ADMINISTRACIÓN DE SISTEMAS 2

Memoria práctica II
Parte I

Grupo Viernes Mañana

28/02/2024

GUILLERMO BAJO LABORDA, 842748@unizar.es

Universidad Zaragoza
1542

Escuela de Ingeniería y Arquitectura Universidad Zaragoza

Resumen

Esta segunda práctica de la asignatura de Administración de Sistemas 2 se ha enfocado en la implementación y configuración de servicios distribuidos, con énfasis en el sistema DNS y el desarrollo de un programa en Ruby. Se han llevado a cabo labores como la configuración de redes y servidores, asignación de subredes IPv6 y la creación de servidores DNS maestro y esclavo. Destacó el uso de la herramienta unbound para configurar el servidor DNS recursivo y con caché, asegurando la resolución eficiente de nombres. Además, se ha empleado la herramienta dig para verificar la resolución de nombres y validar el correcto funcionamiento del servidor DNS implementado. En esta memoria se documentan los procedimientos realizados, los desafíos encontrados y las soluciones aplicadas en la ejecución de esta práctica.

Introducción y objetivos

Esta práctica representa un paso significativo en el despliegue y configuración de servicios distribuidos, centrándonos en la implementación detallada del sistema DNS y el desarrollo de un programa en Ruby para tareas administrativas. Además, la implementación de un servidor DNS recursivo y con caché utilizando unbound amplía nuestra comprensión de los mecanismos internos de resolución de DNS y su impacto en la eficiencia del sistema. El desarrollo de un programa en Ruby para administración remota refuerza nuestra capacidad para automatizar tareas de gestión de servidores.

El propósito principal de esta práctica es lograr un despliegue efectivo de servicios distribuidos, específicamente enfocado en el sistema DNS y en la administración remota de máquinas mediante Ruby.

Arquitectura de elementos relevantes

La infraestructura desplegada en esta práctica consta de varias máquinas virtuales y servidores configurados para llevar a cabo las funcionalidades requeridas. En primer lugar, se establece una red con dos subredes IPv6: una subred exterior y una subred interna. El router central actúa como punto de conexión entre estas subredes y direcciona el tráfico adecuadamente. Además, se implementan servidores DNS maestro y esclavo en máquinas virtuales distintas.

Las máquinas virtuales (VM2, VM3 y VM4) desempeñan roles específicos en la infraestructura. VM2 actúa como servidor NTP adicional y como servidor DNS recursivo con caché. VM3 se configura como servidor DNS maestro (primario), mientras que VM4 asume el papel de servidor DNS esclavo (secundario). Cada una de estas máquinas virtuales tiene asignada una dirección IPv6 según el esquema definido en el enunciado.

En cuanto a los servicios, se utiliza la herramienta unbound para configurar un servidor DNS recursivo y con caché en VM2, permitiendo la resolución eficiente de nombres y optimizando las consultas DNS. Se establecen servidores DNS autorizados (ns1 y ns2) en VM3 y VM4, respectivamente, para gestionar la resolución de nombres en la zona DNS definida.

Además, se configura un conjunto de máquinas clientes DNS, que se comunican con el servidor DNS recursivo en VM2 para resolver consultas DNS. Estas máquinas son fundamentales para verificar la funcionalidad del sistema DNS implementado.

Comprehensión de elementos significativos de la práctica

Para la configuración de clientes DNS ha sido necesario modificar el fichero */etc/resolv.conf* de cada una de las máquinas del sistema. Para ello, se ha comentado el contenido del fichero y se ha añadido la siguiente línea:

```
Unset
nameserver 2001:470:736b:1bff::2
```

Esta dirección corresponde a la dirección vlan de la máquina o1BFF2, la cual funcionará en el sistema como servidor ntp adicional y **DNS recursivo con cache**. Esto supondrá que las consultas DNS se envíen al servidor recursivo y con cache, es decir, las máquinas del sistema utilizará el servidor DNS con la dirección IPv6 "2001:470:736b:1bff::2" para realizar búsquedas de nombres de dominio.

Para realizar una configuración IPv6 estática de las máquinas, se ha modificado el fichero */etc/hostname.vlan2799* de las máquinas cliente, estableciendo el siguiente contenido:

```
Unset
inet6 alias 2001:470:736b:1bff::x 64 vlandev vio0
#x toma el valor 1, 2 o 3 dependiendo de la máquina.
```

Para permitir el encaminamiento a las máquinas clientes, se ha modificado el fichero /etc/mygate de cada una de ellas introduciendo la dirección de la interfaz VLAN del router.

