

PRÁCTICA 5.4

INSTALACIÓN, CONFIGURACIÓN Y GESTIÓN DE UN SERVIDOR DNS

FECHA DE INICIO: 23/01/2025

FECHA DE FINALIZACIÓN ESPERADA: 27/01/2025

RA ASOCIADO: RA5. Verifica la ejecución de aplicaciones web comprobando los parámetros de configuración de servicios de red.

Contenido

OBJETIVOS	1
ENUNCIADO	2
PARTE 1. INSTALACIÓN Y CONFIGURACIÓN DE BIND9	2
PARTE 2. CONFIGURACIÓN DEL SERVIDOR UBUNTU CON BIND9 COMO SERVIDOR DNS	4
CACHÉ	4
PARTE 3. CONFIGURACIÓN DE UN SERVIDOR DNS MAESTRO PARA LA ZONA	11
"INFORMATICA.ORG." CREACIÓN DE ZONA MAESTRA DIRECTA	11
PARTE 4. CONFIGURACIÓN DEL SERVIDOR DNS MAESTRO PARA LA ZONA INVERSA.....	15
"168.192.IN-ADDR.ARPA"	15
PARTE 5. GESTIÓN DEL SERVIDOR DNS. INSTALACIÓN Y CONFIGURACIÓN DE WEBMIN.....	17
Instalación y Configuración de Webmin en el Servidor Ubuntu	17
Pruebas de Configuración del Servidor DNS usando Webmin	20
DOCUMENTACIÓN	28

OBJETIVOS

- Instalar y configurar BIND9 en un servidor Ubuntu para que funcione como servidor DNS.
- Configurar la red del servidor y del cliente para permitir la comunicación y el uso del servidor DNS.
- Configurar BIND9 para funcionar como servidor DNS caché con reenviadores a servidores DNS públicos.

- Crear una zona DNS directa con registros A, CNAME y MX.
- Configurar una zona inversa y comprobar la resolución de nombres con nslookup.

ENUNCIADO

PARTE 1. INSTALACIÓN Y CONFIGURACIÓN DE BIND9

1) Configura una máquina virtual con Ubuntu Server en NAT y configuración de red automática.

Red

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ *Habilitar adaptador de red*

Conectado a: NAT

Nombre:

Red

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ *Habilitar adaptador de red*

Conectado a: Red interna

Nombre: intnet

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

```

adrian@servidor-adrian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:48:0e:67 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 81115sec preferred_lft 81115sec
    inet6 fd00::a00:27ff:fe48:e67/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86183sec preferred_lft 14183sec
    inet6 fe80::a00:27ff:fe48:e67/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:54:ac:e1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.222.1/24 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe54:ace1/64 scope link
        valid_lft forever preferred_lft forever
adrian@servidor-adrian:~$ _

```

2) Instala la aplicación “bind9” en el servidor para que pueda trabajar como servidor DNS.

- Abre el terminal e introduce el comando de instalación:

```

sudo apt update
sudo apt install bind9 bind9-utils -y

```

3) Comprueba que la aplicación está instalada correctamente verificando su estado.

- Introduce el comando correspondiente para ver el estado del servicio:

```

sudo service bind9 status  ó
systemctl status bind9.service

```

Una vez realizada la instalación esta sería la revisión:

```

adrian@servidor-adrian:~$ systemctl status bind9.service
• named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2025-01-29 23:56:51 UTC; 14min ago
     Docs: man:named(8)
   Main PID: 2681 (named)
    Tasks: 8 (limit: 4564)
   Memory: 7.1M
      CPU: 690ms
   CGroup: /system.slice/named.service
           └─2681 /usr/sbin/named -u bind

ene 29 23:57:28 servidor-adrian named[2681]: validating QIDPTSN7PHFA4KH4FBHLL0NRHAD3F493.webmin.c>
ene 29 23:57:40 servidor-adrian named[2681]: validating webmin.com/SOA: no valid signature found
ene 29 23:57:40 servidor-adrian named[2681]: validating I9A32AR57CKC18CAUN99K9K9UNH2RCMR.webmin.c>
ene 29 23:57:40 servidor-adrian named[2681]: validating 56TTAA9J2I9OASKRBSADUHO2DHTHU3V8.webmin.c>
ene 29 23:57:40 servidor-adrian named[2681]: validating 5KJ0Q090B7TCCG0SEC2U76KBJ1F1DUIQ.webmin.c>
ene 29 23:57:40 servidor-adrian named[2681]: validating download.webmin.com/A: no valid signature f>
ene 29 23:57:40 servidor-adrian named[2681]: validating download.webmin.com/AAAA: no valid signatur>
ene 30 00:02:47 servidor-adrian named[2681]: validating announce.webmin.com/A: no valid signature f>
ene 30 00:02:47 servidor-adrian named[2681]: validating webmin.com/SOA: no valid signature found
ene 30 00:02:47 servidor-adrian named[2681]: validating R619EOI7BOS6M6KS6IU07NAI3B4SDLD2.webmin.c>
lines 1-21/21 (END)

```

PARTE 2. CONFIGURACIÓN DEL SERVIDOR UBUNTU CON BIND9 COMO SERVIDOR DNS CACHE

1) Configuración de red del servidor Ubuntu • Agregar una tarjeta de red adicional:

Antes de encender la máquina, añade una tarjeta de red desde la configuración VirtualBox.

Configura:

- **Primera tarjeta de red:** NAT (para acceso a internet).
- **Segunda tarjeta de red:** Red interna (para comunicación con el cliente).
- **Editar la configuración de red:** En Ubuntu Server con **Netplan** (versión reciente), edita el archivo de configuración en `/etc/netplan/01-netcfg.yaml`:

```

network:
  version: 2
  ethernet:
    enp0s3:
      dhcp4: true # Red NAT
    enp0s8:
      addresses:
        - 192.168.222.1/24 # Dirección estática para la red interna

```

Asegúrate de usar los nombres correctos de las interfaces (`enp0s3`, `enp0s8`). Puedes verificarlos con `ip a`.

- **Aplica cambios:** Ejecuta:
`sudo netplan apply`
- **Activar reenvío de paquetes (ip_forward):** Para permitir que el tráfico entre las redes NAT e interna pueda circular, habilita el reenvío de paquetes editando el archivo de configuración del sistema: `sudo nano /etc/sysctl.conf` ◦ Descomenta o agrega la siguiente línea:
`net.ipv4.ip_forward = 1` ◦
Aplica los cambios con:
`sudo sysctl -p`

Habilitar NAT (mascarado) en el servidor Ubuntu:

1. Habilitar enmascaramiento de IP:

- Para permitir que el tráfico de la red interna se enrute a través de la red NAT, ejecuta el siguiente comando:

```
sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

Nota: Asegúrate de que enp0s3 es la interfaz correcta de la red NAT (puedes verificar las interfaces con `ip a`).

2. Hacer que la configuración de iptables persista:

- Para que la configuración del NAT persista después de un reinicio, guarda las reglas de iptables con el siguiente comando:

