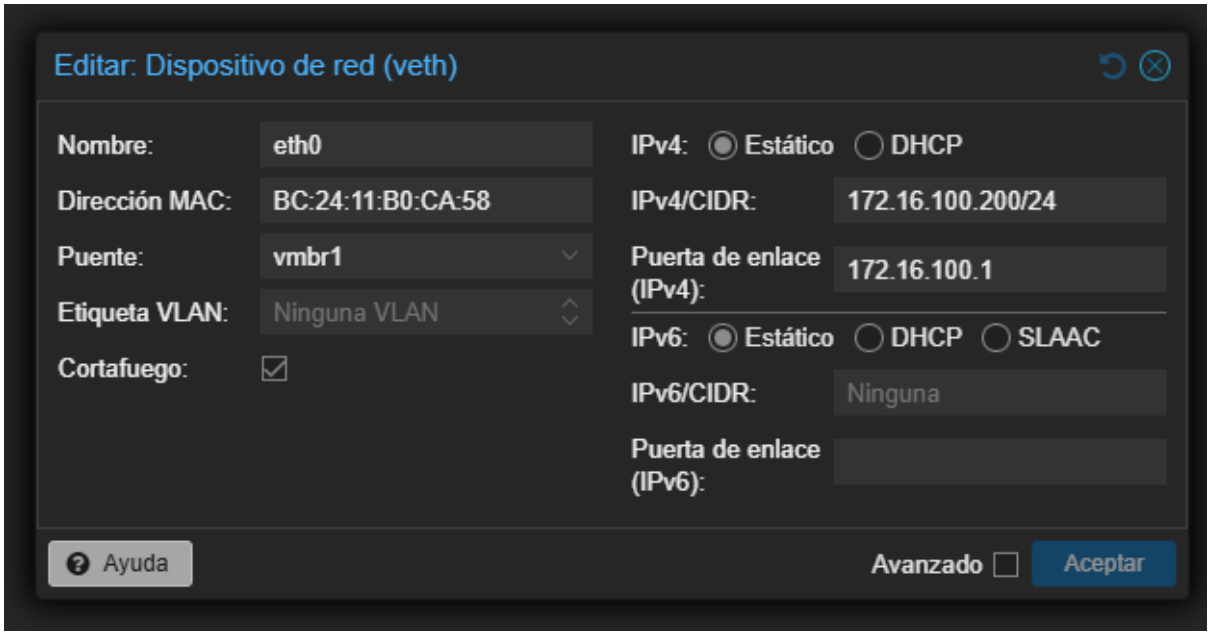
16-10-25

SPRINT 1 SRI (teoría DNS)

Creación de un contenedor en Debian (IP: 172.16.100.200/24, GW: 172.16.100.6.101)

(Cogemos la ISO de Debian de las plantillas de CT)



Instalación de BIN9

```
sudo apt update
sudo apt install bind9
```

```
root@DNS:/usr/share/doc/bind9# apt-get install bind9
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
bind9 is already the newest version (1:9.18.33-1~deb12u2).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
root@DNS:/usr/share/doc/bind9#
```

21-10-2025

Vamos a configurar las directivas globales: named.conf.options

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

        recursion yes

        allow-recursion {
        172.16.100.1;
        172.16.100.254;
        };

        version "No, no puedes verla";



        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;
```

```
//------------------------------------------------------------
dnssec-validation auto;

listen-on port 53{any;};
listen-on-v6 { any; };

allow-transfer{none;};

allow-query{
        172.16.100.1; 172.16.100.254;
        };
```

Vamos a crear las **zonas** **“intranet.g100.asix”.**

Configuramos un servidor máster, y, por lo tanto, autoritario, para el dominio (g100 .asix) (el fichero de zona será /var/cache/bind/db.master.g100.asix), incluyendo su zona inversa (fichero /var/cache/bind/db.master.172.16.100.200.asix)

Zona master

```
zone "g100.asix" {
        type master;
        file "/var/cache/bind/db.master.g100.asix";
};
```

```
root@DNS:/var/cache/bind# cat db.master.g100.asix
$TTL 86400
@ IN SOA ns1.g100.asix. admin.g100.asix. (
        2025102001 ; serial YYYYMMDDNN
        3600       ; refresh
        1800       ; retry
        604800     ; expire
        86400 )    ; minimum

; Name servers
        IN      NS ns1.g100.asix.