Configuramos el arranque de **nsd** en la máquina que funcionará como servidor DNS maestro añadiendo la línea *nsd_flags=””* al fichero r*c.conf.local*. Posteriormente, generamos la clave nsd-control mediante *nsd-control-setup* y configuramos los ficheros */var/nsd/etc/nsd.conf* estableciendo el siguiente contenido:

```
Unset
server:
    hide-version: yes
    ip-address: 2001:470:736b:1bff::3
```

```
    database: "/var/nsd/db/nsd.db" # disable database
    username: _nsd
    logfile: "/var/log/nsd.log"
    pidfile: "/var/nsd/run/nsd.pid"
    port: 53
    verbosity: 1


remote-control:
    control-enable: yes
    control-interface: ::1
#key:
    #name: "mskey"
    #algorithm: hmac-sha256
    #secret: "bWVrbWl0YXNkaWdvYXQ="

pattern:
     name: "toslave"
     notify: 2001:470:736b:1bff::4 NOKEY
     provide-xfr: 2001:470:736b:1bff::4 NOKEY

zone:
    name: "1b.ff.es.eu.org"
    zonefile: "1b.ff.es.eu.org.directo"
    include-pattern: "toslave"

zone:
    name: "b.1.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa."
    zonefile: "1b.ff.es.eu.org.inverso"
    include-pattern: "toslave"
```

El fichero de configuración de la máquina 4 (esclavo) es bastante similar, cambiando algunos aspectos como el toslave -> to master, y las direcciones IP correspondientes.

La sección server tiene configuraciones básicas del servidor:

- hide-version: Oculta la versión NSD para evitar que posibles atacantes conozcan la versión exacta del software que estás ejecutando.
- La dirección IP: Es aquella en la que el servidor NSD escuchará las peticiones.
- Database: Contiene la ruta al archivo de la base de datos que NSD usa para almacenar datos relacionados con la configuración del servidor.
- Logfile: Especifica la ubicación del archivo de registro donde NSD escribirá sus mensajes y registros de actividad.

- Pidfile: Establece la ubicación del archivo PID que contendrá el ID de proceso del servidor NSD cuando esté en funcionamiento.
- port: Define el puerto en el que el servidor NSD escuchará las solicitudes DNS estándar.
- server-count: Indica el número de instancias de servidor NSD que se ejecutarán. En este caso, solo se ejecutará una instancia.
- ip6-only: Esta opción indica que el servidor NSD solo aceptará conexiones IPv6.
- tcp-count: Establece el número máximo de conexiones TCP concurrentes permitidas por el servidor NSD. Esto controla cuántas conexiones TCP puede manejar el servidor simultáneamente.
- zonesdir: Especifica el directorio donde se encuentran almacenadas las zonas de DNS (archivos de zona) que el servidor NSD está autorizado a servir.

La sección remote-control corresponde a la configuración del control remoto del servidor NSD:

- control-enable: Esta opción indica si la funcionalidad de control remoto está habilitada (yes) o deshabilitada (no).
- control-interface: Especifica la interfaz de red en la que el servidor NSD escuchará las solicitudes de control remoto. En este caso, el servidor NSD solo aceptará conexiones de control remoto desde la interfaz de loopback (localhost) IPv6.
- control-port: Define el puerto en el que el servidor NSD escuchará las solicitudes de control remoto. El 8952 es el correspondiente a las conexiones entre el servidor NSD y los programas o servicios que desean utilizarlo de forma remota.
- server-key-file: Especifica la ubicación del archivo de clave privada del servidor NSD utilizado para establecer conexiones seguras.
- server-cert-file: Establece la ubicación del archivo de certificado SSL/TLS del servidor NSD utilizado para autenticar su identidad en conexiones seguras.
- control-key-file: Especifica la ubicación del archivo de clave privada utilizado para autenticar las solicitudes de control remoto.
- control-cert-file: Define la ubicación del archivo de certificado SSL/TLS utilizado para autenticar la identidad del cliente en conexiones seguras de control remoto.

En la sección key se define lo siguiente:

- name: Este es el nombre de la clave.
- algorithm: Especifica el algoritmo que se utilizará para la generación de la clave.
- secret: Es la clave secreta misma.

La sección pattern define un patrón de transferencia de zona:

- name: Nombre del patrón.

- notify: Especifica la configuración para la notificación de cambios de zona a un servidor esclavo. 2001:470:736b:f000::4 es la dirección IP del servidor esclavo al que se notificarán los cambios de zona.
- NOKEY indica que no se utilizará ninguna clave para autenticar la notificación.
- provide-xfr: Esto especifica la configuración para proporcionar la transferencia de zona a un servidor esclavo.

