Práctica 2

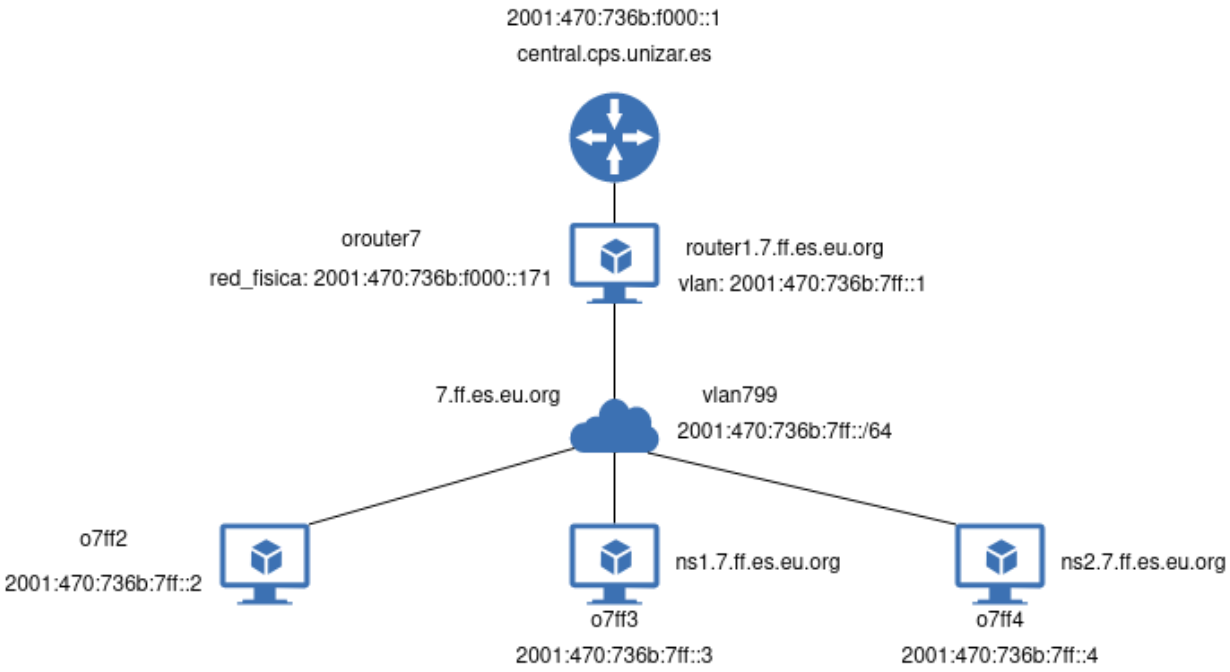
Germán Garcés - 757024

Resumen

Puesta en marcha de servicios distribuidos básicos, NTP y DNS, con la configuración de red y VMs necesarias.

Arquitectura de elementos relevantes

Novedad respecto a la 1a práctica es que `orouter7` tiene un nombre en el servicio de nombres, `router1`. También se han añadido dos máquinas `o7ff3` y `o7ff4` con direcciones ipv6 `2001:470:736b:7ff::3` y `2001:470:736b:7ff::4` respectivamente. Estas máquinas van a ser los servidores con autoridad primario y secundario y tendrán de nombre `ns1` y `ns2`.



Comprehensión de elementos significativos de la práctica

Puesta en marcha servicio DNS y NTP

Clientes DNS

Para indicar a todas las máquinas quienes son sus **servidores de nombres**, en la ruta `/etc/resolv.conf` añadir las siguientes líneas:

```
search 7.ff.es.eu.org
nameserver 2001:470:736b:7ff::3 ; ns1
nameserver 2001:470:736b:7ff::4 ; ns2
```

Basicamente lo que hacemos es indicar a las VM quienes son los servidores de nombres. En este caso, la dirección `2001:470:4736b:7ff::3` es el servidor primario o master y la dirección `2001:470:736b:7ff::4` es el servidor secundario o

esclavo.
Tras la configuración del servidor `unbound`, se quitaron ambos `nameserver` y se añadió la línea:

```
nameserver 2001:470:736b:7ff::2 #Nuevo servidor al que hacer preguntas
```

La línea `search W.ff.es.eu.org` lo que hace es autocompletar el nombre de los dominios cuando no se indica un dominio en concreto. Por ejemplo si hiciesemos `ssh ns1`, se autocompletaría a `ssh ns1.7.ff.es.eu.org`.
Y para poner en marcha el demonio `nsd`, en `/etc/rc.conf.local` se ha añadido la siguiente línea:

```
nsd_flags=""
```

Para comunicar a las máquinas que son clientes de un **servidor NTP**, se ha escrito lo siguiente en `/etc/ntpd.conf`

```
server 2001:470:0:50::2
server 2001:470:0:2c8::2
```

y se ha reiniciado el demonio ntpd con `rcctl restart ntpd`

Configuración servidor con autoridad primario

> En la maquina `o7ff3`.

