ADMINISTRACIÓN DE SISTEMAS 2

PRÁCTICA 2

Pablo Moreno Muñoz 841972

Identificador W->E

ÍNDICE

Resumen

Se llevarán a cabo la implementación de dos nuevas VMs y la redefinición de ciertas partes de las VMs existentes. Específicamente, un servidor DNS principal para la subred y un servidor UNBOUND que se encargará de gestionar las solicitudes de todas las máquinas, almacenando en caché estas solicitudes.

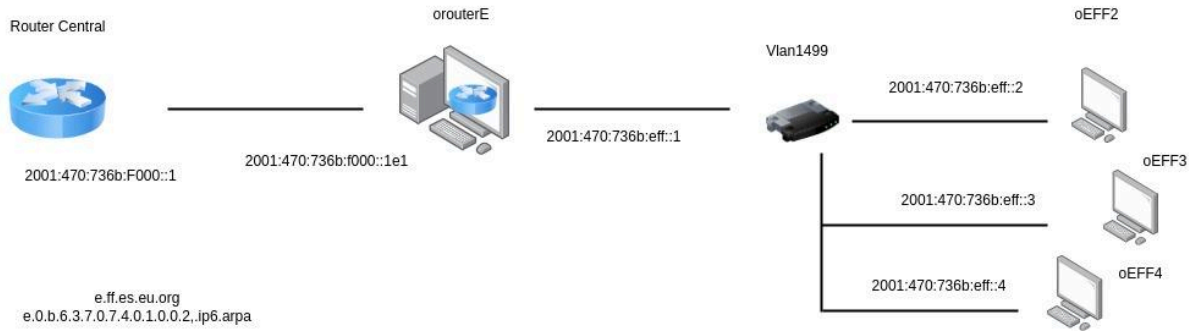
Introducción y objetivos

Vamos a crear las nuevas máquinas virtuales 3 y 4, así como modificar la máquina virtual 2 para que esta tenga una IP estática asociada.
Poner en funcionamiento el servicio nsd en la máquina virtual 3, comprobar el correcto funcionamiento, posteriormente realizar la configuración de la zona directa, realizar todo lo anterior para la zona inversa de la misma forma.
Poner en funcionamiento el servicio unbound en la máquina virtual 4, testear con el comando dig -6 que este funciona adecuadamente.

Objetivos

- Ser capaces de acceder mediante un DNS público a la subred
- Acostumbrarse y dominar el uso de ruby
- Configurar de forma adecuada los servidores DNS y UNBOUND de la red de forma que estos funcionen de forma adecuada con los glue records.

Arquitectura de elementos relevantes



Comprehensión de elementos significativos de la práctica

oEFF2 (DNS recursivo *Unbound*)

Esta máquina ha sido configurada con dos roles principales: servidor DNS recursivo con caché.

En cuanto al servidor DNS recursivo con caché implementado con Unbound, se ha realizado una configuración en el archivo `/var/unbound/etc/unbound.conf`.
Se ha configurado la escucha en el interfaz 2001:470:736b:EFF::2 y se han permitido las peticiones sólo a máquinas pertenecientes al mismo segmento de red.
Además, se ha definido el servidor Hurricane al cual forwardear en caso de no encontrar resolución local.
Se han creado dos zonas de enlace "*stub-zones"* (Directa e Inversa) especificando los servidores DNS desplegados en la VLAN, lo que asegura que el tráfico de resolución de nombres se dirija directamente a los servidores DNS locales en lugar de ser redirigido a Internet y luego volver al servidor Hurricane para su resolución. Esto optimiza el proceso de resolución de nombres dentro de la red local.

oEFF3 (DNS Maestro)

Esta máquina ha sido configurada como un servidor DNS Maestro, encargado de proporcionar servicios de resolución de nombres a las máquinas dentro de su misma red. Trabaja en conjunto con la máquina oEFF4, la cual actúa como servidor esclavo, estableciendo así una relación de autoridad conjunta para la gestión de las zonas DNS.

La configuración se llevó a cabo mediante la modificación del archivo /var/nsd/etc/nsd.conf, donde se definió la información a enviar al servidor esclavo, y se configuraron las zonas directa e inversa del DNS.

Se crearon dos archivos, e.ff.es.eu.org.directo y e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. ,para definir la zona directa e inversa respectivamente.
Estos archivos contienen registros de información SOA, registros de servidores NS y registros de resolución directa (AAAA) e inversa (PTR).

¿ Cuáles son los valores numéricos definidos en el registro SOA , qué significan y cuál es la utilidad de cada uno ?
:

• Serial Number: se trata de la fecha de actualización de la zona y el número de versión de ese día una buena práctica sería actualizar este número cada vez que haya una actualización significativa en el DNS.