```
sudo sh -c "iptables-save > /etc/iptables/rules.v4"
```

```
adrian@servidor-adrian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:48:0e:67 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 81115sec preferred_lft 81115sec
    inet6 fd00::a00:27ff:fe48:e67/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86183sec preferred_lft 14183sec
    inet6 fe80::a00:27ff:fe48:e67/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:54:ac:e1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.222.1/24 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe54:ace1/64 scope link
        valid_lft forever preferred_lft forever
adrian@servidor-adrian:~$ _
```

2) Configuración del cliente Ubuntu para usar el servidor DNS

- **Configura los parámetros de red del cliente:**
 - a) **Accede a la configuración de red:**
 - a. Haz clic en el icono de red en la barra superior (generalmente en la esquina derecha).
 - b. Selecciona la opción "Configuración de red" o "Configuración de conexiones de red" (dependiendo de la versión de Ubuntu Desktop).
 - b) **Selecciona la conexión:**
 - a. En la ventana de configuración de red, busca la conexión de red activa (por ejemplo, Ethernet).
 - b. Haz clic en el icono de engranaje o selecciona "Configuración".
 - c) **Configura los parámetros de red manualmente:**
 - a. Ve a la pestaña **IPv4**.
 - b. Cambia el método de "Automático (DHCP)" a "Manual".
 - c. Ingresa los siguientes parámetros:
 - i. **Dirección IP:** 192.168.222.2
 - ii. **Máscara de red:** 255.255.255.0 o el prefijo /24.
 - iii. **Puerta de enlace (Gateway):** Si tienes un servidor que actúa como puerta de enlace, coloca su IP aquí (por ejemplo, 192.168.222.1).
 - iv. **Servidores DNS:** Escribe la dirección del servidor DNS (por ejemplo, 192.168.222.1).
 - d) **Guarda los cambios:**
 - a. Haz clic en "Guardar" o "Aplicar".
 - b. Apaga y enciende la interfaz para actualizar

Cancelar **Cableada** Aplicar

Detalles Identidad **IPv4** IPv6 Seguridad

Método IPv4

☐ Automático (DHCP) ☐ Sólo enlace local

☒ Manual ☐ Desactivar

☐ Compartida con otros equipos

Direcciones

Dirección	Máscara de red	Puerta de enlace	
192.168.222.2	255.255.255.0	192.168.222.1	

DNS Automático ☒

192.168.222.1

Direcciones IP separadas por comas

- **Verifica la conectividad:**

- Abre una

terminal y ejecuta los siguientes comandos:
`ping 192.168.222.1` (`nslookup www.google.com`
DNS).

- `ping 192.168.222.1` para comprobar conexión con el servidor).
- `dig www.google.com` (para comprobar resolución

```
adrian@cliente-ubuntu:~$ ping 192.168.222.1
PING 192.168.222.1 (192.168.222.1) 56(84) bytes of data.
64 bytes from 192.168.222.1: icmp_seq=1 ttl=64 time=1.14 ms
64 bytes from 192.168.222.1: icmp_seq=2 ttl=64 time=0.758 ms
64 bytes from 192.168.222.1: icmp_seq=3 ttl=64 time=0.938 ms
```

```
adrian@cliente-ubuntu:~$ nslookup www.google.com 192.168.222.1
Server:      192.168.222.1
Address:     192.168.222.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.200.132
Name:   www.google.com
Address: 2a00:1450:4003:808::2004

adrian@cliente-ubuntu:~$
```

3) Configuración del servidor DNS con reenviadores de Google

- **Configura los reenviadores:** Edita el archivo `/etc/bind/named.conf.options`:
`sudo nano /etc/bind/named.conf.options` Asegúrate

de que contiene:

```
options {
    directory "/var/cache/bind";

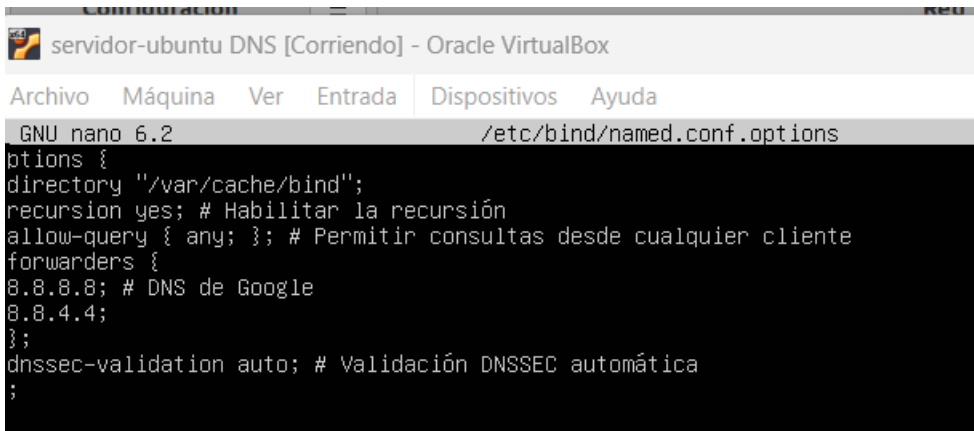
    recursion yes;      # Habilitar la recursión
    allow-query { any; }; # Permitir consultas desde cualquier cliente

    forwarders {
        8.8.8.8;      # DNS de Google
        8.8.4.4;
    };

    dnssec-validation auto; # Validación DNSSEC automática
};
```

- **Reinicia BIND9:**
`sudo systemctl restart bind9`

Tiene que quedar tal que así:



```
servidor-ubuntu DNS [Corriendo] - Oracle VirtualBox
GNU nano 6.2 /etc/bind/named.conf.options
options {
directory "/var/cache/bind";
recursion yes; # Habilitar la recursión
allow-query { any; }; # Permitir consultas desde cualquier cliente
forwarders {
8.8.8.8; # DNS de Google
8.8.4.4;
};
dnssec-validation auto; # Validación DNSSEC automática
;
```

4) Pruebas con nslookup

Desde el cliente Ubuntu, realiza consultas DNS para comprobar la resolución de nombres:

```
nslookup www.uned.es
www.twitter.com nslookup
www.amazon.es nslookup
www.ubuntu.com
```

Verifica que las respuestas provengan del servidor Ubuntu configurado.

```

adrian@cliente-ubuntu:~$ nslookup www.uned.es
nslookup www.twitter.com
nslookup www.amazon.es
nslookup www.ubuntu.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.uned.es   canonical name = k8swin.uned.es.
Name:   k8swin.uned.es
Address: 62.204.213.111

Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.twitter.com canonical name = twitter.com.
Name:   twitter.com
Address: 104.244.42.129

Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.amazon.es canonical name = tp.1fe6d5bb2-frontier.amazon.es.
tp.1fe6d5bb2-frontier.amazon.es canonical name = d12yd29zmqmfwy.cloudfront.net.
Name:   d12yd29zmqmfwy.cloudfront.net
Address: 18.67.249.20
Name:   d12yd29zmqmfwy.cloudfront.net
Address: 2600:9000:24de:7200:15:da86:494:7521

```

```

Name:   d12yd29zmqmfwy.cloudfront.net
Address: 2600:9000:24de:1800:15:da86:494:7521
Name:   d12yd29zmqmfwy.cloudfront.net
Address: 2600:9000:24de:1000:15:da86:494:7521
Name:   d12yd29zmqmfwy.cloudfront.net
Address: 2600:9000:24de:9c00:15:da86:494:7521
Name:   d12yd29zmqmfwy.cloudfront.net
Address: 2600:9000:24de:9e00:15:da86:494:7521
Name:   d12yd29zmqmfwy.cloudfront.net
Address: 2600:9000:24de:cc00:15:da86:494:7521
Name:   d12yd29zmqmfwy.cloudfront.net
Address: 2600:9000:24de:b200:15:da86:494:7521
Name:   d12yd29zmqmfwy.cloudfront.net
Address: 2600:9000:24de:4a00:15:da86:494:7521

Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.ubuntu.com
Address: 185.125.190.29
Name:   www.ubuntu.com
Address: 185.125.190.20
Name:   www.ubuntu.com
Address: 185.125.190.21
Name:   www.ubuntu.com
Address: 2620:2d:4000:1::27
Name:   www.ubuntu.com
Address: 2620:2d:4000:1::26
Name:   www.ubuntu.com

```

5) Mostrar la caché de consultas

- **Generar y visualizar la caché de consultas:** En el servidor, ejecuta:

```
sudo rndc dumpdb -cache
```

```
sudo nano /var/cache/bind/named_dump.db
```

Observa las consultas realizadas desde el cliente en el archivo named_dump.db.

