22-2-2023

Resolución DNS

Ubuntu Server

MANUEL MARTIN ALONSO

ÍNDICE

1. Instalación del paquete bind9.

Paquete bind9

```
miadmin@mma-used:~$ sudo apt update
[sudo] password for miadmin:
Obj:1 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Des:2 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease [99,8 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Des:5 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [762 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [170 kB]
Des:7 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [11,4 kB]
Des:8 http://es.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [493 kB]
Des:9 http://es.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [75,6 kB]
Des:10 http://es.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [53
2 B]
Des:11 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [765 kB]
Des:12 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [130 kB]
Des:13 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [14,2
 kB]
Des:14 http://es.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [7.300 B]
Des:15 http://es.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [2.432 B]
Des:16 http://es.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [42
0 B]
```

```
miadmin@mma-used:~$ sudo apt install bind9
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
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 76 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? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 bind9-utils amd64 1:9.18.
1-1ubuntu1.2 [150 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu jammy/main amd64 dns-root-data all 2021011101 [5.2
56 B]
```

2. Servicio.

sudo service bind9 {status|start|stop|restart}

```
miadmin@mma-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 12:05:29 UTC; 59s ago
       Docs: man:named(8)
    Process: 2161 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 2162 (named)
      Tasks: 4 (limit: 2238)
     Memory: 7.0M
        CPU: 47ms
     CGroup: /system.slice/named.service
             └─2162 /usr/sbin/named -u bind

dic 13 12:05:29 mma-used named[2162]: network unreachable resolving './DNSKEY/IN': 2001:500>
dic 13 12:05:29 mma-used named[2162]: network unreachable resolving './NS/IN': 2001:500:200>
dic 13 12:05:29 mma-used named[2162]: network unreachable resolving './DNSKEY/IN': 2001:500>
dic 13 12:05:29 mma-used named[2162]: network unreachable resolving './NS/IN': 2001:500:2f:>
dic 13 12:05:29 mma-used named[2162]: network unreachable resolving './DNSKEY/IN': 2001:dc3>
dic 13 12:05:29 mma-used named[2162]: network unreachable resolving './NS/IN': 2001:dc3::35>
dic 13 12:05:29 mma-used named[2162]: network unreachable resolving './DNSKEY/IN': 2001:500>
dic 13 12:05:29 mma-used named[2162]: network unreachable resolving './NS/IN': 2001:500:1::>
dic 13 12:05:29 mma-used named[2162]: managed-keys-zone: Initializing automatic trust ancho>
dic 13 12:05:29 mma-used named[2162]: resolver priming query complete: success
lines 1-22/22 (END)
```

3. Cambiar la configuración de red del servidor.

DNS y Sufijo-DNS

```
  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:
    - 192.168.3.204/24
   routes:
    - to: default
      via:  192.168.3.1
   nameservers:
     addresses: [192.168.3.204]
     search: [manuel.local]
```

```
miadmin@mma-used:~$ sudo netplan apply
miadmin@mma-used:~$
```

4. Crear zonas.

a. Zona de resolucion directa (IP a Nombre).

Editar el fichero /etc/bind/named-conf.local

zone "tunombre.local"{

type master;

file "/etc/bind/db.tunombre.local";

};

```
 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 your
// organization
//include "/etc/bind/zones.rfc1918";
zone "manuel.local" {
        type master;
        file "/etc/bind/db.manuel.local";
};

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

b. Zona de resolucion inversa (Nombre a IP).

Editar el fichero /etc/bind/named-conf.local.

zone "3.368.192.in-addr.arpa"{

type master;

file "/etc/bind/db.3.368.192.in-addr.arpa";

};

Chequear los ficheros de configuración.

sudo named-checkconf

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

Si no sale nada, todo está correcto.

5. Crear la base de datos que almacena los registros de recursos.

```
  GNU nano 6.2                    /etc/bind/db.manuel.local
;
; BIND data for manuel.local
;
$TTL    604800
@               IN SOA  mma-used.manuel.local. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         3600 )         ; Negative Cache TTL
;
@               IN      NS      mma-used.manuel.local.
; Registros Host
@               IN      A       192.168.3.204
mma-used        IN      A       192.168.3.204

; Registros Alias

daw201  IN      CNAME   mma-used.manuel.local.
daw202  IN      CNAME   mma-used.manuel.local.
daw203  IN      CNAME   mma-used.manuel.local.
daw204  IN      CNAME   mma-used.manuel.local.
```

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

Zona Inversa.

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

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

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 manuel.local
;
$TTL    604800
@               IN SOA  mma-used.manuel.local. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         3600 )         ; Negative Cache TTL
;
@               IN      NS      mma-used.manuel.local.
;Registros Puntero
204             IN      PTR     manuel.local.
204             IN      PTR     mma-used.manuel.local.
```

