**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](#_Toc189121438)

[ENUNCIADO 2](#_Toc189121439)

[PARTE 1. INSTALACIÓN Y CONFIGURACIÓN DE BIND9 2](#_Toc189121440)

[PARTE 2. CONFIGURACIÓN DEL SERVIDOR UBUNTU CON BIND9 COMO SERVIDOR DNS 4](#_Toc189121441)

[CACHÉ 4](#_Toc189121442)

[PARTE 3. CONFIGURACIÓN DE UN SERVIDOR DNS MAESTRO PARA LA ZONA 11](#_Toc189121443)

["INFORMATICA.ORG." CREACIÓN DE ZONA MAESTRA DIRECTA 11](#_Toc189121444)

[PARTE 4. CONFIGURACIÓN DEL SERVIDOR DNS MAESTRO PARA LA ZONA INVERSA 15](#_Toc189121445)

["168.192.IN-ADDR.ARPA" 15](#_Toc189121446)

[PARTE 5. GESTIÓN DEL SERVIDOR DNS. INSTALACIÓN Y CONFIGURACIÓN DE WEBMIN 17](#_Toc189121447)

[Instalación y Configuración de Webmin en el Servidor Ubuntu 17](#_Toc189121448)

[Pruebas de Configuración del Servidor DNS usando Webmin 20](#_Toc189121449)

[DOCUMENTACIÓN 28](#_Toc189121450)

# 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.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Texto

Descripción generada automáticamente

1. 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:

Texto

Descripción generada automáticamente

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

# CACHÉ

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

ethernets

:

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 o Descomenta o agrega la siguiente línea:

net.ipv4.ip\_forward = 1 o Aplica los cambios con:

sudo sysctl -p

**Habilitar NAT (mascarado) en el servidor Ubuntu:**

1. **Habilitar enmascaramiento de IP**:

o 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**:

o 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"

Texto

Descripción generada automáticamente

1. **Configuración del cliente Ubuntu para usar el servidor DNS**

* + **Configura los parámetros de red del cliente**:
    1. **Accede a la configuración de red**:
       - 1. Haz clic en el icono de red en la barra superior (generalmente en la esquina derecha).
         2. Selecciona la opción "Configuración de red" o "Configuración de conexiones de red" (dependiendo de la versión de Ubuntu Desktop).
    2. **Selecciona la conexión**:
       - 1. En la ventana de configuración de red, busca la conexión de red activa (por ejemplo, Ethernet).
         2. Haz clic en el icono de engranaje o selecciona "Configuración".
    3. **Configura los parámetros de red manualmente**:
       - 1. Ve a la pestaña **IPv4**.
         2. Cambia el método de "Automático (DHCP)" a "Manual".
         3. Ingresa los siguientes parámetros:

**Dirección IP**: 192.168.222.2

**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).

* + 1. **Guarda los cambios**:
       - 1. Haz clic en "Guardar" o "Aplicar".
         2. Apaga y enciende la interfaz para actualizar

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

* + **Verifica la conectividad**:

o Abre una terminal y ejecuta los siguientes comandos:

|  |  |
| --- | --- |
| ping 192.168.222.1 | ( |
| nslookup www.google.com | |

para comprobar conexión con el servidor).

o dig www.google.com (para comprobar resolución

DNS).

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

1. **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:

Texto

Descripción generada automáticamente

1. **Pruebas con nslookup**

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

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

Verifica que las respuestas provengan del servidor Ubuntu configurado.

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

1. **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.

Texto

Descripción generada automáticamente

# 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.**
    - Sustituiye 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

1. **Añade registros para resolver las siguientes consultas:**
   * **Registros A:**
     + www.informatica.org. → 122.122.125.46 o penacastillo.informatica.org. → 34.1.34.32 o alisal.informatica.org. → 192.168.52.100 o torrelavega.informatica.org. → 100.168.168.10 o 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

1. **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

1. **Añade registros MX para los servidores de correo:**
   * Servidores de correo:
     + correo.informatica.org. (prioridad 10) o 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:

Texto

Descripción generada automáticamente

**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 nslookup web.informatica.org

nslookup www.informatica.org

Texto

Descripción generada automáticamente

# 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.

1. **Añadir registros PTR en el archivo de zona inversa:**
   * + Editar el archivo db.192:

sudo nano /etc/bind/db.192

* + - Añadie 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.

