A DNS-szolgáltatás beüzemelése Debian rendszeren általában a **BIND9** (Berkeley Internet Name Domain) nevű DNS-szerver használatával történik. Az alábbiakban a telepítés és a konfiguráció részletesen bemutatása olvasható:

---

1. BIND9 telepítése

Frissítsd a csomaglistát, majd telepítsd a BIND9-et:

`sudo apt update`	
`sudo apt install bind9`	A BIND DNS-szerver maga. Ez a csomag tartalmazza a DNS-szerver futtatásához szükséges alapvető programokat és fájlokat.
`sudo apt install bind9utils`	Ez a csomag olyan segédprogramokat tartalmaz, amelyek a BIND DNS-szerver kezeléséhez és hibakereséséhez hasznosak, például: • **rndc:** Távoli vezérlés a BIND szerverhez. • **named-checkconf:** A konfigurációs fájlok ellenőrzésére. • **named-checkzone:** A zónafájlok szintaktikai ellenőrzésére.
`sudo apt install bind9-doc`	Ez a csomag tartalmazza a BIND részletes dokumentációját, amely segít a DNS-szerver konfigurálásában és testreszabásában. A dokumentáció általában a */usr/share/doc/bind9-doc/* könyvtárban található.
`sudo apt install dnsutils`	Ez a csomag olyan eszközöket tartalmaz, amelyek DNS-lekérdezések végrehajtására és tesztelésére szolgálnak. Főbb eszközök: • **dig**: Részletes DNS-lekérdezések végrehajtására. • **nslookup**: Egyszerű DNS-lekérdezésekhez. • **host**: DNS-információk gyors lekérdezésére.

---

2. BIND9 szolgáltatás ellenőrzése

Ellenőrizd, hogy a BIND9 telepítése sikeres volt-e, és a szolgáltatás fut-e:

```
sudo systemctl status bind9
```

Ha a szolgáltatás nem fut, indítsd el:

```
sudo systemctl start bind9
```

Engedélyezd az automatikus indítást a rendszer újraindításakor:

```
sudo systemctl enable bind9
```

---

3. Alapértelmezett konfigurációs fájlok helye

A BIND9 konfigurációs fájljai általában a következő helyeken találhatók:

- **/etc/bind/named.conf**: A fő konfigurációs fájl, amely más konfigurációs fájlokat is betölt.
- **/etc/bind/named.conf.options**: Globális opciók, például forwarderek és ACL-ek beállítása.
- **/etc/bind/named.conf.local**: Saját zónák és egyedi beállítások helye.
- **/etc/bind/named.conf.default-zones**: Alapértelmezett zónák (például localhost és 127.0.0.1).

- **Zónaadatok:** `/etc/bind/db.*`
- **Naplózás:** `/var/log/named/`

---

4. DNS-szolgáltatás konfigurálása

4.1 Forwarderek beállítása

Ha a BIND szervernek továbbítania kell a kéréseket más DNS-szerverek felé (például az internetszolgáltató DNS-e), a **/etc/bind/named.conf.options** fájlt szükséges szerkeszteni:

```
sudo nano /etc/bind/named.conf.options
```

Példa forwarderek beállítására:

```
options {
    directory "/var/cache/bind";
    forwarders {
        8.8.8.8;  // Google DNS
        8.8.4.4;  // Google DNS
    };
    dnssec-validation auto;
    listen-on-v6 { any; };
};
```

`directory:` Ez a sor meghatározza azt a könyvtárat, ahol a BIND a működéséhez szükséges fájlokat tárolja, például gyorsítótárat vagy egyéb ideiglenes adatokat.

`forwarders:` megadja azokat a DNS-szervereket, amelyekhez a BIND továbbítja a kliens által indított DNS-lekérdezéseket, ha a saját adatbázisában nincs rá válasz.

