Practica 2 - NTP y DNS

Hayk Kocharyan
Administración de sistemas 2
757715@unizar.es

March 22, 2020

1 Resumen

En esta segunda práctica se ha continuado con el despliegue del sistema de la práctica 1.
En este caso se han añadido 2 nuevas máquinas en la subred de la vlan. En esta configuración del sistema tenemos 3 máquinas principales que cumplen los siguientes papeles:

- **VM2:** Servidor NTP y Servidor DNS recursivo con caché.
- **VM3:** Servidor DNS maestro.
- **VM3:** Servidor DNS esclavo.

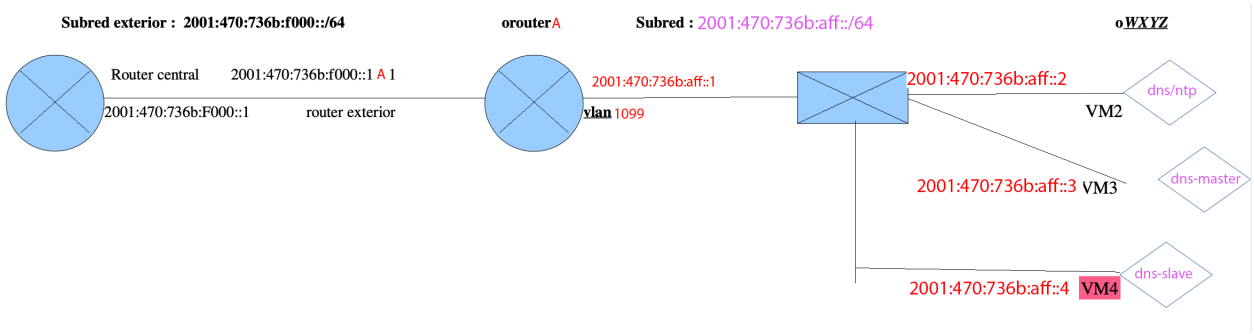

Figure 1: Depliegue del sistema

2 Introducción y Objetivos

En primer lugar, se estudió muy detalladamente cada uno de los componentes del sistema a desarrollar, para ello se usó la documentación del manual, además se buscaron difernetes implementaciones de cada componente para ver y entender su uso, y además, para ver detalladamente como se configura cada uno de las máquinas. Los objetivos que se buscaban en esta práctica eran los siguientes:

- **Configuración servidor DNS maestro.**
  1. Configurar fichero de configuración de nsd.
  2. Configurar fichero de zonas de resolución directa.
  3. Configurar fichero de zonas de resolución inversa.
  4. Comprobar correcto funcionamiento del demonio.
- **Configuración servidor DNS esclavo.**
  1. Configurar fichero de configuración de nsd.

2. Comprobar correcto funcionamiento del demonio.

- **Configuración servidor DNS recursivo con caché a través de unbound.**
  1. Configurar fichero de configuración de nsd.
  2. Configurar fichero de zonas de resolución directa.
  3. Configurar fichero de zonas de resolución inversa.
  4. Comprobar correcto funcionamiento del demonio.
- **Configuración servidor ntp.**

3 Arquitectura

Para este sistema tenemos 3 elementos princiaples:

- **Servidor ntp y servidor DNS con caché recursivo:** Estas funciones corresponden a la **MV2**, su función será la de cachear las peticiones que hagan los clientes. Además, acturará como servidor ntp para el resto de máquinas, estas serán clientes.
- **Servidor DNS maestro:** Esta función la cumplirá la **MV3**, se encargará de traducir los nombres de dominio a IPs.
- **Servidor DNS esclavo:** Esta función la desarrolla la **MV4**, se encargará de ser un backup en caso de fallo del servidor maestro. Esta tambien es útil en el caso de tener una gran cantidad de peticiones, en tal situación se podrían distribuir las peticiones.

También entran en juego la máquina **MV1**, la cual hace el papel de router, como vimos en la práctica 1.
Adicionalmente, se ha añadido una nueva máquina **oAOTRA**, cuyo nombre DNS es **otro_servidor**. Esta máquina se añade tras finalizar toda la configuración para comprobar que al introducir una nueva entrada en los ficheros de zonas, se cumple que el DNS es capaz de resolver la traducción de nombres a IPs.