Finalmente, las secciones zone definen zonas en el servidor NSD:

- name: Especifica el nombre de la zona.
- zonefile: Especifica el nombre del archivo de zona que contiene los registros directos para esta zona.
- include-pattern: Indica que esta zona debe incluirse en el patrón de transferencia de zona llamado "toslave".

Posteriormente se procede a configurar los **archivos de zona directa e inversa**, los cuales definen la zona de búsqueda para el dominio 1b.ff.es.eu.org. El fichero de zona directa proporciona una lista de registros AAAA que asignan direcciones IPv6 a nombres host de la zona, mientras que el fichero de zonas inverso contiene registros del tipo PTR que asignan nombres de host a direcciones IPv6.

Fichero de zonas directo:

```
Unset
$ORIGIN 1b.ff.es.eu.org.
@    IN   SOA  ns1.1b.ff.es.eu.org.  842748.unizar.es. (
               2013022503 ; serial number
               21600  ; refresh after 6 hours
               3600   ; retry after 1 hour
               604800 ; expire after 1 week
               86400) ; minimun TTL of 1 day


    IN   NS   ns1.1b.ff.es.eu.org.  ;Maestro


ns1          IN   AAAA  2001:470:736b:1bff::3  ;Maestro - Maq3
ns2          IN   AAAA  2001:470:736b:1bff::4  ;Esclavo - Maq4
router1      IN   AAAA  2001:470:736b:1bff::1  ;Router
ntp          IN   AAAA  2001:470:736b:1bff::2  ;NTP
```

ORIGIN 1b.ff.es.eu.org.: establece el origen de la zona para todos los nombres de dominio que aparecen en este archivo. Indica que cualquier nombre de dominio que no termine con un punto (.) se completará automáticamente con 1b.ff.es.eu.org..

El registro SOA (Start of Authority) especifica la autoridad para la zona.@ se refiere al origen de la zona, 1b.ff.es.eu.org.. IN indica el espacio de nombres de Internet y ns1.1b.ff.es.eu.org. es el nombre del servidor de nombres primario.

El registro NS (Name Server) especifica el servidor de nombres primario (maestro) para esta zona.

Los registros AAAA asignan direcciones IP a nombres de host.

Fichero de zonas inverso:

```
Unset
$ORIGIN b.1.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.
@    IN   SOA  ns1.1b.ff.es.eu.org.  a842748.1b.ff.es.eu.org. (
               2402202402
               21600
               3600
               604800
               86400

)

       NS   ns1.1b.ff.es.eu.org.  ;Maestro

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.f.f   IN   PTR  ntp.1b.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.f.f   IN   PTR  ns1.1b.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.f.f   IN   PTR  ns2.1b.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.f.f   IN   PTR  router1.1b.ff.es.eu.org.
```

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

- Número de serie: Se utiliza para identificar la versión actual de la zona. Cada vez que se realiza una modificación en la zona, este número debe incrementarse para que los servidores secundarios sepan que necesitan actualizar su copia de la zona. Permite a los servidores secundarios determinar si necesitan actualizar su copia de la zona.

- Refresco: Indica cuánto tiempo en segundos deben esperar los servidores secundarios antes de solicitar una actualización de la zona al servidor primario.

- Reintento: Especifica cuánto tiempo deben esperar los servidores secundarios antes de intentar nuevamente si no pueden contactar al servidor primario.

- Caducidad: Indica cuánto tiempo pueden mantener los servidores secundarios una copia de la zona antes de considerarla obsoleta si no pueden contactar al servidor primario.

- TTL Mínimo: Especifica el tiempo de vida mínimo (en segundos) que un registro individual puede permanecer en caché en los servidores DNS.

Se ha asignado a cada máquina su nuevo nombre correspondiente modificando el fichero */etc/myname* (router1, ntp, ns1, ns2).

Posteriormente, se ejecutan los comandos *nsd-checkconf /var/nsd/etc/nsd.conf* y *nsd-checkzone* nombrezona */var/nsd/zones/nombrezona* para comprobar la correcta configuración de estos ficheros.