; A records

ns1 IN A  172.16.100.200


root@DNS:/var/cache/bind#
```

Dig a la zona master desde el localhost.

```
root@DNS:/etc/bind# dig ns1.g100.asix @127.0.0.1

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> ns1.g100.asix @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1639
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: e02cb82ffad44b490100000068fa0a1754be70756702f1a0 (good)
;; QUESTION SECTION:
;ns1.g100.asix.                 IN      A

;; ANSWER SECTION:
ns1.g100.asix.          86400   IN      A       172.16.100.200

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu Oct 23 10:57:27 UTC 2025
;; MSG SIZE  rcvd: 86

root@DNS:/etc/bind#
```

23-10-2025

- Revisar zonas máster e inversa, rectificar fallos encontrados.

Zona inversa.

```
zone "100.16.172.in-addr.arpa" {

        type master;

        file "/var/cache/bind/db.172.16.100";

        allow-transfer { 172.16.100.204; };
};
```

allow-transfer { 172.16.100.204; }; // para redirección DNS secundario

Antiguo fichero de zona.

```
  GNU nano 7.2                                    db.master.172.16.100.200.asix
$TTL 86400
@ IN SOA ns1.g100.asix. admin.g100.asix. (
        2025102001 ; serial YYYYMMDDNN
        3600       ; refresh
        1800       ; retry
        604800     ; expire
        86400 )    ; minimum

; Name servers
        IN      NS      ns1.g100.asix.


;Registros PTR

200     IN      PTR     ns1.g100.asix.
```

Nuevo fichero de zona.

```
  GNU nano 7.2                                              db.172.16.100
$TTL 86400
@ IN SOA ns1.g100.asix. admin.g100.asix. (
        2025102001 ; serial YYYYMMDDNN
        3600       ; refresh
        1800       ; retry
        604800     ; expire
        86400 )    ; minimum

; Name servers
        IN      NS      ns1.g100.asix.


;Registros PTR

200     IN      PTR     ns1.g100.asix.
```

Dig a la zona inversa desde el localhost.

```
root@DNS:/etc/bind# dig -x 172.16.100.200 @127.0.0.1

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> -x 172.16.100.200 @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39538
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 5c45724c8e5dd7a70100000068fa0670cde0929748628bb9 (good)
;; QUESTION SECTION:
;200.100.16.172.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
200.100.16.172.in-addr.arpa. 86400 IN   PTR     ns1.g100.asix.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu Oct 23 10:41:52 UTC 2025
;; MSG SIZE  rcvd: 111

root@DNS:/etc/bind#
```

27-10-2025 | 28-10-2025

Actualizamos los archivos de las zonas, añadiendo el $ORIGIN que nos faltaba

```
root@DNS:/var/cache/bind# cat db.master.g100.asix
$TTL 86400
$ORIGIN g100.asix
@ IN SOA DNS.g100.asix. admin.g100.asix. (
        2025102001 ; serial YYYYMMDDNN
        3600       ; refresh
        1800       ; retry
        604800     ; expire
        86400 )    ; minimum

; Name servers
        IN      NS DNS.g100.asix.

; A records

DNS IN A  172.16.100.200


root@DNS:/var/cache/bind# cat db.172.16.100
$TTL 86400
$ORIGIN g100.asix
@ IN SOA DNS.g100.asix. admin.g100.asix. (
        2025102001 ; serial YYYYMMDDNN
        3600       ; refresh
        1800       ; retry
        604800     ; expire
        86400 )    ; minimum

; Name servers
        IN      NS      DNS.g100.asix.