`dnssec-validation auto`: a BIND automatikusan letölti és használja a gyökérzónák DNSSEC hitelesítési kulcsait, hogy ellenőrizze a DNS-válaszok hitelességét és sértetlenségét. A DNSSEC védi a DNS-rendszert a manipulációktól, például hamisított DNS-adatoktól.

`listen-on-v6:` ez a sor azt határozza meg, hogy a BIND milyen IPv6-címeken figyeljen bejövő DNS-lekérdezésekre. **any** esetén a BIND az összes elérhető IPv6-címen fogadja a lekérdezéseket. Ha korlátozni szeretnénk, hogy a BIND csak bizonyos IPv6-címeken figyeljen, konkrét címek is megadhatók például: listen-on-v6 { 2001:db8::1; };

4.2 Helyi zóna hozzáadása:

Nyisd meg a **/etc/bind/named.conf.local** fájlt: `sudo nano /etc/bind/named.conf.local`

Add hozzá a következő konfigurációt:

```
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
};
```

```
zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};
```

`example.com:` ez a DNS-zóna neve.

`type master:` ez a szerver tartalmazza a zóna adatainak elsődleges másolatát.

`file "/etc/bind/db.example.com":` Ez egy zónafájl, amely tartalmazza az example.com domainhez tartozó rekordokat (pl. A, CNAME, MX stb.)

`1.168.192.in-addr.arpa:` Ez egy fordított DNS-zóna (reverse DNS zone). Az ilyen zónák IP-címeket oldanak fel domain nevekké. Ebben az esetben a 192.168.1.0/24 alhálózatra vonatkozik.

4.3 Zónafájl létrehozása:

Hozd létre a zónafájlt az előzőekben megadott helyen.

Másold le az alapértelmezett zónafájlt:

```
sudo cp /etc/bind/db.local /etc/bind/db.example.com
sudo cp /etc/bind/db.127 /etc/bind/db.192
```

iii) Szerkeszd a zónafájlokat:

Nyisd meg a **/etc/bind/db.example.com** fájlt: `sudo nano /etc/bind/db.example.com`

Módosítsd az alábbiak szerint:

```
$TTL    604800
@       IN      SOA     ns.example.com. admin.example.com. (
                         1         ; Serial
                         604800    ; Refresh
                         86400     ; Retry
                         2419200   ; Expire
                         604800 )  ; Negative Cache TTL

@       IN      NS      ns.example.com.
ns      IN      A       192.168.1.1
www     IN      A       192.168.1.10
mail    IN      A       192.168.1.20
@       IN      MX      10 mail.example.com.
```

Nyisd meg a **/etc/bind/db.192** fájlt: `sudo nano /etc/bind/db.192`

Módosítsd az alábbiak szerint:

```
$TTL    604800
@       IN      SOA     ns.example.com. admin.example.com. (
                         1         ; Serial
                         604800    ; Refresh
                         86400     ; Retry
                         2419200   ; Expire
                         604800 )  ; Negative Cache TTL

@       IN      NS      ns.example.com.
1       IN      PTR     ns.example.com.
10      IN      PTR     www.example.com.
20      IN      PTR     mail.example.com.
```

`$TTL:` Meghatározza az alapértelmezett élettartamot (Time-To-Live) a zónafájlban található rekordokhoz.

`604800:` Az alapértelmezett TTL értéke másodpercben van megadva, ami ebben az esetben 604800 másodperc, vagyis 7 nap. Ez azt jelenti, hogy a rekordokat a DNS-cache-ek 7 napig tárolhatják frissítés nélkül.

SOA (Start of Authority) rekord:

`@:` A zóna gyökérnevére (example.com) hivatkozik.

`IN SOA:` A SOA rekord jelzi a zóna hatósági információit.

`ns.example.com.:` Az elsődleges névkiszolgáló neve a zónához.

`admin.example.com.:` Az adminisztrátor e-mail címe, ahol a . helyettesíti a @ jelet (azaz admin@example.com).