1. **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

Texto

Descripción generada automáticamente

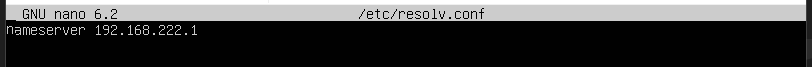
**Comprobación del Servidor DNS Inverso 1) Configurar el cliente Ubuntu:**

* + - 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



1. **Conectar el cliente y el servidor en una red interna.**
2. **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 192.168.3.215 nslookup 192.168.2.217 nslookup 192.168.23.129 nslookup 192.168.13.131

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

Texto

Descripción generada automáticamente

# 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

1. **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 -

1. **Instalar Webmin:**

Actualizar la lista de paquetes y luego instalar Webmin:

|  |  |
| --- | --- |
| sudo apt update |  |
| sudo apt install webmin -y | |

1. **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:

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

Inicia sesión con un usuario con permisos de root:

Imagen que contiene Diagrama

Descripción generada automáticamente

# 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).

Imagen que contiene Diagrama

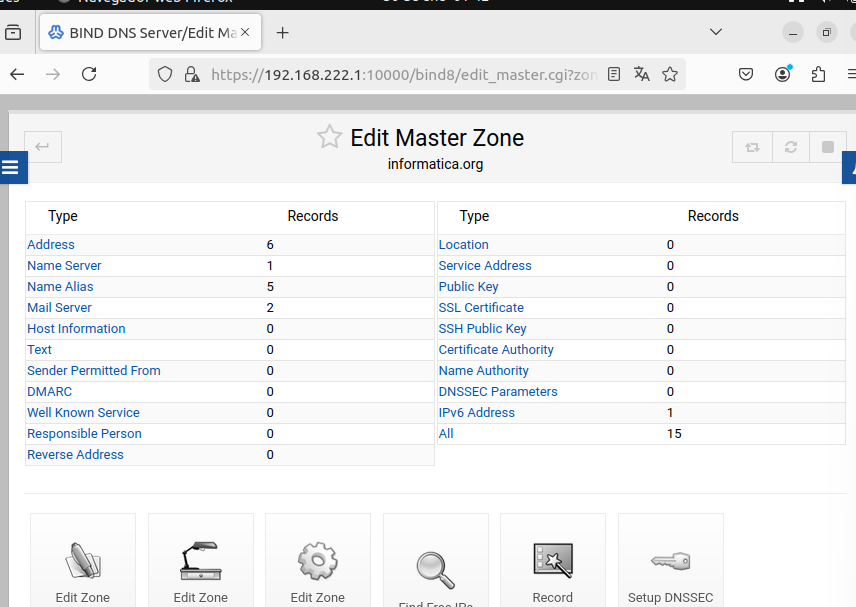
Descripción generada automáticamente

1. **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.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. **Verifica las Zonas DNS Configuradas:** 
   * En la pantalla principal del módulo de BIND DNS Server:
     + Localiza la zona directa: **informatica.org**.



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

Interfaz de usuario gráfica, Aplicación, Correo electrónico

Descripción generada automáticamente

* + Verifica que ambas zonas aparecen correctamente configuradas.

1. **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.

Interfaz de usuario gráfica

Descripción generada automáticamente

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

Tabla

Descripción generada automáticamente

1. **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.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

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

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. **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:**

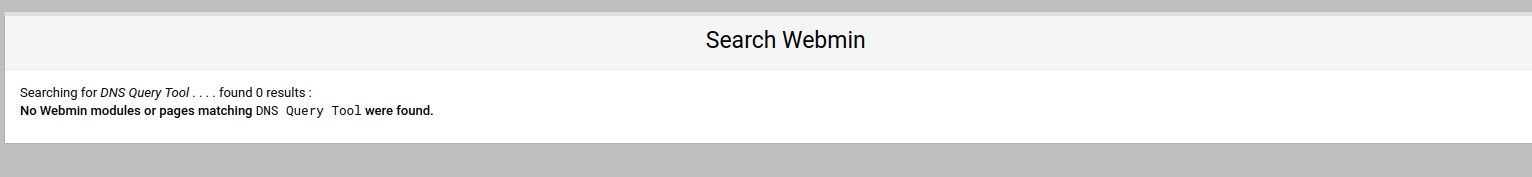
* + - * Consulta web.informatica.org.

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.

1. **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 o Para un registro CNAME:

nslookup web.informatica.org IP\_DEL\_SERVIDOR o Para un registro PTR: nslookup 192.168.1.123 IP\_DEL\_SERVIDOR

Texto

Descripción generada automáticamente

1. **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.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

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.