9-3-2023

Práctica Nº2

Administración de Sistemas 2

Ismael Berdusán Muñoz (796902)

Contenido

1. Resumen 2
2. Introducción y objetivos 2
3. Arquitectura de elementos relevantes 3
4. Elementos significativos de la práctica 3
5. Problemas encontrados y su solución 4
6. Pruebas realizadas 4
7. Anexo 5

1. Resumen

En esta práctica se ha puesto en marcha el servicio DNS mediante 3 servidores: un maestro (máquina **odff3**), un esclavo (máquina **odff4**), y un servidor recursivo y con caché mediante unbound (máquina **odff2**). Este último también se ha configurado como servidor ntp para las máquinas de la **vlan1399**.

2. Introducción y objetivos

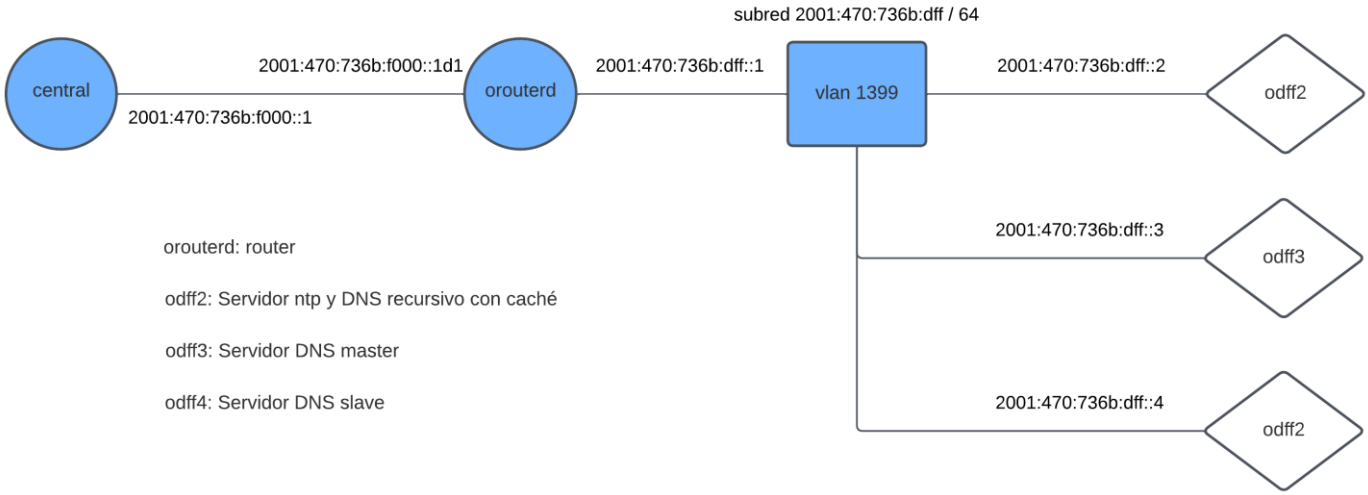
La práctica ha consistido en añadir dos máquinas más a la **vlan1399** (odff3 y odff4) que teníamos en la práctica anterior, configurarlas como un servidor DNS master y esclavo, respectivamente, y configurar la máquina **odff2** como un servidor DNS recursivo con caché, además de servidor ntp. Esto se ha realizado mediante la modificación de los ficheros **/var/nsd/etc/nsd.conf** y **/var/unbound/etc/ unbound.conf**, y las zonas del directorio **/var/nsd/zones.**

También ha sido necesario configurar todas las máquinas como clientes NTP y DNS para que puedan disponer de esos servicios. Para logar esto ha sido necesario modificar los ficheros **/etc/resolv.conf** y **/etc/ntpd.conf**.

En cuanto a la automatización, se han realizado una serie de scripts para comprobar qué maquinas se encuentran en funcionamiento, y para facilitar el uso de virsh.

Todos los detalles de los ficheros de configuración y scripts mencionados en este apartado se pueden encontrar en el anexo.

3. Arquitectura de elementos relevantes



- **oruterd**: Proporciona acceso a internet a la **vlan1399** mediante la subred virtual interior **2001:470:736b:dff/64**. Su nombre de dominio es **router1.d.ff.es.eu.org**.
- **odff2**: Servidor ntp y DNS recursivo con caché que proporciona servicio ntp y unbound a las máquinas de la **vlan1399**. Su nombre de dominio es **ntp1.d.ff.es.eu.org**.
- **odff3**: Servidor DNS master que proporciona servicio DNS a las máquinas de la **vlan1399**. Su nombre de dominio es **ns1.d.ff.es.eu.org**.
- **odff4**: Servidor DNS slave que proporciona servicio DNS a las máquinas de la **vlan1399**. Su nombre de dominio es **ns2.d.ff.es.eu.org**.