;Registros PTR

200     IN      PTR     DNS.g100.asix.


root@DNS:/var/cache/bind#
```

Dig DESDE Máquina IAW2 hacia el DNS

```
root@IAW2:/# dig DNS.g100.asix @172.16.100.200

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> DNS.g100.asix @172.16.100.200
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50888
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c5892b7dc940ac810100000069007e98fb81617a8e57d861 (good)
;; QUESTION SECTION:
;DNS.g100.asix.                 IN      A

;; ANSWER SECTION:
DNS.g100.asix.          86400   IN      A       172.16.100.200

;; Query time: 0 msec
;; SERVER: 172.16.100.200#53(172.16.100.200) (UDP)
;; WHEN: Tue Oct 28 08:28:08 UTC 2025
;; MSG SIZE  rcvd: 86
```

EN LA CONFIGURACIÓN DELS DNS PRIMARIO: /etc/bind/named.conf.local, AÑADIMOS EL DNS SECUNDARIO:

```
zone "g100.asix" {

        type master;

        file "/var/cache/bind/db.master.g100.asix";

        allow-transfer { 172.16.100.204; };   // IP del DNS secundario

        also-notify { 172.16.100.204; };
};
```

CREAMOS UN NUEVO CONTENEDOR E INSTALAMOS BIND9 PARA LA DNSSEC

- apt update
- apt install -y bind9 bind9utils bind9-dnsutils
- systemctl enable bind9
- systemctl start bind9

Archivo de zona directa: /var/cache/bind/db.master.g100.asix

```
  GNU nano 7.2          db.master.g100.asix
$TTL 86400
$ORIGIN g100.asix
@ IN SOA DNS.g100.asix. admin.g100.asix. (
        2025102001 ; serial YYYYMMDDNN
        3600       ; refresh
        1800       ; retry
        604800     ; expire
        86400 )    ; minimum

; Name servers
@       IN      NS DNS.g100.asix.
@       IN      NS DNSSECUNDARIO.g100.asix

; A records

DNS IN A  172.16.100.200

DNSSECUNDARIO IN A 172.16.100.204

; subdomain delegations
intranet IN NS IAW2.intranet.g100.asix
DC01.intranet IN A 172.16.100.201
```

Archivo de zona inversa: var/cache/bind/db.172.16.100

```
  GNU nano 7.2              db.172.16.100
$TTL 86400
$ORIGIN g100.asix
@ IN SOA DNS.g100.asix. admin.g100.asix. (
        2025102001 ; serial YYYYMMDDNN
        3600       ; refresh
        1800       ; retry
        604800     ; expire
        86400 )    ; minimum

; Name servers
@       IN      NS      DNS.g100.asix.
@       IN      NS      DNSSECUNDARIO.g100.asix

;Registros PTR

200     IN      PTR     DNS.g100.asix.
204     IN      PTR     DNSSECUNDARIO.g100.asix
```

3. Configuración del DNS secundario (DNSSECUNDARIO)

Archivo: /etc/bind/named.conf.local

```
zone "slave.g100.asix" {
    type slave;
    masters { 172.16.100.200; };
    file "/var/cache/bind/db.slave.g100.asix";
};


