



BIND9

Servidor DNS Linux



Índice:

1. Tipos de servicio DNS.....	3
1.1. Explica si has montado un servicio DNS maestro, caché o esclavo.	3
1.2. Explica esta frase: “El servicio Bind no sustituye a servidores DNS como los que podemos usar de Google (8.8.8.8), Cloudflare (1.1.1.1) u otros, sino que se complementa con ellos”.	3
1.3. Busca en tu sistema el archivo /etc/hosts y explica que tiene en común con un servicio de resolución de nombres.	3
2. Instalar y configurar el servicio DNS en Ubuntu Server.	3
2.1. Instalar un servidor DNS en Ubuntu Server usando bind9.	3
2.2. Configurar los forwarders de Bind usando servidores DNS públicos.....	4
2.3 Configura un DNS maestro creando un dominio ficticio(zona) llamado tuapellidoDAW2.org (el mismo que usaste para los Virtual Host web).	4
2.3 Contesta ahora las siguientes preguntas INCLUYENDO AQUÍ LAS CAPTURAS DE LA PARTE ANTERIOR.....	5
3. Comprueba el buen funcionamiento del servicio.	7
3.1 PRUEBA 1: nslookup ftp.tuapellidoDAW2.org	7
3.2 PRUEBA 2: resolver los nombres de los sites.	7
3.3 PRUEBA 3: resolver "www.xataka.com". ¿Qué mensaje te devuelve el servicio?	7
3.4 PRUEBA 4: Comprueba ahora que sin indicar el dominio también te resuelve el nombre gracias a la línea 'search' con el dominio por defecto a buscar que metiste en /etc/resolv.conf. resolver "ftp"	8
3.5 Comprueba como el servidor DNS funciona como DNS caché mejorando los tiempos de respuesta en la segunda y posteriores búsquedas de un nombre.....	8
4. (NO OBLIGATORIO, cuenta para nota) Configuración y prueba de la zona inversa.	9
4.1. Configura también la zona inversa con todos y gran parte de los registros.....	9
4.2. 4.2 Comprueba la sintaxis correcta de los ficheros con los comandos named-checkconf zona ficherodezona	9
4.3. Prueba a resolver de forma inversa: nslookup IP	9

Objetivo:

- Configurar el servicio DNS en las máquinas virtuales.
- Probar el funcionamiento del servicio creando un dominio, dar de alta los equipos y un alias.

1. Tipos de servicio DNS.

Webgrafía sobre DNS: <http://www.dominios-internet.com/>

1.1. Explica si has montado un servicio DNS maestro, caché o esclavo.

1.2. Explica esta frase: “El servicio Bind no sustituye a servidores DNS como los que podemos usar de Google (8.8.8.8), Cloudflare (1.1.1.1) u otros, sino que se complementa con ellos”.

1.3. Busca en tu sistema el archivo /etc/hosts y explica que tiene en común con un servicio de resolución de nombres.

Nota importante: recuerda eliminar si las hubiese las entradas del archivo para asegurarte que a partir de ahora todo se resuelve por DNS.

2. Instalar y configurar el servicio DNS en Ubuntu Server.

Siguiendo los manuales colgados en Moodle:

2.1. Instalar un servidor DNS en Ubuntu Server usando bind9. CAPTURA LAS SIGUIENTES PANTALLAS

- Comprueba si tienes el servicio instalado (dpkg -I SERVICIO). Instálalo si no.

Aquí podemos observar que está instalado el servicio bind9:

```
UbuntuServer-Despliegues [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
javi@ubuntu:~$ dpkg -I bind9
Desinstalado=desconocido(U)/Instalar/eliminar/Purgar/retener(H)
Estado=No/Inst/ficheros-Conf/desempaquetado/medio-conf/medio-inst(H)/espera-disparo(W)/pendiente
// Err?=(ninguno)/requiere-Reinst (Estado,Err: mayúsc.=malo)
// Nombre Versión Arquitectura Descripción
-----
ii bind9 1:9.16.1-0ubuntu2.8 amd64 Internet Domain Name Server
lines 1-6/6 (END)
```

- Comprueba el estado del servicio. Debe estar activo:

\$ systemctl status SERVICIO

Aquí podemos observar como el servicio bind9 está activo:

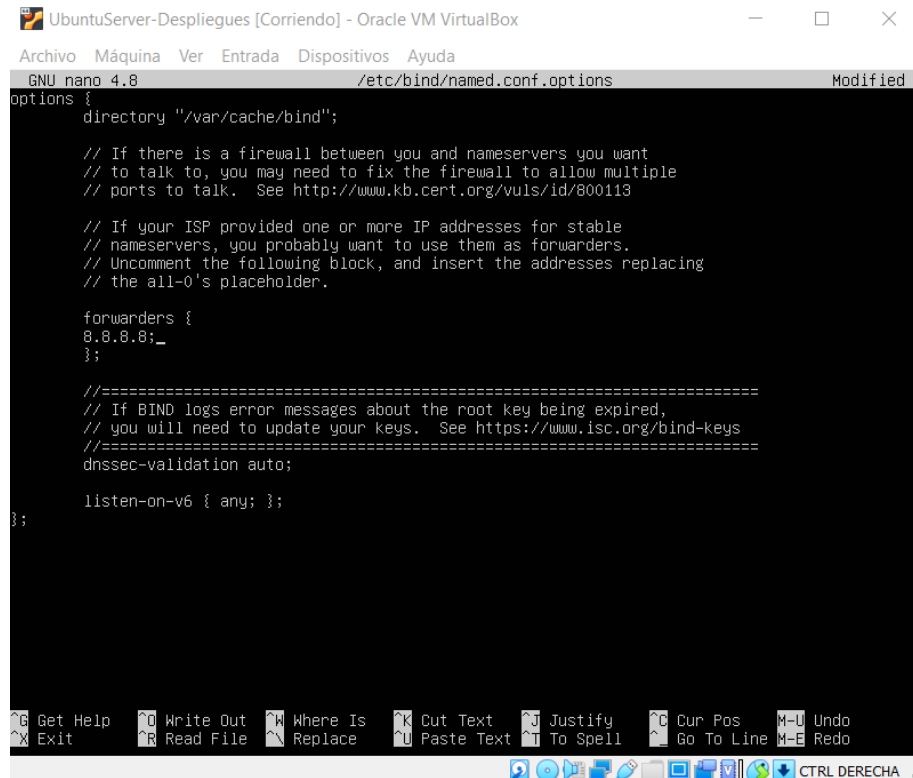
```
UbuntuServer-Despliegues [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
javi@ubuntu:~$ systemctl status bind9
• named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-10-14 09:06:48 UTC; 4min 52s ago
     Docs: man:named(8)
    Main PID: 653 (named)
      Tasks: 5 (limit: 2279)
     Memory: 23.2M
    CGroup: /system.slice/named.service
            └─653 /usr/sbin/named -f -u bind

oct 14 09:06:49 ubusrv-jepi named[653]: network unreachable resolving './NS/IN': 2001:500:2::c#53
oct 14 09:06:49 ubusrv-jepi named[653]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
oct 14 09:06:49 ubusrv-jepi named[653]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
oct 14 09:06:49 ubusrv-jepi named[653]: network unreachable resolving './NS/IN': 2001:503:c27::2:30
oct 14 09:06:49 ubusrv-jepi named[653]: network unreachable resolving './NS/IN': 2001:500:200::b#53
oct 14 09:06:49 ubusrv-jepi named[653]: network unreachable resolving './NS/IN': 2001:500:1::53#53
oct 14 09:06:49 ubusrv-jepi named[653]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
oct 14 09:06:49 ubusrv-jepi named[653]: network unreachable resolving './NS/IN': 2001:dc3::35#53
oct 14 09:06:49 ubusrv-jepi named[653]: managed-keys-zone: Key 20326 for zone . is now trusted (acc
oct 14 09:06:49 ubusrv-jepi named[653]: resolver priming query complete
lines 1-20/20 (END)
```

2.2. Configurar los forwarders de Bind usando servidores DNS públicos

Lo primero que vamos a hacer es configurar unos servidores DNS de forwarding, es decir, los servidores DNS públicos para reenviar las consultas de cara a Internet. El archivo de configuración que se encarga de esta tarea es «named.conf.options».

En la siguiente captura podemos observar como hemos modificado los forwarders:



```
GNU nano 4.8 /etc/bind/named.conf.options Modified
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        0.0.0.0;_
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    listen-on-v6 { any; };
};

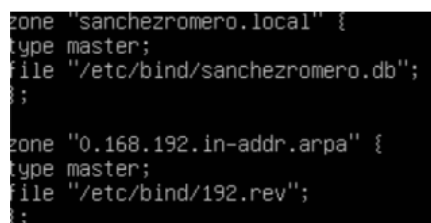
Get Help  Write Out  Where Is  Cut Text  Justify  Cur Pos  M-U  Undo
Exit      Read File  Replace  Paste Text  To Spell  Go To Line  M-E  Redo
CTRL DERECHA
```

2.3 Configura un DNS maestro creando un dominio ficticio(zona) llamado tuapellidoDAW2.org (el mismo que usaste para los Virtual Host web).

