



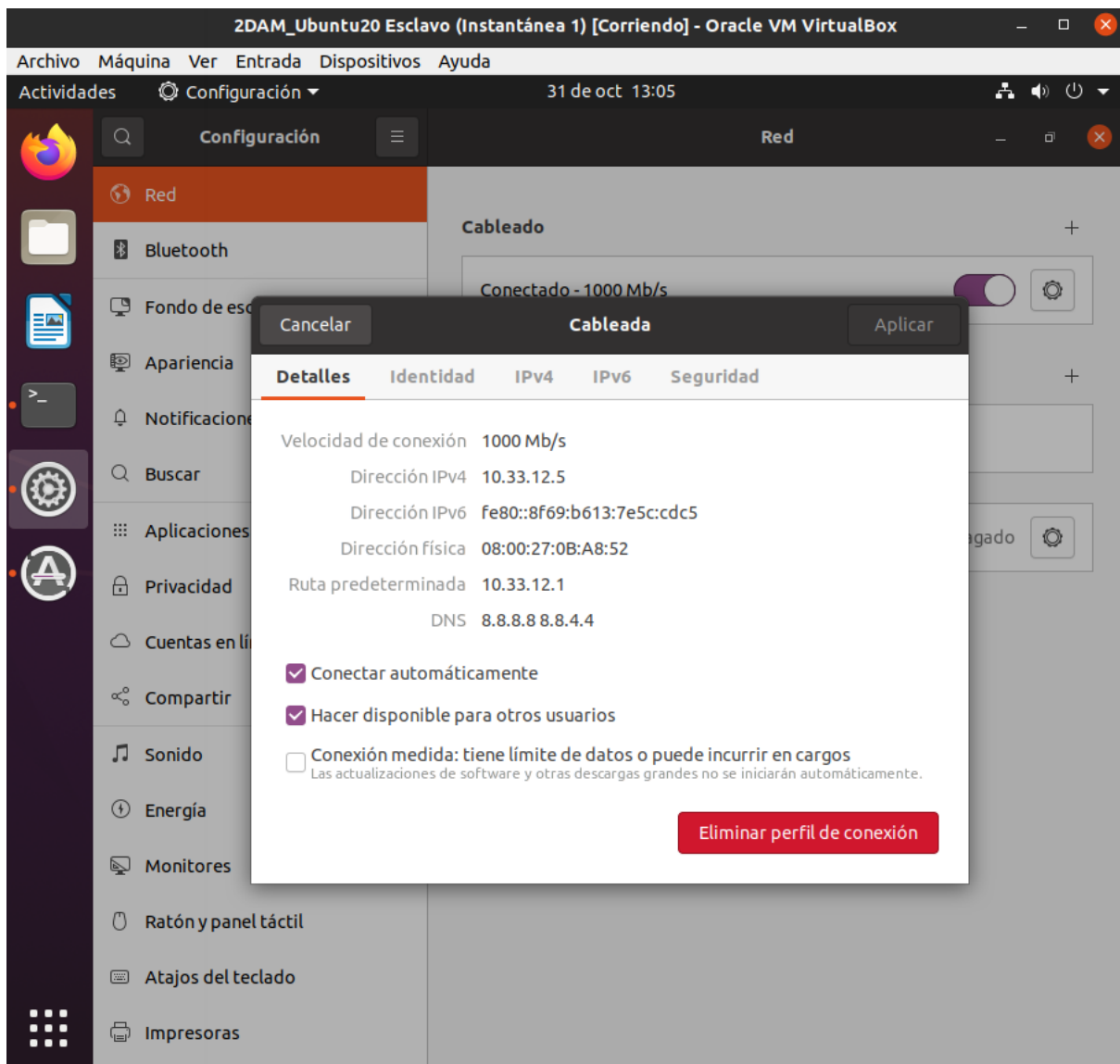
DNS Bind9 Esclavo

Nicolás López Flores

MANUAL DE CONFIGURACION DE UN SERVIDOR DNS BIND ESCLAVO EN UBUNTU	3
CONFIGURACION SERVIDOR MAESTRO	4
ZONA DIRECTA	4
ZONA INVERSA	5
VALIDACION DE ZONAS	5
CONFIGURACION ARCHIVO NAMED.CONF.LOCAL	5
CONFIGURACION SERVIDOR ESCLAVO	7
CONFIGURACION ARCHIVO NAMED.CONF.LOCAL	7
VERIFICACION DEL FUNCIONAMIENTO DE LA CONEXION ENTRE ZONAS	8
COMPROBACIONES	9
NSLOOKUP	9
PING Y DIG	10

MANUAL DE CONFIGURACION DE UN SERVIDOR DNS BIND ESCLAVO EN UBUNTU

Para la creación del servidor DNS Bind Esclavo, crearemos una **nueva MV (Máquina Virtual) Ubuntu** y en los ajustes de red cambiaremos la IP a 10.33.12.5



Una vez configurada instalaremos el paquete de **bind9** introduciendo siguiente comando en la terminal:

```
sudo apt install bind9
```

Esta máquina actuará como servidor esclavo del servidor DNS maestro configurado en la práctica anterior.

