

DNS MAESTRO-ESCLAVO

Maquinas.....	2
2.2. Equipos.....	3
3. Datos del DNS.....	4
1. Activa solamente la escucha del servidor para el protocolo IPv4.....	4
2. Establecer la opción dnssec-validation a yes.....	4
3. Los servidores permitirán las consultas recursivas sólo a los ordenadores en la red 127.0.0.0/8 y en la red 192.168.57.0/24, para ello utilizarán la opción de listas de control de acceso o acl.....	4
4. El servidor maestro será tierra.sistema.test y tendrá autoridad sobre la zona directa e inversa.....	5
5. El servidor esclavo será venus.sistema.test y tendrá como maestro a tierra.sistema.test.....	6
6. El tiempo en caché de las respuestas negativas de las zonas (directa e inversa) será de dos horas (se pone en segundos).....	6
7. Aquellas consultas que reciba el servidor para la que no está autorizado, deberá reenviarlas (forward) al servidor DNS 208.67.222.222 (OpenDNS).....	7
8. Se configurarán los siguientes alias:.....	9
a. ns1.sistema.test. será un alias de tierra.sistema.test.....	9
b. ns2.sistema.test. será un alias de venus.sistema.test.....	9
9. mail.sistema.test. será un alias de marte.sistema.test.....	9
10. El equipo marte.sistema.test. actuará como servidor de correo del dominio de correo sistema.test.....	10
4. Comprobación Comprueba con dig o nslookup que:.....	11
• Puedes resolver los registros tipo A.....	11
• Comprueba que se pueden resolver de forma inversa sus direcciones IP.....	11
• Puedes resolver los alias ns1.sistema.test y ns2.sistema.test.....	12
• Realiza la consulta para saber los servidores NS de sistema.test. Debes obtener tierra.sistema.test y venus.sistema.test.....	12
• Realiza la consulta para saber los servidores MX de sistema.test.....	12
• Comprueba que se ha realizado la transferencia de la zona entre el servidor DNS maestro y el esclavo. Revisa los logs o realiza una consulta del registro AXFR.....	12
• Comprueba que tanto maestro como esclavo pueden contestar a las mismas preguntas.....	13

Maquinas

En vagrant file debajo de las máquinas en provision he agregado cada uno de los archivos de configuración para que cuando la máquina arranque tenga todos los archivos configurados como nos hacen falta.

2.2. Equipos

```
Vagrant.configure("2") do |config|

  # Maquinaria imaginaria marte 192.168.57.101

  # Configuración de Debian en modo texto (venus)
  config.vm.define "venus" do |venus|
    venus.vm.box = "debian/bookworm64"
    venus.vm.hostname = "venus.sistema.test"
    venus.vm.network "private_network", ip: "192.168.57.102"
    venus.vm.provision "shell", inline: <<-SHELL
      apt-get update
      apt-get install -y bind9 dnsutils
      cp /vagrant/venus/named.conf.local /etc/bind/named.conf.local
      cp /vagrant/venus/named.conf.options /etc/bind/named.conf.options
      systemctl restart bind9
    SHELL
  end

  # Configuración de Debian en modo texto (tierra)
  config.vm.define "tierra" do |tierra|
    tierra.vm.box = "debian/bookworm64"
    tierra.vm.hostname = "tierra.sistema.test"
    tierra.vm.network "private_network", ip: "192.168.57.103"
    tierra.vm.provision "shell", inline: <<-SHELL
      apt-get update
      apt-get install -y bind9 dnsutils
      cp /vagrant/tierra/named.conf.local /etc/bind/named.conf.local
      cp /vagrant/tierra/named.conf.options /etc/bind/named.conf.options
      cp /vagrant/tierra/db.sistema.test /var/lib/bind/db.sistema.test
      cp /vagrant/tierra/db.192.168.57 /var/lib/bind/db.192.168.57
      systemctl restart bind9
    SHELL
  end

  # Maquinaria imaginaria marte 192.168.57.104

end
```

3. Datos del DNS

1. Activa solamente la escucha del servidor para el protocolo IPv4.

```
sudo nano /etc/bind/named.conf.options
```

2. Establecer la opción dnssec-validation a yes

```
sudo nano /etc/bind/named.conf.options
```

```
// Validación DNSSEC activada
```

```
dnssec-validation yes;
```