El comando **dig** es una herramienta de línea de comandos que se ha utilizado para realizar consultas DNS.
El siguiente comando utiliza dig para realizar una consulta de resolución de nombres de dominio IPv6 para el nombre ns1.1b.ff.es.eu.org hacia el servidor DNS de Google con la dirección IPv6 2001:4860:4860::8888:

```
ns1$ doas dig -6 @2001:4860:4860::8888 AAAA ns1.1b.ff.es.eu.org

; <<>> dig 9.10.8-P1 <<>> -6 @2001:4860:4860::8888 AAAA ns1.1b.ff.es.eu.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7790
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;ns1.1b.ff.es.eu.org.           IN      AAAA

;; ANSWER SECTION:
ns1.1b.ff.es.eu.org.    3600    IN      AAAA    2001:470:736b:1bff::3

;; Query time: 101 msec
;; SERVER: 2001:4860:4860::8888#53(2001:4860:4860::8888)
;; WHEN: Sun Feb 25 19:55:50 CET 2024
;; MSG SIZE  rcvd: 76

ns1$
```

Es decir, nos muestra que el nombre de dominio ns1.1b.ff.es.eu.org se mapea a la dirección IPv6 2001:470:736b:1bff::3.

Este siguiente comando dig realiza una búsqueda inversa para encontrar el nombre de dominio asociado con la dirección IPv6 2001:470:736b:1bff::3. La sección de respuesta indica que la dirección IPv6 2001:470:736b:1bff::3 se resuelve al nombre de dominio ns1.1b.ff.es.eu.org.

```
ns1$ doas dig -6 @2001:4860:4860::8888 -x 2001:470:736b:1bff::3

; <<>> dig 9.10.8-P1 <<>> -6 @2001:4860:4860::8888 -x 2001:470:736b:1bff::3
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15415
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.b.1.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. IN PTR

;; ANSWER SECTION:
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.b.1.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 21600 IN PTR ns1.1b.ff.es.eu.org.

;; Query time: 256 msec
;; SERVER: 2001:4860:4860::8888#53(2001:4860:4860::8888)
;; WHEN: Sun Feb 25 20:01:52 CET 2024
;; MSG SIZE  rcvd: 134

ns1$
```

Para configurar el servidor DNS recursivo y con cache utilizaremos el **unbound**, un servidor de nombres de dominio recursivo y de resolución rápida de consultas. Para ello, se ha activado e iniciado el demonio unbound mediante *rcctl enable unbound* y *rcctl start unbound,* se ha modificado el fichero */var/unbound/etc/unbound.conf* con el contenido que se mostrará a continuación, se ha comprobado su correcta configuración con *unbound-checkconf,* y se ha configurado la comunicación segura entre el cliente y el servidor Unbound, generando claves criptográficas y estableciendo permisos adecuados en el sistema mediante el comando *unbound-control-setup.* Con *unbound-control dump_cache* podemos ver lo que se ha guardado en la caché.

Fichero unbound.conf:

```
Unset
server:
    interface: ::0
    interface: ::1
    access-control: 0.0.0.0/0 refuse
    access-control: 2001:470:736b:1bff::0/64 allow
    access-control: ::0/0 refuse
    access-control: ::1 allow
    hide-identity: yes
```

```
    hide-version: yes

    auto-trust-anchor-file: "/var/unbound/db/root.key"
    val-log-level: 2

    aggressive-nsec: yes

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

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

stub-zone:
        name: "1b.ff.es.eu.org"
        stub-addr: 2001:470:736b:1bff::3
        stub-addr: 2001:470:736b:1bff::4
```

Para la ejecución del **Script en Ruby**, ha sido necesaria la instalación de determinadas gemas con los siguientes comandos:

```
Unset
gem install net-ping --user-install
gem install net-ssh --version 3.0.1 --user-install
```

A su vez, ejecutando el comando *export PATH=$PATH:/home/a842748/.u/* podemos ejecutar el script simplemente con el comando *u <subcomando>*.

Las librerías importadas para la realización del script han sido 'net/ping' 'net/ssh' y 'timeout'. Se ha seguido un diseño de descomposición funcional para hacer el código más simple, legible y depurable.

Problemas encontrados y su solución

A la hora de realizar los digs para verificar el correcto funcionamiento de las configuraciones establecidas, se obtenían diversos errores de conexión (Network Errors). Tras consultar el fichero de logs, me percaté de que los ficheros de zonas estaban mal ubicados ya que debían estar en el directorio /var/nsd/zones.

Pese a no haber encontrado muchos problemas a lo largo del desarrollo de esta práctica, la mayoría han sido fruto de pequeños gazapos en los ficheros de configuración modificados.

El Script de Ruby causó diversos problemas principalmente relacionados con la instalación de las gemas, pero tras la ejecución de los comandos mostrados anteriormente estos fueron solucionados.