

📁 LPIC-2 / 🌐 Examen 207 - Servidor de Nombres de Dominio - Ejercicios

*Nota: Estos ejercicios implican configurar BIND para ser autoritativo. Realízalos **SIEMPRE en una VM de prueba dedicada**. Un servidor DNS mal configurado puede causar problemas de resolución en tu red o en internet. Necesitarás privilegios de superusuario (sudo).*

Ejercicio 7.2.1: Explorando Archivos de Zona por Defecto

- **Objetivo:** Ver ejemplos de archivos de zona (localhost, zonas inversas estándar).
- **Requisitos:** BIND instalado. Acceso a la línea de comandos.
- **Desarrollo Paso a Paso:**
 1. Abre una terminal.
 2. **Identifica el directorio de archivos de zona por defecto (Diferencias):**
 - En Debian/Ubuntu: Suele ser `/etc/bind/` o `/var/lib/bind/` si se usa chroot. Busca archivos como `db.local`, `db.127`.
 - En Red Hat/CentOS/Fedora: Suele ser `/var/named/`. Busca archivos como `named.localhost`, `named.loopback`. Asegúrate de tener permisos de lectura (puedes usar `sudo less`).
 3. **Visualiza el archivo de zona para localhost:** Ejecuta `sudo less <ruta_a_archivo_zona_localhost>`. Identifica el registro SOA, NS para localhost, y registros A/AAAA para `127.0.0.1::1`.
 4. **Visualiza el archivo de zona inversa para 127.0.0.0/8:** Ejecuta `sudo less <ruta_a_archivo_zona_127.in-addr.arpa>`. Identifica el SOA, NS, y el registro PTR para `1.0.0.127.in-addr.arpa` apuntando a `localhost..`

Ejercicio 7.2.2: (Conceptual) Definiendo una Nueva Zona Maestra en `named.conf`

- **Objetivo:** Entender cómo indicar a BIND que es autoritativo para un dominio.
- **Requisitos:** BIND instalado. Privilegios de superusuario (sudo). **VM de prueba.** Tener decidido un nombre de dominio de prueba (ej: `mytest.local`).
- **Desarrollo Paso a Paso:**
 1. Abre una terminal.
 2. **Edita el archivo de configuración de BIND donde se definen las zonas locales (requiere sudo):** En Debian, suele ser `/etc/bind/named.conf.local`. En Red Hat, puede ser `/etc/named.conf` (dentro del bloque `options { }`) o un archivo en `/etc/named.conf.d/`. Ejecuta `sudo vi <ruta_archivo>`.
 3. **Añade la definición de la zona maestra:**

```
zone "mytest.local" {
    type master;
    file "/etc/bind/zones/db.mytest.local"; // Ruta al archivo de
zona (ejemplo Debian)
    // file "db.mytest.local"; // Ruta relativa si usas el
'directory' en options (ejemplo Red Hat con /var/named como
directorio)
    allow-query { any; }; // Permitir consultas desde cualquier IP
(ajustar según necesidad)
```

```
};
```

- Reemplaza la ruta al archivo de zona según la convención de tu distribución o el directorio definido en `options { directory ...; };`. Asegúrate de que el directorio existe.
- `allow-query { any; };` permite que cualquier cliente consulte esta zona. Ajusta esto en un entorno real por seguridad.

4. Guarda y sal.

Ejercicio 7.2.3: Creando un Archivo de Zona Simple (Zona Directa)

- **Objetivo:** Crear el archivo que contiene los registros de recurso para la zona definida.
- **Requisitos:** Privilegios de superusuario (`sudo`). Directorio de archivos de zona identificado. Nombre de dominio de prueba. IP de tu VM.
- **Desarrollo Paso a Paso:**

