

DNS

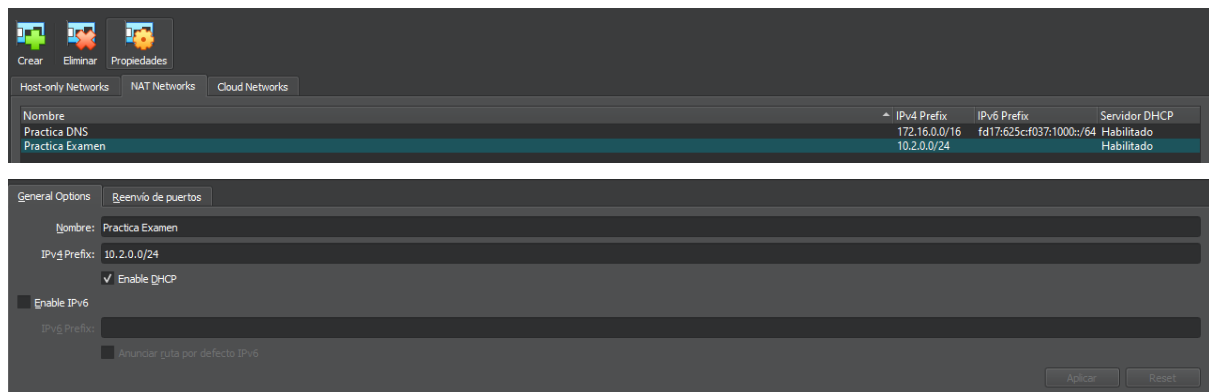
Práctica para el examen

Ejemplo para practicar:

1. Crear una un servidor dns principal y otro esclavo
 - a. Principal -> IP 10.2.0.2/24
 - b. Esclavo -> IP 10.2.0.3/24
2. Server principal:
 - a. Que si no puede resolver la solicitud se lo pase al 8.8.8.8
 - b. Crear un dominio "<nombre>.com"
 - c. Que tenga del pc1 a pc5 con ip 10.2.0.10 hasta 10.2.0.14
 - d. Tenga un correo
 - e. Tiene un server llamado "paco" ip 10.2.0.20
 - f. Un alias con el server paco que sea ftp y www
 - g. Que puede resolver las inversas
 - h. Transfiere el archivo directo e inverso al esclavo
3. Server Esclavo
 - a. Que si no puede resolver la solicitud se lo pase al 8.8.8.8
 - b. Pueda resolver el inverso y directo del dominio "<nombre>.com"

[Enlace](#)

VirtualBox



2-Master DNS

Primero llamamos al server servermaster con el comando: “**sudo hostnamectl set-hostname servermaster**” reiniciamos el equipo.

Configuramos la red la máquina:

Dirección	Máscara de red	Puerta de enlace
10.2.0.2	24	10.2.0.1

Servidores DNS: 10.2.0.2, 8.8.8.8

Domínios de búsqueda:

ID del cliente DHCP:

☐ Requiere dirección IPv4 para que esta conexión se complete

Una vez configurada debes desconectar y conectar de nuevo la conexión.

Ahora hay que instalar el bind9:

“sudo apt-get install bind9 bind9utils bind9-doc”

```
marmol89@servermaster:~$ sudo apt-get install bind9 bind9utils bind9-doc
```

En caso de que no te deje ejecutar el comando prueba a hacer un “sudo apt-get update” previo.

Ahora vamos a configurar que si no puede resolver la petición se lo mande al dns 8.8.8.8: Editamos el fichero “/etc/bind/named.conf.options”

```
GNU nano 6.2 /etc/bind/named.conf.options *
options {
    directory "/var/cache/bind";

    // 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
    //=====
```

Ponemos el siguiente comando para saber si lo hemos hecho bien “sudo named-checkconf”, si no hace nada es que lo has hecho bien.

Vamos a crear una carpeta llamada zones con el comando:

“sudo mkdir /etc/bind/zones/” (las zonas son los dominios)

```
marmol89@servermaster:~$ sudo mkdir /etc/bind/zones/
```

Zona Directa

Hora copiamos el fichero que viene de ejemplo y lo llamamos <nombre>.local:

“sudo cp /etc/bind/db.local /etc/bind/zones/<nombre>.local”

```
marmol89@servermaster:~$ sudo cp /etc/bind/db.local /etc/bind/zones/marmol.local
```

Ahora editamos el fichero recién copiado y hacemos lo que nos pide el ejercicio:

“sudo nano /etc/bind/zones/<nombre>.local”

```
GNU nano 6.2 /etc/bind/zones/marmol.local
$TTL 604800
;marmol.com es el nombre de nuestro dominio
;admin.marmol.com es como el correo de del administrador del dominio

@      IN      SOA      marmol.com. admin.marmol.com. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@      IN      NS       marmol.com.
@      IN      A        10.2.0.2

;Esto son los pc
pc1     IN      A        10.2.0.10
pc2     IN      A        10.2.0.11
pc3     IN      A        10.2.0.12
pc4     IN      A        10.2.0.13
pc5     IN      A        10.2.0.14

;Correo
@      IN      MX       10      admin.marmol.com.

;Server Paco
paco    IN      A        10.2.0.20

;CNAME es alias
ftp     IN      CNAME    paco.marmol.com.
www     IN      CNAME    paco.marmol.com.
```