4 Compresión de elemementos

4.1 Configuración servidores DNS

En primer lugar habilitaremos el demonio a través de la modificación del fichero **rc.conf.local**, para ello incluiremos la entrada **nsd_flags=""**, esto se realizará tanto en maestro como en esclavo. Para continuar, configuraremos el demonio. Esta configuración que se ve a continuación es igual para ambos servidores DNS, la única diferencia es que se cambia la dirección ip en la entrada **ip_address**.
Respecto al resto de la configuración, indicamos el directorio de los ficheros de zonas con **zonesdir**, incluimos un fichero de log para tratar posibles errores (logfile), le indicamos que solo escucharemos ipv6.
Configuraremos el remote-control para poder usar el comando **nsd-control**, exigiendo que solo escuche en la red local. Por ultimo, inidcamos la ruta de los ficheros de claves y certificados, estos son generados con nsd-control-setup.
Para terminar, especificamos una key, que en un principio no se ha usado, pero se puede incluir para el control de accesos.

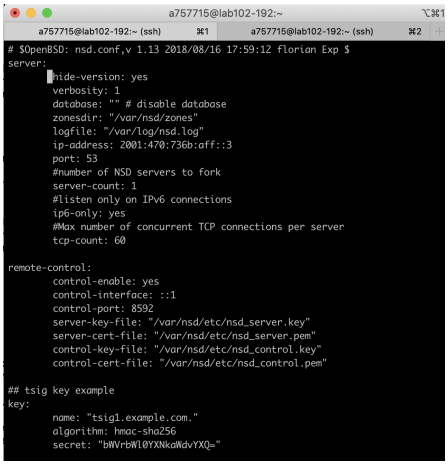

Figure 2: Configuración demonio

Para continuar, crearemos un *"pattern"* con una opciones para asociar a las zonas.
En la máquina del maestro, el pattern se llamará **"toslave"** y permitirá notificar al escalvo. También proveerá actualizacion de zonas a la ip indicada, en este caso, debe ser la del esclavo. En cambio, en la maquina esclvo, este pattern se llamará *"tomaster"*. Este, permitirá mandar notificaciones al maestro (allow-notify @ipMaestro) y la ip que se incluya tras **request-xfr** será imprescindible para actualizar el fichero de zonas.
En cuanto a las zonas, definiremos el directo con nombre **a.ff.es.eu.org**, asignandole el fichero correspondiente, y el inverso, **a.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa**. El pattern *"tomaster"* se asignará a la máquina esclavo y el pattern *"toslave"* se asgina a la máquina maestro.

Figure 3: Configuración demonio

Por último, configuraremos el fichero de zonas en el maestro, tanto el directo como el inverso.
Para el fichero de zonas directo, añadimos nuestro service of authority que es ns1, y además indicamos los dos name servers, ns1 y ns2. Por último, pondremos las entradas de todas nuestras máquinas y sus direcciones ip. Para el inverso, será al reves, las entradas comenzarán con la dirección ipv6 al revés y pondremos su registro PTR.
Para terminar, con los comandos nsd-checkzone y nsd-checkconf nos asegurarnos de que si tenemos errores. Adi-

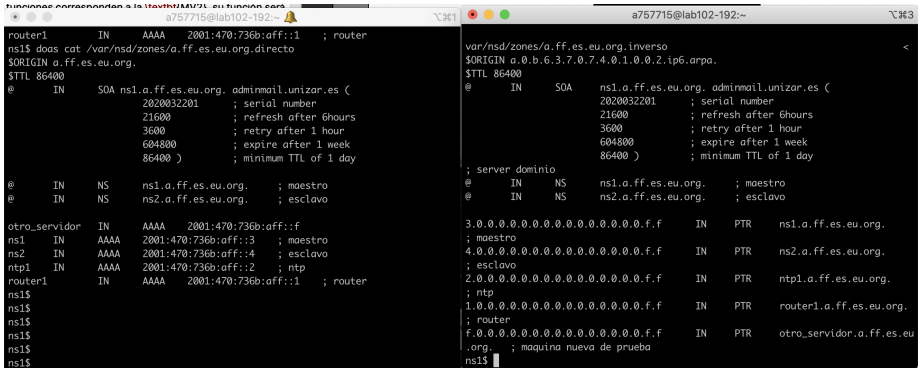

Figure 4: Configuración demonio

cionalmente, se pueden realizar comprobaciones en el fichero de log especificado en la configuración.
Ahora para realizar prubeas, en el fichero **resolv.conf** incluiremos los nameserver @maestro y @esclavo y probaremos con dig si nos responde correctamente nuestro servidor dns maestro. Para probar que nos responde el esclavo, podemos apagar la máquina maestra o realizar el dig al esclavo (dig -6 @ipEsclavo dominio).