Configuración servicio NSD

El archivo `/var/nsd/etc/nsd.conf` ha quedado así:

```
server:
        hide-version: yes
        database: "/var/nsd/db/nsd.db"
        username: _nsd
        verbosity: 1
        port: 53
        server-count: 1
        ip6-only: yes
        zonesdir: "/var/nsd/zones"
        logfile: "/var/log/nsd.log"
        pidfile: "/var/nsd/run/nsd.pid"

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

zone:
        name: "7.ff.es.eu.org"
        zonefile: "master/7.ff.es.eu.org"
        notify: 2001:470:736b:7ff::4 NOKEY
        provide-xfr: 2001:470:736b:7ff::4 NOKEY

zone:
        name: "7.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa"
        zonefile: "master/7.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa"
        notify: 2001:470:736b:7ff::4 NOKEY
        provide-xfr: 2001:470:736b:7ff::4 NOKEY
```

> Para comprobar que no existieran errores sintácticos se usó `nsd-checkconf`.

Creación base de datos DNS

En la ruta `/var/nsd/zones/master` se ha creado un nuevo archivo de nombre `7.ff.es.eu.org` y se han incluido en el las siguientes líneas:

```
; Start of authority record for 7.ff.es.eu.org
$ORIGIN 7.ff.es.eu.org.

7.ff.es.eu.org. IN      SOA     ns1.7.ff.es.eu.org.     757024.unizar.es. (
                                2009070200 ; Serial number
                                10800      ; Refresh (3 horas)
                                1200       ; Retry (20 minutos)
                                3600000    ; Expire (40+ dias)
                                3600 )     ; Minimum (1 hora)
        NS      ns1.7.ff.es.eu.org.        ; Authority server (primary)
        NS      ns2.7.ff.es.eu.org.        ; Authority server (secondary)

; Resolucion directa

ns1     IN      AAAA    2001:470:736b:7ff::3
ns2     IN      AAAA    2001:470:736b:7ff::4
router1 IN      AAAA    2001:470:736b:7ff::1
ntp1    IN      AAAA    2001:470:736b:7ff::2
otro_servidor IN      AAAA    2001:470:736b:7ff::f


; CNAME

o7ff3   IN      CNAME   ns1
o7ff4   IN      CNAME   ns2
o7ff2   IN      CNAME   ntp1
orouter7        IN      CNAME   router1
```

> Para comprobar que no existieran errores sintácticos se usó `nsd-checkzone`.

- En primer lugar, en la variable `$ORIGIN` se guarda el valor del dominio (`7.ff.es.eu.org`) para evitar escribir de más.
- El registro `SOA` se encarga de definir el nombre de la zona, el servidor master, una dirección de "soporte técnico" y algunos detalles.
- Las entradas `NS` definen quienes son los servidores con autoridad de la zona, en este caso `ns1.7.ff.es.eu.org` es el primario y `ns2.7.ff.es.eu.org` el secundario.
- La tercera entrada indica cual es la dirección ip de estos servidores
- El apartado `CNAME` permite usar nicknames, en este caso le indicamos que si se usan los nombres de las VM, estos se transformen en el nombre que le corresponde para el servidor de nombres.

Para la resolución inversa se ha creado otro archivo `7.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa` y se ha escrito lo siguiente:

```
@       IN      SOA     ns1.7.ff.es.eu.org.     757024.unizar.es. (
                                2009070200 ; Serial number
                                10800      ; Refresh (3 horas)
                                1200       ; Retry (20 minutos)
                                3600000    ; Expire (40+ dias)
                                3600 )     ; Minimum (1 hora)

; Resolucion inversa

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     ns1.7.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     ns2.7.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     router1.7.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     ntp1.7.ff.es.eu.org.
f.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     otro_servirdor.7.ff.es.eu.org.
```

> Para comprobar que no existieran errores sintácticos se usó `nsd-checkzone`.

- `@` indica el nombre de la zona, en este caso `7.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa`

Configuración servidor con autoridad secundario

> En la maquina `o7ff4`.

