IES de Teis
Avenida. de Galicia, 101
36216 – Vigo

Tfno.: 886 12 04 64
e-mail: ies.teis@edu.xunta.es
http://www.iesteis.es

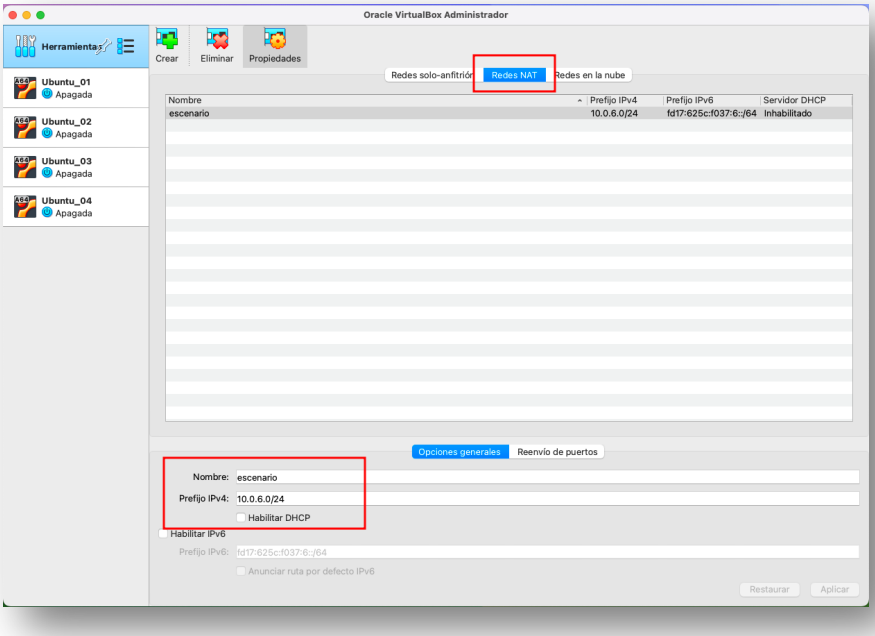
Práctica DNS

Objetivo

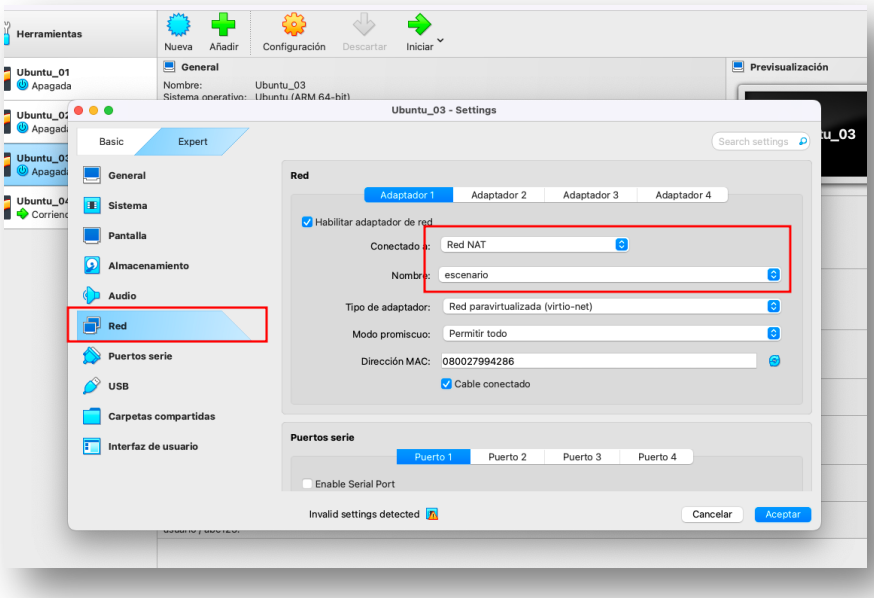
Instalar y configurar con un dominio personalizado un servidor DNS para una red interna.