```
GNU nano 6.2 /var/cache/bind/named_dump.db

Start view _default

Cache dump of view '_default' (cache _default)

using a 0 second stale ttl
$DATE 20250130002216
$ secure
516912 IN NS a.root-servers.net.
516912 IN NS b.root-servers.net.
516912 IN NS c.root-servers.net.
516912 IN NS d.root-servers.net.
516912 IN NS e.root-servers.net.
516912 IN NS f.root-servers.net.
516912 IN NS g.root-servers.net.
516912 IN NS h.root-servers.net.
516912 IN NS i.root-servers.net.
516912 IN NS j.root-servers.net.
516912 IN NS k.root-servers.net.
516912 IN NS l.root-servers.net.
516912 IN NS m.root-servers.net.
$ secure
516912 RRSIG NS 8 0 518400 (
20250211230000 20250129220000 26470 .
kS33VHF5bJw1S+434xLQA74SY0je1peVibTm
AKyXxIahgx39jxG71812I0rm46RNmvin/R0+
gUQOVZyFku0ohyDxwxkIsF4r9hCKCmQQSGEu
Mhanh2opu/q0kw50Z1ZDu223jH2qt7hLTyNk
10CeCmfF0VEaeYK1xFEGvkXu3sYpNxcHJwZ
yBFZiensevW4WS3wkHrqk0zviKb111kE+ZN1
wtd2+BuGF2YGtMIJKDgjUrQ3+0ys8P0ExMZ8
CNRZ+8x/ZCIK6t4W+ix5jfiTPzbE5LFmfJvB
[ Read 1196 lines ]

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify    ^_ Go To Line M-E Redo
```

PARTE 3. CONFIGURACIÓN DE UN SERVIDOR DNS MAESTRO PARA LA ZONA "INFORMATICA.ORG." CREACIÓN DE ZONA MAESTRA DIRECTA

Instrucciones:**1) Crea los archivos de zona para la zona "informatica.org."**

- Abre el archivo named.conf.local: `sudo nano /etc/bind/named.conf.local`
- Introduce al final de este archivo: `zone "informatica.org" {
type master;
file "/etc/bind/db.informatica.org";
};`
- Copia la plantilla con el nombre db.informatica.org: `sudo cp /etc/bind/db.local
/etc/bind/db.informatica.org`
- Edita el archivo de zona: `sudo nano /etc/bind/db.informatica.org`
- Realiza las siguientes modificaciones:
 - Cambia **localhost** por **informatica.org**.
 - Sustituye la dirección IP por la del servidor.
- Verificar que el archivo no contiene errores antes de reiniciar el servicio:
`named-checkzone informatica.org /etc/bind/db.informatica.org`
- Reiniciar el servicio Bind9 si no hay errores:
`sudo systemctl restart bind9.service`

2) Añade registros para resolver las siguientes consultas:

- **Registros A:**
 - `www.informatica.org. → 122.122.125.46`
 - `penacastillo.informatica.org. → 34.1.34.32`
 - `alisal.informatica.org. → 192.168.52.100`
 - `torrelavega.informatica.org. → 100.168.168.10`
 - `castro.informatica.org. → 192.35.35.35`
- Edita el archivo db.informatica.org: `sudo nano /etc/bind/db.informatica.org`
- Añade los registros A:


```
www.informatica.org.    IN A 122.122.125.46
penacastillo.informatica.org. IN A 34.1.34.32
alisal.informatica.org.  IN A 192.168.52.100
torrelavega.informatica.org. IN A 100.168.168.10
castro.informatica.org.  IN A 192.35.35.35
```
- Verifica el archivo de zona: `named-checkzone informatica.org /etc/bind/db.informatica.org`
- Reinicia Bind9 si no hay errores:
`sudo systemctl restart bind9.service`

3) Añade alias para los registros anteriores:

- **Alias (CNAME):**
 - `web.informatica.org. → www.informatica.org.`
 - `ateca.informatica.org. → penacastillo.informatica.org.`
 - `atenea.informatica.org. → alisal.informatica.org.`
 - `aula3.informatica.org. → torrelavega.informatica.org.`
 - `aula5.informatica.org. → castro.informatica.org.`

- Edita el archivo db.informatica.org: `sudo nano /etc/bind/db.informatica.org`
 - Añade los registros CNAME:
`web.informatica.org. IN CNAME www.informatica.org.`
`ateca.informatica.org. IN CNAME penacastillo.informatica.org.`
`atenea.informatica.org. IN CNAME alisal.informatica.org.`
`aula3.informatica.org. IN CNAME torrelavega.informatica.org.`
`aula5.informatica.org. IN CNAME castro.informatica.org.`
 - Verifica el archivo de zona: `named-checkzone informatica.org /etc/bind/db.informatica.org`
 - Reinicia Bind9 si no hay errores:
`sudo systemctl restart bind9.service`
-

4) Añade registros MX para los servidores de correo:

- Servidores de correo:
 - correo.informatica.org. (prioridad 10)
 - email35.arlo.es. (prioridad 20)
 - Edita el archivo db.informatica.org: `sudo nano /etc/bind/db.informatica.org` • Añade los registros MX:
`@ IN MX 10 correo.informatica.org.`
`@ IN MX 20 email35.arlo.es.`
 - Verifica el archivo de zona: `named-checkzone informatica.org /etc/bind/db.informatica.org`
 - Reinicia Bind9 si no hay errores:
`sudo systemctl restart bind9.service`
-

Debería quedar el archivo modificado tal que así:

```
GNU nano 6.2 /etc/bind/db.informatica.org
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      informatica.org. root.informatica.org. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN      NS       informatica.org.
@         IN      A        192.168.222.1
@         IN      AAAA     ::1

www.informatica.org. IN A 122.122.125.46
penacastillo.informatica.org. IN A 34.1.34.32
alisal.informatica.org. IN A 192.168.52.100
torrelavega.informatica.org. IN A 100.168.168.10
castro.informatica.org. IN A 192.35.35.35

web.informatica.org. IN CNAME www.informatica.org.
ateca.informatica.org. IN CNAME penacastillo.informatica.org.
atenea.informatica.org. IN CNAME alisal.informatica.org.
aula3.informatica.org. IN CNAME torrelavega.informatica.org.
aula5.informatica.org. IN CNAME castro.informatica.org.

@ IN MX 10 correo.informatica.org.
@ IN MX 20 email35.arlo.es.
```

[Read 29 Lines]

Comprobación del servidor DNS:

1. Configura el cliente Ubuntu para usar el servidor DNS.
2. Usa nslookup en el cliente para verificar los registros:

```
nslookup -type=mx informatica.org
web.informatica.org
nslookup www.informatica.org
```

```

adrian@cliente-ubuntu:~$ nslookup web.informatica.org 192.168.222.1
Server:      192.168.222.1
Address:     192.168.222.1#53

web.informatica.org    canonical name = www.informatica.org.
Name:   www.informatica.org
Address: 122.122.125.46

adrian@cliente-ubuntu:~$ nslookup www.informatica.org 192.168.222.1
Server:      192.168.222.1
Address:     192.168.222.1#53

Name:   www.informatica.org
Address: 122.122.125.46

adrian@cliente-ubuntu:~$ nslookup -type=mx informatica.org 192.168.222.1
Server:      192.168.222.1
Address:     192.168.222.1#53

informatica.org mail exchanger = 20 email35.arlo.es.
informatica.org mail exchanger = 10 correo.informatica.org.

```

PARTE 4. CONFIGURACIÓN DEL SERVIDOR DNS MAESTRO PARA LA ZONA INVERSA "168.192.IN-ADDR.ARPA"

1) Crea los archivos de zona para la zona inversa:

- Abre el archivo named.conf.local: `sudo nano /etc/bind/named.conf.local` • Introduce al final de este archivo:

```

zone "168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};

```

- Copia la plantilla con el nombre db.192:

```
sudo cp /etc/bind/db.127 /etc/bind/db.192
```

- Debes indicar el nombre de la zona: El nombre de la zona es "168.192.in-addr.arpa" como está especificado en el archivo named.conf.local.

2) Añadir registros PTR en el archivo de zona inversa:

- Editar el archivo db.192:
`sudo nano /etc/bind/db.192`
- Añade los siguientes registros PTR para resolver las consultas especificadas:

```

123.1 IN PTR aula1.agl.org.
215.3 IN PTR aula2.alisal.es.
217.2 IN PTR aula3.decroly.org.
129.23 IN PTR aula4.miguelherrero.edu.
131.13 IN PTR aula5.colegio.edu.

```

3) Verificar que el archivo de zona no contiene errores:

- Utilizar el comando `named-checkzone` para validar el archivo de zona:

`named-checkzone 168.192.in-addr.arpa /etc/bind/db.192` 4)

Reiniciar el servicio Bind9 si no hay errores:

- Reiniciar el servicio:
`sudo service bind9 restart`