4. Elementos significativos de la práctica

Subred:

- **vlan1399: 2001:470:736b:dff / 64**

Servidores DNS:

- **orouterd (router1)**: Router que proporciona acceso a internet a las máquinas de la **vlan1399**.
- **odff2 (ntp1)**: Servidor NTP y DNS recursivo, con caché que proporciona servicio NTP y DNS a las máquinas de la **vlan1399**.
- **odff3 (ns1)**: Servidor DNS master que proporciona servicio DNS a las máquinas de la **vlan1399**.
- **odff4 (ns2)**: Servidor DNS slave que proporciona servicio DNS a las máquinas de la **vlan1399**.

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

Son:

1. Número de serie de la zona.
2. Tiempo (en segundos) que los servidores secundarios deben esperar antes de pedir a los servidores primarios el registro SOA para comprobar si se ha actualizado.
3. Tiempo que debe esperar un servidor para volver a pedir una actualización a un servidor de nombres primario que no responde.
4. Tiempo en el que, si un servidor secundario no recibe una respuesta del servidor primario, debe dejar de responder a las consultas de la zona.
5. TTL mínimo.

5. Problemas encontrados y su solución

A la hora de configurar las máquinas se han encontrado varios problemas:

- Cuando intentaba lanzar los servicios **nsd** y **unbound** me daba problemas, pero era porque ya estaban activos y al intentar lanzarlos estando activos fallaban.
- Al probar si funcionaba el DNS desde fuera de la vlan me econtré conque no iba, pero esto puede no deberse a mi configuración, así que lo ignoré.

6. Pruebas realizadas

Comando para comprobar que el servicio NTP funciona, y que los relojes de las máquinas se hayan sincronizado correctamente:

(En cada máquina) **ntpctl -sa**

(Ejecutado desde central) **ntpdate -q 2001:470:736b:dff::2**

Comandos para comprobar que el servicio DNS funciona correctamente (ejecutados en cada máquina):

dig -6 <máquina>.d.ff.es.eu.org

dig -6 -x 2001:470:736b:dff::<máquina>

dig -6 @2001:4860:4860::8888 <máquina>.d.ff.es.eu.org

dig -6 @2001:4860:4860::8888 -x 2001:470:736b:dff::<máquina>

ping6 <máquina>.d.ff.es.eu.org

ping6 2001:470:736b:dff::<máquina>

7. Anexo

Contenido del script de nombre **p** para realizar ping a una serie de máquinas:

```ruby
#!/usr/bin/env ruby

require 'net/ping'

#direcciones
host_file = File.expand_path("hosts.txt", ".u")
hostnames = File.read(host_file)
lines = hostnames.split("\n")

#colores
rojo = "\033[1;31m"
verde = "\033[1;32m"

def putColor(color, host, linea)
    reset = "\033[0m"
    puts "#{host} #{color}#{linea}#{reset}"
end

time = 0.5
puts "Timeout: #{time}"
lines.each do |hostname|
    ping = Net::Ping::TCP.new(hostname, 22, time)

    if ping.ping?
        putColor(verde, hostname, "FUNCIONA")
    else
        putColor(rojo, hostname, "FALLA")
    end
end
```

Contenido del script de nombre **vir** para facilitar el uso de los comandos de virsh:

```ruby
#!/usr/bin/env ruby

require "net/ssh"

def execute(ssh, command, target = "")
    result = ssh.exec!("virsh -c qemu:///system #{command} #{target}")
    puts result
end

def option(command, flags, ssh, lines)
    if flags == 'all'
        lines.each do |host|
            execute(ssh, command, host)
        end
    else
        execute(ssh, command, host)
    end
end

if ARGV.length != 0
    host = "155.210.154.#{ARGV[0]}"
    username = 'a796902'

    host_file = File.expand_path("maquinas.txt", ".u")
    hostnames = File.read(host_file)
    lines = hostnames.split("\n")

    Net::SSH.start(host, username) do |ssh|
        if ARGV[1] == 'e'
            option("start", ARGV[2], ssh, lines)
        elsif ARGV[1] == 'a'
            option("shutdown", ARGV[2], ssh, lines)
        elsif ARGV[1] == 'u'
            option("undefine --domain", ARGV[2], ssh, lines)
        elsif ARGV[1] == 'l'
            execute(ssh, "list --all")
        else
            puts "Parámetros incorrectos"
            puts "script2.ruby [n_maquina] [opcion] [flags] "
        end
        ssh.close
    end
else
    puts "Parámetros incorrectos"
    puts "script2.ruby [n_maquina] [opcion] [flags] "
end
```

Contenido del fichero **/etc/resolv.conf** todas lasa máquinas:

```
lookup file bind
nameserver 2001:470:736b:dff::2
```

