PRÁCTICA. SERVICIO DE NOMBRES DE DOMINIO (DNS), BIND.

En un documento detalla y sube a agora al finalizar la sesión de prácticas:

1. Las repuestas a las preguntas que se han ido realizando durante el guion de la práctica y:

    a. La configuración del fichero named.conf, explicando lo que has modificado o incluido en él a modo de comentarios, y los ficheros de zona necesarios.

    b. Cómo has configurado el cliente desde el que haces las consultas

    c. Capturas de pantalla de las capturas del tráfico y explicación.

1. Configuración del Servidor de Nombres de Dominio

El servicio de nombres de dominio en UNIX y Linux se implementa mediante el programa **BIND** (Berkeley Internet Name Domain). El archivo principal de configuración de BIND es /etc/named.conf. Los archivos de registros de DNS de cada zona administrada se crearán en el directorio /var/named (por defecto). El programa (demonio) servidor de BIND se llama **named**, y no arrancará correctamente hasta que no haya errores en el archivo de configuración (/etc/named.conf).

Para comprobar si el servidor named se está ejecutando se puede utilizar el comando **ps** o intoducir el comando:

```
# service named status
```

Si nos dice que no existe el servicio, lo instalaremos, por ejemplo mediante yum:

```
# yum install bind
```

En esta práctica vamos a configurar un servidor de dominio primario. Éste es el caso más completo.

> *NOTA IMPORTANTE: Todas las direcciones IP y todos los nombres de dominios y máquinas que aparecen a continuación son inventados, en los ejercicios a realizar en el laboratorio se deberá usar un nombre de dominio que se elija libremente pero las direcciones IP deberán ser las que tienen asignadas los equipos.*

Archivo /etc/named.conf

IMPORTANTE: Antes de empezar a modificar el fichero /etc/named.conf **HAZ UNA COPIA DE SEGURIDAD DEL MISMO.**

La sección **`options`** define opciones de configuración globales para el servidor y opciones por defecto para otras secciones del fichero de configuración.
Algunas de las opciones que se usan habitualmente son:

`allow-query:` especifica que hosts pueden consultar este servidor de nombres.
`directory:` especifica el directorio por defecto donde se almacenan los ficheros de las zonas que sirve este servidor de nombres.
`listen-on:` especifica la interfaz de red en la que named escucha las consultas DNS.

Este servidor DNS tiene que actuar como local DNS server, para ello trae por defecto la declaración:

```
zone "." IN {
type hint;
file "named.ca";
};
```

1. **PREGUNTA: ¿Para qué sirve esta zona? ¿Qué incluye el fichero named.ca?**

Además, en el archivo named.conf incluiremos las definiciones para las zonas de las que el servidor sea responsable. En el caso de que el servidor DNS fuese el servidor de dominio principal de la Universidad de Mordor con dominio "unimordor.com", aparecería la siguiente entrada en el archivo:

```
zone "unimordor.com" IN{
type master;
file "unimordor.com.zone";
};
```

La declaración de zona se indica mediante el indicativo zone, seguido del nombre de la zona o dominio. Entre llaves aparece la configuración de la zona. El campo type dice si el servidor es primario (master) o secundario (slave) (en esta práctica configuraremos

un servidor primario solamente). El campo file dice el nombre del archivo que guarda los registros DNS (de tipo NS, A, CNAME, MX, etc) para esa zona o dominio. Por defecto, todos estos archivos de zona se crean y guardan en el directorio /var/named (en este caso, la ruta del archivo sería /var/named/unimordor.com.zone .

Si se quisiese indicar que el servidor es secundario (no será el caso de esta práctica), se pondría:

```
zone "unimordor.com" IN{
type slave;
file "unimordor.com.zone";
masters { 192.168.1.101; };
 };
```

De este modo se define servidor secundario, que buscará su información en el servidor primario indicado por la dirección IP 192.168.1.101.

Archivos de zona.

Los archivos que tienen los registros correspondientes a cada zona deben llamarse como se indica en el atributo file visto anteriormente y se encontrarán en el directorio /var/named si no se indica lo contrario. Dentro podrán ir directivas y registros que vemos a continuación.