(LAS CAPTURAS LAS DEBES INCLUIR EN EL APARTADO 2.3 EN LA RESPUESTA ADECUADA)

A. - Configura el archivo principal /etc/bind/named.conf.local donde se indica los nombres de las zonas de las que este servidor va a tener “autoridad”. Observa que también hay que indicar dónde estarán archivos de configuración de cada zona que se defina.

Mira este ejemplo como ayuda:



```
zone "sanchezromero.local" {
    type master;
    file "/etc/bind/sanchezromero.db";
};

zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/192.rev";
};
```

Para crear el archivo de zona directa te recomiendo que uses como base el local.db; haz una copia de él y renómbrala con tu nombre de zona (en la foto anterior es sanchezromero.db). Si decides hacer la zona inversa (opcional, ver ejercicio 4) usa el 127.rev como plantilla. ¿Cuál es el archivo de zona inversa en la foto anterior?

B.- Crea registros para el propio servidor tal y como lo hayas llamado en "/etc/hostname".

Nota: Puedes también crear para los clientes (aunque si no tienen IP fija o reservada, no es lo más adecuado)

C.- Ahora crea un registro para los nombres de los servicios:

- Crea registro para el propio servidor DNS "dns".

¡OJO! este es imprescindible pues en el primer registro del fichero se indica el nombre del servidor dns primario (... IN NS dns. Dominio) y por supuesto éste también tiene que poder resolverse.

- Crea registro para el servidor web "www"
- Crea registros para tus distintos "sites".
- Crea un registro para el servidor ftp: "ftp".

Recomendación: Si tienes todos o varios servicios en la misma máquina e IP (dns, ftp, www), puedes usar un "alias". Esto se suele hacer con todos los registros que se resuelvan con la misma IP. Esto es muy útil ya que si cambiase la IP del servidor se modificaría de una tacada todo en lugar de revisar registro a registro.

Ejemplo para ayuda:

```
;
; BIND data file for sanchezromero.local
;
$TTL 604800
@      IN      SOA      sanchezromero.local. root.sanchezromero.local. (
                                2      ; Serial
                                604800 ; Refresh
                                86400  ; Retry
                                2419200 ; Expire
                                604800 ) ; Negative Cache TTL
;
sanchezromero.local.  IN      NS      dns.sanchezromero.local.
aula5pc1             IN      A        192.168.0.200
aula5pc2             IN      A        192.168.0.201
www                  IN      A        192.168.0.1
dns                  IN      A        192.168.0.1
```

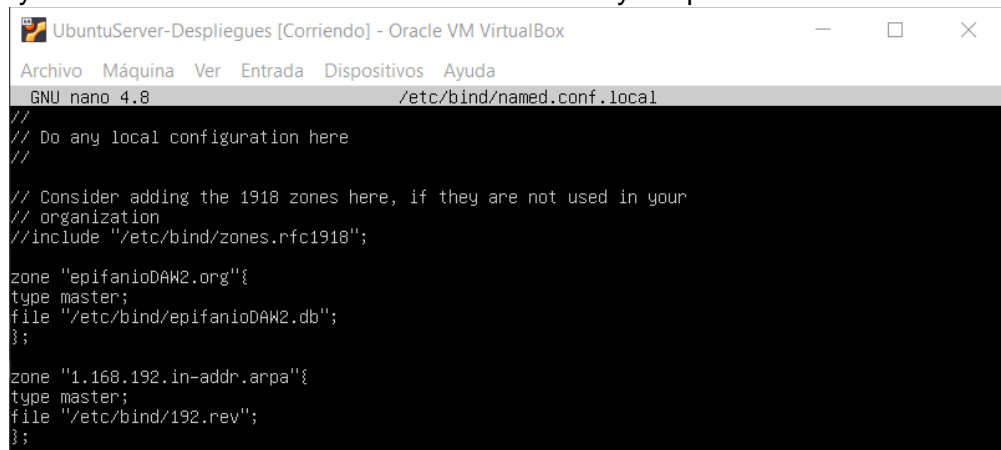
Comprueba la sintaxis correcta de los ficheros con el comando `named-checkzone nombre_zona ficherozona` y haz captura

Ej: `sudo named-checkzone sanchezromero.local /etc/bind/sanchezromero.db`

- Si todo ha ido bien, reinicia el servicio.

