

DNS

Domain Name System



Índice

Instalación.....	3
1.Paquete bind9.....	3
2.-Servicio.....	4
3.-Cambiar la configuración de red del servidor DNS y sufijo -DNS.....	4
4.-Editar fichero /etc/bind/named-conf.local.....	5
5. Crear base de datos que almacena los registros de recursos.....	6
Creamos el fichero de resolución directa.....	6
6.Crear zona inversa, copiamos el archivo que contiene la zona directa.....	7
7.Configuración puerto 53.....	8
8.Comprobación correcto funcionamiento servicio DNS.....	9
9.Configuración DNS máquina local.....	11
10.Comprobación sitios activos.....	13

Instalación.

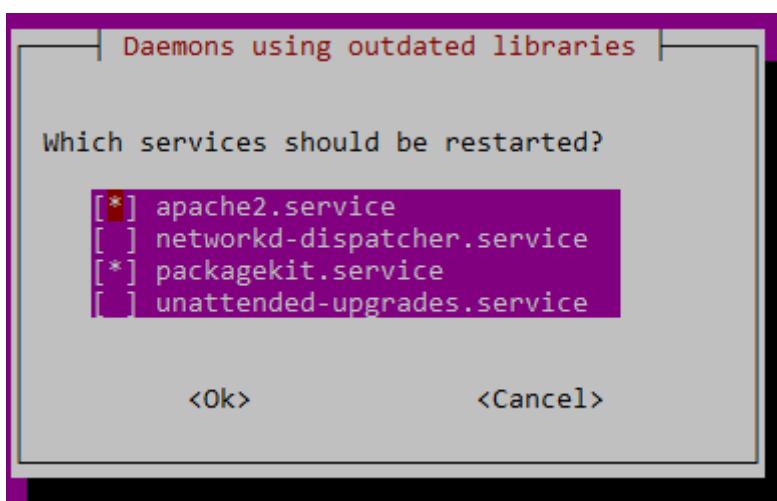
1. Paquete bind9

Esta máquina es una Ubuntu Server versión 20.04.

Ejecutamos comando hostname para saber el nombre de esta máquina y a continuación, la descarga del paquete de instalación bind9 con confirmación 'S' cuando nos lo solicite.

```
Last login: Tue Dec 13 11:29:43 2022
miadmin@RST-USED:~$ hostname
RST-USED
miadmin@RST-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
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libflashrom1 libftdi1-2 openjdk-11-jdk-headless
Utilice «sudo apt autoremove» para eliminarlos.
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 8 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
```

Al terminar la descarga e instalación, el servidor nos pide reiniciar el servicio apache2, damos ok y continuamos.



2.-Servicio

Comprobamos el estado del servicio recién instalado con el comando `sudo service bind9 {status|start|stop|restart}`

```
miadmin@RST-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 11:43:02 UTC; 47s ago
     Docs: man:named(8)
  Process: 9799 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 9801 (named)
    Tasks: 4 (limit: 2238)
   Memory: 7.0M
      CPU: 59ms
  CGroup: /system.slice/named.service
          └─9801 /usr/sbin/named -u bind

dic 13 11:43:02 RST-USED named[9801]: network unreachable resolving './DNSKEY/IN': 2001:7fe::53#53
dic 13 11:43:02 RST-USED named[9801]: network unreachable resolving './NS/IN': 2001:7fe::53#53
dic 13 11:43:02 RST-USED named[9801]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
dic 13 11:43:02 RST-USED named[9801]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
dic 13 11:43:02 RST-USED named[9801]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
dic 13 11:43:02 RST-USED named[9801]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
dic 13 11:43:02 RST-USED named[9801]: network unreachable resolving './DNSKEY/IN': 2001:500:1::53#53
dic 13 11:43:02 RST-USED named[9801]: network unreachable resolving './NS/IN': 2001:500:1::53#53
dic 13 11:43:02 RST-USED named[9801]: managed-keys-zone: Initializing automatic trust anchor management for zone '.'
dic 13 11:43:02 RST-USED named[9801]: resolver priming query complete: success
lines 1-22/22 (END)
```

3.-Cambiar la configuración de red del servidor DNS y sufijo - DNS.

De esta manera, el dominio principal será la máquina actual.