1. Abre una terminal.
2. **Ve al directorio donde guardarás el archivo de zona:** Ejecuta `cd /etc/bind/zones/` (ejemplo Debian) o `cd /var/named/` (ejemplo Red Hat). Asegúrate de tener permisos para escribir (usa `sudo cd` o crea el directorio y ajusta permisos).
3. **Crea el archivo de zona (requiere sudo):** Ejecuta `sudo vi db.mytest.local` (usando el nombre de archivo que especificaste en `named.conf`).
4. **Añade el contenido básico (adapta los valores):**
DNS Zone file

```
$TTL      604800      ; TTL por defecto

@          IN          SOA      ns1.mytest.local. hostmaster.mytest.local. (
                                2023102701 ; Serial (YYYYMMDDVV)
                                604800    ; Refresh
                                86400     ; Retry
                                2419200   ; Expire
                                604800 )   ; Minimum TTL

; Name Servers
@          IN          NS       ns1.mytest.local.

; A records (IPv4)
@          IN          A        <IP_de_tu_VM> ; IP para el dominio raiz
(mytest.local)
ns1        IN          A        <IP_de_tu_VM> ; IP para ns1.mytest.local
www        IN          A        <IP_de_tu_VM> ; IP para www.mytest.local
host1      IN          A        192.168.1.101 ; Ejemplo de otro host

; AAAA records (IPv6) - Opcional
; @          IN          AAAA    <IP_IPv6_de_tu_VM>
; ns1        IN          AAAA    <IP_IPv6_de_tu_VM>

; CNAME records
```

```
ftp      IN      CNAME    www.mytest.local. ; ftp.mytest.local es
alias de www

; MX records
; @      IN      MX 10    mail.mytest.local. ; mail.mytest.local es
el servidor de correo con prioridad 10
; mail   IN      A        <IP_servidor_correo>
```

- Reemplaza <IP_de_tu_VM> con la dirección IP de tu máquina de prueba.
- Ajusta los nombres de los servidores de nombres, email del administrador y el serial.

5. Guarda y sal.

Ejercicio 7.2.4: Verificando la Sintaxis del Archivo de Zona y Recargando BIND

- **Objetivo:** Asegurarse de que el archivo de zona no tiene errores de sintaxis antes de aplicarlo.
- **Requisitos:** Archivo de zona creado. BIND instalado. Privilegios de superusuario (sudo).
- **Desarrollo Paso a Paso:**
 1. Abre una terminal.
 2. **Verifica la sintaxis del archivo de zona:** Ejecuta `sudo named-checkzone mytest.local <ruta_al_archivo_zona>`. Si la sintaxis es correcta, la salida debería ser algo como `zone mytest.local/IN: loaded serial 2023102701` y OK. Si hay errores, mostrará dónde están; corrígelos en el archivo de zona.
 3. **Verifica la sintaxis del archivo de configuración principal:** Ejecuta `sudo named-checkconf <ruta_a_named.conf>`.
 4. **Recarga la configuración de BIND (Diferencias):** Ejecuta `sudo systemctl reload bind9.service` (Debian) o `sudo systemctl reload named.service` (Red Hat).
 5. **Verifica el estado del servicio:** `systemctl status bind9.service` o `named.service`. Asegúrate de que no hay errores relacionados con la carga de la zona.

Ejercicio 7.2.5: Probando la Zona con Herramientas Cliente

- **Objetivo:** Confirmar que el servidor BIND responde consultas para la nueva zona.
- **Requisitos:** BIND cargó la zona sin errores. Herramientas cliente instaladas. IP de tu VM.
- **Desarrollo Paso a Paso:**
 1. Abre una terminal.
 2. **Consulta la zona usando tu propio servidor BIND (especifica la IP de tu VM):**
 - Ejecuta `dig @<IP_de_tu_VM> www.mytest.local A`. Debería devolver la IP que configuraste para `www`.
 - Ejecuta `dig @<IP_de_tu_VM> ftp.mytest.local CNAME`. Debería mostrar el registro CNAME y luego el registro A para `www`.