Sorok jelentése:

- `Serial (1):` A zóna verziószáma. Ezt kell növelni minden alkalommal, amikor a zónafájl változik.
- `Refresh (604800):` A slave DNS-szerverek ennyi idő (7 nap) után kérnek frissítést a master szervertől.
- `Retry (86400):` Ha a slave szerver nem tudja elérni a master szervert, 86400 másodperc (1 nap) múlva újra próbálkozik.
- `Expire (2419200):` Ha a slave szerver 2419200 másodperc (28 nap) alatt sem tud frissíteni, akkor lejártnak tekinti a zónát.
- `Negative Cache TTL (604800):` A sikertelen névfeloldásokra vonatkozó cache időtartama (7 nap).

NS (Name Server) rekord: `@       IN      NS      ns.example.com.`

`NS rekord:` Meghatározza a zóna névkiszolgálóját.

`ns.example.com.:` Ez az example.com zóna névkiszolgálója.

A rekordok:

```
ns      IN      A       192.168.1.1
www     IN      A       192.168.1.10
mail    IN      A       192.168.1.20
```

A rekordok: IP-címeket rendelnek hosztnevekhez.

- `ns:` Az ns.example.com névkiszolgáló az 192.168.1.1 IP-címen érhető el.
- `www:` A www.example.com hoszt az 192.168.1.10 IP-címen érhető el.
- `mail:` A mail.example.com hoszt az 192.168.1.20 IP-címen érhető el.

MX (Mail Exchanger) rekord: `@ IN MX 10 mail.example.com.`

`MX rekord:` Az e-mailek kézbesítésére szolgáló szervert határozza meg.

`10:` Az MX rekord prioritása. Alacsonyabb szám magasabb prioritást jelent. Több MX rekord esetén a levelezőszerverek először a legalacsonyabb prioritású szervert próbálják elérni.

`mail.example.com.:` Az example.com domainhez tartozó levelezőszerver neve.

4.4 Hozzáférés korlátozása ACL-el:

A BIND9 konfigurációs fájlban az ACL használatával korlátozhatod a hozzáférést a DNS-szerver különböző funkcióihoz, például zónákhoz, lekérdezésekhez vagy frissítésekhez. Az ACL-eket a `named.conf` fájlban vagy annak includolt fájljaiban lehet definiálni.

ACL Konfiguráció Formátuma: Az ACL-eket az acl kulcsszóval definiáljuk. Az alábbi a szintaxis:

```
acl <név> {
    <IP-címek vagy hálózatok>;
};
```

`<név>:` Az ACL neve, amire később a konfigurációban lehet hivatkozni.
`<IP-címek vagy hálózatok>:` Egy vagy több IP-cím vagy hálózat, amelyhez hozzáférést szeretnél adni. Használhatsz egyedi IP-címeket, CIDR-formátumú hálózatokat, vagy kulcsszavakat (pl. any, none, localhost, localnets).

Példa ACL-ekre:

```
acl trusted {
    192.168.1.0/24;
    10.0.0.0/8;
    localhost;
    localnets;
};
```

ACL-ek használata:

Lekérdezések korlátozása: csak az ACL-ben definiált kliensek számára engedélyezi a DNS-lekérdezéseket.

```
options {
    allow-query { trusted; };
};
```

Zónafrissítések korlátozása: csak a 192.168.1.100 IP-címről engedélyezi a dinamikus DNS-frissítéseket az example.com zónához.

```
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
    allow-update { 192.168.1.100; };
};
```

Átirányítások korlátozása: csak az ACL-ben definiált kliensek számára engedélyezi a rekurzív lekérdezéseket.

```
options {
    allow-recursion { trusted; };
};
```

Átviteli engedélyek (zone transfer): csak a 192.168.1.200 IP-című slave szerver számára engedélyezi a zóna átvitelét.

```
zone "example.com" {
    type master;
```

```
    file "/etc/bind/db.example.com";
    allow-transfer { 192.168.1.200; };
};
```

---

5. Konfiguráció ellenőrzése és a BIND9 újraindítása

A konfiguráció módosítása után ellenőrizd a szintaxist: `sudo named-checkconf`

Ellenőrizd a zónafájlokat:

```
sudo named-checkzone example.com /etc/bind/db.example.com
sudo named-checkzone 1.168.192.in-addr.arpa /etc/bind/db.192
```

Ha nincs hiba, indítsd újra a BIND9 szolgáltatást: `sudo systemctl restart bind9`

---

6. Helyi tesztelés

a) Helyi gép beállítása a DNS használatára

Állítsd be a helyi gépet, hogy a saját DNS-szerverét használja.