CONFIGURACION SERVIDOR MAESTRO

Debemos realizar algunos ajustes en el servidor maestro para que el DNS **incluya los registros de esta nueva máquina**. En la máquina que contiene el servidor DNS maestro, utilizaremos los siguientes comandos.

ZONA DIRECTA

```
sudo nano /etc/bind/db.daw12.leonardo.es
```

- **Incrementaremos el número de serial en la configuración SOA:** Esto permite que el servidor esclavo detecte los cambios realizados en la zona. El esclavo compara este número con el que tiene registrado, y si el serial en el maestro es mayor, iniciará una actualización de su copia.
- **Agregaremos el registro NS (servidor de nombres) correspondiente:** Esto define ubuntu-esclavo como un servidor autorizado para resolver consultas de la zona, permitiendo distribuir la carga de consultas entre el servidor maestro y el esclavo.
- **Añadiremos un registro para el host de la nueva máquina (10.33.12.5),** al que llamaremos ubuntu-esclavo. Esto le permitirá ser identificado correctamente dentro de la red DNS.

```
GNU nano 4.8                                db.daw12.leonardo.es                                Modificado
$TTL 1D
@ IN SOA daw12.leonardo.es. nicolas (
    13 ; serial
    1500 ; refresh
    600 ; retry
    172800 ; expiration
    360 ; TTL negative cache
)

@ NS lserver.daw12.leonardo.es.
@ NS ubuntu-esclavo.daw12.leonardo.es.
lserver IN A 10.33.12.4
dns1 IN CNAME wserver2012.daw12.leonardo.es.
ipcop IN A 10.33.12.1
ubuntu22 IN A 10.33.12.4
windows10 IN A 10.33.12.2
wserver2012 IN A 10.33.12.3
www IN CNAME windows10.daw12.leonardo.es.
nicolas IN CNAME windows10.daw12.leonardo.es.
@ IN MX 10 windows10.daw12.leonardo.es.
dns1 IN CNAME wserver2012.daw12.leonardo.es.
ubuntu-esclavo IN A 10.33.12.5

^G Ver ayuda  ^O Guardar    ^W Buscar     ^K Cortar Text^J Justificar  ^C Posición
^X Salir      ^R Leer fich. ^_ Reemplazar  ^U Pegar      ^T Ortografía ^_ Ir a línea
```

Ahora configuraremos la **zona inversa**, accedemos al archivo con el comando:

ZONA INVERSA

```
Sudo nano /etc/bind/named.conf.local
```

- Incrementaremos el número de **serial** en la configuración SOA

-Agregaremos el registro **NS** (Servidor de nombres)

-Agregaremos el **PTR** (Puntero)

```
GNU nano 4.8                                db.12.33.10
$TTL 1D
@ IN SOA daw12.leonardo.es nicolas (
    7 ; serial number
    1500 ; refresh
    600 ; retry
    172800 ; expire
    360 ; default TTL
)
@ IN NS lserver.daw12.leonardo.es.
@ IN NS ubuntuclavo.daw12.leonardo.es.
1 IN PTR ipcop.daw12.leonardo.es.
2 IN PTR windows10.daw12.leonardo.es.
3 IN PTR wserver2012.daw12.leonardo.es.
4 IN PTR lserver.daw12.leonardo.es.
5 IN PTR ubuntuclavo.daw12.leonardo.es.

[ 15 líneas leídas ]
^G Ver ayuda  ^O Guardar   ^W Buscar    ^K Cortar Text^J Justificar  ^C Posición
^X Salir      ^R Leer fich.^E Reemplazar ^U Pegar      ^T Ortografía ^_ Ir a línea
```

VALIDACION DE ZONAS

Una vez actualizado el servidor maestro verificaremos si ambas zonas funcionan correctamente con el siguiente comando:

```
alumno@alumnov:/etc/bind$ named-checkzone daw12.leonardo.es db.daw12.leonardo.es
zone daw12.leonardo.es/IN: loaded serial 13
OK
alumno@alumnov:/etc/bind$ named-checkzone 12.33.10 db.12.33.10
zone 12.33.10/IN: loaded serial 7
OK
```

CONFIGURACION ARCHIVO NAMED.CONF.LOCAL

Procederemos a configurar el archivo “*named.conf.local*” para permitir las transferencias de zonas al servidor esclavo.

```
Sudo nano etc/bind/named.conf.local
```

Agregaremos las filas:

-allow-transfer {10.33.12.5; }

- Esta directiva especifica qué servidores (en este caso, 10.33.12.5) están autorizados para solicitar una transferencia de zona desde el servidor maestro.
- La transferencia de zona es el proceso por el cual el servidor esclavo obtiene una copia de la zona del maestro, garantizando que ambos tengan la misma información DNS.