Primero listamos el contenido del directorio `/etc/netplan/` y vemos que allí está, efectivamente, el fichero `00-installer-config.yaml` que tenemos que editar.

```
miadmin@RST-USED:~$ ls /etc/netplan/
00-installer-config.yaml
miadmin@RST-USED:~$
```

Nota importante:

Siempre que se edite un fichero hay que ser muy escrupuloso con la sintaxis y el tabulado/espaciado, un simple espacio o mayúscula/minúscula mal colocado y la configuración será incorrecta.

Para editar el fichero ejecutamos `sudo nano /etc/netplan/00-installer-config.yaml`.

Tendremos que cambiar la addreses: configurada por la ip de esta máquina y cambiaremos también search: poniendo el dominio que nos interese.

```
miadmin@RST-USED: ~  
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:  
        - 192.168.3.207/24  
      routes:  
        - to: default  
          via: 192.168.3.1  
      nameservers:  
        addresses: [192.168.3.207]  
        search: [ricardo.local]
```

Y ‘aplicamos’ cambios, si nos devuelve la línea de comandos limpia, es que nuestra edición del fichero ha sido exitosa.

```
miadmin@RST-USED:~$ miadmin@RST-USED:~$ sudo netplan apply  
miadmin@RST-USED:~$ █
```

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

En este fichero crearemos las 2 zonas del servicio DNS , la directa y la inversa.

En la siguiente captura de pantalla se ve el estado inicial del fichero.

```
miadmin@RST-USED: ~  
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";
```

Fichero ya correctamente configurado (primordial el ser escrupuloso con la sintaxis).

```
miadmin@RST-USED: ~  
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 "ricardo.local" {  
    type master;  
    file "/etc/bind/db.ricardo.local";  
};  
  
zone "3.168.192.in-addr.arpa" {  
    type master;  
    file "/etc/bind/db.3.168.192.in-addr.arpa";  
};
```

En el fichero hemos añadido dos 'zone'(zona de resolución de nombres), la primera se corresponde con la directa (P->nombre) y la segunda con la inversa (nombre->IP)

Ejecutamos el fichero y si no sale nada, es que la edición ha sido correcta.

```
miadmin@RST-USED:~$ sudo named-checkconf
miadmin@RST-USED:~$
```

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

Creamos el fichero de resolución directa.

En este fichero indicaremos nuestro host, ip, y diferentes Alias.

```
miadmin@RST-USED: ~
GNU nano 6.2 /etc/bind/db.ricardo.local
;
; BIND data for ricardo.local
;
$TTL 604800
@ IN SOA RST-USED.ricardo.local. root.localhost. (
    1 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    3600 ) ; Negative Cache TTL
;
@ IN NS RST-USED.ricardo.local.
; Registros Host
@ IN A 192.168.3.207
RST-USED IN A 192.168.3.207

; Registros Alias

daw201 IN CNAME RST-USED.ricardo.local.
daw202 IN CNAME RST-USED.ricardo.local.
daw203 IN CNAME RST-USED.ricardo.local.
daw204 IN CNAME RST-USED.ricardo.local.

www.daw201 IN CNAME RST-USED.ricardo.local.
www.daw202 IN CNAME RST-USED.ricardo.local.
www.daw203 IN CNAME RST-USED.ricardo.local.
www.daw204 IN CNAME RST-USED.ricardo.local.
```

Comprobamos que esté correcto con `sudo named-checkzone "nombre de la zona" "nombre del fichero"`

Si devuelve prompt vacío, es que es correcto, sino, nos informaría del error.

```
miadmin@RST-USED:~$ sudo named-checkzone ricardo.local /etc/bind/db.ricardo.local
zone ricardo.local/IN: loaded serial 1
OK
miadmin@RST-USED:~$
```

6. Crear zona inversa, copiamos el archivo que contiene la zona directa.

Lo llamaremos db.xxx.xxx.in-addr.arpa siendo las x la dirección IP de la red pero en sentido inverso al habitual.

