# Práctica 2 de Administración de Sistemas

Paloma Pérez de Madrid Laguna

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).

**Servidor Local**

Resolución directa: para obtener una dirección IP a partir de un nombre

* dig @servidor (-t tipo) \_\_dominio\_\_

# Dig @localhost [www.constanzalaguna.com](http://www.constanzalaguna.com)

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Resolución inversa: para obtener el dominio a través de una dirección IP

dig @servidor -t \_\_dirección\_IP\_\_ # Dig @localhost -x 172.67.134.61

Texto

Descripción generada automáticamente

**Servidores Remoto**

Servidor remoto de mi máquina Windows:

Imagen en blanco y negro

Descripción generada automáticamente con confianza baja

# Dig @10.80.200.13 [www.constanzalaguna.com](http://www.constanzalaguna.com)

Texto

Descripción generada automáticamente

# Dig @10.80.200.13 -x 172.67.134.61

Texto

Descripción generada automáticamente

**Proceso Iterativo de Búsqueda con trace**

# Dig @localhost [www.constanzalaguna.com](http://www.constanzalaguna.com) -trace

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

1. Instalar el servidor de DNS Bind 9.

Apt-get install bind9



( Si no funciona hacer primero apt update y luego apt-get install bind9)

Para buscar archivos que terminen en .service🡪 find . -type f -name '\*.service'

1. Configuración del servidor Bind:
   * Estudiar el contenido y la ubicación de named.conf

/etc/bind/amed.conf

Texto

Descripción generada automáticamente

La configuración está distribuida en tres secciones:

* + - Local
    - Options
    - Default-zones

Cuando añadamos nuestras zonas en el futuro es importante escribirlas a continuación del include

* + Arrancar servicio named

[netstat -utlp] 🡪 Systemctl start named 🡪 [netstat -utlp]

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

* + El servidor deberá estar escuchando el puerto 53/UDP de todas las direcciones y atender peticiones DNS desde cualquier dirección de origen

[named.conf.options]

* + - Permitir que escuche desde el puerto 53 a todas las direcciones: *listen-on port 53 { any; };*
    - Atender peticiones desde cualquier puerto: *allow-query { any; };*
  + Trabajará en modo recursivo
    - *recursion yes;*

Texto

Descripción generada automáticamente

1. 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)

Rndc dumpdb -cache (vocaldo por defecto al archivo /var/named/data/cache\_dump.db)

Interfaz de usuario gráfica

Descripción generada automáticamente

* + - 1. dig @127.0.0.1 [www.hola.com](http://www.hola.com) (1º consulta)

Texto

Descripción generada automáticamente

* + - 1. dig @127.0.0.1 [www.hola.com](http://www.hola.com) (2º consulta)

Texto

Descripción generada automáticamente

Si la vuelvo a ejecutar veo que tarda mucho menos porque la busca en la caché

* + - 1. Elimino el contenido de la caché: rndc flush
      2. Vuelvo a ejecutar dig: dig @127.0.0.1 [www.hola.com](http://www.hola.com)

Texto

Descripción generada automáticamente

Tarda mucho más, tiene que realizar la consulta directa en lugar de obtenerla de la caché

1. 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.
   * + En /etc/bind/named.conf 🡪 crear zona
       1. Cambiamos /etc/bind/named.conf e incluimos las zonas DIRECTA e INVERSA

Texto

Descripción generada automáticamente

(Importante que estén las zonas debajo de include)

* + - 1. Texto

         Descripción generada automáticamenteCreamos los archivos los archivos de zona.

En Ubuntu todo va en la misma carpeta. Si entramos en named.conf.default-zones vemos que todos los archivos de zonas se guardan ahí. Luego escribiremos los archivos en la carpeta /etc/bind

midominio.net.hosts:

Texto

Descripción generada automáticamente

40.50.160.in-addr.arpa

Texto

Descripción generada automáticamente

* + - Systemctl restart name

1. 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)

Agregamos los registros a midominio.net.hosts:

Texto

Descripción generada automáticamente

Agregamos registros a 40.50.160.in-addr.arpa

Texto

Descripción generada automáticamente

Reiniciamos el servicio “named” y comprobamos

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

1. 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 lP 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. Delegación de un subdominio
2. Editar archivo named.conf.local (VM2):
3. Añade la entrada NS en el servidor maestro (VM1)
4. Configurar la transferencia de Zona
5. Reiniciar los servidores dns1 (VM1) y dns2 (VM2)
6. Verificar funcionamiento

Máquina Virtual Ubuntu (VM1)

named.conf

Texto

Descripción generada automáticamenteTexto

Descripción generada automáticamente

Actualizar entradas NS:

Cambiamos número de serie porque hemos cambiado el archivo

Reiniciamos servidor 🡪 systemctl restart named

Máquina Virtual Rocky (VM2)

Arrancamos bind:

Imagen de la pantalla de un celular de un mensaje en letras negras

Descripción generada automáticamente con confianza media

/etc/named.conf (VM2)

Texto

Descripción generada automáticamente

Comprobación

Funcionamiento VM1 sigue siendo el mismo:

Texto

Descripción generada automáticamente

Desde VM2 podemos hacer dig a las zonas de VM1

Texto

Descripción generada automáticamente

Cambiaremos la IP de una dirección (y el número de serie) para comprobar que la máquina 2 también se actualiza.