• Refresh: Este valor representa el intervalo de tiempo en segundos después del cual los servidores secundarios deben intentar volver a contactar al servidor primario para comprobar si ha habido cambios en la zona

• Retry: Es el tiempo de espera en segundos que un cliente DNS debe esperar antes de intentar volver a enviar una consulta al servidor primario si no recibe respuesta.

• Expire: Tiempo máximo en segundos que un servidor secundario puede utilizar la información de la zona sin comprobar si ha habido cambios.

• Minimum TTL: El tiempo durante el cual los registros de recursos asociados a una zona DNS pueden ser mantenidos en caché

oEFF3 (DNS Esclavo)

Esta máquina ha sido configurada como un servidor DNS Esclavo, cuya función principal es proporcionar servicios de resolución de nombres a las máquinas trabajando en conjunto con la máquina oEFF3, la cual desempeña el rol de servidor maestro, estableciendo así una relación de autoridad compartida para la gestión de las zonas DNS.

La configuración del servidor DNS Esclavo guarda similitudes con la del servidor maestro. En el archivo `/var/nsd/etc/nsd.conf`, la sección que varía es el apartado de pattern.
Aquí se utilizan patrones "tomaster" además de activar la aceptación de recepción de peticiones "notify", lo que indica al servidor esclavo que está dispuesto a recibir actualizaciones de zonas desde el servidor maestro.

Configuración inicial de oEFF3 y oEFF4

La configuración del fichero /etc/hostname.vio0 es la siguiente:

up
-inet6

Creamos el fichero /etc/hostname.vlan1499 y su contenido es el siguiente:

*inet6 2001:470:736b:eff::**Z** 64 vlan 1499 vlandev vio0*

La configuración del fichero /etc/myname es la siguiente:

*oEFF**Z***

Añadimos en el fichero /etc/mygate el enrutador por defecto

2001:470:736b:eff::1

Para aplicar los cambios usamos el comando:

sh /etc/netstart

REConfiguracion de OEFF2

Debido a que en esta práctica tenemos que hacer que la máquina tenga una ip estática necesitamos modificar el fichero /etc/hostname.vlan1499 añadiendo la siguiente línea y sustituyendo la antigua sentencia

inet6 2001:470:736b:eff::1 -> inet6 autoconf

También para permitir que se pueda conectar desde el exterior al la maquina interna es necesario añadir en el fichero /etc/mygate la dirección ipv6 del enrutador por defecto

2001:470:736b:eff::1

Configurar clientes:
Realizar esto en todas las máquinas : Editar el fichero /etc/resolv.conf y escribir lo siguiente:
nameserver 2001:470:736b:eff::2

Configurar el servidor DNS maestro:

Primeramente tenemos que activar el set up inicial del dns
rcctl enable nds
nsd-control-setup

Posteriormente tenemos que crear las zonefiles en la carpeta /var/nsd/zones/:

touch e.ff.es.eu.org.directo
touch e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.

Modificamos el fichero /var/nsd/etc/nsd.conf y lo configuramos de la siguiente manera:

```
server:
        hide-version: yes
        ip-address: 2001:470:736b:eff::3
         verbosity: 1
         database: "/var/nsd/db/nsd.db" # disable database
         username: _nsd
         logfile: "/var/log/nsd.log"
         pidfile: "/var/nsd/run/nsd.pid"
        port: 53

remote-control:
        control-enable: yes
        control-interface: /var/run/nsd.sock
pattern:
      name: "toslave"
      notify: 2001:470:736b:EFF::4 NOKEY
      provide-xfr: 2001:470:736b:EFF::4 NOKEY


## master zone example
zone:
        name: "e.ff.es.eu.org"
        zonefile: "e.ff.es.eu.org.directo"
        include-pattern:"toslave"



zone:
```

```
        name: "e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa."
        zonefile: "e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa."
        include-pattern:"toslave"
```

Finalmente comprobamos que la configuración es correcta con el comando:
nsd-checkconf /var/nsd/etc/nsd.conf

Configurar el servidor DNS slave:

Primeramente tenemos que activar el set up inicial del dns
rcctl enable nds
nsd-control-setup

Modificamos el fichero /var/nsd/etc/nsd.conf y lo configuramos de la siguiente manera:

```
server:
        hide-version: yes
        ip-address: 2001:470:736b:eff::4
         verbosity: 1
         database: "/var/nsd/db/nsd.db" # disable database
         username: _nsd
         logfile: "/var/log/nsd.log"
         pidfile: "/var/nsd/run/nsd.pid"
        port: 53

remote-control:
        control-enable: yes
        control-interface: /var/run/nsd.sock

pattern:
        name: "tomaster"
        allow-notify: 2001:470:736b:EFF::3 NOKEY
        request-xfr:AXFR 2001:470:736b:EFF::3 NOKEY

## slave zone example
zone:

      name: "e.ff.es.eu.org"
      zonefile: "e.ff.es.eu.org.directo"
      include-pattern:"tomaster"
zone:
```

```
name: "e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa."
zonefile: "e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa."
include-pattern:"tomaster"
```

