Actividad DNS. Ubuntu Server

Usando las máquinas virtuales vamos a construir una red sobre la que montar una estructura DNS. La red tienen la siguientes características.

- Está formada por cuatro máquinas (M1, M2, M3 y M4) todas Ubuntu Server. La primera tiene dos tarjetas de red, una conectada a NAT para acceder a internet y otra conectada al segmento de red virtual para conectar con el resto. Las demás sólo tienen una tarjeta de red conectada al segmento de red virtual.
- Las direcciones IP debes ponerlas tú, siendo automática la que da conexión a internet y fijas todas las demás.

  En cuanto al sistema DNS, sus características serán las siguientes.
- Dominio: ***2asir.edu***
- Nombres canónicos de las máquinas:
  - ***ns1.2asir.edu*** para la máquina 1
  - ***ns2.2asir.edu*** para la máquina 2
  - ***pc01.2asir.edu*** para la máquina 3
  - ***pc02.2asir.edu*** para la máquina 4
- Otros nombres
  - *ns1* será también ***www*** y ***servidor***
  - *ns2* será también ***pcprof***
- *ns1* será el **servidor DNS maestro**
- *ns2* será un **servidor DNS esclavo**, que tomará la información de *servidor*
- Todas las máquinas deben usar como servidor de nombres a las máquinas que hemos hecho servidoras de nombres (máquina 1 y máquina 2). Además, el cliente DNS de todas las máquinas debe estar configurado para responder a **nombres cortos** (sin el dominio).
- Los nombres que no se puedan resolver deben ser **redirigidos** a un servidor dns de internet. Búscalos en la web.
- Sólo se pueden hacer consultas al sistema DNS montado desde las máquinas de la red local.

  Debes configurar tanto los dos servidores como los clientes.

Un resumen de los pasos sería:

1. Establecer la **configuración IP** de todas las máquinas
2. Establecer el nombre M1 a M4 de cada máquina (archivo ***/etc/hostname***). Recuerda modificar también ***/etc/hosts*** para que no se ralenticen los comandos sudo.
3. **Instalar bind9** en los dos servidores (en la máquina 2 habrá que hacer una conexión a internet temporal para descargar e instalar bind9, por lo que habrá que conectarla a NAT y dejar que tome la dirección IP automáticamente; luego, se restaurará la configuración que hemos indicado).

Captura de instalación exitosa

4. Configurar del **servidor primario**
   a. Editar **/etc/bind/named.conf.local** con las zonas directa e inversa. Habrá que indicar en cada zona su nombre, el archivo que va a contener su correspondiente base de datos y posiblemente alguna opción que restrinja las consultas sólo a las máquinas de la red (opción *allow-query*), creando previamente una lista de control de acceso (*acl*) o indicando directamente el conjunto de direcciones. Mira algún *named.conf.local* de ejemplo para guiarte.

Captura de /etc/bind/named.conf.local

   b. Editar **/etc/bind/named.conf.options** añadiendo las opciones necesarias. Habrá que indicar opciones para redireccionar las consultas que no se puedan resolver a otros servidores DNS en internet (está opción es *forwarders*). También es posible incluir una opción para restringir a la red local las consultas, si no se ha hecho en cada zona en el *named.conf.local*.

Captura de /etc/bind/named.conf.options

c. Chequear **named.conf** con el comando ***named-checkconf*** y corregir los errores. Presta atención en los mensajes de error al número de línea, que te da pistas de dónde puede estar el fallo (aunque no significa que el fallo por fuerza deba estar ahí).

Captura de ejecución exitosa de named-checkconf

d. Crear los **archivos de base de datos de las zonas** directas e inversa. Dichos archivos deben tener:

- Zona directa
  1) Registro SOA que defina la zona, con el número de serie y resto de parámetros temporales.
  2) Registros NS para indicar quiénes van a ser los servidores de nombres
  3) Registros A para asociar nombres canónicos con direcciones IP
  4) Registros CNAME para asociar otros nombres con nombres canónicos.

Captura de archivo de base de datos de zona directa

- Zona inversa
  1) Registro SOA que defina la zona, con el número de serie y resto de parámetros temporales.
  2) Registros NS para indicar quiénes van a ser los servidores de nombres
  3) Registros PTR para asociar a direcciones IP nombres.