3. Los servidores permitirán las consultas recursivas sólo a los ordenadores en la red 127.0.0.0/8 y en la red 192.168.57.0/24, para ello utilizarán la opción de listas de control de acceso o acl.

```
sudo nano /etc/bind/named.conf.options
```

```
// Listas de control de acceso (acl) para las consultas recursivas
```

```
acl "internal" { 127.0.0.0/8; # Permitir consultas desde localhost
```

```
192.168.57.0/24; # Permitir consultas desde la red interna
```

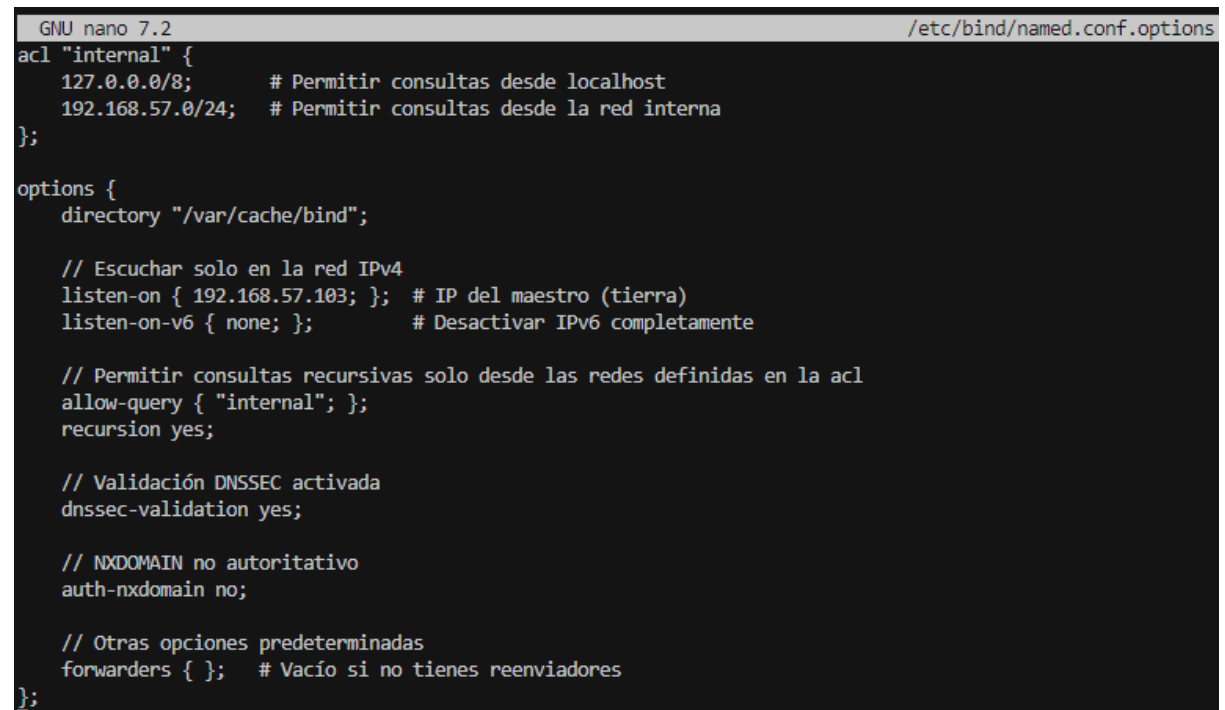
```
};
```

```
// Permitir consultas recursivas solo desde las redes definidas en la acl
```

```
allow-query { "internal"; };
```

```
recursion yes;
```

Archivo Maestro **TIERRA**



```
GNU nano 7.2 /etc/bind/named.conf.options
acl "internal" {
    127.0.0.0/8;      # Permitir consultas desde localhost
    192.168.57.0/24; # Permitir consultas desde la red interna
};

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

    // Escuchar solo en la red IPv4
    listen-on { 192.168.57.103; }; # IP del maestro (tierra)
    listen-on-v6 { none; };       # Desactivar IPv6 completamente

    // Permitir consultas recursivas solo desde las redes definidas en la acl
    allow-query { "internal"; };
    recursion yes;

    // Validación DNSSEC activada
    dnssec-validation yes;

    // NXDOMAIN no autoritativo
    auth-nxdomain no;

    // Otras opciones predeterminadas
    forwarders { }; # Vacío si no tienes reenviadores
};
```