Nyisd meg a hálózati konfigurációt: `sudo nano /etc/resolv.conf`

Add hozzá: `nameserver 127.0.0.1`

b) Teszteld a DNS-szolgáltatást

Használj dig vagy nslookup parancsot a teszteléshez: `dig example.com` vagy `dig -x 192.168.1.10`

---

7. (Opcionális) Távoli hozzáférés engedélyezése

Ha a DNS-szervert távolról is szeretnéd elérni, szerkeszd a **/etc/bind/named.conf.options** fájlt.

Nyisd meg: `sudo nano /etc/bind/named.conf.options`

Keress rá a következő sorra, és módosítsd:

```
listen-on { any; };
allow-query { any; };
```

Indítsd újra a BIND9-et: `sudo systemctl restart bind9`

---

8. Biztonsági beállítások

Hozzáférés korlátozása: Csak meghatározott IP-címekről engedélyezd a DNS-lekérdezéseket.

Tűzfal beállítása: Engedélyezd a 53-as portot (TCP és UDP) a DNS-szolgáltatás számára:

```
sudo ufw allow 53
```

---

9. Inverz DNS működése:

Az inverz DNS (Reverse DNS, rDNS) a hagyományos DNS-keresés ellentéte. Míg egy normál DNS-keresés során egy domain nevet (pl. example.com) alakítunk át IP-címmé, addig az inverz DNS esetében egy IP-címből kapunk vissza egy domain nevet.

Mire jó az inverz DNS?

- **E-mail szerverek hitelesítése**: Az e-mail szolgáltatók sokszor ellenőrzik, hogy egy küldő IP-nek van-e érvényes PTR rekordja. Ha nincs, a küldött levelek spamként kezelhetők.
- **Hálózati diagnosztika**: A traceroute vagy ping parancsok sokszor inverz DNS-t használnak, hogy az IP-címekhez ember által olvasható neveket rendeljenek.
- **Biztonság és naplózás**: Rendszerek és alkalmazások gyakran használják az rDNS-t a logfájlokban az IP-címekhez tartozó hostnevek megjelenítésére.

Hogyan lehet ellenőrizni az inverz DNS-t?

`nslookup 192.0.2.1` (Ha nincs PTR rekord beállítva, a keresés sikertelen lesz.)

Hogyan működik az inverz DNS?

- Az inverz DNS a **PTR rekordokat** használja.
- A DNS-szerver ellenőrzi, hogy létezik-e ilyen rekord, és ha igen, visszaadja a hozzá tartozó domain nevet.
- Az IPv4-címek esetén a cím számjegyeit visszafelé kell írni, és hozzá kell fűzni az `.in-addr.arpa` zónát.
- Például a 192.0.2.1 IP-címhez tartozó PTR rekord így néz ki: `1.2.0.192.in-addr.arpa`

PTR rekord beállítása saját DNS-szerveren

- A normál zónafájlok **/etc/bind/** könyvtárban találhatók.
- Az inverz DNS zónafájlt például így nevezhetjük el: `/etc/bind/db.192`
- Egyetlen IP-címhez **csak egy PTR rekord rendelhető**. Ha egy szerver több domain nevet szolgál ki, akkor az inverz DNS-ben csak egy név szerepelhet.
- Az, hogy melyik domainnév kerüljön a PTR rekordba, attól függ, hogy melyiket használjuk fő domain-ként (pl. az e-mail szerver).