zone "100.16.172.in-addr.arpa" {
    type slave;
    masters { 172.16.100.200; };
    file "/var/cache/bind/db.172.16.100";
};
```

4. Configurar reenviadores (ambos servidores)

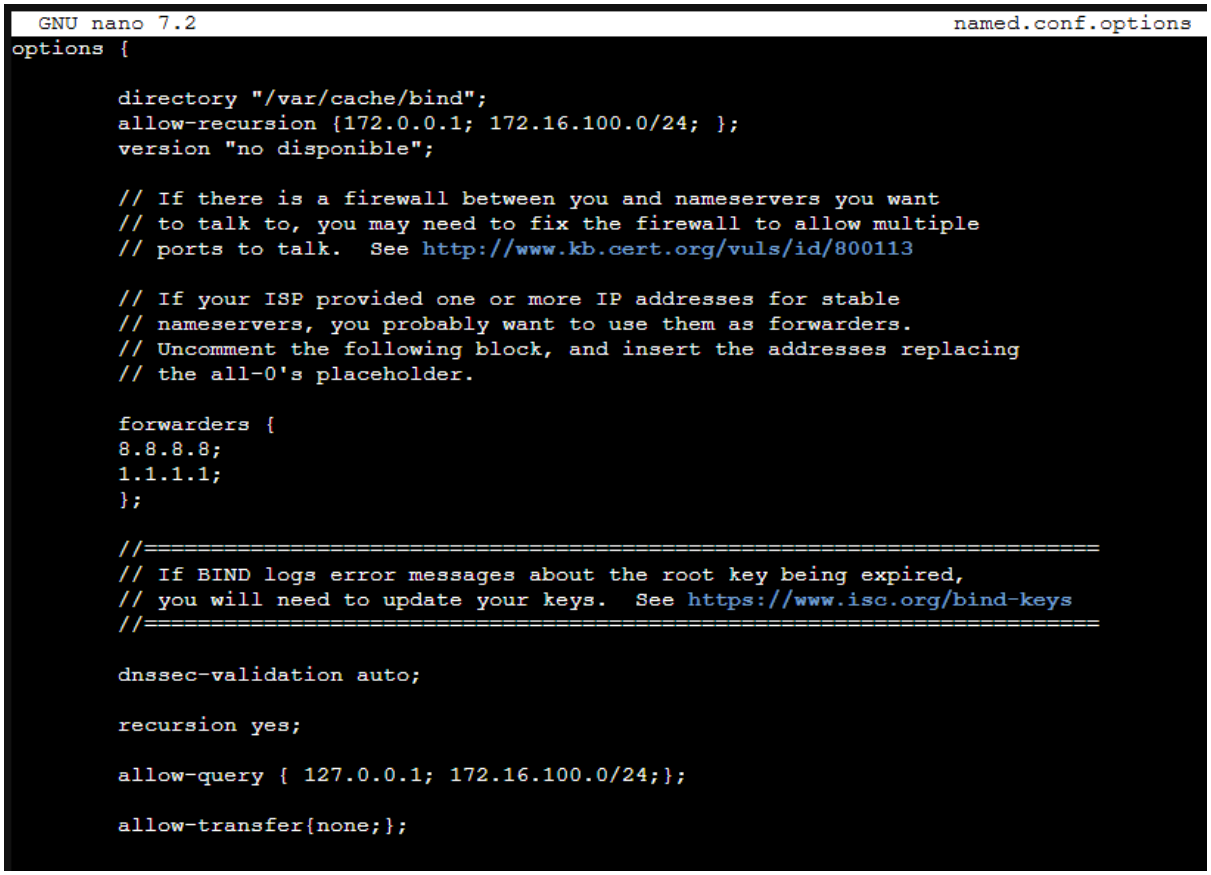
Archivo: /etc/bind/named.conf.options

DNS PRIMARIO

```
options {
    //configurar directorio
    directory "/var/cache/bind";

    //permitir recursion
    recursion yes;

    //permitir recursión a la red
    allow-recursion{127.0.0.1; 172.16.100.0/24;
    };

    //No mostrar version de Bind
    version "No, no puedes verla";

     // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.
```

```
        forwarders {
        8.8.8.8;
        };


//========================================================================
===
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys

//========================================================================
        dnssec-validation auto;
         //escuchar en puerto 53
        listen-on port 53{any;};
        listen-on-v6 { any; };
         allow-transfer{none;};

        //permitir consultas a la red
        allow-query{ 127.0.0.1; 172.16.100.0/24;};