```
GNU nano 6.2 /etc/bind/db.192
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@ IN SOA localhost. root.localhost. (
    1          ; Serial
    604800     ; Refresh
    86400      ; Retry
    2419200    ; Expire
    604800 )   ; Negative Cache TTL
;
@ IN NS localhost.
1.0.0 IN PTR localhost.
123.1 IN PTR aula1.ag1.org.
215.3 IN PTR aula2.alisal.es.
217.2 IN PTR aula3.decroly.org.
129.23 IN PTR aula4.miguelherrero.edu.
131.13 IN PTR aula5.colegio.edu.
```

Comprobación del Servidor DNS Inverso 1)

Configurar el cliente Ubuntu:

- Asignar una dirección IP estática en el cliente y asegurarse de que esté en la misma red que el servidor.
- Editar el archivo `/etc/resolv.conf` para añadir la dirección del servidor DNS:
`sudo nano /etc/resolv.conf`
- Añadir:
`nameserver IP_del_servidor`

```
GNU nano 6.2 /etc/resolv.conf
nameserver 192.168.222.1
```

2) Conectar el cliente y el servidor en una red interna.

3) Verificar la resolución de nombres inversa desde el cliente:

- Usar la herramienta `nslookup` en el cliente para comprobar las consultas PTR:
`nslookup 192.168.1.123`
`nslookup 192.168.23.12`

Si todo está configurado correctamente, el comando devolverá el nombre DNS correspondiente (FQDN).

```
adrian@cliente-ubuntu:~$ nslookup 192.168.1.123
nslookup 192.168.3.215
nslookup 192.168.2.217
nslookup 192.168.23.129
nslookup 192.168.13.131
123.1.168.192.in-addr.arpa      name = aula1.agl.org.

Authoritative answers can be found from:

215.3.168.192.in-addr.arpa      name = aula2.alisal.es.

Authoritative answers can be found from:

217.2.168.192.in-addr.arpa      name = aula3.decroly.org.

Authoritative answers can be found from:

129.23.168.192.in-addr.arpa     name = aula4.miguelherrero.edu.

Authoritative answers can be found from:

131.13.168.192.in-addr.arpa     name = aula5.colegio.edu.

Authoritative answers can be found from:

adrian@cliente-ubuntu:~$
```

PARTE 5. GESTIÓN DEL SERVIDOR DNS. INSTALACIÓN Y CONFIGURACIÓN DE WEBMIN

Webmin se puede instalar tanto en el **servidor Ubuntu** como en un equipo dedicado para administrar otros servidores. Sin embargo, lo más común es instalar Webmin directamente en el **servidor Ubuntu** y acceder a él desde el cliente mediante un navegador web.

Instalación y Configuración de Webmin en el Servidor Ubuntu

1. Actualizar el sistema:

Asegúrate de que el servidor tiene los paquetes actualizados:

```
sudo apt update && sudo apt upgrade -y
```

2. Agregar el repositorio de Webmin:

- Editar el archivo de repositorios:

```
sudo nano /etc/apt/sources.list
```
- Añadir la línea siguiente al final del archivo: **deb**

```
http://download.webmin.com/download/repository sarge contrib
```

- Importar la clave GPG para el repositorio: `wget -qO - http://www.webmin.com/jcameron-key.asc | sudo apt-key add -`

3. Instalar Webmin:

Actualizar la lista de paquetes y luego instalar Webmin:

```
sudo apt update
```

```
sudo apt install webmin -y
```

4. Configurar el acceso remoto:

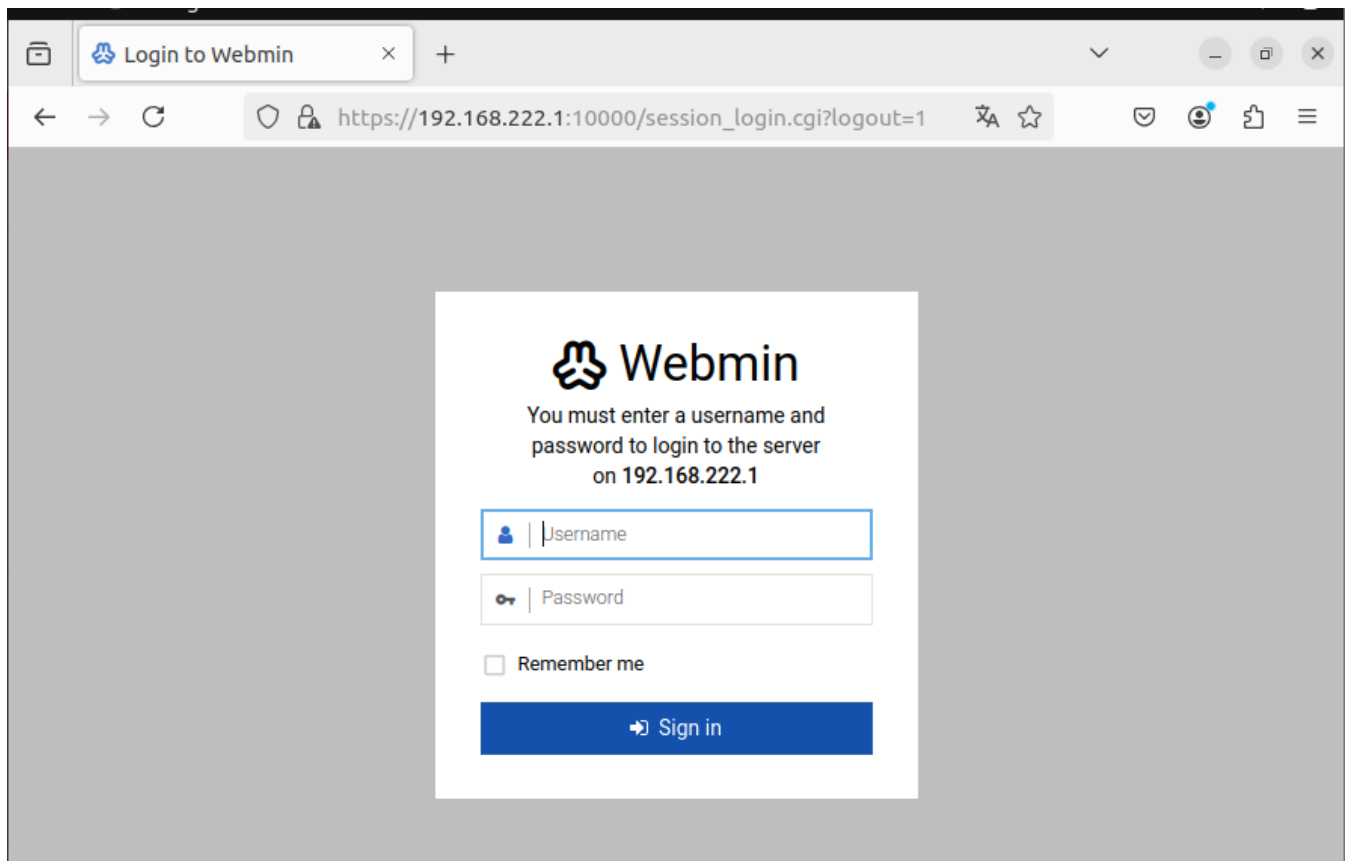
Webmin usa el puerto **10000** por defecto. Asegúrate de que este puerto esté abierto en el firewall:

```
bash
```

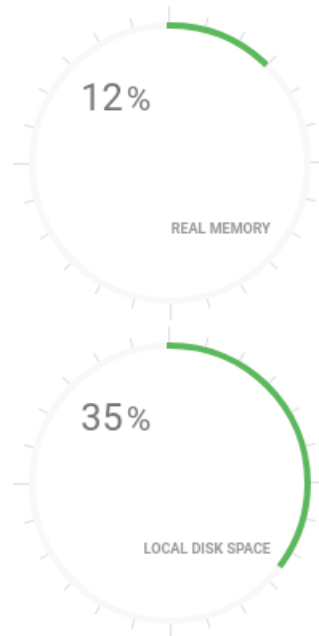
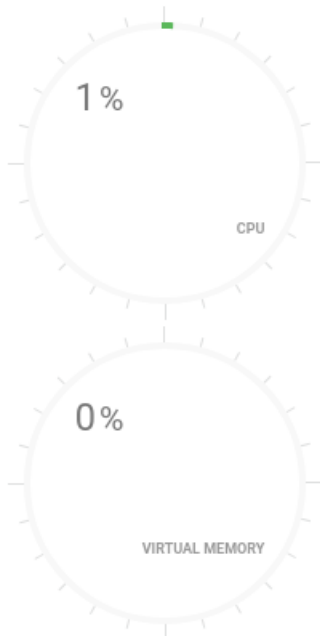
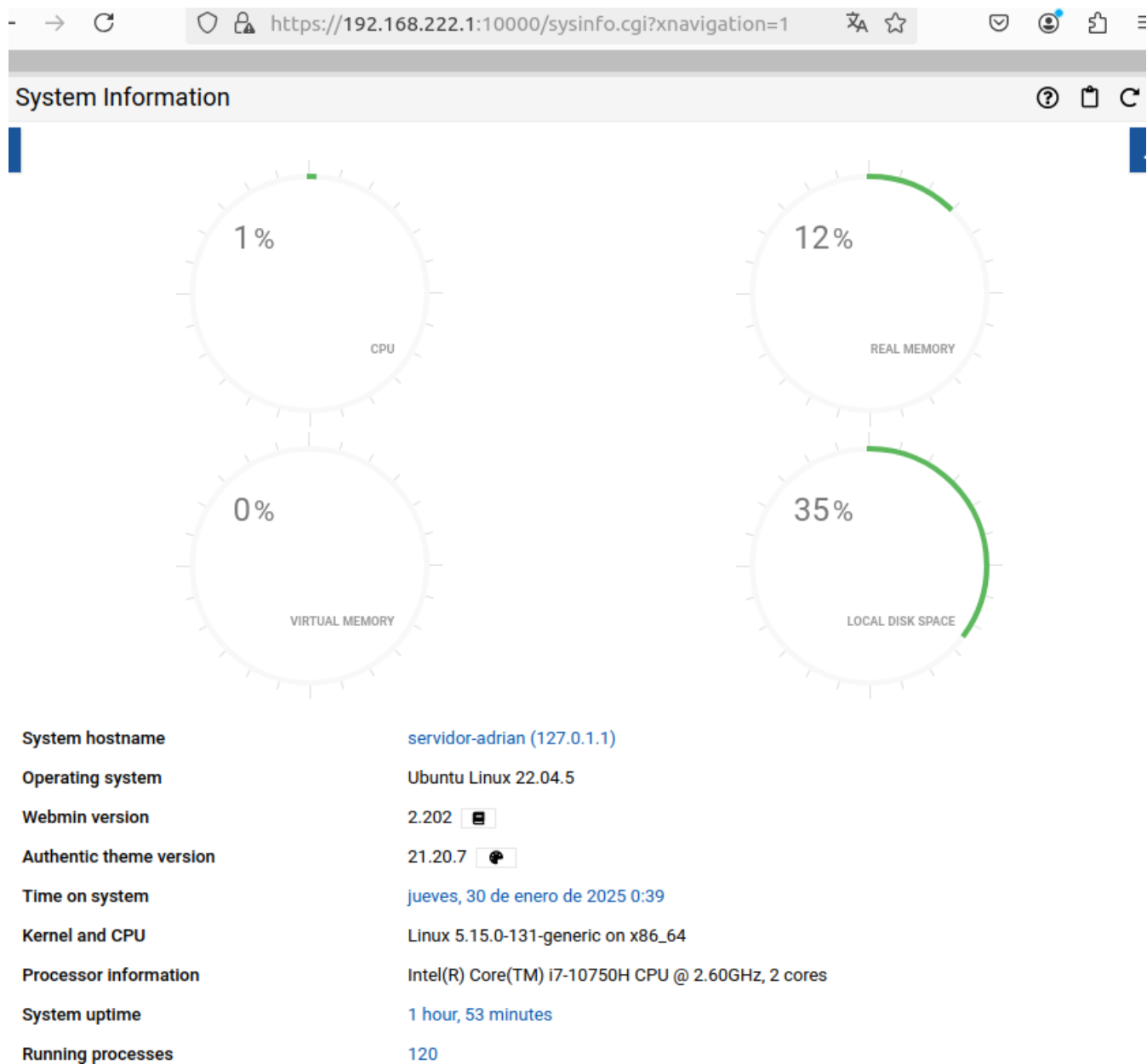
```
sudo ufw allow 10000/tcp
```

