Repaso DNS

Práctica 7

UT 2: Servicio de Nombres de Dominio (DNS)

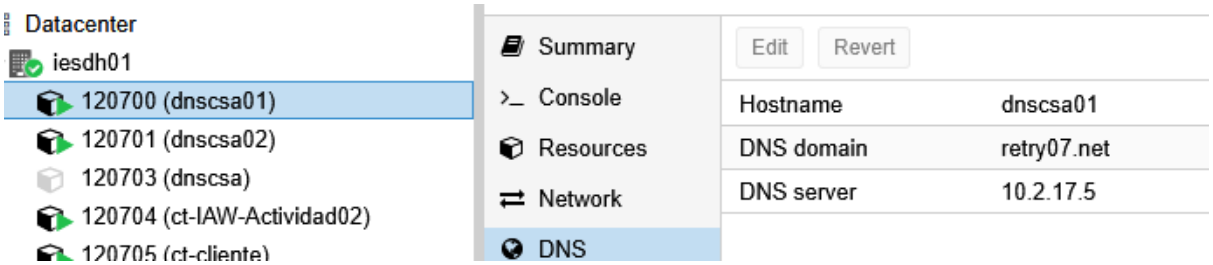
SERVICIOS DE RED E INTERNET

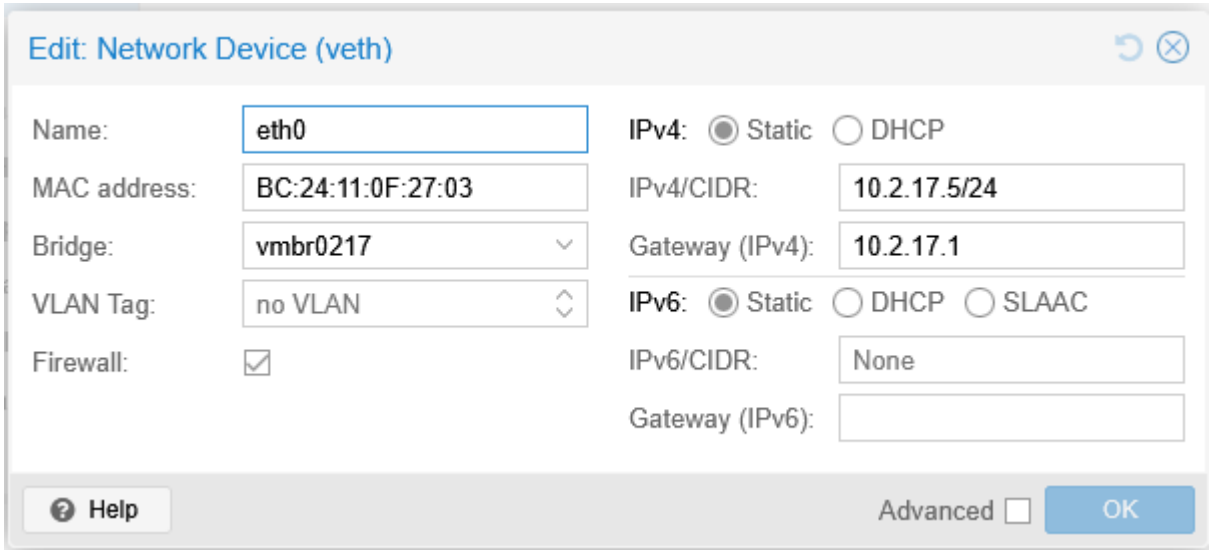
Cristóbal Suárez Abad

Práctica de repaso de DNS.

1. Instala (comprueba si está instalado) el Servidor DNS ***bind9*** en tu CT Ubuntu con prompt personalizado e ip fija. Su nombre de máquina debe ser dnsIniciales01 (dnsdjfr01, etc...)

apt -y update && apt -y install bind9 && apt install dnsutils
systemctl status bind9
ls -l /etc/bind