Directivas

$ORIGIN, indica el dominio por defecto, que se agregará a los nombres que no sean FQDN (Fully Qualified Domain Name) dentro del archivo. Normalmente no hará falta poner esta directiva, ya que el valor por defecto del dominio se toma de lo indicado en el archivo named.conf después de cada sentencia zone.

Ejemplo: $ORIGIN unileon.es

Otra directiva que sí se suele usar es **$TTL**, que indica el TTL por defecto.

Registros de recursos (Resource Records ó RR).

Son los datos correspondientes a las entradas DNS, con el significado visto en teoría.

- Registro tipo A

<host> IN A <dirección-IP>

• Registro tipo CNAME

<nombre-alias> IN CNAME <nombre-real>

• Registro tipo MX

IN MX <precedencia> <nombre-servidor-correo-e>

• Registro NS

IN NS <nombre-del-servidor-de-nombres>

• Registro SOA

Es el primer registro de todos los que aparecen en un archivo de zona de un servidor primario después de la sección de directivas. La sintaxis es como la que sigue (poner los paréntesis tal como aparecen en el ejemplo):

@ IN SOA <nombre-del-servidor-de-nombres-primario>
<direccion-de-correo-e-del-administrador> (
<numero-de-serie>
<tiempo-para-actualizar>
<tiempo-para-reintentar>
<tiempo-de-expiracion>
<Tiempo_caché_respuesta_negativa>
)

OJO, LOS DATOS DEL REGISTRO SOA SE ENCIERRAN ENTRE PARÉNTESIS

El símbolo @ hace referencia al dominio indicado en la directiva $ORIGIN o en el nombre que va después de zone en el archivo named.conf.

<nombre-del-servidor-de-nombres-primario> es el nombre del servidor de nombres de dominio primario, indicado mediante FQDN. Todos los nombres que sean FQDN deben acabar en punto.

<direccion-de-correo-e-del-administrador> es la dirección del correo electrónico del administrador responsable del dominio o zona. La arroba se sustituirá por un punto y también se indica como FQDN.

<numero-de-serie> es un número que el servidor de nombres secundario comprobará cada vez que se conecte con el primario para realizar la sincronización. Si el número que hay en el primario no coincide con el secundario se realizará la copia del archivo. Si el número coincide es que la información no ha cambiado y no necesita ser actualizada. Este número se actualiza manual o automáticamente (en el caso de usar DDNS) en el servidor primario cuando se cambian datos. Suele utilizarse la fecha y hora del cambio. Ejemplo: 201211231000

<tiempo-para-actualizar> es un número que representa, en segundos, el tiempo, transcurrido el cual, el servidor secundario conectará con el primario para realizar la sincronización.

<tiempo-para-reintentar> es un número que representa, en segundos, el tiempo, transcurrido el cual, el servidor secundario realizará un reintento de conexión con el primario si éste no ha respondido en un intento anterior.

<tiempo-de-expiracion> Cuando el servidor secundario no puede contactar durante un largo periodo de tiempo por el primario se establece un tiempo durante el cual el secundario puede seguir sirviendo información. Transcurrido este tiempo, expresado en este campo, el secundario dejará de considerar su información como autorizativa y no responderá más peticiones.

<Tiempo_caché_respuesta_negativa> Cuando un servidor de nombres no encuentra un registro para un determinado dato que se le está pidiendo devuelve un código NXDOMAIN. Este mensaje de error será cacheado como respuesta a la consulta en el cliente que hizo la pregunta durante el tiempo especificado en este campo. El valor especificado no debe ser mayor de 10800 segundos. Este campo ha cambiado su significado respecto a versiones anteriores del protocolo DNS (y por tanto respecto a versiones anteriores de BIND). Antes, este campo era utilizado como TTL por defecto, ahora se usa la directiva $TTL para este fin, como se ha visto.