Archivo Cliente VENUS

```
GNU nano 7.2 /etc/bind/named.conf.options
acl "internal" {
    127.0.0.0/8;      # Permitir consultas desde localhost
    192.168.57.0/24;  # Permitir consultas desde la red interna
};

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

    // Escuchar solo en la red IPv4
    listen-on { 192.168.57.102; }; # IP del esclavo (venus)
    listen-on-v6 { none; };        # Desactivar IPv6 completamente

    // Permitir consultas recursivas solo desde las redes definidas en la acl
    allow-query { "internal"; };
    recursion yes;

    // Validación DNSSEC activada
    dnssec-validation yes;

    // NXDOMAIN no autoritativo
    auth-nxdomain no;

    // Otras opciones predeterminadas
    forwarders { }; # Vacío si no tienes reenviadores
};
```

4. El servidor maestro será tierra.sistema.test y tendrá autoridad sobre la zona directa e inversa.

conectamos al servidor maestro tierra

vagrant ssh tierra

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

```
GNU nano 7.2 /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 "sistema.test" {
    type master;
    file "/var/lib/bind/db.sistema.test";
    allow-transfer { 192.168.57.102; }; # Permite transferencias de zona al esclavo (venus)
};

zone "57.168.192.in-addr.arpa" {
    type master;
    file "/var/lib/bind/db.192.168.57";
    allow-transfer { 192.168.57.102; }; # Permite transferencias de zona al esclavo
};
```

Archivo de zona directa (/var/lib/bind/db.sistema.test):

```
GNU nano 7.2 /var/lib/bind/db.sistema.test
$TTL      604800
@         IN      SOA     tierra.sistema.test. root.sistema.test. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL

; Servidores de nombres
@         IN      NS      tierra.sistema.test.

; Registros A para los hosts
tierra    IN      A       192.168.57.103
venus     IN      A       192.168.57.102
```

Archivo de zona inversa (/var/lib/bind/db.192.168.57):

```
GNU nano 7.2 /var/lib/bind/db.192.168.57
$TTL      604800
@         IN      SOA     tierra.sistema.test. root.sistema.test. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL

; Servidores de nombres
@         IN      NS      tierra.sistema.test.

; Registros PTR (para resolución inversa)
103       IN      PTR     tierra.sistema.test.
102       IN      PTR     venus.sistema.test.
```

5. El servidor esclavo será venus.sistema.test y tendrá como maestro a tierra.sistema.test.

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

```
GNU nano 7.2 /etc/bind/named.conf.local
zone "sistema.test" {
    type slave;
    file "/var/lib/bind/db.sistema.test";
    masters { 192.168.57.103; }; # IP del servidor maestro (tierra)
};

zone "57.168.192.in-addr.arpa" {
    type slave;
    file "/var/lib/bind/db.192.168.57";
    masters { 192.168.57.103; }; # IP del servidor maestro
};
```

6. El tiempo en caché de las respuestas negativas de las zonas (directa e inversa) será de dos horas (se pone en segundos).

En el servidor maestro TIERRA

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

añadimos esta línea:

negative-cache-time 7200;

```
GNU nano 7.2 /etc/bind/named.conf.options
acl "internal" {
    127.0.0.0/8;      # Permitir consultas desde localhost
    192.168.57.0/24;  # Permitir consultas desde la red interna
};

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

    // Escuchar solo en la red IPv4
    listen-on { 192.168.57.102; }; # IP del esclavo (venus)
    listen-on-v6 { none; };        # Desactivar IPv6 completamente

    // Permitir consultas recursivas solo desde las redes definidas en la acl
    allow-query { "internal"; };
    recursion yes;

    // Validación DNSSEC activada
    dnssec-validation yes;

    // NXDOMAIN no autoritativo
    auth-nxdomain no;

    // Otras opciones predeterminadas
    forwarders { }; # Vacío si no tienes reenviadores

    //cache negativa 7200s 2h
    negative-cache-time 7200;
};
```

Al agregar la línea `negative-cache-time 7200`; da fallo `bind9` y la he cambiado por:
`max-ncache-ttl 7200`;

7. Aquellas consultas que reciba el servidor para la que no está autorizado, deberá reenviarlas (forward) al servidor DNS 208.67.222.222 (OpenDNS).