2.3 Contesta ahora las siguientes preguntas INCLUYENDO AQUÍ LAS CAPTURAS DE LA PARTE ANTERIOR.

- ¿Qué hay en el fichero `/etc/hostname` del server? Incluye capturas.



```
UbuntuServer-Despliegues [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 4.8 /etc/bind/named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "epifanioDAW2.org"{
type master;
file "/etc/bind/epifanioDAW2.db";
};
zone "1.168.192.in-addr.arpa"{
type master;
file "/etc/bind/192.rev";
};
```

- ¿Qué has añadido al fichero /etc/resolv.conf del servidor? ¿Y del cliente? Incluye capturas y asegurate que incluyes “search”

```
GNU nano 4.8 /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search gcap.net
```

- ¿Qué has añadido al fichero /etc/bind/named.conf.local?

```
UbuntuServer-Despliegues [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 4.8 /etc/bind/named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "epifanioDAW2.org"{
type master;
file "/etc/bind/epifanioDAW2.db";
};

zone "1.168.192.in-addr.arpa"{
type master;
file "/etc/bind/192.rev";
};
```

- ¿Qué nuevo fichero has creado para la búsqueda directa? ¿Y para la inversa?

```
UbuntuServer-Despliegues [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 4.8 /etc/bind/epifanio.db Modified
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA epifanioDAW2.org. root.epifanioDAW2.org. (
2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Negative Cache TTL
;
@ IN NS ubusrv-jepi.
ubusrv-jepi IN A 192.168.1.1
www IN A 192.168.1.1
ftp IN A 192.168.1.1
```

- Comprueba la sintaxis correcta de los ficheros con el comando named-checkzone nombre_zona fichero de zona y haz captura

Ej: sudo named-checkzone sanchezromero.local /etc/bind/sanchezromero.db

```
javiepi@ubusrv-jepi:~$ sudo named-checkzone epifanio.local /etc/bind/epifanio.db
zone epifanio.local/IN: loaded serial 2
OK
javiepi@ubusrv-jepi:~$ _
```

3. Comprueba el buen funcionamiento del servicio.

Haz consultas al servidor DNS mediante el comando `host`, `dig` o `nslookup` y comprueba su correcto funcionamiento tanto resolviendo nombres por búsqueda directa como inversa y tanto para máquinas locales como para externas. Importante: No olvides antes reiniciar el servicio para tomar los cambios (`systemctl restart bind9`) y eliminar las entradas de `/etc/hosts`

3.1 PRUEBA 1: `nslookup ftp.tuapellidoDAW2.org`

Si ya tienes montado el servicio FTP en el server. ¿cómo accederías ahora el servicio desde Filezilla?

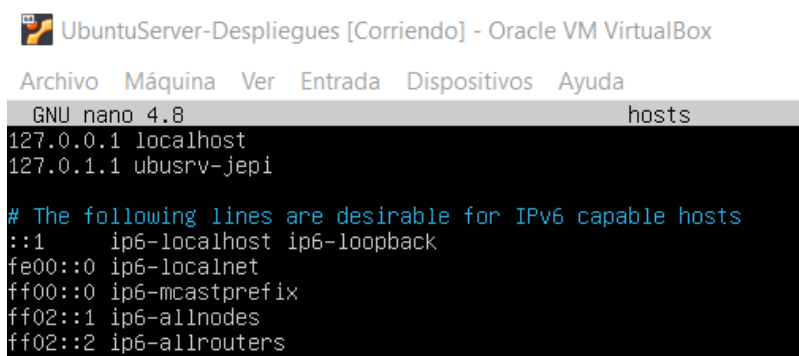
Accedería con el name en mi caso epifanioDAW2.org.

```
javi@epifanioDAW2:~$ host ftp.epifanioDAW2.org
ftp.epifanioDAW2.org has address 192.168.1.1
javi@epifanioDAW2:~$ nslookup www.epifanioDAW2.org
Server:      127.0.0.1
Address:     127.0.0.1#53

Name:   www.epifanioDAW2.org
Address: 192.168.1.1
```

3.2 PRUEBA 2: resolver los nombres de los sites.

Nota: recuerda haber eliminado las entradas de `/etc/hosts`




```
GNU nano 4.8 hosts
127.0.0.1 localhost
127.0.1.1 ubusrv-jepi

# The following lines are desirable for IPv6 capable hosts
::1          ip6-localhost ip6-loopback
fe00::0      ip6-localnet
ff00::0      ip6-mcastprefix
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

3.3 PRUEBA 3: resolver "www.xataka.com". ¿Qué mensaje te devuelve el servicio?

Captura y Explica lo que significa con tus palabras.

Al principio, no nos deja acceder con la IP que aparece en el pantallazo porque no está autorizado, para poder acceder al sitio he tenido que declarar en el fichero `resolv.conf` otro name server, esta vez con los datos de Google, el cual si está autorizado y nos permite acceder al sitio especificado.



