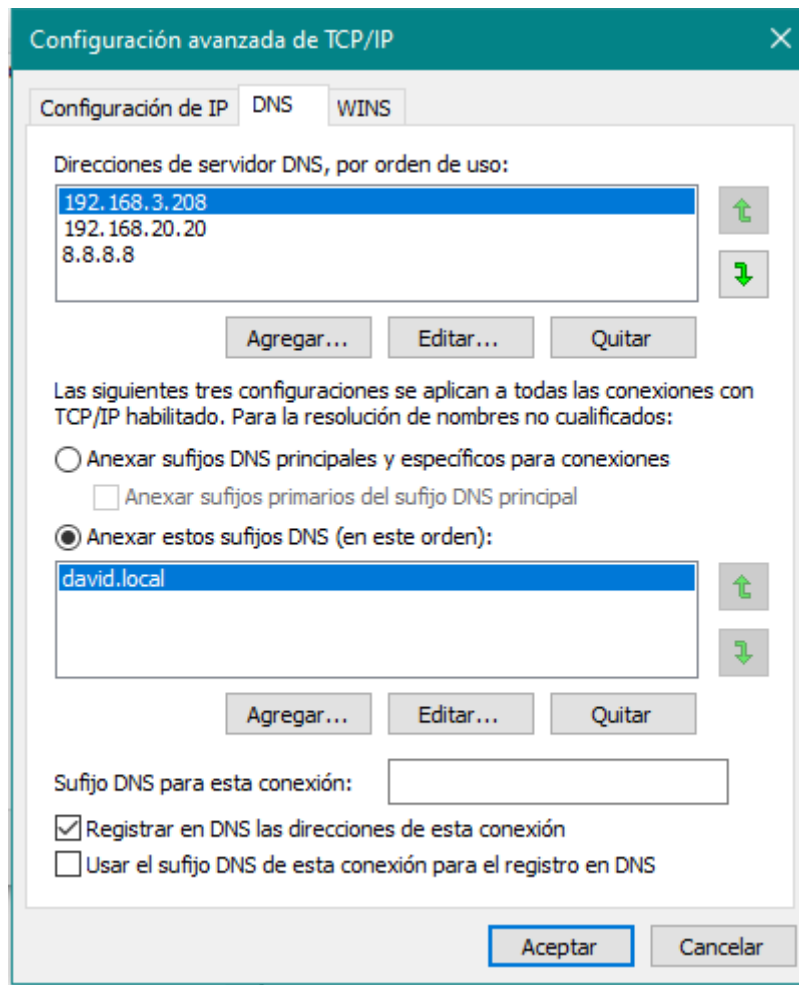
Authoritative answers can be found from:
> david.local
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   david.local
Address: 192.168.3.208
> das-used.david.local
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   das-used.david.local
Address: 192.168.3.208
> das-used
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   das-used.david.local
Address: 192.168.3.208
```

Configuramos en la maquina local el dns



Comprobamos desde Windows 10 que funcione correctamente

```
Microsoft Windows [Versión 10.0.19045.2251]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\daw2>nslookup
Servidor predeterminado:  david.local
Address:  192.168.3.208

> das-used
Servidor:  david.local
Address:  192.168.3.208

Nombre:  das-used.david.local
Address:  192.168.3.208

> daw201
Servidor:  david.local
Address:  192.168.3.208

Nombre:  das-used.david.local
Address:  192.168.3.208
Aliases:  daw201.david.local

> 192.168.3.208
Servidor:  david.local
Address:  192.168.3.208

Nombre:  das-used.david.local
Address:  192.168.3.208
```

Comprobamos los sitios activos de apache2 en el servidor

```
miadmin@das-used:~$ sudo apache2ctl -S
VirtualHost configuration:
*:80                  david.local (/etc/apache2/sites-enabled/puerto80.conf:1)
*:81                  david.local (/etc/apache2/sites-enabled/puerto81.conf:1)
```

Comprobamos que funcione el dns en Chrome