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

Estado original

```
miadmin@RST-USED: ~
GNU nano 6.2 /etc/bind/db.3.168.192.in-addr.arpa
;
; BIND data for ricardo.local
;
$TTL      604800
@         IN      SOA     RST-USED.ricardo.local. root.localhost. (
                        1      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        3600 ) ; Negative Cache TTL
;
@         IN      NS      RST-USED.ricardo.local.
; Registros Host
@         IN      A       192.168.3.207
RST-USED  IN      A       192.168.3.207
; Registros Alias
daw201    IN      CNAME    RST-USED.ricardo.local.
daw202    IN      CNAME    RST-USED.ricardo.local.
daw203    IN      CNAME    RST-USED.ricardo.local.
daw204    IN      CNAME    RST-USED.ricardo.local.
www.daw201 IN      CNAME    RST-USED.ricardo.local.
www.daw202 IN      CNAME    RST-USED.ricardo.local.
www.daw203 IN      CNAME    RST-USED.ricardo.local.
www.daw204 IN      CNAME    RST-USED.ricardo.local.
```

Editar fichero y eliminar todos los registros 'cname'.

A continuación cambiar todos los registros 'a' por 'ptr'.

Estado final.

```
miadmin@RST-USED: ~
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     RST-USED.ricardo.local. root.localhost. (
                        1      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        3600 ) ; Negative Cache TTL
;
@         IN      NS      RST-USED.ricardo.local.
; Registros Puntero
207       IN      PTR     ricardo.local.
207       IN      PTR     RST-USED.ricardo.local.
```

Comprobamos ejecutando el fichero. Si devuelve prompt vacío, está bien configurado.

```
miadmin@RST-USED:~$ miadmin@RST-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@RST-USED:~$
```

Y reiniciamos el servicio bind9 para aplicar cambios.

```
miadmin@RST-USED:~$ sudo service bind9 restart
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-12-13 12:37:34 UTC; 28s ago
     Docs: man:bind(8)
  Process: 10238 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 10239 (named)
    Tasks: 4 (limit: 2238)
   Memory: 5.3M
      CPU: 43ms
  CGroup: /system.slice/bind9.service
          └─10239 /usr/sbin/named -u bind
```

A continuación, visualización del estado del servicio bind9.

```
miadmin@RST-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 12:37:34 UTC; 28s ago
     Docs: man:named(8)
  Process: 10238 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 10239 (named)
    Tasks: 4 (limit: 2238)
   Memory: 5.3M
      CPU: 43ms
  CGroup: /system.slice/named.service
          └─10239 /usr/sbin/named -u bind

dic 13 12:37:34 RST-USED named[10239]: network unreachable resolving './DNSKEY/IN': 2001:500:1::53#53
dic 13 12:37:34 RST-USED named[10239]: network unreachable resolving './NS/IN': 2001:500:1::53#53
dic 13 12:37:34 RST-USED named[10239]: network unreachable resolving './DNSKEY/IN': 2001:500:2::c#53
dic 13 12:37:34 RST-USED named[10239]: network unreachable resolving './NS/IN': 2001:500:2::c#53
dic 13 12:37:34 RST-USED named[10239]: network unreachable resolving './DNSKEY/IN': 2001:503:c27::2:30#53
dic 13 12:37:34 RST-USED named[10239]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
dic 13 12:37:34 RST-USED named[10239]: network unreachable resolving './DNSKEY/IN': 2001:7fd::1#53
dic 13 12:37:34 RST-USED named[10239]: network unreachable resolving './NS/IN': 2001:7fd::1#53
dic 13 12:37:34 RST-USED named[10239]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
dic 13 12:37:34 RST-USED named[10239]: resolver priming query complete: success
miadmin@RST-USED:~$
```

7. Configuración puerto 53.

Este puerto será por el que se comuniquen los servicios bind9.

Así que lo habilitamos.

```
miadmin@RST-USED:~$ sudo ufw allow 53
Rule added
Rule added (v6)
miadmin@RST-USED:~$
```


Y comprobamos su estado.

```
miadmin@RST-USED:~$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
80 ALLOW Anywhere
9003 ALLOW Anywhere
8080/tcp ALLOW Anywhere
81 ALLOW Anywhere
53 ← ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
80 (v6) ALLOW Anywhere (v6)
9003 (v6) ALLOW Anywhere (v6)
8080/tcp (v6) ALLOW Anywhere (v6)
81 (v6) ALLOW Anywhere (v6)
53 (v6) ← ALLOW Anywhere (v6)

miadmin@RST-USED:~$
```

8.Comprobación correcto funcionamiento servicio DNS.