Para comprobar si hemos hecho bien el fichero <nombre>.local hay que usar el siguiente comando: “sudo named-checkzone <nombre>.local /etc/bind/zones/<nombre>.local”

Si responde al final del todo lo siguiente estará bien: “OK”

Ya hemos terminado el fichero de zona directa hora vamos hacer el fichero de zona inversa

Zona Inversa

Copiamos el fichero “/etc/bind/zones/<nombre>.local” y lo llamamos “db.<ip al revés>.in-addr.arpa” => “sudo cp /etc/bind/zones/<nombre>.local /etc/bind/zones/db.<ip al revés>.in-addr.arpa”

```
marmol89@servermaster:~$ sudo cp /etc/bind/zones/marmol.local /etc/bind/zones/db.0.2.10.in-addr.arpa
```

Ejemplo si tenemos la red 10.2.0.0/24 se pondría “db.0.2.10.in-addr.arpa” por que el ultimo numero de la red no se pone por que termina en /24

Luego de crear el fichero lo editamos y reformamos:

```
GNU nano 6.2 /etc/bind/zones/db.0.2.10.in-addr.arpa
$TTL 604800
;marmol.com es el nombre de nuestro dominio
;admin.marmol.com es como el correo de del administrador del dominio

@      IN      SOA      marmol.com. admin.marmol.com. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@      IN      NS       marmol.com.

;Esto son los pc
10     IN      PTR      pc1.marmol.com.
11     IN      PTR      pc2.marmol.com.
12     IN      PTR      pc3.marmol.com.
13     IN      PTR      pc4.marmol.com.
14     IN      PTR      pc5.marmol.com.

;Server Paco
20     IN      PTR      paco.marmol.com.
```

Para ver si funciona utilizamos el siguiente comando: “sudo named-checkzone db.<ip al revés>.in-addr.arpa /etc/bind/zones/<ip al revés>.in-addr.arpa” y tiene que dar al final un OK.

Ya hemos terminado los fichero de zonas

Ahora vamos a editar el fichero “/etc/bind/named.conf.local” para hacer funcionar las zonas (ojito con las llaves, tabulaciones y “;”)
(allow transfer y notify no se pone si no hay esclavo)

```
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";

//Zona Directa
zone "marmol.com" in
{
    type master;
    file "/etc/bind/zones/marmol.local";
    //Para el esclavo
    allow-transfer{10.2.0.3;};
    notify yes;
};

//Zona Inversa
zone "0.2.10.in-addr.arpa" in
{
    type master;
    file "/etc/bind/zones/db.0.2.10.in-addr.arpa";
    //Para el esclavo
    allow-transfer{10.2.0.3;};
    notify yes;
};
```

Para comprobar si está bien “sudo named-checkconf” y si no responde nada esta todo bien.

Ahora reiniciamos el servicio con el comando:

```
marmol89@servermaster:~$ sudo systemctl restart bind9
```

Ahora probamos que resuelve:

Directa:

```
marmol89@servermaster:~$ dig paco.marmol.com

; <<> DiG 9.18.1-lubuntu1.2-Ubuntu <<> paco.marmol.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53198
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;paco.marmol.com.                IN      A

;; ANSWER SECTION:
paco.marmol.com.                7194    IN      A      10.2.0.20

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Dec 08 19:14:58 CET 2022
;; MSG SIZE rcvd: 60
```

Para comprobar la directa tiene que salir en el answer section la ip (10.2.0.20) en este caso.

Inversa

```
marmol89@servermaster:~$ dig -x 10.2.0.20

; <<> DiG 9.18.1-lubuntu1.2-Ubuntu <<> -x 10.2.0.20
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 54916
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;20.0.2.10.in-addr.arpa.          IN      PTR

;; ANSWER SECTION:
20.0.2.10.in-addr.arpa. 604800 IN      PTR      paco.marmol.com.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Dec 08 19:15:55 CET 2022
;; MSG SIZE rcvd: 80
```

Para comprobar la directa tiene que salir en el answer section el dominio (paco.marmol.com) en este caso.

Una vez hecho esto, quitamos la dirección alternativa 8.8.8.8 de dns que hemos colocado previamente, ya que ahora el servidor lo redirige automáticamente.