- Ejecuta `dig @<IP_de_tu_VM> mytest.local NS`. Debería mostrar los servidores de nombres que configuraste.
- 3. **Configura temporalmente tu VM (o usa otra máquina) para usar este servidor BIND como DNS principal:** Edita `/etc/resolv.conf` y cambia la línea `nameserver` a la IP de tu VM. Guarda.
- 4. **Prueba la resolución sin especificar el servidor (ahora tu VM usa tu BIND por defecto):** Ejecuta `host www.mytest.local`. Debería resolver correctamente.
- 5. **Restaura el archivo `/etc/resolv.conf` original (MUY IMPORTANTE).**

Ejercicio 7.2.6: (Conceptual) Configurando una Zona Inversa

- **Objetivo:** Entender cómo configurar la resolución IP a nombre (PTR).
- **Requisitos:** Privilegios de superusuario (`sudo`). **VM de prueba.** Conocer la red y máscara para la zona inversa (ej: 192.168.1.0/24).
- **Desarrollo Paso a Paso:**

1. Abre una terminal.
2. **Determina el nombre de la zona inversa:** Para 192.168.1.0/24, es `1.168.192.in-addr.arpa`.
3. **Define la zona inversa en `named.conf.local` o equivalente (requiere `sudo`):**

```
zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.1.168.192"; // Ruta al archivo de zona
    (ejemplo Debian)
    allow-query { any; };
};
```

4. **Crea el archivo de zona inversa (requiere `sudo`):** Ejecuta `sudo vi db.1.168.192`.

5. **Añade el contenido básico (adapta los valores):**

DNS Zone file

\$TTL 604800

```
@      IN      SOA      ns1.mytest.local. hostmaster.mytest.local. (
                        2023102702 ; Serial (INCREMENTA)
                        604800   ; Refresh
                        86400    ; Retry
                        2419200  ; Expire
                        604800   ) ; Minimum TTL
```

```
@      IN      NS      ns1.mytest.local.
```

; PTR records

```
<ultimo_octeto_ip> IN  PTR      <hostname_completo>. ; ej: 100 IN
PTR www.mytest.local.
<ultimo_octeto_ip> IN  PTR      <hostname_completo>. ; ej:
<IP_de_tu_VM_final> IN  PTR <nombre_de_tu_VM>.
```

- Adapta SOA y NS.

- Añade registros PTR para las IPs que quieres que resuelvan a nombres.
- 6. **Incrementa el serial en la zona inversa cada vez que la modifiques.**
- 7. **Verifica la sintaxis:** `sudo named-checkzone 1.168.192.in-addr.arpa db.1.168.192.`
- 8. **Recarga BIND:** `sudo systemctl reload`
- 9. **Prueba:** `dig -x <ip_que_mapea_a_hostname> @<IP_de_tu_VM>.`

Ejercicio 7.2.7: (Conceptual) Configurando una Zona Esclava

- **Objetivo:** Entender cómo configurar un servidor secundario que obtenga datos de un primario.
- **Requisitos:** Dos VMs de prueba (una como primaria, otra como secundaria). BIND instalado en ambas. Zona maestra configurada en la primaria (con `allow-transfer` configurado para permitir transferencias desde la IP de la secundaria). Privilegios de superusuario (`sudo`).
- **Desarrollo Paso a Paso (En la VM secundaria):**
 1. Abre una terminal.
 2. **Edita el archivo de configuración de zonas (requiere sudo):** `sudo vi <ruta_archivo>.`
 3. **Añade la definición de la zona esclava:**

```
zone "mytest.local" {
    type slave;
    file "/var/lib/bind/db.mytest.local"; // Dónde guardará el
    esclavo la copia (ejemplo Debian)
    // file "db.mytest.local"; // Onde guarda o escravo a copia
    (exemplo Red Hat)
    masters { <IP_del_servidor_primario>; };
};
```

 - Reemplaza la ruta y la IP del primario.
 4. **Guarda y sal.**
 5. **Verifica la sintaxis:** `sudo named-checkconf <ruta_a_named.conf>.`
 6. **Recarga BIND:** `sudo systemctl reload`
 7. **Verifica que la transferencia de zona ocurrió:** Mira los logs de BIND (`journalctl -u bind9.service` o `named.service`) para ver mensajes sobre la transferencia. Verifica la existencia del archivo de zona copiado en la ruta especificada.
 8. **Prueba:** Configura tu máquina o otra para usar la IP del servidor secundario como DNS. Ejecuta `dig www.mytest.local`. La respuesta debería venir del servidor secundario.