```
sudo ufw reload
```

Si has seguido los pasos correctamente tendrías que poder aceptar en la web:



Inicia sesión con un usuario con permisos de root:

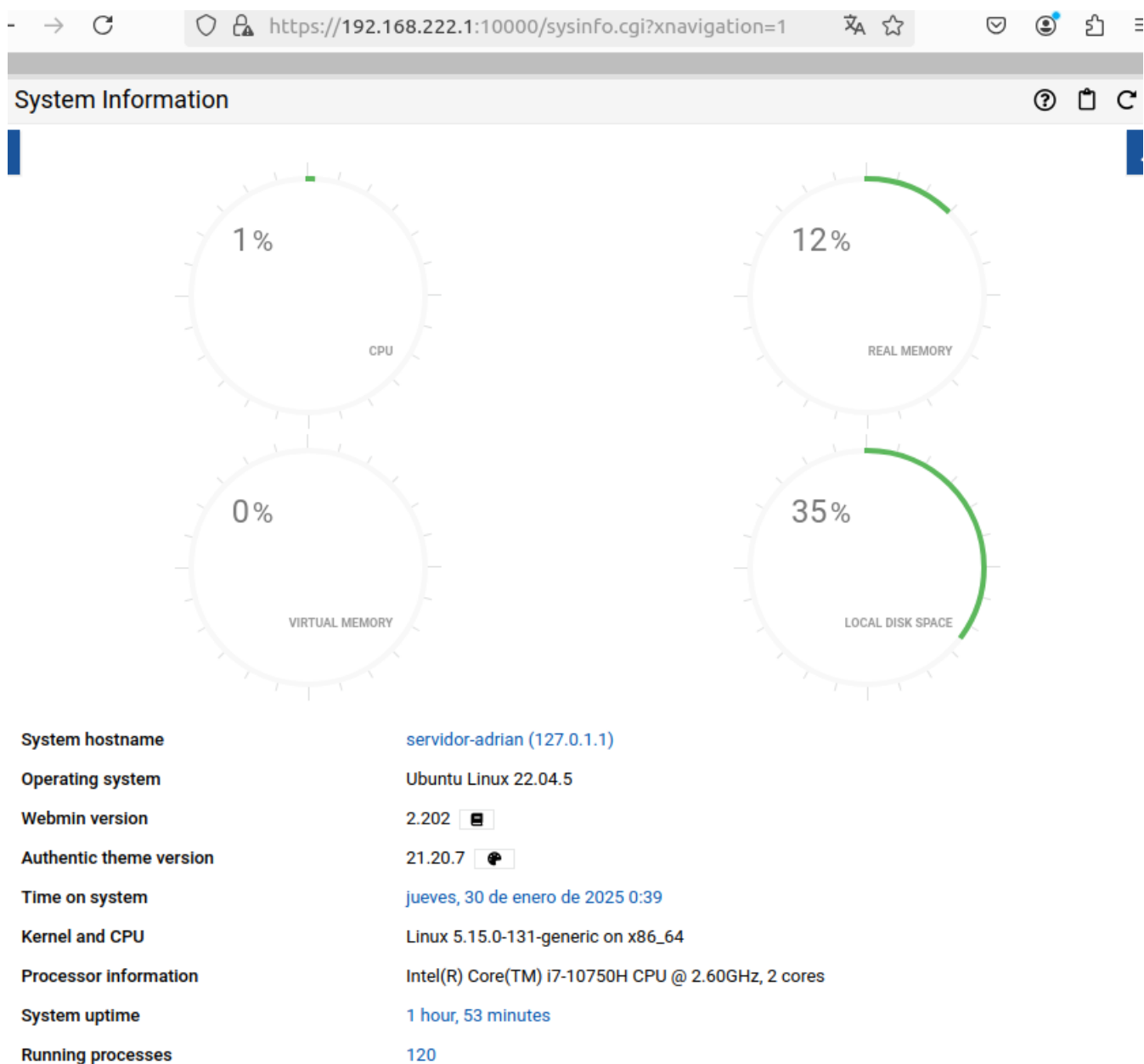


Pruebas de Configuración del Servidor DNS usando Webmin

Una vez que el servidor DNS esté configurado y Webmin instalado en el servidor Ubuntu, puedes realizar pruebas y gestionar el servicio DNS de forma gráfica a través de Webmin. Realizar estas pruebas:

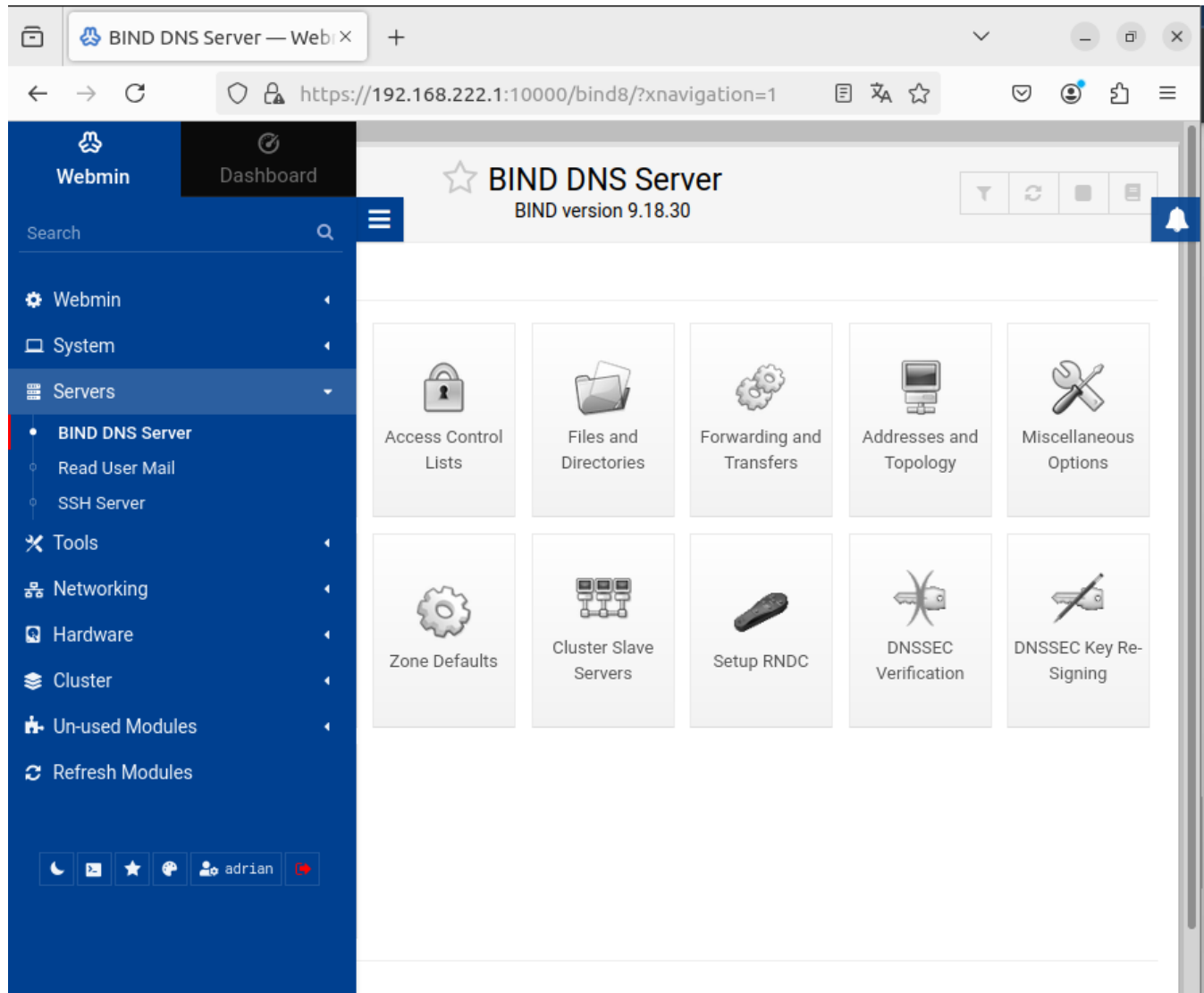
1. Acceso a Webmin desde el Cliente Ubuntu:

- Desde el cliente Ubuntu, abre un navegador web y escribe la dirección IP del servidor seguida del puerto **10000**:
https://IP_DEL_SERVIDOR:10000
- Inicia sesión con las credenciales de un usuario administrador en el servidor (como root o un usuario con privilegios sudo).



2. Localiza el Módulo de DNS:

- En el menú principal de Webmin, ve a: **Servers > BIND DNS Server**.
- Haz clic en este módulo para gestionar la configuración de DNS.



3. Verifica las Zonas DNS Configuradas:


- En la pantalla principal del módulo de BIND DNS Server:
 - Localiza la zona directa: **informatica.org**.


Browser window showing the BIND DNS Server/Edit Master Zone interface. The URL is https://192.168.222.1:10000/bind8/edit_master.cgi?zon.


Edit Master Zone


informatica.org


Type	Records	Type	Records
Address	6	Location	0
Name Server	1	Service Address	0
Name Alias	5	Public Key	0
Mail Server	2	SSL Certificate	0
Host Information	0	SSH Public Key	0
Text	0	Certificate Authority	0
Sender Permitted From	0	Name Authority	0
DMARC	0	DNSSEC Parameters	0
Well Known Service	0	IPv6 Address	1
Responsible Person	0	All	15
Reverse Address	0		



Edit Zone


Edit Zone


Edit Zone


Find Free IP


Record


Setup DNSSEC

- Localiza la zona inversa: **168.192.in-addr.arpa**.

Edit Master Zone
192.168

Type	Records	Type	Records
Reverse Address	6	Name Alias	0
Name Server	1	All	7

Edit Zone Records File

Edit Zone Parameters

Edit Zone Options

Find Free IPs

Record Generators

Setup DNSSEC Key

Freeze Zone

Unfreeze Zone

Check Records

Convert to Slave Zone

Delete Zone

Click this button to freeze a dynamic zone before updating it.

Click this button to unfreeze a dynamic zone after having updated it.

Click this button to have BIND check the records in this zone, and report on any problems.

Turns this master zone into a slave, so that it will receive records from another master server instead of serving them locally.

Click this button to delete this zone from your DNS server.

[Return to zone list](#)

- Verifica que ambas zonas aparecen correctamente configuradas.

4. Comprueba los Registros de las Zonas:

- Selecciona la zona **informatica.org**.
 - Revisa que los registros **A**, **CNAME**, y **MX** configurados en el archivo db.informatica.org aparecen listados.

The screenshot shows the BIND DNS Server web interface. The browser address bar displays the URL: `https://192.168.222.1:10000/bind8/edit_recs.cgi?zone=`. The page title is "All Records" for the zone "In informatica.org".

Below the header, there is a search bar with the text "Show records matching:" and a "Search" button. Below the search bar, there are two buttons: "Select all" and "Invert selection".

The main content is a table of DNS records. The table has four columns: "Name", "Type", "TTL", and "Values". The records are as follows:

Name	Type	TTL	Values