2. Configura los archivos correspondientes para dar resolución **directa** e **inversa** del dominio ***retryXY.net*** en la lan de aula (XY es tu número de lista), sabiendo que:

    a. **DNS**
        i. Es tu máquina dns.retryXY.net, siendo esta la autoritaria para dicha zona.
    b. **Correo**
        i. Los servidores de correo son **smtp1** y **smtp2** con mayor prioridad el segundo.
    c. **Directas**:
        i. El servidor DNS (dnsNombre) es la ip de tu DNS.
        ii. El servidor Web (www) es 172.16.111.200
        iii. Los servidores de correo son las IPs 172.16.111.201 y 202 (respectivamente).
        iv. El servidor de Minecraft (mc) está en la IP 172.16.111.203.
    d. **Alias**:
        i. Crea el alias ***dns*** para el servidor DNS
        ii. Crea el alias ***web*** para el servidor web
        iii. ***mail1*** y ***mail2*** para los servidores de correo.
        iv. servidormc para el servidor Minecraft

/etc/bind/named.conf.options

```
options {
        max-cache-size 256m;
        allow-query-cache { any; };
        allow-query { any; };
        recursion yes;
        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 {
        //      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;
        listen-on-v6 { any; };
};
```

(((/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";

// Archivo para busquedas directas
zone "retry07.net" {
        type master;
        file "bd.retry07.net"; // Debe estar en /var/cache/bind/
        allow-update { none; };
};

// Archivo para busquedas inversas
zone "111.16.172.in-addr.arpa" {
        type master;
        file "172.16.111.rev";
        allow-update { none; };
};


zone "17.2.10.in-addr.arpa" {
        type master;
        file "10.2.17.rev";
        allow-update { none; };
};
```

Archivo de búsqueda directa: /var/cache/bind/bd.retry07.net

```
; Archivo bd.retry07.net
;
; BIND data file for bd.retry.net
;
$TTL 1D
@ IN SOA dnscsa01.retry07.net. root.retry07.net. (
        2025102401 ; Serial Basado en el dia e incrementando
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Default TTL

; Servidores DNS del dominio
        IN NS   dnscsa01.retry07.net.

; Correo

        IN MX 20 smtp1.retry07.net.
        IN MX 10 smtp2.retry07.net.

; Directas

dnscsa01 IN A 10.2.17.5
www IN A 172.16.111.200
smtp1 IN A 172.16.111.201
smtp2 IN A 172.16.111.202
mc IN A 172.16.111.203

; Alias o sinonimo
dns IN CNAME dnscsa01
web IN CNAME www
mail1 IN CNAME smtp1
mail2 IN CNAME smtp2
servidormc IN CNAME mc
```

```
\\\\\\\\\\\\\Zona de busquedas inversas

/var/cache/bind/172.16.111.rev

;ARCHIVO DE ZONA INVERSA
$TTL 1D
@   IN  SOA 111.16.172.in-addr.arp. root.retry07.net. (
        2025102401 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Default TTL

      IN  NS  dnscsa01.retry07.net.

; Registros PTR
200     IN  PTR www.retry07.net.
201             IN  PTR smtp1.retry07.net.
202             IN  PTR smtp2.retry07.net.
203             IN  PTR mc.retry07.net.

\\\\\\\\SEGUNDO ARCHIVO DE BUSQUEDA INVERSA

/var/cache/bind/10.2.17.rev

;ARCHIVO DE ZONA INVERSA
$TTL 1D
@   IN  SOA 17.2.10.in-addr.arp. root.retry07.net. (
        2025102401 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Default TTL

      IN  NS  dnscsa01.retry07.net.