Para comprobarlo, ejecutaremos el comando nslookup e iremos introduciendo tantas líneas como dominios queramos probar, aquí hemos de comprobar la ip, y los diferentes dominios y alias que configuramos en el fichero correspondiente.

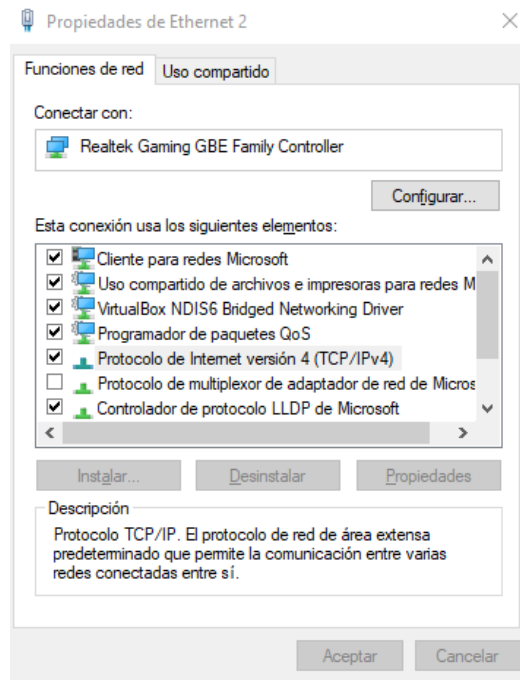
Por cada una de las consultas, nos informará si está correcto o incorrecto e informará de la dirección (con puerto incluido) y de la ip del server.

```
miadmin@RST-USED: ~  
miadmin@RST-USED:~$ nslookup  
> www.daw1.ricardo.local  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
** server can't find www.daw1.ricardo.local: NXDOMAIN  
> www.daw201.ricardo.local  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
Non-authoritative answer:  
www.daw201.ricardo.local    canonical name = RST-USED.ricardo.local.  
Name:   RST-USED.ricardo.local  
Address: 192.168.3.207  
> daw201.ricardo.local  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
Non-authoritative answer:  
daw201.ricardo.local    canonical name = RST-USED.ricardo.local.  
Name:   RST-USED.ricardo.local  
Address: 192.168.3.207  
> 192.168.3.207  
207.3.168.192.in-addr.arpa    name = RST-USED.ricardo.local.  
207.3.168.192.in-addr.arpa    name = ricardo.local.  
  
Authoritative answers can be found from:  
> ricardo.local  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
Non-authoritative answer:  
Name:   ricardo.local  
Address: 192.168.3.207  
> RST-USED.ricardo.local  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
Non-authoritative answer:  
Name:   RST-USED.ricardo.local  
Address: 192.168.3.207  
> RST-USED  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
Non-authoritative answer:  
Name:   RST-USED.ricardo.local  
Address: 192.168.3.207  
> ■
```

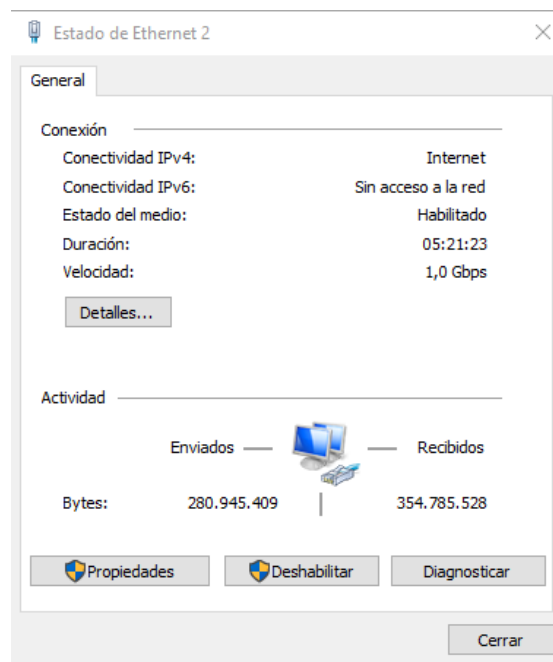
9. Configuración DNS máquina local.

Ha que ir desde el menú de configuración hasta las propiedades de Ethernet.

