1. OBJETIVO

En esta práctica se estudia el servicio de resolución de nombres DNS. Utilizaremos el servidor de DNS *Bind* del *Internet Systems Consortium,* www.isc.org. Sobre este servidor llevaremos a cabo las tareas de administración más comunes:

1. Creación y configuración de zonas de resolución directa e inversa
2. Sincronización entre servidores maestro y esclavos
3. Delegación de subdominios

Para la realización de las prácticas usaremos dos máquinas virtuales (VM1 y VM2). Una de ellas usará la distribución Rocky Linux 9.3, y la otra contará con una distribución Ubuntu Server 22 (se deja a criterio de los alumnos su asignación a VM1 o VM2).

2. PRÁCTICO

1. Comenzamos con la máquina **VM1**. Realizar peticiones DNS utilizando las utilidades *dig* y/o *nslookup*, tanto en resolución directa como inversa, sobre servidores de DNS locales y remotos (servidores de Internet). Llevar a cabo manualmente el proceso iterativo de búsqueda de un recurso de Internet desde los servidores raíz hasta el servidor con autoridad en el dominio a consultar (también puede usar la opción +trace de *dig*).

2. Instalar el servidor de DNS Bind 9.

3. Configuración del servidor Bind. Estudiar el archivo *named.conf* y el contenido del directorio de configuración de Bind. Arrancar el servicio *named*. El servidor deberá escuchar en el puerto 53/udp de todas las direcciones IP del equipo, y atender peticiones de DNS desde cualquier dirección origen. Trabajará de modo recursivo. A continuación, realizar distintas configuraciones sobre el servidor Bind y verificar su correcto funcionamiento:

   a. Comprobar que el servidor mantiene una **caché** de últimos accesos realizados (para eliminar el contenido de la caché se puede utilizar el comando `rndc flush`)

   b. **Creación de zonas primarias**. Supondremos un dominio ficticio **midominio.net**, que administra direcciones en el rango **160.50.40.0/24**. Configurar dos zonas primarias para administrar las resoluciones directa e inversa.

   c. **Mantenimiento de zonas primarias**. Añadir los siguientes registros a las zonas creadas: A (zipi, 160.50.40.1), A (zape, .2), A (mortadelo, .4), A (correo, .50), A (dns1, nuestra propia dirección IP), A (www, a las direcciones 160.50.40.200 y 160.50.40.201), NS (dns1), CNAME (aplicaciones ->mortadelo), MX (correo, prioridad 20). Todos los registros de tipo A deben tener asociado su correspondiente registro PTR. Verificar su funcionamiento con el cliente de DNS (*dig* o *nslookup*)

   d. **Sincronización primaria-secundarias**. Vamos a replicar la zona **midominio.net** en otro servidor de DNS secundario. Arrancar la segunda máquina virtual (**VM2**) e instalar nuevamente el servidor Bind 9. A continuación establecer una zona secundaria del dominio midominio.net. En el servidor maestro añadir otra entrada NS (dns2) apuntando a la dirección IP del nuevo servidor. Configurar en ambos servidores los parámetros que permitirán la transferencia de la zona. Reiniciar ambos servidores y comprobar que el secundario mantiene una copia de la zona. Llevar a cabo algún cambio en la zona maestra incrementando su número de serie. Reiniciar el servidor y verificar que se actualiza la zona secundaria.

      Nota: se recomienda configurar la notificación explícita a las secundarias (`notify explicit`) y la directiva `also-notify` con la dirección IP del servidor secundario.

e. **Delegación de un subdominio**. Crear una nueva zona maestra **pruebas.com** en el servidor **VM2**. Vamos a configurar la delegación de un subdominio (por ejemplo, **ceu.pruebas.com**), cuya zona maestra se ubicará en el otro servidor de DNS (**VM1**). Para hacer las pruebas añadir algún registro A en el nuevo subdominio y verificar que una petición de resolución dirigida al servidor VM2 y relativa al subdominio, es reenviada y resuelta en el servidor VM1. Comprobar igualmente el efecto de la directiva `recursión yes|no` en el comportamiento del servidor que aloja el dominio principal (VM2).

4. **Partes opcionales**:

   a. Estudiar cómo pueden configurarse las **vistas** (***views***) en *bind 9*. Realizar una pequeña maqueta para comprobar su funcionamiento: una misma zona de resolución directa que devuelve diferentes respuestas en función de la dirección IP desde la que se realicen las peticiones.

   b. Establecer un mecanismo de autentificación servidor-servidor basado en secreto compartido (***TSIG***, ***Transaction SIGnatures***) para la transferencia de zonas entre primaria y secundarias. Nota: para este apartado es importante que ambos servidores tengan sus relojes sincronizados;

Nota: los aspectos significativos de la configuración realizada en todos los apartados de la sección 3 tendrán que reflejarse en la memoria de la práctica. Opcionalmente se incluirá todo lo relativo al apartado 4.

Resolución de incidencias

Puede utilizar los comandos **named-checkconf** y **named-checkzone** para detectar errores de sintaxis en la configuración general y en los archivos de zona.

Si detecta errores de escritura que impiden la transferencia de zona en un secundario, verifique los derechos del usuario *named* en el directorio donde se va a copiar la zona esclava.

Para conocer qué está ocurriendo en el servicio es posible consultar los archivos de log (journalctl -u named)

3. REFERENCIAS

RFCs

http://www.ietf.org/rfc/rfc1033.txt (Manual para administradores de Dominio)
http://www.ietf.org/rfc/rfc1034.txt (Conceptos generales)
http://www.ietf.org/rfc/rfc1035.txt (Protocolo e implementación)
http://www.rfc-es.org/rfc/rfc1886-es.txt (Extensiones para IPv6, en castellano)

DNS for Rocket Scientists
http://www.zytrax.com/books/dns/

Manual de administración de Bind 9
https://www.isc.org/downloads/bind/doc/

Bind 9 FAQ (Preguntas más frecuentes)
http://www.bind9.net/BIND-FAQ

Unix and Linux System Administration Handbook
Evi Nemeth – Garth Snyder – Trent R. Hein – Ben Whaley.
Prentice Hall, 4ª Ed, 2011