; Registros PTR
5       IN  PTR dnscsa01.retry07.net.
```

3. Previo a la recarga del DNS, comprueba que los archivos de configuración del DNS y de las zonas están correctos con las utilidades de ***bind9***.

Comprobación de archivo: named-checkconf /etc/bind/named.conf.options

Comprobación de archivo: named-checkconf /etc/bind/named.conf.local

name-checkzone retry07.net. /var/cache/bind/bd.retry07.net

name-checkzone 17.2.10.in-addr-arp /var/cache/bind/10.2.17.rev

4. Recarga el DNS y comprueba el correcto arranque mediante su estado y sus logs. Aporta dichos logs tanto con ***cat*** o ***tail*** del fichero de logs del sistema como con el comando que los lista directamente.

systemctl reload named
systemctl reload bind9
systemctl status named
systemctl status bind9

 # Si tus logs de bind9 están en /var/log/syslog
 # Muestra las últimas líneas del archivo
sudo tail /var/log/syslog | grep named

 # Para ver las últimas líneas en tiempo real
sudo tail -f /var/log/syslog | grep named

#Demasiado largo
sudo cat /var/log/syslog | grep named

journalctl -u bind9 --no-pager | tail -n 20

5. Comprueba que la zona resuelve correctamente, tanto de forma inversa como directa desde el servidor. Comprueba todos los **registros** DNS implicados.

Quienes son los DNS: dig @10.2.17.5 retry07.net NS

Quien es la autoridad DNS: dig @10.2.17.5 retry07.net SOA

Resolución de direcciones:

DNS (dnsIniciales01): dig @10.2.17.5 dnscsa01.retry07.net A

Web (www) dig @10.2.17.5 www.retry07.net A

Correo 1 (smtp1) dig @10.2.17.5 smtp1.retry07.net A

Correo 2 (smtp2) dig @10.2.17.5 smtp2.retry07.net A

Minecraft (mc) dig @10.2.17.5 mc.retry07.net A

Comprobamos que los alias apuntan correctamente a sus nombres canónicos.

dig mail1.retry07.net

dig mail2.retry07.net

dig mc.retry07.net

dig web.retry07.net

BÚSQUEDA INVERSA:

dig -x 10.2.17.5

dig -x 172.16.111.200

dig -x 172.16.111.201

dig -x 172.16.111.202

dig -x 172.16.111.203

6. Crea tu servidor esclavo (nombre dnsIniciales02, cuya ip será IP_master+110) y modifica lo necesario para crear un DNS esclavo para todas las zonas declaradas en el maestro.

En el DNS Master, en /etc/bind/named.conf.local se especifica el also-notify y allow-transfer poniendo la ip del esclavo.

nano /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";
// Archivo para busquedas directas
zone "retry07.net" {
	type master;
	file "bd.retry07.net"; // Debe estar en /var/cache/bind/
	allow-update { none; };
		also-notify { 10.2.17.110; };
		allow-transfer { 10.2.17.110; };
};

// Archivo para busquedas inversas
zone "111.16.172.in-addr.arpa" {
	type master;
	file "172.16.111.rev";
	allow-update { none; };
		also-notify { 10.2.17.110; };
		allow-transfer { 10.2.17.110; };
};

zone "17.2.10.in-addr.arpa" {
	type master;
	file "10.2.17.rev";
	allow-update { none; };
		also-notify { 10.2.17.110; };
		allow-transfer { 10.2.17.110; };
};
```

SEGUIMOS EN EL MAESTRO Y AHORA VAMOS A INCLUIR LA INFORMACIÓN DEL ESCLAVO EN LOS ARCHIVOS DE BÚSQUEDA, TANTO DIRECTA COMO INVERSA

nano /var/cache/bind/bd.retry07.net

```
; Archivo bd.retry07.net
;
; BIND data file for bd.retry.net
;
$TTL 1D
@ IN SOA dnscsa01.retry07.net. root.retry07.net. (
        2025102402 ; Serial Basado en el dia e incrementando
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Default TTL

; Servidores DNS del dominio
        IN NS   dnscsa01.retry07.net.
                IN NS   dnscsa02.retry07.net.

; Correo

        IN MX 20 smtp1.retry07.net.
        IN MX 10 smtp2.retry07.net.

; Directas

dnscsa01 IN A 10.2.17.5
dnscsa02 IN A 10.2.17.110
www IN A 172.16.111.200
smtp1 IN A 172.16.111.201
smtp2 IN A 172.16.111.202
mc IN A 172.16.111.203

; Alias o sinonimo
dns IN CNAME dnscsa01
dns2 IN CNAME dnscsa02
web IN CNAME www
mail1 IN CNAME smtp1
mail2 IN CNAME smtp2
servidormc IN CNAME mc
```

nano /var/cache/bind/10.2.17.rev

```
;ARCHIVO DE ZONA INVERSA
$TTL 1D
@   IN  SOA 17.2.10.in-addr.arp. root.retry07.net. (
        2025102403 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Default TTL

      IN  NS  dnscsa01.retry07.net.
            IN  NS  dnscsa02.retry07.net.

; Registros PTR
5       IN  PTR dnscsa01.retry07.net.
110             IN      PTR dnscsa02.retry07.net.
```