# zipi IN A 160.50.40.11

Texto

Descripción generada automáticamente

(systemctl restart named)

Texto

Descripción generada automáticamente

1. 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).**

**Ficheros de Zona y named.conf:**

* + Máquina VM2 (Rocky) – principal

# vim /var/named/pruebas.com.hosts

Texto

Descripción generada automáticamente

Hemos añadido la dirección uhceu para hacer pruebas.

Texto

Descripción generada automáticamente con confianza baja

* + Máquina VM1 (Ubuntu)

/etc/ceu.pruebas.com.hosts

Texto

Descripción generada automáticamente

Hemos añadido tres direcciones dentro del dominio de ceu.pruebas.com (teleco, gisi y ade)

Texto

Descripción generada automáticamente

**Configuración de Opciones:**

* + VM2 /etc/named.conf

Texto

Descripción generada automáticamente

# *allow-query{any;};* 🡪 permite la consulta desde la propia máquina (localhost) y desde la red 192.168.119.0/24. Hemos activado las querys a todas las direcciones que empiezan por 192.168.119.\_\_\_ ( Para las pruebas era lo más oportuno pues la direcciones IP de las máquinas solían cambiar)

* + VM1 /etc/bind/named.conf.options

Texto

Descripción generada automáticamente

# *allow-query { any; };* 🡪 Permite que cualquier host realice consultas DNS al servidor BIND.

# *allow-transfer { 192.168.119.138; };* 🡪 Permite transferencias de zona desde el servidor con la dirección IP `192.168.119.138` (VM2). Especifica que el servidor principal está autorizado para realizar transferencias de zona.

# *recursion yes ;* 🡪 Habilita la recursión en el servidor BIND, permitiéndole realizar consultas recursivas en nombre de clientes.

¿Porqué no configuramos el servidor de subdominio como slave?

En el contexto de la delegación, se espera que el servidor que maneja el subdominio tenga control total sobre ese subdominio. La utilización de un tipo de zona `slave` implica que el servidor esclavo obtiene su información de zona directamente del servidor maestro. Si el tipo de zona fuera `slave`, la información de la zona estaría vinculada al servidor maestro, y cualquier cambio requeriría modificaciones en el servidor maestro.

Desde VM1 llamamos a VM2 y preguntamos por una IP del dominio ceu.pruebas.com.

Texto

Descripción generada automáticamente

Desde VM2 preguntamos en local por una IP del dominio ceu.pruebas.com

**Texto

Descripción generada automáticamente**

Comprobar igualmente el efecto de la directiva recursión yes|no en el comportamiento del servidor que aloja el dominio principal (VM2).

Texto

Descripción generada automáticamente VM2

Texto

Descripción generada automáticamente

Como se aprecia, no ha devuelto la dirección IP sino la IP del servidor que lleva el dominio ceu.pruebas.com (VM1, 192.168.119.137)

# COMENTARIOS TEO:

* 1. dig -t se usa para indicar un tipo de consulta distinto de A (el valor por defecto). Por ejemplo -t NS, -t MX o -t SOA…
* 2. Nota: es más clara la salida de netstat -u**n**tlp
* 3.b) No se suele usar el directorio /etc/bind para ubicar los archivos de zona (sobre todo en las zonas esclavas). El directorio recomendado en la distribución Ubuntu es /var/cache/bind, y en Rocky /var/named (valores establecidos en la opción directory)
* 3.c) En la zona de resolución directa: falta un segundo registro A para www (en la IP .201) y el registro MX es incorrecto (en la parte izquierda se pone el nombre de la zona, no de un recurso de la zona (puedes dejarla en blanco, o poner midominio.net.). La de resolución inversa es correcta.  
  Mi consejo es que hagas pruebas de todos los registros introducidos (por ejemplo, dig @localhost -t MX midominio.net)
* 3.d) El mismo comentario de antes respecto a la ubicación del archivo de zona. Ahora es más delicado, porque en ese directorio es posible que el usuario named no tenga derecho de escritura: la zona esclava no se actualizará automáticamente cuando hagamos cambios en la zona maestra, incrementemos el número de serie y reiniciemos ese servidor… ¿Has hecho la prueba? ¿Ha funcionado?
* SYSTEMCTL ENABLE NAMED🡪 IMPORTANTE PARA EL EXAMEN