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

Este examen cubre la configuración, mantenimiento y aseguramiento de un servidor DNS, enfocándose principalmente en BIND.

207.1 Configuración básica de DNS

Teoría

El Sistema de Nombres de Dominio (DNS) es un sistema jerárquico y distribuido que se utiliza principalmente para traducir nombres de dominio legibles por humanos (ej: `www.example.com`) a direcciones IP numéricas (ej: `192.168.1.100`) y viceversa (resolución inversa). Es un servicio esencial para el funcionamiento de Internet y las redes modernas.

Conceptos Clave de DNS:

- **Cliente DNS (Resolver):** La parte del sistema que realiza consultas a un servidor DNS para obtener información (generalmente, la IP asociada a un nombre). La configuración del cliente DNS reside en `/etc/resolv.conf`.
- **Servidor DNS:** Un sistema que responde a las consultas DNS. Hay varios tipos:
  - **Servidor Caché (Caching Server):** Recibe consultas de clientes, las reenvía a otros servidores DNS (generalmente servidores forwarder o recursivos externos), almacena las respuestas en caché por un tiempo (TTL - Time To Live) y responde rápidamente a consultas posteriores sobre la misma información. No es autoritativo para ninguna zona.
  - **Servidor Forwarder:** Un servidor caché que reenvía *todas* las consultas (excepto las suyas propias si es autoritativo para algo) a servidores específicos en lugar de realizar la resolución recursiva completa por sí mismo.
  - **Servidor Recursivo:** Un servidor que acepta consultas recursivas de clientes y realiza todas las consultas necesarias a otros servidores DNS en la jerarquía de DNS (desde la raíz hacia abajo) para resolver la consulta completamente antes de enviar la respuesta final al cliente.
  - **Servidor Autoritativo:** Un servidor que contiene la información original para una o más zonas DNS (ej: `example.com`). Es responsable de proporcionar respuestas definitivas para los nombres dentro de esas zonas.
    - **Servidor Primario/Maestro:** El servidor autoritativo principal donde se mantienen y editan los archivos de zona.
    - **Servidor Secundario/Esclavo:** Un servidor autoritativo que obtiene copias de las zonas del servidor primario mediante transferencias de zona. Proporciona redundancia y distribuye la carga.
- **Zona DNS (Zone):** Una porción del espacio de nombres de DNS (ej: `example.com`) para la cual un servidor DNS es autoritativo. Se define en un "archivo de zona".
- **Registros de Recurso (Resource Records - RRs):** Entradas en un archivo de zona que contienen información sobre nombres dentro de la zona (ej: A para IPv4, AAAA para IPv6,

`CNAME` para alias, `MX` para correo, `NS` para servidores de nombres, `PTR` para resolución inversa).

Software de Servidor DNS (BIND):

BIND (Berkeley Internet Name Domain), implementado por ISC (Internet Systems Consortium), es el software de servidor DNS más utilizado en Linux. LPIC-2 se enfoca en BIND (versión 9, `named`).

- **Demonio:** El proceso del servidor BIND es `named`.
- **Archivo de Configuración Principal:** Define la configuración global y las zonas para las que el servidor es autoritativo o que reenvía.
    - **Rama Debian/Ubuntu:** `/etc/bind/named.conf`. Puede incluir otros archivos de configuración desde `/etc/bind/named.conf.options`, `/etc/bind/named.conf.local`, etc.
    - **Rama Red Hat/CentOS/Fedora:** `/etc/named.conf`. A menudo incluye archivos desde `/etc/named.conf.d/`.
- **Estructura Básica de `named.conf`:**
    - **`options { ... };`:** Bloque global que define ajustes como el directorio donde se encuentran los archivos de zona (`directory`), las direcciones IP y puertos donde escuchar (`listen-on`), servidores a los que reenviar consultas (`forwarders`), permisos de consulta (`allow-query`), etc.
    - **`zone "<nombre_zona>" { ... };`:** Define una zona.
        - `type master;`: El servidor es primario para esta zona.
        - `type slave;`: El servidor es secundario para esta zona.
        - `type forward;`: Reenvía todas las consultas de esta zona a servidores específicos.
        - `file "<ruta_archivo_zona>";`: Especifica el archivo que contiene los registros de recurso de la zona.
- **Zonas Estándar (Configuradas por Defecto):**
    - `.` (root): Información sobre los servidores raíz de DNS (generalmente incluida por defecto).
    - `localhost`: Zona para la resolución de `localhost`.
    - `0.in-addr.arpa`, `127.in-addr.arpa`, `255.in-addr.arpa`: Zonas para resolución inversa de rangos de IP estándar (`0.0.0.0/8`, `127.0.0.0/8`, `255.0.0.0/8`).

Herramientas Cliente DNS (Revisión LPIC-1 / Profundización LPIC-2):

- **`host <nombre>` o `host <ip>`:** Herramienta simple para búsquedas (nombre a IP o IP a nombre).

- **`dig <nombre> [<tipo_registro>] [@<servidor_dns>]`:** Herramienta más potente y flexible para consultas DNS. Muestra más detalles de la respuesta (TTL, autoridad, etc.).
    - `dig example.com A`: Consulta el registro A para example.com.
    - `dig -x <ip>`: Consulta inversa (PTR).
    - `dig @8.8.8.8 example.com`: Consulta usando un servidor DNS específico (ej: Google DNS).
- **`nslookup`:** Herramienta interactiva y no interactiva (más antigua que `dig`, menos preferida para scripting pero aún útil).

Diferencias Debian vs. Red Hat (BIND):

- **Nombre del Paquete del Servidor:** `bind9` en Debian/Ubuntu, `bind` en Red Hat/CentOS/Fedora.
- **Nombre del Paquete de Herramientas Cliente:** `bind9-clients` en Debian/Ubuntu, `bind-utils` en Red Hat/CentOS/Fedora.
- **Ubicación del Archivo de Configuración Principal:** `/etc/bind/named.conf` en Debian/Ubuntu, `/etc/named.conf` en Red Hat/CentOS/Fedora.
- **Ubicación de Directorios de Configuración Incluidos:** `/etc/bind/named.conf.options`, `/etc/bind/named.conf.local`, `/etc/bind/zones/` en Debian/Ubuntu. `/etc/named.conf.d/`, `/var/named/` en Red Hat/CentOS/Fedora.
- **Nombre del Servicio Systemd:** `bind9.service` en Debian/Ubuntu, `named.service` en Red Hat/CentOS/Fedora.