AS2 : Práctica Nº 2

---

1. Resumen

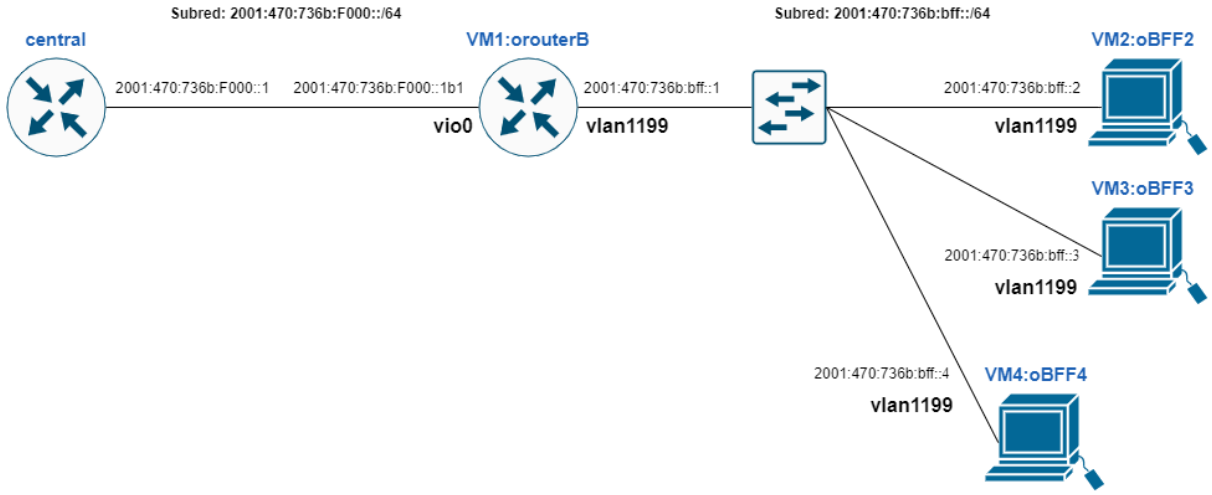
En esta práctica, además de seguir trabajando en la configuración de red, ya que se añaden dos nuevas máquinas al diseño de nuestra arquitectura, se han configurado una serie de servidores en cada una de las máquinas internas.
En la primera máquina interna la VM2 se ha configurado un servidor NTP, este es un protocolo de sincronización de tiempo global en Internet y que suele ser requerido por otros servicios distribuidos. En está máquina además se ha configurado un servidor DNS recursivo con caché mediante la herramienta unbound.
En las otras dos máquinas se ha configurado un servidor DNS, en la VM3 un servidor DNS maestro (primario) y para la VM4 un servidor DNS esclavo (secundario) mediante nsd.
Además se han configurado como clientes DNS, todas las máquinas para que las consultas DNS se envíen al servidor DNS recursivo y con caché de la VM2. De forma similar, se han configurado todas las máquinas como clientes ntp utilizando el servidor ntp de la VM2.

2. Introducción y objetivos

El objetivo principal de esta prácticaes la puesta en marcha de los distintos servicios distribuidos, NTP y DNS, además de la configuración necesaria de red y las máquinas virtuales, y la familiarización con los demonios ntpd, nsd y unbound que permiten la configuración y puesta en marcha de estos servicios.

3. Arquitectura de elementos relevantes

A continuación se muestra el esquema de red que se ha configurado para la práctica, donde se muestran los elementos más relevantes.



4. Comprehensión de elementos significativos

- **Servidor NTP:** el protocolo NTP es lo que nos permite montar el servidor NTP, este protocolo permite que los dispositivos de una red tengan la misma hora de forma coordinada. La sincronización de tiempo NTP proporciona una sincronización de tiempo global en Internet que van a requerir otros servicios distribuidos.
  En nuestro caso, para el sistema openBSD se ha configurado mediante las siguientes herramientas: **demonio ntpd**, fichero de configuración de demonio **ntpd.conf** y se ha gestionado mediante el comando **ntpctl** que gestiona ese demonio concreto y **rcctl** que se utiliza para la gestión de demonios (encenderlos, apagarlos, reiniciarlos, etc).
  En nuestro caso se ha realizado la configuración del servidor NTP en la máquina VM2 indicando en el fichero de configuración ntpd.conf dos servidores de referencia: server 2001:470:0:50::2 y server 2001:470:0:2c8::2, estos son los servidor stratum de referencia que va a utilizar nuestro servidor NTP para sincronizarse.
  Para las máquinas clientes su configuración es distinta, en ellas se tendrá que indicar la dirección de la máquina VM2, ya que el servidor de esta máquina es el que las máquinas clientes tienen como referencia.