Comprobamos que todo está correcto.

```
miadmin@mma-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
miadmin@mma-used:~$
```

Reiniciamos el servicio y comprobamos el estado.

```
miadmin@mma-used:~$ sudo service bind9 restart
miadmin@mma-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 12:37:48 UTC; 8s ago
       Docs: man:named(8)
    Process: 2582 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 2583 (named)
      Tasks: 3 (limit: 2238)
     Memory: 5.2M
        CPU: 36ms
     CGroup: /system.slice/named.service
             └─2583 /usr/sbin/named -u bind

dic 13 12:37:48 mma-used named[2583]: all zones loaded
dic 13 12:37:48 mma-used systemd[1]: Started BIND Domain Name Server.
dic 13 12:37:48 mma-used named[2583]: running
dic 13 12:37:48 mma-used named[2583]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
dic 13 12:37:48 mma-used named[2583]: network unreachable resolving './DNSKEY/IN': 2001:500:2d::d#53
dic 13 12:37:48 mma-used named[2583]: network unreachable resolving './NS/IN': 2001:500:2d::d#53
dic 13 12:37:48 mma-used named[2583]: network unreachable resolving './DNSKEY/IN': 2001:500:a8::e#53
dic 13 12:37:48 mma-used named[2583]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
dic 13 12:37:48 mma-used named[2583]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance
```

Abrimos el puerto 53.

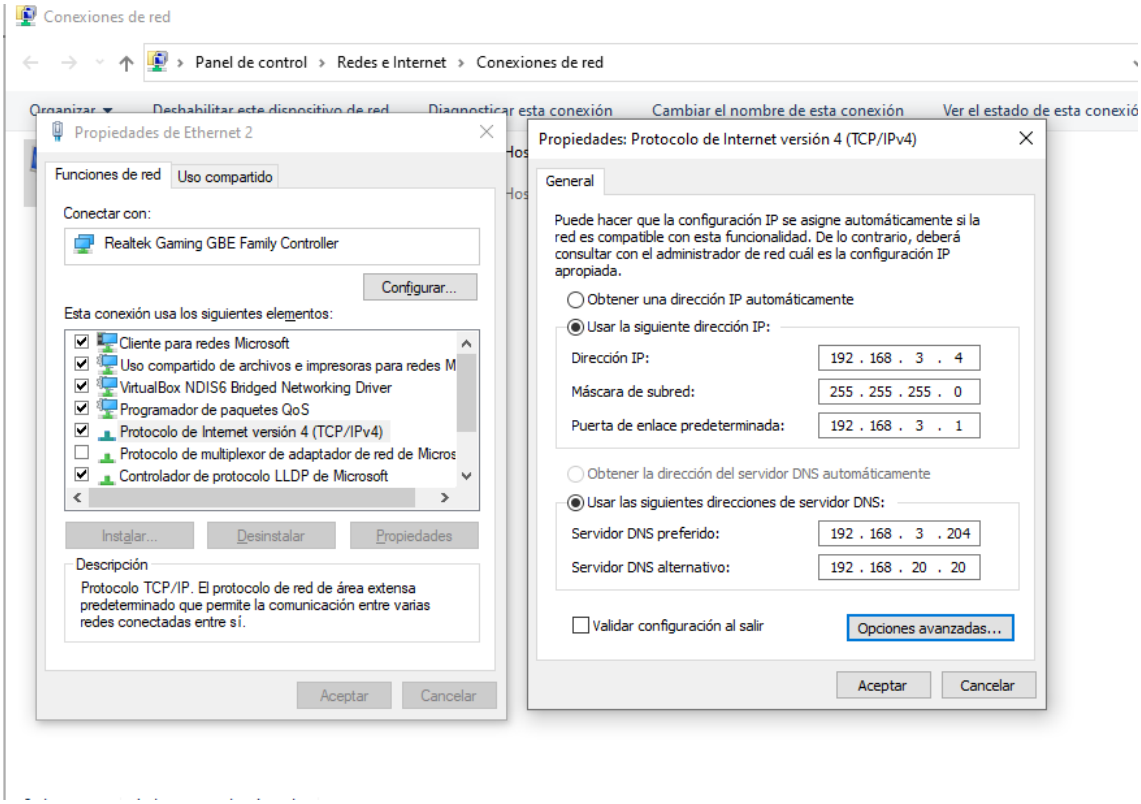
```
miadmin@mma-used:~$ sudo ufw allow 53
Rule added
Rule added (v6)
miadmin@mma-used:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
Apache                     ALLOW       Anywhere
9003                       ALLOW       Anywhere
9000                       DENY        Anywhere
8080/tcp                   ALLOW       Anywhere
8080                       ALLOW       Anywhere
81                         ALLOW       Anywhere
80                         ALLOW       Anywhere
53                         ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
Apache (v6)                ALLOW       Anywhere (v6)
9003 (v6)                  ALLOW       Anywhere (v6)
9000 (v6)                  DENY        Anywhere (v6)
8080/tcp (v6)              ALLOW       Anywhere (v6)
8080 (v6)                  ALLOW       Anywhere (v6)
81 (v6)                    ALLOW       Anywhere (v6)
```