informatica.org.	NS	604800	informatica.org.
informatica.org.	A	604800	192.168.222.1
informatica.org.	AAAA	604800	::1
www.informatica.org.	A	604800	122.122.125.46
penacastillo.informatica.org.	A	604800	34.1.34.32
alisal.informatica.org.	A	604800	192.168.52.100
torrelavega.informatica.org.	A	604800	100.168.168.10
castro.informatica.org.	A	604800	192.35.35.35
web.informatica.org.	CNAME	604800	www.informatica.org.
ateca.informatica.org.	CNAME	604800	penacastillo.informatica.org.
atenea.informatica.org.	CNAME	604800	alisal.informatica.org.
aula3.informatica.org.	CNAME	604800	torrelavega.informatica.org.
aula5.informatica.org.	CNAME	604800	castro.informatica.org.
informatica.org.	MX	604800	10 correo.informatica.org.
informatica.org.	MX	604800	20 email35.arlo.es.

Below the table, there are two buttons: "Select all" and "Invert selection". Below these buttons is a red button labeled "Delete Selected".

At the bottom of the page, there are two blue buttons: "Return to zone list" and "Return to record types".

- Selecciona la zona **168.192.in-addr.arpa**.
 - Verifica que los registros **PTR** configurados en el archivo db.192 están presentes.

☆ All Records
In 192.168

Show records matching:

☒ Select all ☐ Invert selection

Name	Type	TTL	Values
<input type="checkbox"/> 168.192.in-addr.arpa.	NS	604800	localhost.
<input type="checkbox"/> 1.0.0.168.192.in-addr.arpa.	PTR	604800	localhost.
<input type="checkbox"/> 123.1.168.192.in-addr.arpa.	PTR	604800	aula1.agl.org.
<input type="checkbox"/> 215.3.168.192.in-addr.arpa.	PTR	604800	aula2.alisal.es.
<input type="checkbox"/> 217.2.168.192.in-addr.arpa.	PTR	604800	aula3.decroly.org.
<input type="checkbox"/> 129.23.168.192.in-addr.arpa.	PTR	604800	aula4.miguelherrero.edu.
<input type="checkbox"/> 131.13.168.192.in-addr.arpa.	PTR	604800	aula5.colegio.edu.

☒ Select all ☐ Invert selection

5. Valida la Configuración DNS:

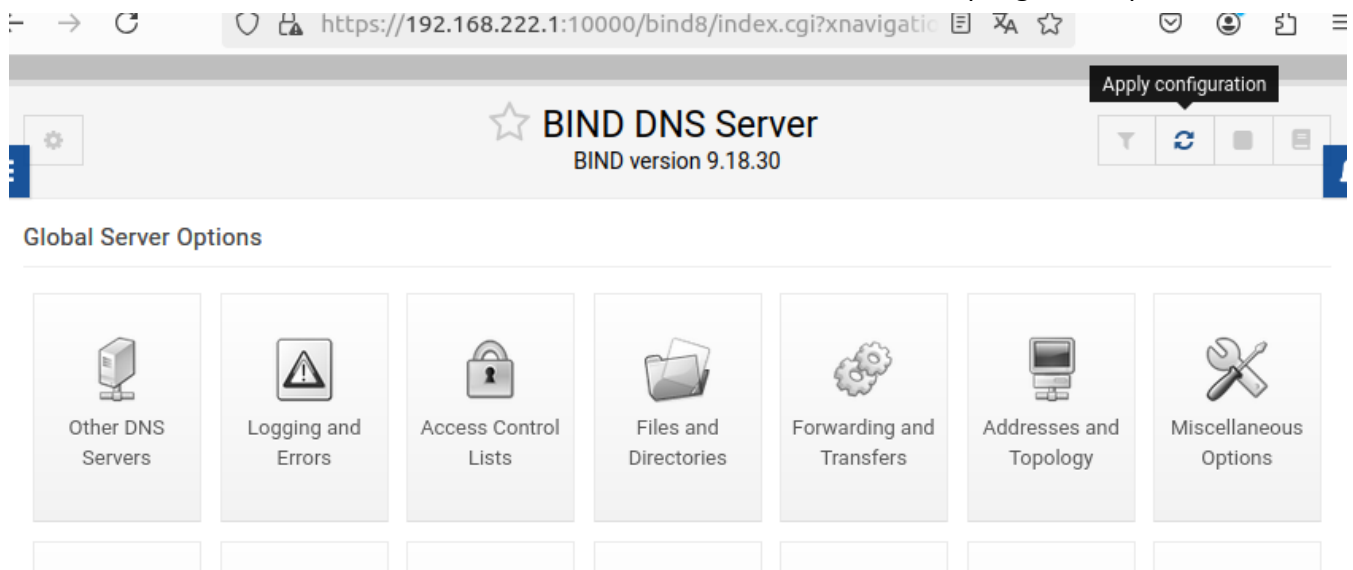
- Haz clic en **Check BIND Configuration** en la parte superior del módulo.
 - Esto realizará un análisis de la configuración DNS para asegurarse de que no hay errores en los archivos de zona ni conflictos.

☆ Check BIND Config

No errors were found in the BIND configuration file /etc/bind/named.conf or referenced zone files.

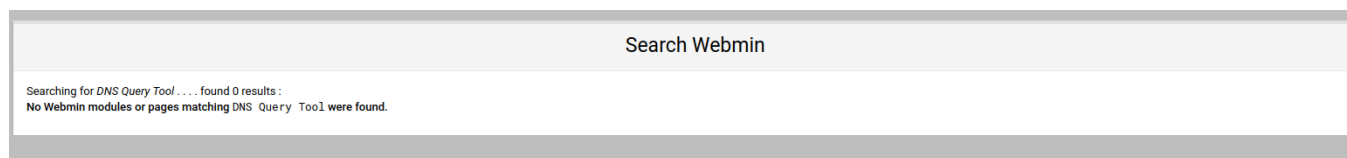
6. Reinicia el Servicio DNS:

- Desde el módulo **BIND DNS Server**, haz clic en **Apply Configuration** para reiniciar BIND y aplicar los cambios.



7. Pruebas de Resolución de Nombres con Webmin:

- Ve a la sección **DNS Query Tool** dentro del módulo BIND DNS Server.
- Realiza pruebas de resolución de nombres con los siguientes tipos de consultas:
 1. **Registros A:**
 - Consulta `www.informatica.org`.
 2. **Registros CNAME:**
 - Consulta `web.informatica.org`.
 3. **Registros MX:**
 - Consulta `informatica.org` para validar los servidores de correo.
 4. **Registros PTR:**
 - Consulta una dirección IP, por ejemplo, `192.168.1.123`.



No he encontrado ningún modulo con ese nombre.

8. Pruebas Manuales desde el Cliente Ubuntu:

Además de las pruebas realizadas desde Webmin, puedes hacer consultas manuales para confirmar que el servidor DNS responde correctamente:

1. Abre un terminal en el cliente Ubuntu.
2. Ejecuta las siguientes consultas usando `nslookup`:
 - Para un registro A: `nslookup www.informatica.org IP_DEL_SERVIDOR`
 - Para un registro CNAME:

```
nslookup web.informatica.org IP_DEL_SERVIDOR
o Para un registro PTR: nslookup 192.168.1.123
IP_DEL_SERVIDOR
```

```
adrian@cliente-ubuntu:~$ nslookup www.informatica.org 192.168.222.1
Server:      192.168.222.1
Address:     192.168.222.1#53

Name:   www.informatica.org
Address: 122.122.125.46

adrian@cliente-ubuntu:~$ nslookup web.informatica.org 192.168.222.1
Server:      192.168.222.1
Address:     192.168.222.1#53

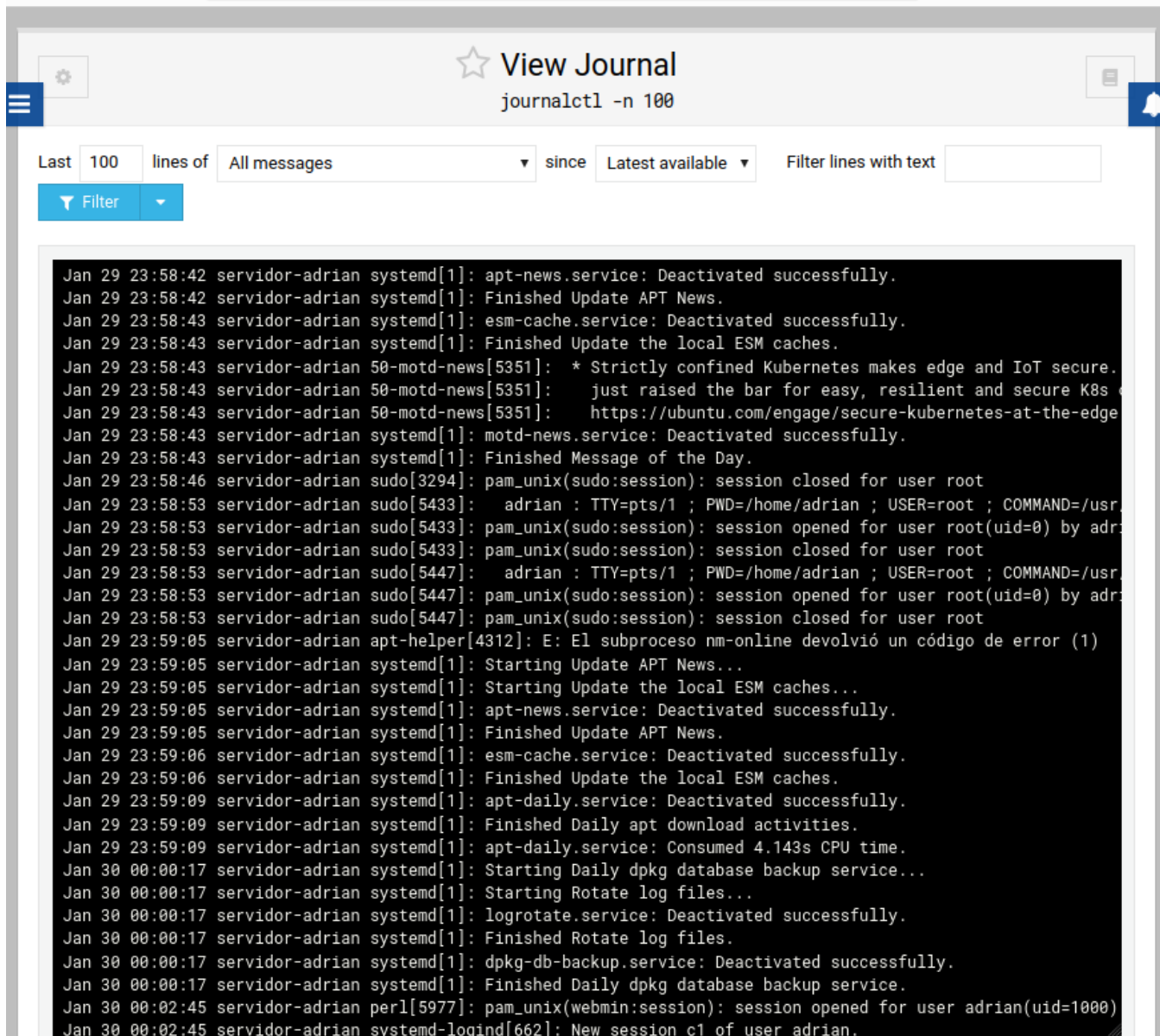
web.informatica.org    canonical name = www.informatica.org.
Name:   www.informatica.org
Address: 122.122.125.46

adrian@cliente-ubuntu:~$ nslookup 192.168.1.123 192.168.222.1
123.1.168.192.in-addr.arpa    name = aula1.agl.org.

adrian@cliente-ubuntu:~$
```

9. Revisión de Logs DNS desde Webmin:

- Ve a **System > System Logs** en Webmin.
- Busca los registros relacionados con **BIND** para analizar solicitudes y respuestas del servidor DNS.



★ View Journal
journalctl -n 100

Last 100 lines of All messages since Latest available Filter lines with text

Filter

```

Jan 29 23:58:42 servidor-adrian systemd[1]: apt-news.service: Deactivated successfully.
Jan 29 23:58:42 servidor-adrian systemd[1]: Finished Update APT News.
Jan 29 23:58:43 servidor-adrian systemd[1]: esm-cache.service: Deactivated successfully.
Jan 29 23:58:43 servidor-adrian systemd[1]: Finished Update the local ESM caches.
Jan 29 23:58:43 servidor-adrian 50-motd-news[5351]: * Strictly confined Kubernetes makes edge and IoT secure.
Jan 29 23:58:43 servidor-adrian 50-motd-news[5351]: just raised the bar for easy, resilient and secure K8s
Jan 29 23:58:43 servidor-adrian 50-motd-news[5351]: https://ubuntu.com/engage/secure-kubernetes-at-the-edge
Jan 29 23:58:43 servidor-adrian systemd[1]: motd-news.service: Deactivated successfully.
Jan 29 23:58:43 servidor-adrian systemd[1]: Finished Message of the Day.
Jan 29 23:58:46 servidor-adrian sudo[3294]: pam_unix(sudo:session): session closed for user root
Jan 29 23:58:53 servidor-adrian sudo[5433]: adrian : TTY=pts/1 ; PWD=/home/adrian ; USER=root ; COMMAND=/usr
Jan 29 23:58:53 servidor-adrian sudo[5433]: pam_unix(sudo:session): session opened for user root(uid=0) by adri
Jan 29 23:58:53 servidor-adrian sudo[5433]: pam_unix(sudo:session): session closed for user root
Jan 29 23:58:53 servidor-adrian sudo[5447]: adrian : TTY=pts/1 ; PWD=/home/adrian ; USER=root ; COMMAND=/usr
Jan 29 23:58:53 servidor-adrian sudo[5447]: pam_unix(sudo:session): session opened for user root(uid=0) by adri
Jan 29 23:58:53 servidor-adrian sudo[5447]: pam_unix(sudo:session): session closed for user root
Jan 29 23:59:05 servidor-adrian apt-helper[4312]: E: El subprocesso nm-online devolvió un código de error (1)
Jan 29 23:59:05 servidor-adrian systemd[1]: Starting Update APT News...
Jan 29 23:59:05 servidor-adrian systemd[1]: Starting Update the local ESM caches...
Jan 29 23:59:05 servidor-adrian systemd[1]: apt-news.service: Deactivated successfully.
Jan 29 23:59:05 servidor-adrian systemd[1]: Finished Update APT News.
Jan 29 23:59:06 servidor-adrian systemd[1]: esm-cache.service: Deactivated successfully.
Jan 29 23:59:06 servidor-adrian systemd[1]: Finished Update the local ESM caches.
Jan 29 23:59:09 servidor-adrian systemd[1]: apt-daily.service: Deactivated successfully.
Jan 29 23:59:09 servidor-adrian systemd[1]: Finished Daily apt download activities.
Jan 29 23:59:09 servidor-adrian systemd[1]: apt-daily.service: Consumed 4.143s CPU time.
Jan 30 00:00:17 servidor-adrian systemd[1]: Starting Daily dpkg database backup service...
Jan 30 00:00:17 servidor-adrian systemd[1]: Starting Rotate log files...
Jan 30 00:00:17 servidor-adrian systemd[1]: logrotate.service: Deactivated successfully.
Jan 30 00:00:17 servidor-adrian systemd[1]: Finished Rotate log files.
Jan 30 00:00:17 servidor-adrian systemd[1]: dpkg-db-backup.service: Deactivated successfully.
Jan 30 00:00:17 servidor-adrian systemd[1]: Finished Daily dpkg database backup service.
Jan 30 00:02:45 servidor-adrian perl[5977]: pam_unix(webmin:session): session opened for user adrian(uid=1000)
Jan 30 00:02:45 servidor-adrian systemd-logind[662]: New session c1 of user adrian.

```

Opcionalmente puedes resolver dudas sobre webmin y hacer otras pruebas para la **administración de DNS bind9 con webmin** visualizando el siguiente video:

<https://www.youtube.com/watch?v=vL9pG8gLI84>

DOCUMENTACIÓN

Deberás documentar los procedimientos indicando:

- los pasos realizados (comandos, modificaciones a ficheros de configuración y rutas de los mismos, etc.).

DAW2. Despliegue de Aplicaciones

Web • capturas de pantalla que demuestren que se han logrado los objetivos planteados.