-notify yes

- Esta directiva indica al servidor maestro que envíe notificaciones automáticas a los servidores esclavos cada vez que haya un cambio en la zona.
- Cuando notify está activado y el número de **serial** del archivo de zona se incrementa, el maestro envía un mensaje de notificación (NOTIFY) a los esclavos configurados, indicándoles que la zona ha cambiado.
- Los servidores esclavos, al recibir esta notificación, comprueban el serial de la zona en el maestro. Si detectan que el serial del maestro es mayor, inician una **transferencia de zona** para actualizarse.
- **Con notify no**, el servidor maestro no enviará notificaciones de cambios, y los esclavos solo actualizarán la zona cuando llegue el tiempo de actualización especificado en el campo refresh del registro SOA, lo que puede resultar en una sincronización más lenta.

```
GNU nano 4.8                                named.conf.local
// Do any local configuration here
//
zone "daw12.leonardo.es" IN {
    type master;
    file "/etc/bind/db.daw12.leonardo.es";
    allow-transfer {10.33.12.5; };
    notify yes;
};

zone "12.33.10.in-addr.arpa" {
    type master;
    file "/etc/bind/db.12.33.10";
    allow-transfer {10.33.12.5; };
    notify yes;
};

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

[ 21 líneas escritas ]
^G Ver ayuda  ^O Guardar   ^W Buscar    ^K Cortar Text ^J Justificar  ^C Posición
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar      ^T Ortografía ^_ Ir a línea
```

Reiniciaremos el servidor DNS con el comando:

Sudo systemctl restart bind9

CONFIGURACION SERVIDOR ESCLAVO

Y con esto daríamos por finalizada la configuración en el servidor maestro.

Ahora iremos a la nueva máquina que va a contener el nuevo servidor DNS esclavo y editaremos el archivo “*named.conf.local*”:

CONFIGURACION ARCHIVO NAMED.CONF.LOCAL

```
Sudo nano /etc/bind/named.conf.local
```

- **file "/etc/bind/db.daw12.leonardo.es."** Define la ubicación donde el servidor esclavo almacenará la copia de la zona.
- **type slave** Indica que esta es una zona esclava, lo que significa que el servidor descargará una copia de la zona desde el servidor maestro.
- **masters { 10.33.12.4; }** Especifica la IP del servidor maestro desde donde se transferirá la zona.

```
GNU nano 4.8                                named.conf.local
//
// Do any local configuration here
//

zone "daw12.leonardo.es" {
    type slave;
    masters {10.33.12.4; };
    file "/etc/bind/db.daw12.leonardo.es.";
};

zone "12.33.10.in-addr.arpa" {
    type slave;
    masters {10.33.12.4; };
    file "/etc/bind/db.12.33.10.in-addr.arpa";
};

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

Reiniciamos el servicio para **aplicar los cambios** con el comando:

```
Sudo systemctl restart bind9
```

VERIFICACION DEL FUNCIONAMIENTO DE LA CONEXION ENTRE ZONAS

Y verificamos que nuestro servidor esclavo se haya conectado correctamente con el maestro mediante el comando:

```
Sudo tail -f /var/log/syslog
```

Nos mostrara las ultimas líneas del archivo “syslog”. Y deberá aparecer un mensaje con la dirección IP del servidor maestro seguida de un mensaje relacionado con la transferencia (Transfer status: success, Transfer completed) si hay algún error también te lo notificara.