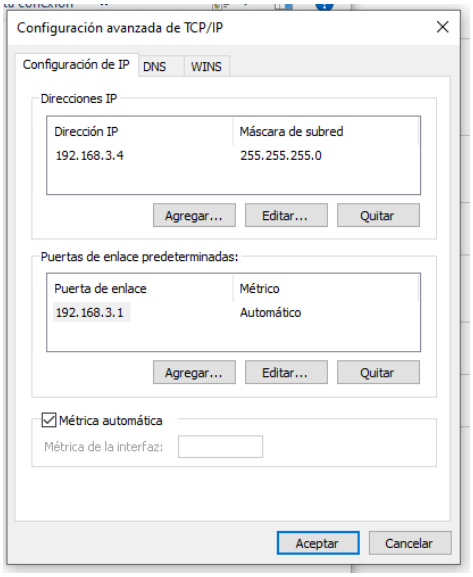
Comprobamos que el servicio DNS funciona correctamente.

```
miadmin@mma-used:~$ nslookup
> 192.168.3.204
204.3.168.192.in-addr.arpa      name = mma-used.manuel.local.
204.3.168.192.in-addr.arpa      name = manuel.local.

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

Non-authoritative answer:
Name:   manuel.local
Address: 192.168.3.204
> mma-used.manuel.local
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   mma-used.manuel.local
Address: 192.168.3.204
> mma-used
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   mma-used.manuel.local
Address: 192.168.3.204
> www.mma-used.local
Server:         127.0.0.53
Address:        127.0.0.53#53
```

```
> www.daw204.manuel.local
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.daw204.manuel.local canonical name = mma-used.manuel.local.
Name:   mma-used.manuel.local
Address: 192.168.3.204
>
```

Comprobamos en la maquina anfitriona si funciona correctamente.



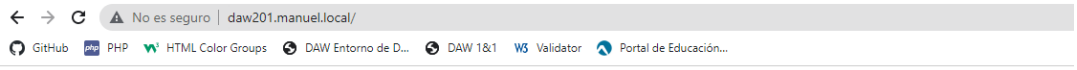


```
C:\Users\daw2>nslookup
Servidor predeterminado:  manuel.local
Address:  192.168.3.204

> mma-used
Servidor:  manuel.local
Address:  192.168.3.204

Nombre:  mma-used.manuel.local
Address:  192.168.3.204

> daw201
Servidor:  manuel.local
Address:  192.168.3.204

Nombre:  mma-used.manuel.local
Address:  192.168.3.204
Aliases:  daw201.manuel.local

> 192.168.3.204
Servidor:  manuel.local
Address:  192.168.3.204

Nombre:  manuel.local
Address:  192.168.3.204
```

Comprobamos los sitios activos de apache2.

```
miadmin@mma-used:~$ sudo apache2ctl -S
VirtualHost configuration:
*:80                   mma-used.manuel.local (/etc/apache2/sites-enabled/puerto80.conf:1)
*:81                   mma-used.manuel.local (/etc/apache2/sites-enabled/puerto81.conf:1)
ServerRoot: "/etc/apache2"
Main DocumentRoot: "/var/www/html"
Main ErrorLog: "/var/log/apache2/error.log"
Mutex default: dir="/var/run/apache2/" mechanism=default
Mutex mpm-accept: using_defaults
Mutex watchdog-callback: using_defaults
PidFile: "/var/run/apache2/apache2.pid"
Define: DUMP_VHOSTS
Define: DUMP_RUN_CFG
User: name="www-data" id=33
Group: name="www-data" id=33
miadmin@mma-used:~$
```

Comprobamos que funcione el DNS en Chrome.



Este es el index de daw201