- **Servidor DNS recursivo con caché:** Un servidor de nombres DNS recursivo con caché va a permitir cachear respuestas para servicios posteriores más rápido tras la primera búsqueda, ya que se guarda en caché la información. Además al ser recursivo se va a ocupar de las peticiones hasta que devuelve respuesta o error.
  En nuestro caso este servidor se ha configurado mediante el demonio **unbound** y va a permitir resolver de forma recursiva las peticiones de las demás máquinas que se han configurado como clientes DNS. Para configurar los clientes DNS se ha indicado en el fichero **/etc/resolv.conf** la dirección de la VM2, para que cualquier resolución de nombres de dominio se redirija a este servidor, en el caso de la propia máquina VM2 se ha añadido la línea nameserver ::1 para que las peticiones se realicen a la propia máquina.
  Por otro, la configuracion del servicio dns se ha configurado en el fichero **/var/unbound/etc/unbound.conf**, en él se ha dado permiso de acceso al servidor a todas las máquias con prefijo **2001:470:736b:bff::/64** mediante **access-control** allow.
  Por último, se han habilitado las opciones **hide-identity** y **hide-version**, para que los clientes no puedan conocer la identidad de nuestro servidor y la versión de unbound de la que disponemos, se han añadido los **forward-zone** dejando el servidor DNS de Hurricane Electrics y por último se ha añadido la opción **stub-zone** para obtener una resolución local de la zona directamente de los servidores DNS con autoridad.

- **Servidor DNS maestro/esclavo:**
  Por último se ha configurado un servicio DNS maestro-esclavo en el que la VM3 va a actuar como maestro y la VM4 como esclavo. Para la configuración de estos servicios se ha tenido que modificar los ficheros de configuración **nsd.conf** en cada una de las

máquinas. En la VM3 se ha realizado la configuración de servidor maestro, para ellos en el fichero **nsd.conf** se ha exigido que solo escuche en la red local, se han indicado la ruta a los ficheros de claves y certificados generados con nsd-control-setup y se ha añadido la opción pattern, en la que se indicará la dirección de la máquina esclava, para permitir que se notifiquen los cambios de zonas a esta máquina y proveer así la actualización de las zonas de esa máquina esclava (VM4).
Por otro lado en la máquina esclava en el pattern se indica la direccion del maestro "tomaster", es imprescindible indicarla en **request-xfr** ya que es atraves de esa ip por la cual se actulizarán los ficheros de zonas automáticamente.
Por último se han configurado los ficheros de zonas (directo e inverso) en la máquina VM3, la VM4 no necesita que se realice esta configuración ya que el maestro será el encargado de transmitir esos ficheros a la máquina esclava.

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

- **2023030301 (serial number)**: Indica el número de serie actual de la zona, este se utiliza para identificar las actualizaciones de la zona y hay que incrementarlo cada vez que se realiza una modificación en la zona para que se transmita a los esclavos . El formato que sigue es aaaammddvv, siendo aaaa el año, mm el mes, dd el día y vv el número de versión.
- **21600 (refresh interval):** Indica el tiempo en segundos que los servidores esclavos deben esperar para actualizar su copia de la zona desde el servidor maestro. Se encarga de la propagación de los cambios realizados en la zona.
- **3600 (retry interval):** Este campo especifica cada cuánto tiempo, en segundos, los esclavos deben esperar antes de volver a intentar actualizar su copia de la zona en caso de que no hayan podido establecer conexión con el servidor maestro.
- **604800 (expiration time):** Es el tiempo máximo que un servidor esclavo puede utilizar una copia de la zona antes de que se considere que ha caducado. Después de ese tiempo, el esclavo tendrá que solicitar una nueva copia de la zona al servidor maestro.
- **86400 (minimum time to live):** Este último campo indica cuánto tiempo los servidores esclavos pueden mantener la información de la zona, específica el valor mínimo del TTL que debe ser utilizado para cualquier exploración de la zona.