Editamos el archivo

Agregamos la línea:

// Otras opciones predeterminadas

`forwarders { 208.67.222.222; }; # OpenDNS`

`forward only; # Reenvía solo a los servidores especificados`

Servidor esclavo venus

```
GNU nano 7.2 /etc/bind/named.conf.options
acl "internal" {
    127.0.0.0/8;      # Permitir consultas desde localhost
    192.168.57.0/24;  # Permitir consultas desde la red interna
};

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

    // Escuchar solo en la red IPv4
    listen-on { 192.168.57.102; }; # IP del esclavo (venus)
    listen-on-v6 { none; };        # Desactivar IPv6 completamente

    // Permitir consultas recursivas solo desde las redes definidas en la acl
    allow-query { "internal"; };
    recursion yes;

    // Validación DNSSEC activada
    dnssec-validation yes;

    // NXDOMAIN no autoritativo
    auth-nxdomain no;

    // Otras opciones predeterminadas
    forwarders { 208.67.222.222; }; # OpenDNS
    forward only; # Reenvía solo a los servidores especificados

    // Cache negativa 7200s (2 horas)
    max-cache-ttl 7200;
};
```

Servidor Maestro Tierra

```
GNU nano 7.2 /etc/bind/named.conf.options
acl "internal" {
    127.0.0.0/8;      # Permitir consultas desde localhost
    192.168.57.0/24;  # Permitir consultas desde la red interna
};

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

    // Escuchar solo en la red IPv4
    listen-on { 192.168.57.103; }; # IP del maestro (tierra)
    listen-on-v6 { none; };        # Desactivar IPv6 completamente

    // Permitir consultas recursivas solo desde las redes definidas en la acl
    allow-query { "internal"; };
    recursion yes;

    // Validación DNSSEC activada
    dnssec-validation yes;

    // NXDOMAIN no autoritativo
    auth-nxdomain no;

    // Otras opciones predeterminadas
    forwarders { 208.67.222.222; }; # OpenDNS
    forward only; # Reenvía solo a los servidores especificados
};
```

8. Se configurarán los siguientes alias:

a. ns1.sistema.test. será un alias de tierra.sistema.test.

b. ns2.sistema.test. será un alias de venus.sistema.test..

Ejecutamos este comando en la maquina maestra (tierra):

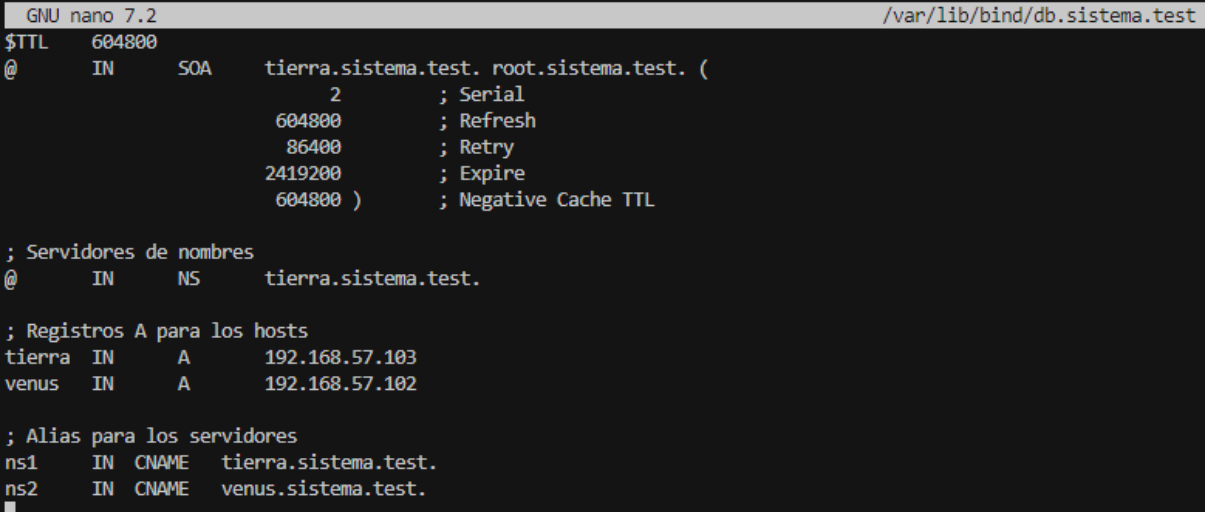
```
sudo nano /var/lib/bind/db.sistema.test
```

Agregamos las lineas:

; Alias para los servidores

```
ns1 IN CNAME tierra.sistema.test.
```

```
ns2 IN CNAME venus.sistema.test.
```



```
GNU nano 7.2 /var/lib/bind/db.sistema.test
$TTL      604800
@         IN      SOA     tierra.sistema.test. root.sistema.test. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL

; Servidores de nombres
@         IN      NS      tierra.sistema.test.

; Registros A para los hosts
tierra    IN      A       192.168.57.103
venus     IN      A       192.168.57.102

; Alias para los servidores
ns1       IN      CNAME    tierra.sistema.test.
ns2       IN      CNAME    venus.sistema.test.
```

9. mail.sistema.test. será un alias de marte.sistema.test.