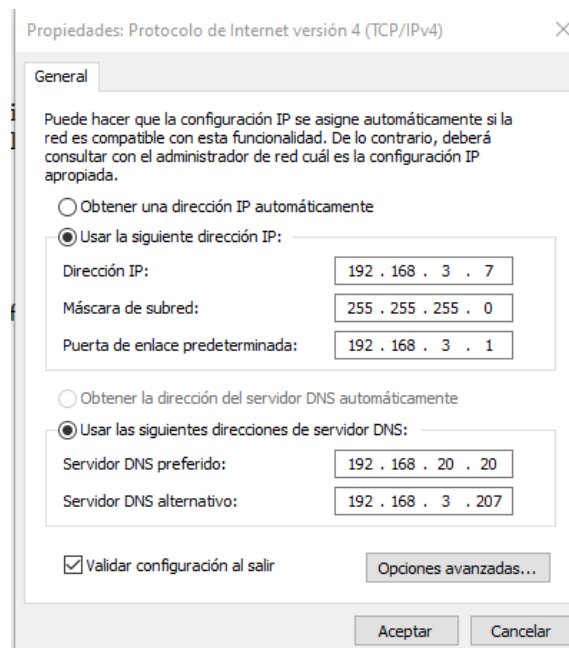
Y allí elegir 'Protocolo de Internet versión 4 (TCP/IPv4)' y clicar en 'Propiedades'.



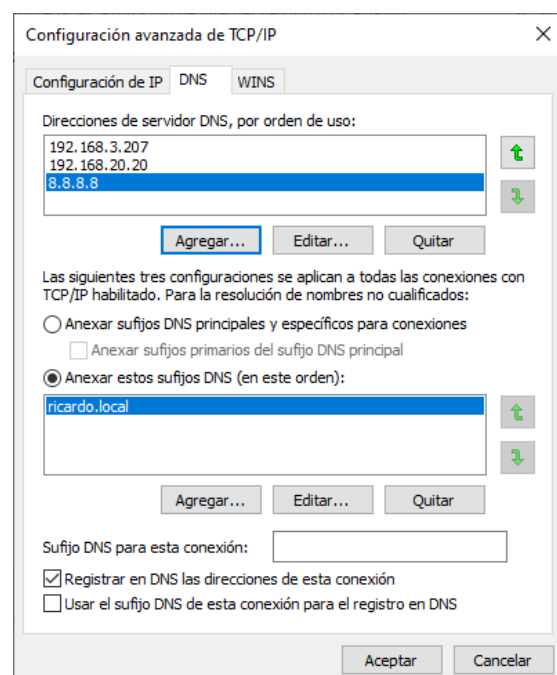
Clickar de nuevo sobre 'Propiedades'



Y cambiar el DNS alternativo al de la ip de nuestro Ubuntu server. A continuación, abrir las ‘Opciones avanzadas...’.



En ‘Opciones avanzadas...’, añadimos también el DNS de Google (8.8.8.8) para tener conexión a internet.



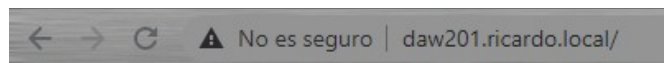
10. Comprobación sitios activos

Primero comprobamos los de apache2 en el servidor.

```
miadmin@RST-USED:~$ sudo apache2ctl -S
VirtualHost configuration:
*:80                ricardo.local (/etc/apache2/sites-enabled/puerto80.conf:1)
*:81                ricardo.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@RST-USED:~$
```

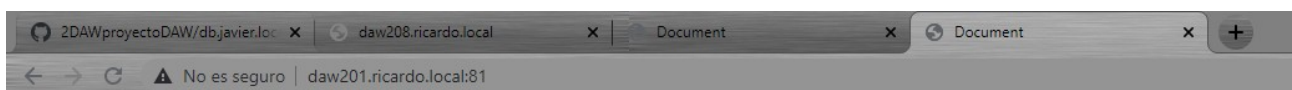
Y para finalizar, comprobamos desde los navegadores que el DNS funcione en ellos.

<http://daw201.ricardo.local:81>



Hola mundo

En el usuario que enjaulamos en la UD3 añadimos un index personalizado a su directorio raíz, si escribimos ahora uno de los dominios registrados (que corresponde a la ip de esta máquina) seguido del puerto (:81), nos mostrará dicho index; si así sucede, será señal de nuestro éxito en la configuración.



Hola desde el puerto 81

FIN.