```
alumno@alumnov:/etc/bind$ sudo systemctl restart bind9
alumno@alumnov:/etc/bind$ sudo tail -f /var/log/syslog
Nov  4 13:55:11 alumnov named[15017]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) missing from hints
Nov  4 13:55:11 alumnov named[15017]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) extra record in hints
Nov  4 13:55:12 alumnov named[15017]: zone 12.33.10.in-addr.arpa/IN: Transfer started.
Nov  4 13:55:12 alumnov named[15017]: transfer of '12.33.10.in-addr.arpa/IN' from 10.33.12.4#53: connected using 10.33.12.4#53
Nov  4 13:55:12 alumnov named[15017]: zone 12.33.10.in-addr.arpa/IN: transferred serial 7
Nov  4 13:55:12 alumnov named[15017]: transfer of '12.33.10.in-addr.arpa/IN' from 10.33.12.4#53: Transfer status: success
Nov  4 13:55:12 alumnov named[15017]: transfer of '12.33.10.in-addr.arpa/IN' from 10.33.12.4#53: Transfer completed: 1 messages, 9 records, 333 bytes, 0.004 secs (83250 bytes/sec) (serial 7)
Nov  4 13:55:12 alumnov named[15017]: zone 12.33.10.in-addr.arpa/IN: sending notifies (serial 7)
Nov  4 13:55:12 alumnov named[15017]: dumping master file: /etc/bind/tmp-VJtgShvzNu: open: permission denied
Nov  4 13:55:12 alumnov kernel: [11416.974518] audit: type=1400 audit(1730724912.030:49): apparmor="DENIED" operation="mknod" profile="/usr/sbin/named" name="/etc/bind/tmp-VJtgShvzNu" pid=15017 comm="isc-net-0000" requested_mask="c" denied_mask="c" fsuid=127 ouid=127
```


COMPROBACIONES

NSLOOKUP

```
alumno@alumnoov:/etc/bind$ nslookup
> server 10.33.12.5
Default server: 10.33.12.5
Address: 10.33.12.5#53
> 10.33.12.1
1.12.33.10.in-addr.arpa name = ipcop.daw12.leonardo.es.
> 10.33.12.2
2.12.33.10.in-addr.arpa name = windows10.daw12.leonardo.es.
> 10.33.12.3
3.12.33.10.in-addr.arpa name = wserver2012.daw12.leonardo.es.
> 10.33.12.4
4.12.33.10.in-addr.arpa name = lserver.daw12.leonardo.es.
> 10.33.12.5
5.12.33.10.in-addr.arpa name = ubuntu22.daw12.leonardo.es.
> ubuntu22.daw12.leonardo.es
Server:      10.33.12.5
Address:     10.33.12.5#53

Name:   ubuntu22.daw12.leonardo.es
Address: 10.33.12.5
> www.daw12.leonardo.es
Server:      10.33.12.5
Address:     10.33.12.5#53

www.daw12.leonardo.es canonical name = windows10.daw12.leonardo.es.
Name:   windows10.daw12.leonardo.es
Address: 10.33.12.2
> nicolas.daw12.leonardo.es
Server:      10.33.12.5
Address:     10.33.12.5#53

nicolas.daw12.leonardo.es canonical name = windows10.daw12.leonardo.es.
Name:   windows10.daw12.leonardo.es
Address: 10.33.12.2

> ipcop.daw12.leonardo.es
Server:      10.33.12.5
Address:     10.33.12.5#53

Name:   ipcop.daw12.leonardo.es
Address: 10.33.12.1
> wserver2012.daw12.leonardo.es
Server:      10.33.12.5
Address:     10.33.12.5#53

Name:   wserver2012.daw12.leonardo.es
Address: 10.33.12.3
> windows10.daw12.leonardo.es
Server:      10.33.12.5
Address:     10.33.12.5#53

Name:   windows10.daw12.leonardo.es
Address: 10.33.12.2
> ubuntu22.daw12.leonardo.es
Server:      10.33.12.5
Address:     10.33.12.5#53

Name:   ubuntu22.daw12.leonardo.es
Address: 10.33.12.4
> █
```

PING Y DIG

```
alumno@alumnov:/etc/bind$ ping -c 3 10.33.12.5
PING 10.33.12.5 (10.33.12.5) 56(84) bytes of data.
64 bytes from 10.33.12.5: icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from 10.33.12.5: icmp_seq=2 ttl=64 time=0.052 ms
64 bytes from 10.33.12.5: icmp_seq=3 ttl=64 time=0.049 ms

--- 10.33.12.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2048ms
rtt min/avg/max/mdev = 0.044/0.048/0.052/0.003 ms
alumno@alumnov:/etc/bind$ dig @10.33.12.5 daw12.leonardo.es

; <<>> DiG 9.18.28-0ubuntu0.20.04.1-Ubuntu <<>> @10.33.12.5 daw12.leonardo.es
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 60101
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 724938fd8d7e6239010000006728c7811f1f2500c43c9e58 (good)
;; QUESTION SECTION:
;daw12.leonardo.es.          IN      A

;; AUTHORITY SECTION:
daw12.leonardo.es.          360     IN      SOA     daw12.leonardo.es. nicolas.daw12.leonardo.es. 13 1500 600 172800 360

;; Query time: 0 msec
;; SERVER: 10.33.12.5#53(10.33.12.5) (UDP)
;; WHEN: Mon Nov 04 14:09:21 CET 2024
;; MSG SIZE rcvd: 118
```