Ejecutamos este comando en la maquina maestra (tierra):

```
sudo nano /var/lib/bind/db.sistema.test
```

Agregamos las lineas:

; Alias para el servidor de correo

```
mail IN CNAME marte.sistema.test.
```



```
GNU nano 7.2 /var/lib/bind/db.sistema.test
$TTL      604800
@         IN      SOA      tierra.sistema.test. root.sistema.test. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL

; Servidores de nombres
@         IN      NS       tierra.sistema.test.

; Registros A para los hosts
tierra    IN      A        192.168.57.103
venus     IN      A        192.168.57.102

; Alias para los servidores
ns1       IN      CNAME    tierra.sistema.test.
ns2       IN      CNAME    venus.sistema.test.

; Alias para el servidor de correo
mail      IN      CNAME    marte.sistema.test.
```

Hacemos una comprobación del email:

dig @192.168.57.103 mail.sistema.test

```
vagrant@tierra:~$ dig @192.168.57.103 mail.sistema.test

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> @192.168.57.103 mail.sistema.test
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 49618
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 079b9abd4e38693e01000000671616302dde9d3073d69fda (good)
;; QUESTION SECTION:
;mail.sistema.test.      IN      A

;; ANSWER SECTION:
mail.sistema.test.      604800 IN      CNAME    marte.sistema.test.

;; AUTHORITY SECTION:
sistema.test.          604800 IN      SOA      tierra.sistema.test. root.sistema.test. 2 604800 86400 2419200 604800

;; Query time: 0 msec
;; SERVER: 192.168.57.103#53(192.168.57.103) (UDP)
;; WHEN: Mon Oct 21 08:52:00 UTC 2024
;; MSG SIZE rcvd: 142
```

10. El equipo marte.sistema.test. actuará como servidor de correo del dominio de correo sistema.test.

Editamos el archivo: /var/lib/bind/db.sistema.test

Agregamos estas líneas:

marte IN A 192.168.57.184

; Registro MX para el dominio sistema.test

@ IN MX 10 marte.sistema.test.

Asi quedaria el archivo /var/lib/bind/db.sistema.test

```
GNU nano 7.2 /var/lib/bind/db.sistema.test
$TTL      604800
@         IN      SOA      tierra.sistema.test. root.sistema.test. (
                        2      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL

; Servidores de nombres
@         IN      NS       tierra.sistema.test.

; Registros A para los hosts
tierra    IN      A        192.168.57.103
venus     IN      A        192.168.57.102
marte     IN      A        192.168.57.184

; Alias para los servidores
ns1       IN      CNAME    tierra.sistema.test.
ns2       IN      CNAME    venus.sistema.test.

; Alias para el servidor de correo
mail      IN      CNAME    marte.sistema.test.

; Registro MX para el dominio sistema.test
@         IN      MX       10 marte.sistema.test.
```

4. Comprobación Comprueba con dig o nslookup que:

- Puedes resolver los registros tipo A.

Ejecutamos el comando: `dig +short @192.168.57.103 venus.sistema.test`, igual con marte y tierra.

```
vagrant@tierra:~$ dig +short @192.168.57.103 tierra.sistema.test
dig +short @192.168.57.103 venus.sistema.test
dig +short @192.168.57.103 marte.sistema.test
192.168.57.103
192.168.57.102
192.168.57.104
```

- Comprueba que se pueden resolver de forma inversa sus direcciones IP.

```
vagrant@tierra:~$ dig +short @192.168.57.103 -x 192.168.57.103
tierra.sistema.test.
vagrant@tierra:~$ dig +short @192.168.57.103 -x 192.168.57.102
venus.sistema.test.
vagrant@tierra:~$ dig +short @192.168.57.103 -x 192.168.57.104
marte.sistema.test.
```

- Puedes resolver los alias ns1.sistema.test y ns2.sistema.test.

```
vagrant@tierra:~$ dig +short @192.168.57.103 ns1.sistema.test
tierra.sistema.test.
192.168.57.103
vagrant@tierra:~$ dig +short @192.168.57.103 ns2.sistema.test
venus.sistema.test.
192.168.57.102
```

- Realiza la consulta para saber los servidores NS de sistema.test. Debes obtener tierra.sistema.test y venus.sistema.test.

```
vagrant@tierra:~$ dig +short @192.168.57.103 NS sistema.test
venus.sistema.test.
tierra.sistema.test.
```