```
javi@epifanioDAW2:~$ nslookup www.xataka.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.xataka.com canonical name = d2t8dj4tr3q9od.cloudfront.net.
Name:   d2t8dj4tr3q9od.cloudfront.net
Address: 13.224.106.105
Name:   d2t8dj4tr3q9od.cloudfront.net
Address: 13.224.106.54
Name:   d2t8dj4tr3q9od.cloudfront.net
Address: 13.224.106.64
Name:   d2t8dj4tr3q9od.cloudfront.net
Address: 13.224.106.117
```

3.4 PRUEBA 4: Comprueba ahora que sin indicar el dominio también te resuelve el nombre gracias a la línea 'search' con el dominio por defecto a buscar que metiste en /etc/resolv.conf. resolver "ftp"

Gracias a search y el nombre por defecto que le hemos puesto a nuestro zone podemos acceder a ftp usando el comando nslookup

```
UbuntuServer-Despliegues [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.1
nameserver 8.8.8.8
options edns0 trust-ad
search epifanioDAW2.org

javierpi@ubusrv-jepi:/etc$ nslookup ftp
Server:      127.0.0.1
Address:     127.0.0.1#53

Name:   ftp.epifanioDAW2.org
Address: 192.168.1.1
```

3.5 Comprueba como el servidor DNS funciona como DNS caché mejorando los tiempos de respuesta en la segunda y posteriores búsquedas de un nombre.

P.ej. usa el comando dig para resolver la dirección www.iesgrancapitan.org y observa el tiempo que tarda. Repítelo y comprueba cuánto ha mejorado. ¿A qué se debe?

Se mejora el tiempo de conexión porque las DNS guardan la información y ya no tiene que preguntar que debe buscar y así tarda menos en devolver la información solicitada.

```
UbuntuServer-Despliegues [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
javierpi@ubusrv-jepi:/etc$ dig www.iesgrancapitan.org

; <<> DiG 9.16.1-Ubuntu <<> www.iesgrancapitan.org
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 45536
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 4096
; COOKIE: 1fee0f5da12a8c88010000006168163da8bb98aad6b1f4bd (good)
;; QUESTION SECTION:
;www.iesgrancapitan.org.          IN      A

;; ANSWER SECTION:
www.iesgrancapitan.org. 4456    IN      A      89.248.100.49

;; Query time: 104 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: jue oct 14 11:36:29 UTC 2021
;; MSG SIZE rcvd: 95
```


4. (NO OBLIGATORIO, cuenta para nota) Configuración y prueba de la zona inversa.

4.1. Configura también la zona inversa con todos y gran parte de los registros.

```
javiepi@ubusrv-jepi:/etc/bind$ sudo cp db.127 db.192
[sudo] password for javiepi:
javiepi@ubusrv-jepi:/etc/bind$ ls
bind.keys  db.192  db.local  named.conf.default-zones  rndc.key
db.0       db.255  epifanio.db  named.conf.local          zones.rfc1918
db.127     db.empty  named.conf  named.conf.options
javiepi@ubusrv-jepi:/etc/bind$ _
```

 UbuntuServer-Despliegues [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
GNU nano 4.8 db.192
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      epifanioDAW2.org. root.epifanioDAW2.org. (
                                1          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN      NS       epifanioDAW2.org.
1         IN      PTR      epifanioDAW2.org.
```

4.2. 4.2 Comprueba la sintaxis correcta de los ficheros con los comandos named-checkconf zona fichero de zona

```
javiepi@ubusrv-jepi:/etc/bind$ sudo named-checkzone www.epifanioDAW2.org /etc/bind/db.192
zone www.epifanioDAW2.org/IN: loaded serial 1
OK
javiepi@ubusrv-jepi:/etc/bind$
```

4.3. Prueba a resolver de forma inversa: nslookup IP

```
javiepi@ubusrv-jepi:/etc/bind$ systemctl restart bind9
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'named.service'.
Authenticating as: JavierEpifanio (javiepi)
Password:
==== AUTHENTICATION COMPLETE ====
javiepi@ubusrv-jepi:/etc/bind$ nslookup 192.168.1.1
1.1.168.192.in-addr.arpa      name = epifanioDAW2.org.

Authoritative answers can be found from:
```