****

nano /var/cache/bind/172.16.111.rev

```
;ARCHIVO DE ZONA INVERSA
$TTL 1D
@   IN  SOA 111.16.172.in-addr.arp. root.retry07.net. (
        2025102403 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Default TTL

      IN  NS  dnscsa01.retry07.net.
            IN  NS  dnscsa02.retry07.net.

; Registros PTR
200         IN  PTR www.retry07.net.
201         IN  PTR smtp1.retry07.net.
202         IN  PTR smtp2.retry07.net.
203         IN  PTR mc.retry07.net.
```

\\\\\\\\\\\\\AHORA PASAMOS AL ESCLAVO:
INSTALARLE EL BIND9
AQUÍ SOLO TENEMOS QUE CONFIGURAR LOS ARCHIVOS: /etc/bind/named.conf.options Y /etc/bind/named.conf.local

En /etc/bind/named.conf.options ponemos lo mismo que en el MASTER.

/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";

// Archivo para busquedas directas
zone "retry07.net" {
	type slave;
	file "bd.retry07.net"; // Debe estar en /var/cache/bind/
	masters { 10.2.17.5; };
		allow-notify { 10.2.17.5; };
};

// Archivo para busquedas inversas
zone "111.16.172.in-addr.arpa" {
	type slave;
	file "172.16.111.rev";
	masters { 10.2.17.5; };
		allow-notify { 10.2.17.5; };
};


zone "17.2.10.in-addr.arpa" {
	type slave;
	file "10.2.17.rev";
	masters { 10.2.17.5; };
		allow-notify { 10.2.17.5; };
};
```

7. Crea tu servidor delegado (nombre dnsIniciales03, cuya ip será IP_master+130) y modifica lo necesario para crear un DNS delegado para la zona ***sz.retryXY.net***. Añade recursos (MX, NS, CNAME) para ese subdominio (P.e. www.***sz.retryXY.net***. **,** dns.***sz.retryXY.net***.**,** **mx.*sz.retryXY.net*.** **,**etc...) que resuelvan a IPs, correo, inversa, etc de la red 192.168.100.0/24 (ips a tu elección).

EN EL MASTER EN EL ARCHIVO de búsqueda directa

/var/cache/bind/bd.retry07.net

```
; Archivo bd.retry07.net
;
; BIND data file for bd.retry.net
;
$TTL 1D
@ IN SOA dnscsa01.retry07.net. root.retry07.net. (
      2025102403 ; Serial Basado en el dia e incrementando
      604800 ; Refresh
      86400 ; Retry
      2419200 ; Expire
      604800 ) ; Default TTL

; Servidores DNS del dominio
@      IN NS   dnscsa01.retry07.net.
@              IN NS   dnscsa02.retry07.net.
sz             IN NS   dnscsa03.sz.retry07.net.

; Correo

      IN MX 20 smtp1.retry07.net.
      IN MX 10 smtp2.retry07.net.

; Directas

dnscsa01 IN A 10.2.17.5
dnscsa02 IN A 10.2.17.110
dnscsa03.sz IN A 10.2.17.130
www IN A 172.16.111.200
smtp1 IN A 172.16.111.201
smtp2 IN A 172.16.111.202
mc IN A 172.16.111.203

; Alias o sinonimo
dns IN CNAME dnscsa01
dns2 IN CNAME dnscsa02
dns3 IN CNAME dnscsa03.sz
web IN CNAME www
mail1 IN CNAME smtp1
```

mail2 IN CNAME smtp2
servidormc IN CNAME mc

\\\\\\\\\\\\\\\\AHORA, EN EL DNS DELEGADO

dnscsa03.sz.retry07.net. 10.2.17.130

INSTALARLE EL BIND9

COPIA /etc/bind/named.conf.options del MASTER

LUEGO nano /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";

// Archivo para busquedas directas
zone "sz.retry07.net" {
        type master;
        file "bd.sz.retry07.net"; // Debe estar en /var/cache/bind/
                        allow-update { none; };
};

// Archivo para busquedas inversas
zone "100.168.192.in-addr.arpa" {
        type master;
        file "192.168.100.rev";
                        allow-update { none; };
};
```