- Realiza la consulta para saber los servidores MX de sistema.test.

```
vagrant@tierra:~$ dig +short @192.168.57.103 MX sistema.test
10 marte.sistema.test.
```

- Comprueba que se ha realizado la transferencia de la zona entre el servidor DNS maestro y el esclavo. Revisa los logs o realiza una consulta del registro AXFR.

```
vagrant@tierra:~$ sudo tail -f /var/log/syslog
2024-10-21T10:39:30.667055+00:00 bookworm named[2678]: zone 0.in-addr.arpa/IN: loaded serial 1
2024-10-21T10:39:30.667092+00:00 bookworm named[2678]: zone 255.in-addr.arpa/IN: loaded serial 1
2024-10-21T10:39:30.667458+00:00 bookworm named[2678]: zone sistema.test/IN: loaded serial 3
2024-10-21T10:39:30.667489+00:00 bookworm named[2678]: all zones loaded
2024-10-21T10:39:30.667966+00:00 bookworm systemd[1]: Started named.service - BIND Domain Name Server.
2024-10-21T10:39:30.669921+00:00 bookworm named[2678]: zone sistema.test/IN: sending notifies (serial 3)
2024-10-21T10:39:30.671337+00:00 bookworm named[2678]: running
2024-10-21T10:39:30.676498+00:00 bookworm named[2678]: client @0x7ff607843168 192.168.57.102#44943 (sistema.test): transfer of 'sistema.test/IN': IXFR version not in journal, falling back to AXFR
2024-10-21T10:39:30.676768+00:00 bookworm named[2678]: client @0x7ff607843168 192.168.57.102#44943 (sistema.test): transfer of 'sistema.test/IN': AXFR-style IXFR started (serial 3)
2024-10-21T10:39:30.677169+00:00 bookworm named[2678]: client @0x7ff607843168 192.168.57.102#44943 (sistema.test): transfer of 'sistema.test/IN': AXFR-style IXFR ended: 1 messages, 11 records, 273 bytes, 0.001 secs (273000 bytes/sec) (serial 3)
```

sending notifies (serial 3): Esto indica que el servidor maestro ha notificado a sus esclavos sobre un cambio en la zona, en este caso, la zona **sistema.test** con un número de serie de 3.

transfer of 'sistema.test/IN': IXFR version not in journal, falling back to AXFR: Aquí, el esclavo intentó realizar una transferencia incremental (IXFR) pero no pudo, por lo que se está utilizando una transferencia completa (AXFR).

AXFR-style IXFR started (serial 3): Esto indica que se inició la transferencia completa de la zona.

AXFR-style IXFR ended: 1 messages, 11 records, 273 bytes: Esto muestra que se completó la transferencia de la zona. Se transfirieron 11 registros en total, y se enviaron 273 bytes.

Consulta AXFR:

dig @192.168.57.102 sistema.test AXFR

```
vagrant@tierra:~$ dig @192.168.57.102 sistema.test AXFR

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> @192.168.57.102 sistema.test AXFR
; (1 server found)
;; global options: +cmd
sistema.test.      604800 IN      SOA     tierra.sistema.test. root.sistema.test. 3 604800 86400 2419200 604800
sistema.test.      604800 IN      NS      venus.sistema.test.
sistema.test.      604800 IN      NS      tierra.sistema.test.
sistema.test.      604800 IN      MX      10 marte.sistema.test.
mail.sistema.test. 604800 IN      CNAME   marte.sistema.test.
mar.te.sistema.test. 604800 IN      A       192.168.57.104
ns1.sistema.test.  604800 IN      CNAME   tierra.sistema.test.
ns2.sistema.test.  604800 IN      CNAME   venus.sistema.test.
tierra.sistema.test. 604800 IN      A       192.168.57.103
venus.sistema.test. 604800 IN      A       192.168.57.102
sistema.test.      604800 IN      SOA     tierra.sistema.test. root.sistema.test. 3 604800 86400 2419200 604800
;; Query time: 0 msec
;; SERVER: 192.168.57.102#53(192.168.57.102) (TCP)
;; WHEN: Mon Oct 21 10:43:36 UTC 2024
;; XFR size: 11 records (messages 1, bytes 312)
```

- Comprueba que tanto maestro como esclavo pueden contestar a las mismas preguntas.

```
vagrant@tierra:~$ dig +short @192.168.57.103 tierra.sistema.test dig +short @192.168.57.102 tierra.sistema.test
192.168.57.103
192.168.57.103
```