Escenario inicial en VirtualBox

Crear una red NAT en VirtualBox, configura la SUBRED que quieras y deshabilita el servidor DHCP. Automáticamente se reservarán 2 IPs. La correspondiente a la primera IP de host de tu red será la dirección de del router de tu red que te conecta con el exterior (puerta de enlace). La correspondiente a la segunda IP de host de tu red será la dirección de un equipo que hace las funciones de DHCP y que NO vamos a usar porque lo hemos deshabilitado en la configuración de la red NAT.



Crearemos varias máquinas virtuales y no aseguramos de configurar su interfaz de red para que esté conectada a la red NAT creada en el paso anterior.



Un equipo que hará las funciones de servidor. Habrá que configurarle un IP de la siguiente manera:

- IP: tu red NAT acabada en .10
- Mascara: la definida en tu red NAT
- Puerta de enlace: tu red NAT acabada en .1
- DNS: por ahora 8.8.8.8 pero lo cambiaremos en el futuro cuando funcione DNS

Dos equipos clientes, uno Linux y otro Windows. Ambos clientes se dejarán con la configuración por defecto que debería estar en automático (configuración a través de DHCP)

Servidor DHCP

Configurar en el equipo servidor (X.X.X.10) un servidor DHCP usando KEA para repartir IPs de tu RED NAT dentro del rango de entre la IP acabada en 100 a la acabada en 200. Como dato extra se les pasará la puerta de enlace para que puedan navegar. Aun NO se les pasará DNS ni dominio de búsqueda local.

Como ayuda, este sería un archivo de configuración de KEA para el servidor DHCP que puedes usar y adaptar a tu escenario.

```
1. {
2. "Dhcp4":
```

```
 3.   {
 4.     "interfaces-config": { "interfaces": ["enp0s1"] },
 5.     "subnet4": [
 6.     {
 7.       "id":1,
 8.       "subnet": "192.168.0.0/24",
 9.       "pools": [ {"pool": "192.168.0.85 - 192.168.0.90"}],
10.       "option-data": [
11.       { "name" : "routers",
12.         "data": "192.168.0.1"
13.       }
14.     ]
15.     }
16.   ]
17.   }
18. }
19.
```

Comprobar que los clientes adquieren automáticamente una IP, que se hacen PING entre ellos y a una IP de internet como la 8.8.8.8 por ejemplo.

Servidor DNS

Instala BIND9 en tu equipo servidor.

Edita el archivo "/etc/default/named" para arrancar el servidor DNS (el programa "named") permitiendo que pueda modificar el "resolvconf" (el mini DNS local que incluyen los Ubuntu) y que solo gestione IP versión 4 (para evitarnos mensajes de advertencia por IPv6 sin configurar)

```
1. #
2. # run resolvconf?
3. RESOLVCONF=yes
4.
5. # startup options for the server
6. OPTIONS="-u bind -4"
7.
```

Edita el archivo "/etc/bind/named.conf.options" para especificar la carpeta donde se guardarán cachés, interfaces (tarjetas de red) en las que el servidor escuchará peticiones, equipos o redes a los que se les permite hacer consultas DNS, otros DNS recursivos a los que escalar la consulta y por último indicar que NO se hace dnssec-validation.

```
1. options {
 2.
 3.         directory "/var/cache/bind";
 4.
 5.         listen-on { any; };
 6.
 7.         allow-query { localhost; 192.168.0.0/24; };
 8.
 9.         forwarders {
10.                 8.8.8.8;
11.         };
12.
13.         dnssec-validation no;
14.
15. };
```

Revisa que el archivo no tenga errores sintácticos con "named-checkconf".