Finalmente comprobamos que la configuración es correcta con el comando:
nsd-checkconf /var/nsd/etc/nsd.conf

Configuración de la zona directa

Vamos a configurar el fichero /var/nsd/zones/e.ff.es.eu.org.directo

```
$ORIGIN e.ff.es.eu.org.
$TTL 86400
@       IN      SOA     ns1.e.ff.es.eu.org. a841972.e.ff.es.eu.org (
        2013022501
        21600
        3600
        604800
        86400
)
        NS              ns1.e.ff.es.eu.org.
ns1     IN      AAAA    2001:470:736b:eff::3
ns2     IN      AAAA    2001:470:736b:eff::4
router1 IN      AAAA    2001:470:736b:eff::1
unbound IN      AAAA    2001:470:736b:eff::2
```

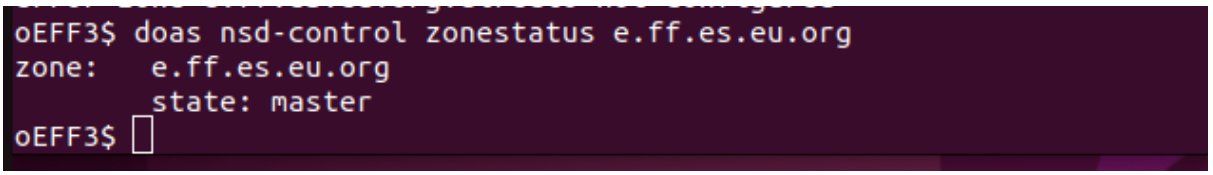
A continuación podemos comprobar la correcta configuración con el siguiente comando:

nsd-checkzone e.ff.es.eu.org /var/nsd/zones/e.ff.es.eu.org.directo
Una vez comprobada la configuración correcta se aplica con el siguiente comando
doas nsd-control reconfig

Y recargamos la zona para que se active correctamente

doas nsd-control reload e.ff.es.eu.org

Si dice que hay un error podemos utilizar este comando para ver el status de la zona
doas nsd-control zonestatus e.ff.es.eu.org



Configuración de la zona indirecta

Vamos a configurar el fichero /var/nsd/zones/e.ff.es.eu.org.directo

```
$ORIGIN e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.
$TTL 86400
@       IN      SOA     ns1.e.ff.es.eu.org. a841972.e.ff.es.eu.org. (
        0000001
        21600
        3600
        604800
        86400
)
                                        NS      ns1.e.ff.es.eu.org.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR router1.e.ff.es.eu.org.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR unbound.e.ff.es.eu.org.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR ns1.e.ff.es.eu.org.
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR ns2.e.ff.es.eu.org.
```

A continuación podemos comprobar la correcta configuración con el siguiente comando:
nsd-checkzone e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.
/var/nsd/zones/e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.
Una vez comprobada la configuración correcta se aplica con el siguiente comando
doas nsd-control reconfig
Y recargamos la zona para que se active correctamente
doas nsd-control reload e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.

Probar correcto funcionamiento del DNS esclavo y maestro:

Usamos los comandos dig -6 @2001:470:736b:eff::4 ns1.e.ff.es.eu.org

```
oEFF3$ dig -6 @2001:470:736b:eff::4 ns1.e.ff.es.eu.org

; <<>> dig 9.10.8-P1 <<>> -6 @2001:470:736b:eff::4 ns1.e.ff.es.eu.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33127
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;ns1.e.ff.es.eu.org.            IN      A

;; AUTHORITY SECTION:
e.ff.es.eu.org.         86400   IN      SOA     ns1.e.ff.es.eu.org. a841972.e.ff.es.eu.org.e.ff.es.eu.org. 2013
022501 21600 3600 604800 86400

;; Query time: 0 msec
;; SERVER: 2001:470:736b:eff::4#53(2001:470:736b:eff::4)
;; WHEN: Tue Feb 20 11:16:35 CET 2024
;; MSG SIZE  rcvd: 106
```

dig -6 @2001:470:736b:eff::3 ns2.e.ff.es.eu.org

```
oEFF3$ dig -6 @2001:470:736b:eff::3 ns2.e.ff.es.eu.org

; <<>> dig 9.10.8-P1 <<>> -6 @2001:470:736b:eff::3 ns2.e.ff.es.eu.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29362
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;ns2.e.ff.es.eu.org.            IN      A

;; AUTHORITY SECTION:
e.ff.es.eu.org.         86400   IN      SOA     ns1.e.ff.es.eu.org. a841972.e.ff.es.eu.org.e.ff.es.eu.org. 2013
022501 21600 3600 604800 86400

;; Query time: 0 msec
;; SERVER: 2001:470:736b:eff::3#53(2001:470:736b:eff::3)
;; WHEN: Tue Feb 20 11:24:42 CET 2024
;; MSG SIZE  rcvd: 110
```