5. Comprobaciones funcionamiento

- **Servidor NTP:**

  central:~/ ntpdate -q ntp.time.nl

  server 2a00:d78:0:712:94:198:159:14, stratum 1, offset -0.000282, delay 0.06372
  server 2a00:d78:0:712:94:198:159:10, stratum 1, offset -0.005948, delay 0.07452
  server 94.198.159.14, stratum 1, offset -0.001213, delay 0.07594

server 94.198.159.10, stratum 1, offset -0.001441, delay 0.07555
7 Mar **19:00:16** ntpdate[5558]: adjust time server 2a00:d78:0:712:94:198:159:14 offset - 0.000282 sec
central:~/ ntpdate -q 2001:470:736b:bff::2
server 2001:470:736b:bff::2, stratum 2, offset 0.000570, delay 0.02606
7 Mar **19:00:27** ntpdate[5581]: adjust time server 2001:470:736b:bff::2 offset 0.000570 sec

- **Servidores DNS:**
  Muestra funcionamiento mediante el comando unbound-host:
  unbound-host orouterB.b.ff.es.eu.org
  orouterB.b.ff.es.eu.org is an alias for router1.b.ff.es.eu.org.
  router1.b.ff.es.eu.org has IPv6 address 2001:470:736b:bff::1

  Muestra funcionamiento caché y resolución directa:
  ntp1$ dig -6 AAAA oBFF4.b.ff.es.eu.org
  Primera consulta:
  ;; QUESTION SECTION:
  ;oBFF4.b.ff.es.eu.org. IN AAAA
  ;; ANSWER SECTION:
  oBFF4.b.ff.es.eu.org. 3600 IN CNAME ns2.b.ff.es.eu.org.
  ns2.b.ff.es.eu.org. 3600 IN AAAA 2001:470:736b:bff::4
  ;; Query time: **258 msec**
  ;; **SERVER: ::1**#53(::1)

  Siguientes consultas:
  ;; QUESTION SECTION:
  ;oBFF4.b.ff.es.eu.org. IN AAAA
  ;; ANSWER SECTION:
  oBFF4.b.ff.es.eu.org. 3600 IN CNAME ns2.b.ff.es.eu.org.
  ns2.b.ff.es.eu.org. 3600 IN AAAA 2001:470:736b:bff::4
  ;; Query time: **0 msec**
  ;; **SERVER: ::1**#53(::1)

  Muestra funcionamiento caché y resolución inversa:
  dig -6 -x 2001:0470:736b:0bff:0000:0000:0000:0004
  Primera consulta:
  ;; QUESTION SECTION:
  ;4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.b.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. IN PTR
  ;; ANSWER SECTION:

4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.b.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 3587 IN PTR ns2.b.ff.es.
eu.org.
;; Query time: **128 msec**
;; SERVER: ::1#53(::1)

Siguientes consulta:
;; QUESTION SECTION:
;4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.b.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. IN PTR
;; ANSWER SECTION:
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.b.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 3587 IN PTR ns2.b.ff.es.
eu.org.
;; Query time: **0 msec**
;; SERVER: ::1#53(::1)

6. Problemas encontrados y su solución

Los principales problemas que se han encontrado en la resolución de la práctica han sido en la configuración de los ficheros de zona y tener en consideración que al realizar una modificación de estos ficheros hay que incrementar el número de versión, y así mediante el comando **nsd-control reload zona** se transmite la actualización de estos ficheros a la máquina esclava.
Otro de los problemas, relacionado también con con los ficheros de zonas han sido la sintaxis que siguen estos ficheros, para los cuales la herramienta **nsd-checkzone** ha sido de gran ayuda.

7. Ejercicio ruby

En el solo se ha realizado la primera parte del ejercicio, el comando ping:

```
#!/usr/bin/ruby -w
require 'net/ping/tcp'
# Archivo con la lista de host
hosts_file = File.expand_path("~/.u/hosts")
hosts = File.readlines(hosts_file).map(&:chomp)

if ARGV[0] == "p" then
    # Iterar sobre todas las maaquinas y realizar ping al puerto 2
    hosts.each do |host|
        t = Net::Ping::TCP.new("#{host}",22,0.01) #Ping en puerto 22 con timeout 0.02
        if t.ping?
            puts "#{host}: FUNCIONA"
```

```
            else
                puts "#{host}: falla"
            end
        end
elsif ARGV[0] == "s"
#Esta opción no se ha realizado
end
```