Antes de definir las zonas hay que decidir el nombre del dominio que vamos a usar, el nombre de los equipos que queremos identificar y tener claras sus IPs. El dominio que usarás será tu nombre ".es". Identificaremos al servidor como "servidor" en la IP X.X.X.10 y también identificaremos a "puertaenlace" como X.X.X.1

Registramos las zonas directa e inversa en "/etc/bind/named.conf.local" y posteriormente comprobamos con "named-checkconf" que no tiene errores sintácticos.

```
zone "javi.local" IN {
        type master;
        file "/etc/bind/zonas/db.javi.local";
};


zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/zonas/db.0.168.192";
};
```

Para cada una de las zonas creamos y editamos el archivo correspondiente. En cada uno de los archivos tendremos los REGISTROS DNS de esa zona concreta. La zona directa quedaría en algo parecido a esto:

```
;
; BIND data file for javi.local
;
$TTL    604800
@       IN      SOA     dns.javi.local. root.javi.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
        IN      NS      dns.javi.local.
dns     IN      A       192.168.0.80
router  IN      A       192.168.0.1
gw      IN      CNAME   router

```

Y la zona inversa en algo parecido a esto:

```
;
; BIND data file for zona inversa
;
$TTL  604800
@     IN        SOA       dns.javi.local. root.javi.local. (
                                2             ; Serial
                           604800             ; Refresh
                            86400             ; Retry
                          2419200             ; Expire
                           604800 ) ; Negative Cache TTL
;
      IN        NS        dns.javi.local.
0     IN        PTR       dns.javi.local.

```

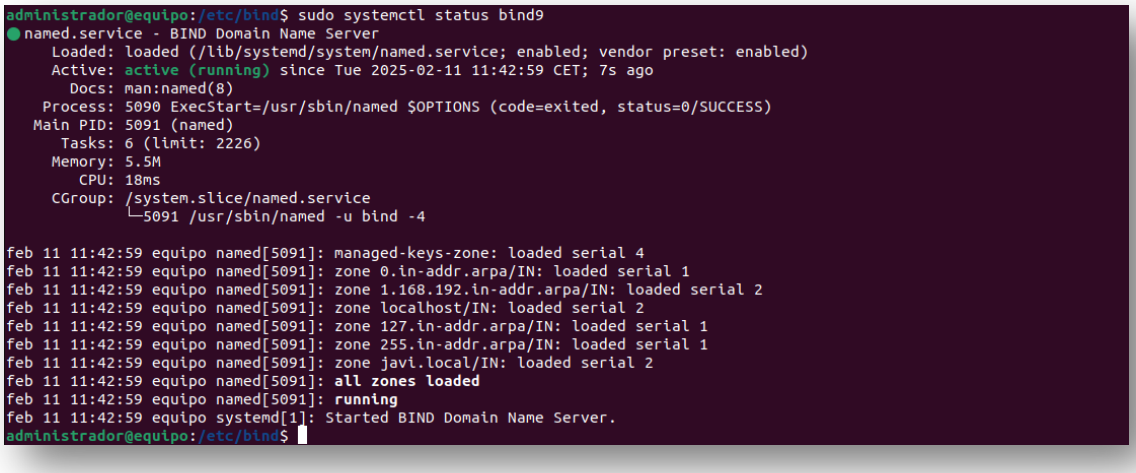
Comprobamos sintácticamente las zonas usando "named-checkzone" indicando dominio y archivo, por ejemplo:

```
named-checkconf
named-checkzone javi.local. db.javi.local
named-checkzone 0.168.192.in-addr.arpa db.0.168.192
```