Contenido del fichero **/var/nas/etc/nsd.conf** (odff3):

```
server:
        hide-version: yes
        verbosity: 1
        ip-address: 2001:470:736b:dff::3
                database:"/var/nsd/db/nsd.db"
                username: _nsd
                logfile: "/var/log/nsd.log"
                pidfile: "/var/nsd/run/nsd.pid"
        port: 53
        server-count: 1
        ip6-only: yes
        tcp-count: 60
        zonesdir: "/var/nsd/zones"

remote-control:
        control-enable: yes
        control-interface: ::1
        control-port: 8952
        server-key-file: "/var/nsd/etc/nsd_server.key"
        server-cert-file: "/var/nsd/etc/nsd_server.pem"
        control-key-file: "/var/nsd/etc/nsd_control.key"
        control-cert-file: "/var/nsd/etc/nsd_control.pem"

key:
        name: "mskey"
        algorithm: hmac-sha256
        secret: "bWVrbWl0YXNkaWdvYXQ="
```

```
pattern:
        name: "toslave"
        notify: 2001:470:736b:dff::4 mskey
        provide-xfr: 2001:470:736b:dff::4 mskey


zone:
        name: "d.ff.es.eu.org"
        zonefile: "d.ff.es.eu.org.directo"
        include-pattern: "toslave"


zone:
        name: "d.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa"
        zonefile: "d.ff.es.eu.org.inverso"
        include-pattern: "toslave"
```

Contenido del fichero **/var/nsd/zones/d.ff.es.eu.org.directo** (odff3):

```
$ORIGIN d.ff.es.eu.org.
@       IN      SOA     ns1.d.ff.es.eu.org.     a796902.d.ff.es.eu.org. (
                                                2020031112; numero serie
                                                21600   ; Refresca cada 6 horas
                                                3600    ; Reintenta cada 1 hora
                                                604800 ; Expira despues de 1 semana
                                                86400 ) ; TTL minimo cliente de 1 dia
        IN      N       ns1.d.ff.es.eu.org.
        IN      NS      ns2.d.ff.es.eu.org.
ns1     IN      AAAA    2001:470:736b:dff::3
ns2     IN      AAAA    2001:470:736b:dff::4
ntp1    IN      AAAA    2001:470:736b:dff::2
router1 IN      AAAA    2001:470:736b:f000::1d1
otro_servidor   IN      AAAA    2001:470:736b:dff::f
odff2   IN      CNAME           ntp1
odff3   IN      CNAME           ns1
odff4   IN      CNAME           ns2
orouterd        IN              CNAME           router1
```

Contenido del fichero **/var/nsd/zones/d.ff.es.eu.org.inverso** (odff3):

```
$ORIGIN d.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.
@       IN      SOA     ns1.d.ff.es.eu.org.     a796902.d.ff.es.eu.org. (
                                                2020031102      ; numero serie
                                                21600   ; Refresca cada 6 horas
                                                3600    ; Reintenta cada 1 hora
                                                604800 ; Expira despues de 1 semana
                                                 86400 )        ; TTL minimo cliente de 1 dia
        IN      NS      ns1.d.ff.es.eu.org.
        IN      NS      ns2.d.ff.es.eu.org.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR     ntp1.d.ff.es.eu.org.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR     ns1.d.ff.es.eu.org.
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR     ns2.d.ff.es.eu.org.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR     router1.d.ff.es.eu.org.
f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR     otro_servidor.d.ff.es.eu.org.
```

Contenido del fichero **/var/nsd/etc/nsd.conf** (odff4):

```
server:
        hide-version: yes
        verbosity: 1
        ip-address: 2001:470:736b:dff::4
                database: "/var/nsd/db/nsd.db"
                username: _nsd
                logfile: "/var/log/nsd.log"
                pidfile: "/var/nsd/run/nsd.pid"
        port: 53
        server-count: 1
        ip6-only: yes
        tcp-count: 60
        zonesdir: "/var/nsd/zones"
```

```
remote-control:
        control-enable: yes
        control-interface: ::1
        control-port: 8952
        server-key-file: "/var/nsd/etc/nsd_server.key"
        server-cert-file: "/var/nsd/etc/nsd_server.pem"
        control-key-file: "/var/nsd/etc/nsd_control.key"
        control-cert-file: "/var/nsd/etc/nsd_control.pem"

key:
        name: "mskey"
        algorithm: hmac-sha256
        secret: "bWVrbWl0YXNkaWdvYXQ="

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

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

zone:
        name: "d.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa"
        zonefile: "d.ff.es.eu.org.inverso"
        include-pattern: "tomaster"
```

Contenido del fichero **/var/unbound/etc/unbound.conf** (odff2):

```
server:
        interface: 0.0.0.0
        interface: ::0
        verbosity: 1
        access-control: 2001:470:736b::/48 allow
        access-control: ::1 allow
        hide-identity: yes
        hide-version: yes

remote-control:
        control-enable: yes
        control-use-cert: no

forward-zone:
        name: "."                               # Utilizar para todas las peticiones
        forward-addr: 2001:470:20::2            # he.net v6
        forward-addr: 2001:4860:4860::8888      # google.com v6
        forward-first: yes                      # si forwarder falla, intentar directo
```

Contenido del fichero **/etc/ntpd.conf** (odff2):

```
listen on ::1
listen on 2001:470:736b:dff::2
servers 2001:470:0:50::2
servers 2001:470:0:2c8::2
```

Contenido del fichero **/etc/ntpd.conf** (Todas las máquinas excepto odff2):

```
server ntp1.d.ff.es.eu.org
```