Editarando Conexión cableada 1

Nombre de la conexión: Conexión cableada 1

General Cableada Seguridad 802.1x DCB Proxy **Ajustes de IPv4** Ajustes de IPv6

Método: Manual

Dirección

Dirección	Máscara de red	Puerta de enlace
10.2.0.2	24	10.2.0.1

Añadir Eliminar

Servidores DNS: 10.2.0.2

Dominios de búsqueda:

ID del cliente DHCP:

☐ Requiere dirección IPv4 para que esta conexión se complete

Rutas...

Cancelar Guardar

Y volvemos a desconectar y a conectar la conexión

Si hacemos un ping ahora al 8.8.8.8 te lo tienes que resolver.

```
marmol89@servermaster:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=16.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=17.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=17.1 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 16.828/17.106/17.348/0.213 ms
marmol89@servermaster:~$
```

Ya hemos terminado de configurar el servidor maestro.

3-Esclavo - DNS

Primero llamamos al server servermaster con el comando: “**sudo hostnamectl set-hostname serveresclavo**” reiniciamos el equipo con el comando “reboot”.

Una vez hecho esto procedemos a ejecutar un update: “sudo apt-get update”.

Y después procedemos a instalar bind9: “sudo apt-get install bind9 bind9utils bind9-doc”.

```
marmol89@serveresclavo:~$ sudo apt-get install bind9 bind9utils bind9-doc
```

Configuración de la ip:

Dirección	Máscara de red	Puerta de enlace
10.2.0.3	24	10.2.0.1

Servidores DNS: 10.2.0.2, 10.2.0.3

Dominios de búsqueda:

ID del cliente DHCP:

☒ Requiere dirección IPv4 para que esta conexión se complete

Rutas...

En caso de no tener internet en servidor dns añadimos la dirección 8.8.8.8 como dirección secundaria.

Ahora vamos a configurar que si no puede resolver la petición se lo mande al dns 8.8.8.8:
Editamos el fichero “/etc/bind/named.conf.options”

```
GNU nano 6.2 /etc/bind/named.conf.options *
options {
    directory "/var/cache/bind";

    // 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
    //=====
```

Ponemos el siguiente comando para saber si lo hemos hecho bien “sudo
named-checkconf”, si no hace nada es que lo has hecho bien.

Ahora vamos a editar el fichero “/etc/bind/named.conf.local” para hacer funcionar las zonas
(ojito con las llaves, tabulaciones y “;”)

```
GNU nano 6.2 /etc/bind/named.conf.local *
// organization
//include "/etc/bind/zones.rfc1918";

//Zona Directa
zone "marmol.com" in
{
    type slave;
    masters{10.2.0.2;};
    allow-notify{10.2.0.2;};
    file "/var/cache/bind/db.marmol.local";
};

zone "0.2.10.in-addr.arpa" in
{
    type slave;
    masters{10.2.0.2;};
    allow-notify{10.2.0.2;};
    file "/var/cache/bind/db.0.2.10-in-addr.arpa";
};
```

Para comprobar si está bien “sudo named-checkconf” y si no responde nada esta todo bien.

Una vez hecho todo esto, vamos a reiniciar el esclavo y vamos a tener abiertos tanto el
esclavo como el servidor y en el esclavo nos dirigimos a la ruta /var/cache/bind y si
hacemos un ll deberían aparecer 4 ficheros.

```
marmol89@serveresclavo:/var/cache/bind$ ls
db.0.2.10-in-addr.arpa  managed-keys.bind
db.marmol.local         managed-keys.bind.jnl
marmol89@serveresclavo:/var/cache/bind$
```


Comprobamos que funciona:

Directa

```
marmol89@serveresclavo:/var/cache/bind$ dig @10.2.0.3 paco.marmol.com

; <<>> DiG 9.18.1-lubuntu1.2-Ubuntu <<>> @10.2.0.3 paco.marmol.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4990
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 830d189fea553a380100000063923b13de396593d22179fb (good)
;; QUESTION SECTION:
;paco.marmol.com.                IN      A

;; ANSWER SECTION:
paco.marmol.com.                604800  IN      A      10.2.0.20

;; Query time: 0 msec
;; SERVER: 10.2.0.3#53(10.2.0.3) (UDP)
;; WHEN: Thu Dec 08 20:29:23 CET 2022
;; MSG SIZE rcvd: 88
```

Inversa

```
marmol89@serveresclavo:/var/cache/bind$ dig @10.2.0.3 -x 10.2.0.20

; <<>> DiG 9.18.1-lubuntu1.2-Ubuntu <<>> @10.2.0.3 -x 10.2.0.20
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14188
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6d5e04eda8b576ec0100000063923b45acfedcf3506c55f1 (good)
;; QUESTION SECTION:
;20.0.2.10.in-addr.arpa.        IN      PTR

;; ANSWER SECTION:
20.0.2.10.in-addr.arpa. 604800  IN      PTR    paco.marmol.com.

;; Query time: 0 msec
;; SERVER: 10.2.0.3#53(10.2.0.3) (UDP)
;; WHEN: Thu Dec 08 20:30:13 CET 2022
;; MSG SIZE rcvd: 108
```