\\\\\\\ Archivos de búsqueda

((/var/cache/bind/sz.retry07.net))

```
; Archivo bd.sz.retry07.net
;
; BIND data file for bd.sz.retry07.net
;
$TTL 1D
@ IN SOA dnscsa02.sz.retry07.net. root.sz.retry07.net. (
        2025102501 ; Serial Basado en el dia e incrementando
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Default TTL

; Servidores DNS del dominio
                IN NS   dnscsa03.sz.retry07.net.

; Correo

        IN MX 10 mx64.sz.retry07.net.
        IN MX 20 mx360.sz.retry07.net.

; Directas

dnscsa03 IN A 10.2.17.130
www IN A 192.168.100.10
mx64 IN A 192.168.100.11
mx360 IN A 192.168.100.12
carmack IN A 192.168.100.13
romero IN A 192.168.100.14

; Alias o sinonimo
dns3 IN CNAME dnscsa03
web IN CNAME www
nintendo IN CNAME mx64
xbox IN CNAME mx360
doom IN CNAME carmack
quake IN CNAME romero
```

####### AHORA búsqueda Inversa

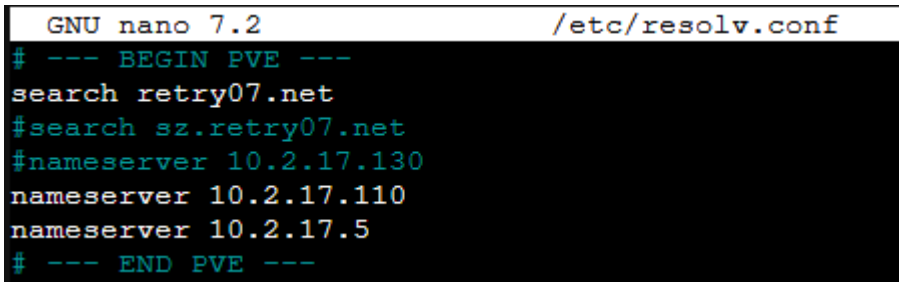
((/var/cache/bind/192.168.100.rev))

```
;ARCHIVO DE ZONA INVERSA
$TTL 1D
@   IN  SOA 100.168.192.in-addr.arp. root.sz.retry07.net. (
        2025102501 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Default TTL

      IN  NS  dnscsa03.sz.retry07.net.

; Registros PTR
10          IN  PTR www.sz.retry07.net.
11          IN  PTR mx64.sz.retry07.net.
12          IN  PTR mx360.sz.retry07.net.
13          IN  PTR carmack.sz.retry07.net.
14          IN  PTR romero.sz.retry07.net.
```

8. Configura tu cliente anfitrión para que las peticiones DNS sean resueltas por tus servidores DNS (Primero el esclavo y luego el maestro). Comprueba todos los **registros** DNS implicados. Ahora, usando las utilidades de cliente DNS y apuntando al DNS delegado comprueba los registros del subdominio.



dig retry07.net NS

dig retry07.net SOA

dig www.retry07.net A

dig mc.retry07.net A

dig dns.retry07.net A

dig www.retry07.net MX

Comprobar Alias:

dig web.retry07.net

Comprobar inversa:

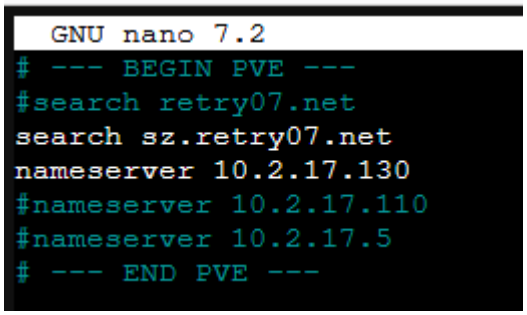
dig -x 172.16.111.200

dig -x 172.16.111.201

dig -x 172.16.111.202

dig -x 172.16.111.203

Apuntando al DNS Delegado:



dig sz.retry07.net NS

También se puede hacer sin cambiar “resolv.conf”.

dig sz.retry07.net NS @10.2.17.130

Usamos comandos parecidos a los anteriores, pero teniendo en cuenta el Subdominio y apuntando (si no modificamos resolv.conf) a la ip del DNS Delegado.

dig -x 192.168.100.10

dig -x 192.168.100.10 @10.2.17.130