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

207.2 Crear y mantener zonas DNS

Teoría

Una zona DNS es una porción del espacio de nombres de dominio para la cual un servidor DNS tiene autoridad. La información sobre los nombres de host y servicios dentro de esa zona se almacena en un **archivo de zona** (zone file).

Estructura y Contenido de un Archivo de Zona:

Un archivo de zona es un archivo de texto plano que contiene registros de recurso (Resource Records - RRs). Comienza con directivas y el registro SOA.

1. **Directivas:**
    - `$TTL <segundos>`: Define el Time To Live (TTL) por defecto para los registros en la zona. Indica cuánto tiempo los servidores DNS caché deben almacenar la información de esta zona antes de consultarla de nuevo al servidor autoritativo. Se define al principio del archivo.
    - `$ORIGIN <nombre_zona>`: Opcional, define el nombre de dominio que se añadirá automáticamente a los nombres que no terminan en punto (`.`). Normalmente se define en `named.conf` y no es necesario aquí.
2. **Registros de Recurso (RRs):**
    - **SOA (Start of Authority):** Es el *primer* registro en un archivo de zona. Define la autoridad principal para la zona.
        - Formato: `<nombre> IN SOA <ns_primario> <email_admin> ( <serial> <refresh> <retry> <expire> <minimum TTL> )`
            - `<nombre>`: Normalmente `@`, que representa el nombre de la zona en sí misma.
            - `IN`: Clase (Internet).
            - `SOA`: Tipo de registro.
            - `<ns_primario>`: El nombre del servidor DNS primario para la zona (ej: `ns1.example.com.`). El punto final es importante para indicar que es un nombre de dominio completamente calificado (FQDN).
            - `<email_admin>`: Email del administrador (ej: `hostmaster.example.com.` - se reemplaza el `@` por un punto en el formato del archivo de zona).
            - `<serial>`: Número de serie de la zona. Un entero que *debe* incrementarse cada vez que se modifica el archivo de zona. Los servidores secundarios lo usan para detectar cambios y solicitar

transferencias de zona. Un formato común es YYYYMMDDVV (AñoMesDíaVersión, ej: 2023102701).
        - `<refresh>`: Tiempo que un servidor secundario espera antes de consultar al primario si ha habido cambios (ej: 3600 segundos = 1 hora).
        - `<retry>`: Tiempo que un secundario espera antes de reintentar una consulta al primario si la primera falla.
        - `<expire>`: Tiempo que un secundario mantendrá los datos de la zona como válidos si no puede contactar al primario. Después de este tiempo, dejará de responder consultas para la zona.
        - `<minimum TTL>`: TTL mínimo para respuestas negativas (NXDOMAIN).
- **NS (Name Server):** Define los servidores de nombres autoritativos para la zona. Debe haber un registro NS para cada servidor listado en el SOA, y registros NS adicionales para servidores secundarios.
    - Formato: `<nombre> IN NS <nombre_servidor>` (ej: `@ IN NS ns1.example.com.`, `ns1 IN A <ip_ns1>`)
- **A (Address):** Mapea un hostname a una dirección IPv4.
    - Formato: `<nombre> IN A <direccion_ipv4>` (ej: `www IN A 192.168.1.100`, `@ IN A 192.168.1.10` - `@` es la IP para el dominio raíz).
- **AAAA (IPv6 Address):** Mapea un hostname a una dirección IPv6.
    - Formato: `<nombre> IN AAAA <direccion_ipv6>` (ej: `www IN AAAA 2001:db8::1`).
- **CNAME (Canonical Name):** Crea un alias para un hostname. El nombre a la izquierda es el alias; el nombre a la derecha es el nombre canónico.
    - Formato: `<nombre> IN CNAME <nombre_canónico>` (ej: `ftp IN CNAME www.example.com.`). **Importante:** Un CNAME no puede tener otros registros asociados (excepto RRSIG para DNSSEC). No puedes tener un CNAME para `@` (el dominio raíz).
- **MX (Mail Exchanger):** Define los servidores de correo para el dominio y su prioridad.
    - Formato: `<nombre> IN MX <prioridad> <nombre_servidor_correo>` (ej: `@ IN MX 10 mail.example.com.`, `mail IN A <ip_mail_server>`). La prioridad más baja es la preferida.
- **PTR (Pointer):** Se usa en zonas inversas para mapear una IP a un hostname.
    - Formato: `<último_octeto> IN PTR <hostname>` (ej: `100 IN PTR www.example.com.` en la zona inversa para 192.168.1.0/24).