La razón por la que no obtienes una respuesta en la sección ANSWER es porque estás consultando el servidor maestro directamente y no se espera que devuelva registros de datos para consultas de este tipo. El servidor maestro generalmente solo proporciona información de autoridad sobre la zona.

dig -6 @2001:470:736b:eff::3 -x 2001:470:736b:eff::1

```
;; MSG SIZE  rcvd: 114

ns1$ dig -6 @2001:470:736b:eff::3 -x 2001:470:736b:eff::2

; <<>> dig 9.10.8-P1 <<>> -6 @2001:470:736b:eff::3 -x 2001:470:736b:eff::2
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58732
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. IN PTR

;; ANSWER SECTION:
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 86400IN PTR unbound.e.ff.es.eu.org.

;; AUTHORITY SECTION:
e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 86400 IN NS ns1.e.ff.es.eu.org.

;; Query time: 0 msec
;; SERVER: 2001:470:736b:eff::3#53(2001:470:736b:eff::3)
;; WHEN: Sun Feb 25 21:14:10 CET 2024
;; MSG SIZE  rcvd: 155

ns1$
```

Configuración del unbound

Primero deberíamos activar el servidor unbound con los siguientes comandos:

rcctl enable unbound
unbound-control-setup

Modificamos el fichero /var/unbound/etc/unbound.conf:

server:
server:
interface: 2001:470:736b:EFF::2
do-ip6: yes

access-control: 0.0.0.0/0 refuse
access-control: 2001:470:736b:EFF::/64 allow
access-control: ::0/0 refuse
access-control: ::1 allow

hide-identity: yes
hide-version: yes
val-log-level: 2

```
        aggressive-nsec: yes

        remote-control:
        control-enable: yes
        control-interface: /var/run/unbound.sock

stub-zone:
        name:"e.ff.es.eu.org"
        stub-addr: 2001:470:736b:eff::3
        stub-first:yes
stub-zone:
        name:"e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa."
        stub-addr: 2001:470:736b:eff::3
        stub-first:yes
forward-zone:
        name: "."                       # use for ALL queries
        forward-addr: 2001:470:20::2            # example address only
        forward-first: yes              # try direct if forwarder fails
```

Comprobamos que la configuración es correcta y reiniciamos el servicio con los siguientes comandos:

unbound-checkconf
unbound-control reload

Problemas encontrados y su solución.

Un pequeño problema fue a la hora de crear la imagen diferencial , en un principio intenté hacerla en base a la imagen de la máquina oEFF2 ya que tendría cierta configuración ya realizada y pensaba que sería más fácil, pero al hacer esto me daba un error de que esa imagen estaba en uso ya que tenia permisos de escritura y se podía modificar así que no me permitió hacer la imagen diferencial

Al cambiar de ip automática a estática en las máquinas, no se podía hacer ni ping ni ssh desde el lab a las máquinas 3 y 4. El problema se soluciono poniendo en dichas máquinas en su gate la dirección del router que no era necesaria para las ips automáticas pero sí que lo es para las estáticas.

Otro problema encontrado fue a la hora de realizar el script de Ruby, en el apartado de SSH debido a que utilizaba las claves públicas ed25519 las cuales no estaban soportadas por la versión de Ruby por lo tanto tuve que crear unas nuevas claves RSA y enviarlas a cada una de las máquinas.

Posteriormente tuve que especificar en el comando de ssh que usar las llaves RSA en vez de la ed25519

Net::SSH.start(host,"a841972" ,keys: ["~/.ssh/id_rsa"])

ANEXO

A parte de lo requerido en la práctica se ha realizado un pequeño script en bash que combinado con las nuevas funcionalidades del script de la primera práctica, permite una vez definidos y iniciados las máquinas, abrir automáticamente una terminal por máquina virtual encendida y conectarse a cad auna de estas máquinas mediante la lectura de un fichero con sus ip's

```
Unset
#!/bin/bash

# Verifica si el archivo m1.txt existe
if [ ! -f "m1.txt" ]; then
  echo "El archivo m1.txt no existe."
  exit 1
fi

# Itera sobre cada línea del archivo m1.txt
while IFS= read -r ip_address; do
  gnome-terminal -- ssh -t -Y a841972@central.cps.unizar.es "ssh -t -Y
a841972@$ip_address"
done < "m1.txt"
```