El archivo `/var/nsd/etc/nsd.conf` ha quedado así:

```
server:
        hide-version: yes
        verbosity: 1
        database: "" # disable database
        username: _nsd
        port: 53
        server-count: 1
        ip6-only: yes
        zonesdir: "/var/nsd/zones"
        logfile: "/var/log/nsd.log"
        pidfile: "/var/nsd/run/nsd.pid"

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

zone:
        name: "7.ff.es.eu.org"
        zonefile: "slave/7.ff.es.eu.org"
        allow-notify: 2001:470:736b:7ff::3 NOKEY
        request-xfr: AXFR 2001:470:736b:7ff::3 NOKEY

zone:
        name: "7.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa"
        zonefile: "slave/7.ff.es.eu.org.inversa"
        allow-notify: 2001:470:736b:7ff::3 NOKEY
        request-xfr: AXFR 2001:470:736b:7ff::3 NOKEY
```

Creacion servidor recursivo con cache Unbound

> En la maquina `o7ff2`

Se activó el demonio de `unbound` escribiendo `unbound_flags=""` en el fichero `/etc/rc.conf.local`

Para la configuración de este servidor tan solo se ha editado el fichero `/var/unbound/etc/unbound.conf` y se ha escrito lo siguiente:

```
server:
        interface: ::0
        do-ip6: yes

        access-control: 2001:470:736b:7ff::/64 allow
        access-control: ::1 allow

        hide-identity: yes
        hide-version: yes

        # Use TCP for "forward-zone" requests. Useful if you are making
        # DNS requests over an SSH port forwarding.
        #
```

```
        tcp-upstream: yes

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

forward-zone:
        name: "."                               # use for ALL queries
        forward-addr: 2001:470:20::2            # he.net v6
        forward-first: yes                      # try direct if forwarder fails

stub-zone:
        name: "7.ff.es.eu.org"
        stub-addr: 2001:470:736b:7ff::3

stub-zone:
        name: "7.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa"
        stub-addr: 2001:470:736b:7ff::3
```

Configuración servicio de tiempo NTP

En la máquina `o7ff2`, en el fichero `/etc/ntpd.conf` se añadieron las lineas:

```
server 2001:470:0:50::2
server 2001:470:0:2c8::2
listen on *
sensor *
constraints from "https://www.google.com"
```

y se añadió en `/etc/rc.conf.local` la línea: `ntpd_flags="-s"` para que el demonio de ntp establezca el tiempo al iniciarse.

Pruebas realizadas

- Para comprobar el correcto funcionamiento de los servidores dns se probó a hacer una query a los servidores de google de resolucion directa `dig -6 @2001:4860:4860::8888 AAAA ns1.7.ff.es.eu.org` y se observó que devolvía la respuesta correcta:

```
;; ANSWER SECTION:
ns1.7.ff.es.eu.org.     317     IN      AAAA    2001:470:736b:7ff::3
```

Y se utilizó el comando `dig -6 @2001:4860:4860::8888 -x 2001:470:736b:7ff::3` para probar la resolución inversa, respuesta obtenida:

```
;; ANSWER SECTION:
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.7.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 3599 IN PTR ns1.7.ff.es.eu.org.
```

- Para probar el funcionamiento del servidor secundario se realizaron los mismos comandos pero pidiendole la respuesta al servidor esclavo `@2001:470:736b:7ff::2`

- Para comprobar el servidor unbound simplemente se repitieron los comandos anteriores prestando especial atenciño a los tiempos de respuesta de cada petición. Se vió que la primera petición tardaba siempre mas de 100ms (cuando la query no era interna) pero que las siguientes peticiones iguales, tardaban tan solo [30-50]ms.
  También se uso el comando `unbound-host -6 hostname` para hacer querys que usase el servidor unbound, respuesta obtenida `ns1.7.ff.es.eu.org has IPv6 address 2001:470:736b:7ff::3`

    - Para comprobar el servicio ntp, desde central se usó el comando: `nptdate -q 2001:470:736b:7ff::2`

Problemas encontrados

- Al configurar `nsd`, no se conseguía obtener ninguna resolución, se había puesto `ip-address: 2001:470:736b:7ff::2` sin entender lo que era, tras eso la opción de escuchar por un interfaz fue retirada
- No se conseguía hacer ping a google, a las 2 horas me dí cuenta de que estaba haciendo `ping google.com` y no `ping6 2001:4860:4860::8888` como debería hacer.
- Las máquinas virtuales dejaron de arrancar correctamente, se resolvió volviendo a un punto anterior obtenido de las copias de seguridad.