Ubicación de Archivos de Zona (Diferencias):

- **Rama Debian/Ubuntu:** Los archivos de zona por defecto y de ejemplo a menudo se encuentran en `/etc/bind/`. Los archivos de zona personalizados se suelen colocar en `/var/lib/bind/` o se crea un subdirectorio como `/etc/bind/zones/` y se define en el bloque `options` de `named.conf.options`.
- **Rama Red Hat/CentOS/Fedora:** Los archivos de zona por defecto y personalizados se suelen colocar en `/var/named/`. Este directorio debe tener permisos adecuados para que `named` pueda leer los archivos (típicamente propiedad del usuario/grupo `named`).

Proceso de Creación y Mantenimiento de una Zona Maestra (Primaria):

1. **Definir la Zona en `named.conf`:** En el archivo de configuración principal (o un archivo incluido como `named.conf.local`), añade una entrada `zone {}` para tu dominio, especificando `type master;` y la ruta al archivo de zona.
2. **Crear el Archivo de Zona:** Crea el archivo especificado en el paso 1. Puedes copiar un archivo de zona de ejemplo (ej: el de `localhost`) y modificarlo, o crearlo desde cero. Asegúrate de incluir el SOA, NS y los registros de recurso necesarios (A, AAAA, MX, CNAME, etc.).
3. **Incrementar el Número de Serie (Serial):** Cada vez que **modifiques** el archivo de zona, incrementa el número de serie en el registro SOA. Usa un formato consistente (ej: YYYYMMDDVV) para facilitar la gestión.
4. **Verificar la Sintaxis del Archivo de Zona:** Usa el comando `named-checkzone <nombre_zona> <ruta_archivo_zona>`. Es crucial; un error aquí puede impedir que BIND cargue la zona.
5. **Verificar la Sintaxis de `named.conf`:** Usa `named-checkconf <ruta_a_named.conf>`.
6. **Recargar la Configuración de BIND:** Ejecuta `sudo systemctl reload bind9.service` (Debian) o `sudo systemctl reload named.service` (Red Hat). BIND releerá los archivos de configuración y de zona.
7. **Probar la Zona:** Usa herramientas cliente como `dig` desde otra máquina (o desde la misma máquina, asegurándote de que consulta tu servidor BIND) para verificar que los nuevos registros se resuelven correctamente.

Zonas Inversas (Reverse Zones):

- Se utilizan para la resolución inversa (IP a hostname) usando registros PTR.
- La zona se define en el espacio de nombres `in-addr.arpa` para IPv4 o `ip6.arpa` para IPv6.
- El nombre de la zona se deriva de la red IP, con los octetos (IPv4) o nibbles (IPv6) en orden inverso, seguidos de `.in-addr.arpa.` o `.ip6.arpa.`.
    - Ejemplo IPv4: Para la red 192.168.1.0/24, la zona inversa es `1.168.192.in-addr.arpa`.
    - Ejemplo IPv6: Para el prefijo 2001:db8:1234::/48, la zona inversa es `4.3.2.1.8.b.d.0.1.0.0.2.ip6.arpa`.

- El archivo de zona inversa contiene registros PTR para cada IP a la que quieres asignarle un nombre. La clave para el registro PTR es la parte restante de la IP invertida.
    - Ejemplo: En la zona `1.168.192.in-addr.arpa`, un registro para la IP 192.168.1.100 sería `100 IN PTR www.example.com.`.

Servidores Secundarios (Slave Servers):

- Un servidor secundario obtiene una copia de una zona de un servidor primario mediante una **transferencia de zona** (Zone Transfer - AXFR para completa, IXFR para incremental).
- Para configurar una zona esclava en `named.conf`:

```
zone "example.com" {
    type slave;
    file "<ruta_archivo_zona>"; # Dónde el esclavo guardará la copia
    masters { <ip_del_servidor_primario>; };
};
```

- El servidor secundario consultará periódicamente al primario (basado en el serial y los tiempos de refresh/retry/expire en el SOA) para ver si el serial ha cambiado. Si es así, solicitará una transferencia de zona.