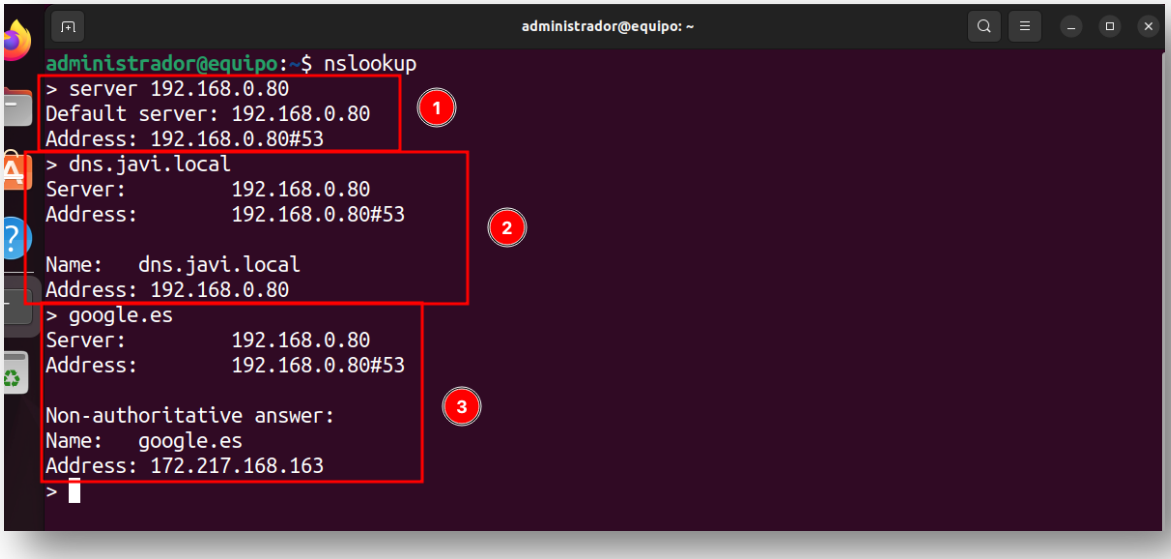
Reiniciamos el servicio BIND con un "restart" y comprobamos su estado con un "status":

```
sudo systemctl restart bind9
sudo systemctl status bind9
```

Debería salir un "status" como este en el que aparecen nuestras zonas ok.



Probar que el DNS está funcionado bien mediante la herramienta "nslookup". Primero cambiando de servidor DNS al que queremos hacer la consulta y colocando el nuestro. Segundo haciendo una consulta a un nombre interno a nuestro dominio. Tercero haciendo una consulta a un dominio externo.



IES de Teis
Avenida. de Galicia, 101
36216 – Vigo
Tfno.: 886 12 04 64
e-mail: ies.teis@edu.xunta.es
http://www.iesteis.es

Modificación del servicio DHCP para añadir el nuevo DNS

Modifica el archivo de configuración del servicio DHCP que gestiona "KEA" para que sustituya el DNS que tenía configurado para los clientes (el 8.8.8.8) por tu nuevo DNS (X.X.X.10). Reinicia el servicio

Enciende alguno de los PCs clientes y comprueba que ha recibido la nueva configuración. Realiza las siguientes pruebas y analiza si lo que sucede es lo que esperabas.

- Ping a la X.X.X.1 (la puerta de enlace)
- Ping a "puertaenlace.tunombre.es" (también la puerta de enlace pero llamándola por su nombre de dominio)
- Ping a "localhost"
- Ping a "servidor"
- Ping a "puertaenlace"
- Ping a 8.8.8.8 (una IP pública cualquiera de fuera de nuestra red)

Modificación del servicio DHCP para añadir búsqueda local

Modifica el archivo de configuración del servicio DHCP que gestiona "KEA" para que incluya una búsqueda local en tu dominio sin necesidad de escribirlo todo cuando se hacen consultas de equipos internos. Debes usar la opción "domain-search". Reinicia el servicio

Enciende alguno de los PCs clientes y comprueba que ha recibido la nueva configuración. Realiza las siguientes pruebas y analiza si lo que sucede es lo que esperabas.

- Ping a la X.X.X.1 (la puerta de enlace)
- Ping a "puertaenlace.tunombre.es" (también la puerta de enlace pero llamándola por su nombre de dominio)
- Ping a "localhost"
- Ping a "servidor"
- Ping a "puertaenlace"
- Ping a 8.8.8.8 (una IP pública cualquiera de fuera de nuestra red)

Actualización del servidor

Actualiza la configuración IP fija de tu servidor para incluir el nuevo DNS (y eliminar el anterior?) y como reto (no está entre los apuntes) averiguar cómo incluir el "domain-search" en la configuración manual del servidor...