Figure 5: Dig con respuesta del servidor maestro 2001:470:736b:aff::3

4.2 Servidor DNS recursivo con caché

Para empezar, modificaremos el fichero rc.conf.local de la MV2 añadiendo unbound_flags para que el demonio se inicio al encender la máquina. Para la configuración del unbound, comenzamos indicando en que interface es-

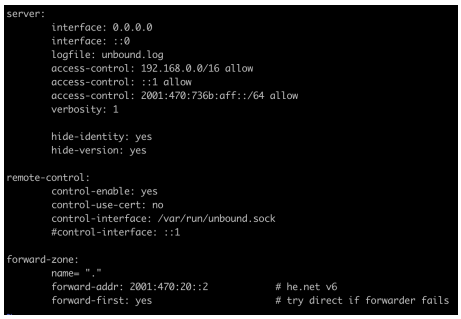

Figure 6: Configuraación unbound

cucharemos y responderemos a los clientes, y permitimos peticiones no recursivas (acces-control) a nuestra máquina desde localhost y desde la subred de nuestra vlan (2001:470:736b:aff::/64). Habilitamos hide-identity y hide-version para que los clientes no conozcan la identidad de nuestro servidor y nuestra versión de unbound.
De nuevo, como con nsd, habilitamos la herramienta unbound-control configurando remote-control. Y, por último, añadimos los forward-zone, dejando unicamente el servidor DNS de Hurricane Electrics.

Para probar que nuestra configuración es correcta, ejecutamos unbound-checkconf y lanzamos el demonio con unbound-control start. También añadimos en resolv.conf el **nameserver ::1** para que las peticiones se realicen a nuestro servidor dns con caché. Tras esto un ping6 google.es debería funcionar y un dig nos deberia devoler una respuesta al servidor dns local.

Para terminar con la configuración del dns, en todas las máquinas que usemos (clientes), modificaremos resolv.conf

```
ntp1$ dig -6 google.es

; <<>> DiG 9.4.2-P2 <<>> -6 google.es
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26367
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.es.                     IN      A

;; ANSWER SECTION:
google.es.              122     IN      A       172.217.21.227

;; Query time: 48 msec
;; SERVER: ::1#53(::1)
;; WHEN: Sun Mar 22 18:01:42 2020
;; MSG SIZE  rcvd: 43
```

añadiendo el nameserver de la MV2.

4.3 NTP

Como con los anteriores demonios, habilitamos este añadiendo ntpd_flags. A continuación, en el fichero /etc/ntpd.conf añadimos las entradas:

servers 2001:470:0:50::2 #stratum 1
servers 2001:470:0:2c8::2 #stratum 2
listen on *

En el resto de máquinas, es decir, aquellas que necesiten a MV2 como servidor ntp, añadiremos estas entradas:

servers 2001:470:736:aff::2
listen on *

Para comprobar el correcto funcionamiento se realiza la siguiente prueba desde central: Podemos ver una correcta

```
lab102-192:~/ ntpdate -q canon.inria.fr
server 138.96.64.10, stratum 1, offset -0.607431, delay 0.06989
22 Mar 18:18:47 ntpdate[6717]: step time server 138.96.64.10 offset -0.607431 sec
lab102-192:~/ ntpdate -q 2001:470:736b:aff::2
server 2001:470:736b:aff::2, stratum 2, offset -0.609536, delay 0.04225
22 Mar 18:18:58 ntpdate[6733]: step time server 2001:470:736b:aff::2 offset -0.609536 sec
lab102-192:~/
```

sincronización y un offset similar en ambos servidores.

5 Problemas

En esta práctica se han encontrado problemas sobre todo con el DNS principalmente por no saber usar la herramienta dig, pero tras una buena documentación de esta, se consiguieron resolver los problemas generados.
También hubo problemas con el ntp ya que en algunas ocasiones tardaba 30 minutos en sincronizar.