Un ejemplo de registro SOA sería (se incluye en la primera línea la declaración $TTL, que es con la que comienza el fichero, aunque no pertenece al registro SOA):

```
$TTL 86400
@ IN  SOA    dns1.unimordor.com.  javi.unimordor.com.  (
2000001645
86400
3600
3600000
604800
)
```

Justo debajo vendrían los datos correspondientes a las traducciones directas nombre -> IP, por ejemplo:

```
        IN      NS      dns1.unimordor.co
dns1    IN      A       192.168.3.39
eq16    IN      A       192.168.3.41
www     IN      CNAME   eq16
```

En resumen, para un servidor primario, el archivo de resoluciones empezará con un registro SOA seguido de registros tipo NS, A, CNAME o MX. En el caso de resolución inversa tendremos un registro SOA al comienzo también y luego registros NS y PTR.

2. Configuración del cliente (resolver).

Arrancamos otra máquina virtual con Centos que será la que haga las consultas DNS a nuestro servidor DNS.

Para configurar el cliente (resolver) vamos a la configuración de red del equipo Sistema -> Preferencias -> Conexiones de Red y edito las propiedades de la interfaz de red, indicando configuración manual (estática) y poniendo la IP, máscara y puerta de enlace que tenga el equipo actualmente.

Borro los servidores DNS actuales e indico como único servidor DNS la IP del equipo que he configurado a tal fin.

En el campo “Dominios de búsqueda” indico el nombre de dominio que haya elegido para configurar (por ejemplo “unimordor.com”).

A continuación, reinicio el servicio de red:

```
# service network restart
```

2. **PREGUNTA: Comprueba que la configuración de red se ha cambiado y la IP del servidor DNS es la del tuyo.**

3. Herramientas

named- checkconf

Con esta herramienta podemos comprobar si es correcta la sintaxis el fichero de configuración del servidor de DNS BIND (el demonio named). Comprueba la sintaxis, no la semántica, por ejemplo puede encontrar errores tipográficos pero no puede detectar una asignación incorrecta de una dirección IP.

```
# named-checkconf /etc/named.conf
```

Si no hay salida es que la sintaxis es correcta.

Ejemplo de error en el fichero:

```
# named-checkconf /etc/named.conf
/etc/named.conf:58: open: /etc/named.root.hints: file not found
/etc/named.conf:32: missing ';' before 'zone'
```

named-checkzone

Esta herramienta comprueba los ficheros de zona. Se le pasa como argumento el nombre de zona y el fichero de zona. Por ejemplo:

```
[root@localhost ~]# named-checkzone midominiof3.com
/var/named/midominiof3.directa
```

La salida sería, por ejemplo:

```
/var/named/midominiof3.directa:1: no TTL specified; using SOA MINTTL
instead zone midominiof3.com/IN: loaded serial 20051101
```

3. **PREGUNTA: ¿Para qué sirve la utilidad rncd? Indica alguno de los comandos que permite.**

Hay dos herramientas para consultar registros DNS relacionados con un nombre de dominio, dig y host.

dig (domain information groper)

Esta utilidad nos permite obtener información de los servidores DNS. Realiza consultas DNS y muestra los resultados. Muchos administradores de DNS usan dig para solucionar problemas de DNS gracias a su facilidad de uso y claridad en el formato de salida. Por ejemplo:

```
[root@localhost ~]# dig midominiof3.com

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.10.rc1.el6_3.3 <<>> midominiof3.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43921
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL:
0

;; QUESTION SECTION:
;midominiof3.com.       IN    A

;; AUTHORITY SECTION:
midominiof3.com.  604800      IN    SOA   dns1.midominiof3.com.
pepe.midominiof3.com. 20051101 86400 3600 3600000 604800

;; Query time: 2 msec
;; SERVER: 10.20.48.38#53(10.20.48.38)
;; WHEN: Tue Nov 20 15:57:47 2012
;; MSG SIZE  rcvd: 79
```

host

Esta herramienta permite hacer búsquedas en el DNS. Se utiliza básicamente para convertir nombres en direcciones IP y viceversa. Los resultados son más explícitos que con dig y tan completos como el usuario quiera, permitiendo ver mejor las diferencias entre zonas, incluso pudiendo copiar una zona con su texto plano mediante los registros AXFR

host [opciones] <dominio> [servidor]

Algunas opciones:

* -t <tipo> : indica el tipo de record a devolver. Puede ser A, ANY, PTR, NS, etc.

* -R <n> : permite modificar el número de intentos que se hacen para obtener la respuesta ya que por defecto es uno.