Captura de archivo de base de datos de zona inversa

e. Chequear los archivos de base de datos de las zonas definidas en el paso anterior con el comando ***named-checkzone***

Captura de ejecución exitosa de named-checkzone para zona directa

Captura de ejecución exitosa de named-checkzone para zona inversa

5. **Reiniciar** el **servicio** con ***/etc/init.d/bind9 restart***

Captura de reinicio exitoso del servicio DNS

6. **Configurar clientes** modificando el archivo **/etc/resolv.conf**, usando las opciones ***nameserver, domain, search,*** etc.. Se deben poder resolver direcciones de la red usando nombres cortos (sin .2asir.edu)

Captura de /etc/resolv.conf de una máquina

7. Comprobar el **funcionamiento del servidor primario** usando los comandos ***dig, host, nslookup, ping,*** etc. desde las otras máquinas. Si algo no funciona bien no dudes por empezar reiniciando de nuevo el sistema DNS (paso 4). Si sigue fallando, comienza a analizar qué comandos fallan y por qué.

Captura de ejecución exitosa de nslookup www.2asir.edu

Captura de ejecución exitosa de nslookup pc02

Captura de ejecución exitosa de nslookup www.google.es

8. Configurar el **servidor secundario**

a. Editar ***/etc/bind/named.conf.local*** con las zonas directa e inversa, pero del servidor secundario. Serán las dos mismas zonas que el servidor primario, pero en lugar de ser *type master* serán *type slave*, indicando además el nombre del archivo que definirá la zona y la dirección IP de la máquina maestra. Además, hay que indicar cuál será el servidor maestros con la opción *masters*. Un ejemplo (que no corresponde a esta práctica, usa zonas y direcciones IP

diferentes):

```
zone “practica.com” {
        type slave;
        file “slave.db.practica.com”;
        masters {192.168.10.1; };
};
```

La zona inversa es similar, cambiando sólo los nombres de la zona y el archivo.

Captura de /etc/bind/named.conf.local del servidor secundario

b. Editar ***/etc/bind/named.conf.options*** añadiendo las opciones necesarias, si hay alguna.

Captura de /etc/bind/named.conf.options del servidor secundario

c. No es necesario crear los ficheros de zona, se generan automáticamente cuando se sincronicen el servidor secundario, por defecto los ficheros de zona se crean en /var/cache/bind.

9. **Reconfigurar el servidor primario** para que pueda hacer transferencias al secundario. En principio, será necesario:

a. Añadir en cada zona de *named.conf.local* las opciones para permitir hacer transferencias y actualizaciones a la máquina configurada como servidor secundario. Para permitir transferencias se usa la opción *allow-transfer*, con la lista de direcciones a las que se van a permitir transferencias (en principio sólo el servidor secundario). Un ejemplo de cómo quedaría teniendo el servidor secundario en la IP 192.168.10.2 y que no corresponde a esta práctica sería:

```
zone “practica.com” {
        type master;
        allow-query {127.0.0.1; red_int; };
        allow-transfer {192.168.10.2; };
        file “/etc/bind/db.practica.com”;
};
```

Captura de /etc/bind/named.conf.local del servidor primario

b. Añadir en las bases de datos de las zonas el segundo servidor DNS, si es que no se ha hecho antes, con un nuevo registro NS.

10. **Reconfigurar los clientes** añadiendo la IP del servidor secundario.

Captura de /etc/resolv.conf de una máquina

11. **Comprobar el funcionamiento del servidor secundario.** Para ello:
    a. Reiniciar los servicios DNS de los dos servidores, primero y el primario y luego el secundario, para que se “sincronicen”.

Captura de reinicio exitoso del servicio DNS del servidor secundario

b. Realizar una consulta en cualquier cliente y comprobar que funciona y que el servidor que responde es el primario (con ***nslookup*** es suficiente).

Captura de ejecución exitosa de nslookup pc01 (respondiendo el servidor primario)

c. Detener el servicio en el servidor primario.

Captura de parada exitosa del servicio DNS del servidor primario

d. Realizar una consulta con el mismo cliente y comprobar que funciona y que el servidor que responde es el secundario (con ***nslookup*** es suficiente).

Captura de ejecución exitosa de nslookup pc01 (respondiendo el servidor secundario)

Captura ejecución exitosa nslookup www.google.es (respondiendo el servidor primario)

Imaginemos ahora que se añade una nueva máquina, que vamos a llamar ***pc03.2asir.edu*** . ¿Qué hay que modificar (ordenador/es, archivo/s, línea/s)?