};
```

DNS SECUNDARIO



Service bin9 reload / o /

systemctl restart bind9

30-10-25

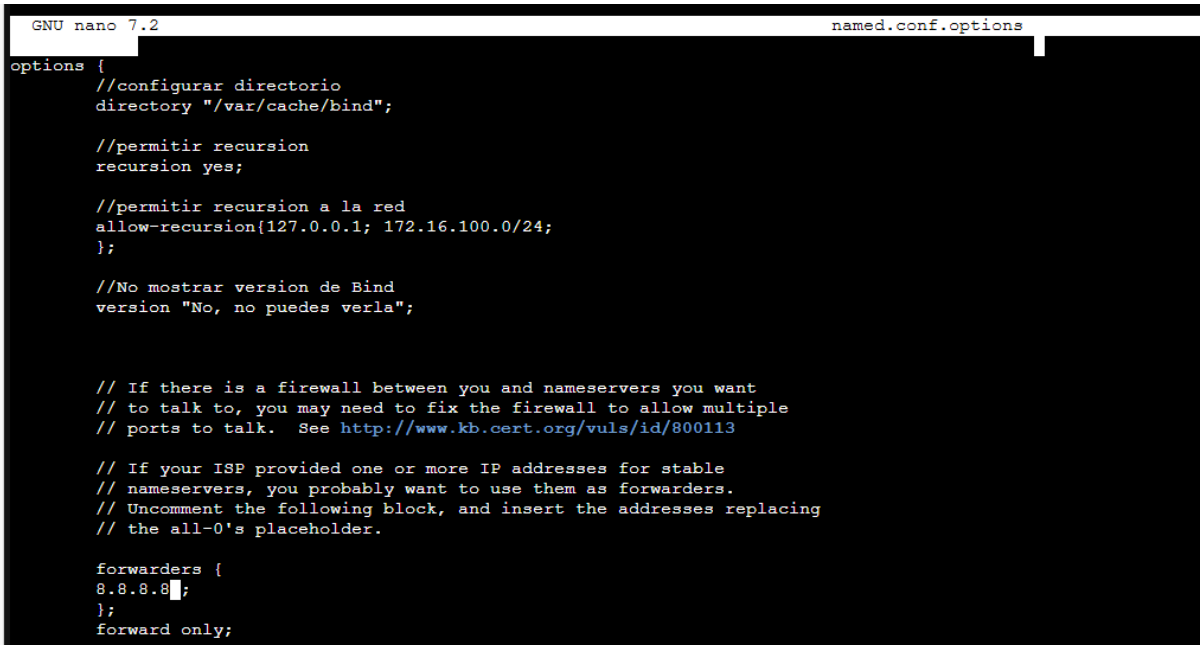
Hemos configurado la zona SLAVE del DNSSECUNDARIO

Revisamos y comprobamos el funcionamiento de ambas zonas.

```
zone "g100.asix" {

    type slave;

    masters { 172.16.100.200; };

    file "/var/cache/bind/db.g100.asix";

    allow-notify {172.16.100.200; };

};


zone "100.16.172.in-addr.arpa" {

    type slave;

    masters { 172.16.100.200; };

    file "/var/cache/bind/db.172.16.100";

    allow-notify {172.16.100.200; };

};
```

```
; <<>> DiG 9.18.41-1~deb12u1-Debian <<>> @172.16.100.204 ns g100.asix
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29276
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c41a9fa3c8056a3e01000000690354980bca859483ed515c (good)
;; QUESTION SECTION:
;g100.asix.                     IN      NS

;; ANSWER SECTION:
g100.asix.              86400   IN      NS      DNSSECUNDARIO.g100.asix.
g100.asix.              86400   IN      NS      DNS.g100.asix.

;; ADDITIONAL SECTION:
DNS.g100.asix.          86400   IN      A       172.16.100.200
DNSSECUNDARIO.g100.asix. 86400  IN      A       172.16.100.204

;; Query time: 0 msec
;; SERVER: 172.16.100.204#53(172.16.100.204) (UDP)
;; WHEN: Thu Oct 30 12:05:44 UTC 2025
;; MSG SIZE  rcvd: 144
```

Forwards: 8888


GNU nano 7.2
named.conf.options
options {
//configurar directorio
directory "/var/cache/bind";
//permitir recursion
recursion yes;
//permitir recursion a la red
allow-recursion{127.0.0.1; 172.16.100.0/24;
};
//No mostrar version de Bind
version "No, no puedes verla";
// If there is a firewall between you and nameservers you want
// to talk to, you may need to fix the firewall to allow multiple
// ports to talk. See http://www.kb.cert.org/vuls/id/800113
// If your ISP provided one or more IP addresses for stable
// nameservers, you probably want to use them as forwarders.
// Uncomment the following block, and insert the addresses replacing
// the all-0's placeholder.
forwarders {
8.8.8.8;
};
forward only;