* -l : lista toda la información del dominio

Ejemplos:.

```
[root@localhost ~]# host -t  ns midominiof3.com

midominiof3.com name server dns1.midominiof3.com.


[root@localhost ~]# host -t  AXFR midominiof3.com
Trying "midominiof3.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23539
```

```
;; flags: qr aa ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;midominiof3.com.       IN    AXFR

;; ANSWER SECTION:
midominiof3.com.  604800 IN    SOA   dns1.midominiof3.com.
pepe.midominiof3.com. 20051101 86400 3600 3600000 604800
midominiof3.com.  604800 IN    NS    dns1.midominiof3.com.
dns1.midominiof3.com.    604800 IN    A     10.20.48.38
eqcentos.midominiof3.com. 604800 IN A     10.20.48.38
eqcentos1.midominiof3.com. 604800 IN      A     10.20.48.106
www.midominiof3.com.    604800      IN    CNAME
      eqcentos1.midominiof3.com.
midominiof3.com.  604800      IN    SOA   dns1.midominiof3.com.
pepe.midominiof3.com. 20051101 86400 3600 3600000 604800

Received 214 bytes from 10.20.48.38#53 in 4 ms


[root@localhost ~]# host -l disaic.cu
disaic.cu. SOA alma.disaic.cu. alina.maildi.disaic.cu. 88 10800 900
604800 86400
disaic.cu. name server alma.disaic.cu.
disaic.cu. name server odin.disaic.cu.
yixie.disaic.cu. is an alias for odin.disaic.cu.
odin.disaic.cu. has address 192.168.200.3
tuxco.disaic.cu. is an alias for nemo.disaic.cu.
nemo.disaic.cu. has address 192.168.100.4
 …..
```

EJERCICIOS

4. **PREGUNTA:** Configurar un equipo como servidor de nombres de dominio para la red a la que pertenece el propio equipo (la del laboratorio o la que tengamos virtualizada). Tienes que configurar adecuadamente la sección options y tener la zona "." Configura un equipo cliente para que utilice tu servidor DNS y comprueba que funciona.

Haz ping a www.google.com y otros sitios para comprobarlo.

Asegúrate que estas usando tu servidor DNS para que el cliente resuelva los nombres (utiliza el comando dig, al final verás el nombre del servidor DNS que te está sirviendo el servicio).

5. **PREGUNTA:** Tu servidor DNS va a ser servidor DNS autoritativo y maestro, para el dominio uniTierraMedia.com. Crea en named.conf la zona para ello y el fichero de zona correspondiente. Incluye el registro SOA con los siguientes datos:

Tiempo válido para guardar el registro en las caches de DNSs remotos: 3 horas

Dirección del administrador paco@uniTierraMedia.com OJO porque en el fichero no se pone @, se sustituye por un punto

20301120 ;serial
1D ;refresh
1H ;retry
1W ;expire
3H ;non-answer

Introduce los registros de recursos correspondiente al servidor de dominio y resuelve el nombre de una máquina (puede ser tu propio sistema anfitrión, el Windows en el caso del laboratorio) que se denominará eq16 y que tendrá el alias www . Tienes que ser capaz de dar resolución a ambos nombres de máquinas.

Comprueba que funciona haciendo ping a:

- dns1. uniTierraMedia.com
- www.uniTierraMedia.com
- eq16. uniTierraMedia.com

Haz consultas a tu servidor DNS usando las herramientas dig y host.

6. **PREGUNTA:** ¿Con qué comando y argumento visualizas los servidores DNS que está utilizando el sistema?
7. **PREGUNTA**: Explica para qué sirve el comando nslookup y su sintaxis general para ejecutar una consulta.
8. **PREGUNTA**: Ejecuta el comando `nslookup www.usal.es` y explica lo que devuelve y quién te está proporcionando esa información.
9. **PREGUNTA**: Ejecuta el comando nslookup –type=NS usal.es y explica lo que devuelve y quién te está proporcionando esa información.
10. **PREGUNTA**: Ejecuta el comando nslookup alumni.usal.es topacio.usal.es y explica lo que devuelve y quién te está proporcionando esa información.