A Debian 12-t NTP (Network Time Protocol) szerverként beállítani viszonylag egyszerű. Az alábbi lépések segítségével konfigurálhatjuk a rendszert, hogy pontos időt biztosítson más hálózati eszközök számára.

---

1. Telepítsük az NTP csomagot

Debian 12 alapértelmezés szerint a chrony nevű NTP implementációt használja, amely gyorsabb és rugalmasabb, mint a régi ntpd.

Telepítsük a chrony csomagot:

```
sudo apt update
sudo apt install chrony -y
```

Ellenőrizzük, hogy a szolgáltatás fut-e:

```
sudo systemctl status chronyd
```

Ha nem fut, indítsuk el:

```
sudo systemctl start chronyd
```

Engedélyezzük az automatikus indulását a rendszerrel:

```
sudo systemctl enable chronyd
```

---

2. Konfiguráljuk az NTP szervert

Nyisd meg a chrony.conf fájlt szerkesztésre:

```
sudo nano /etc/chrony/chrony.conf
```

A legfontosabb beállítások:

Válasszuk ki a felsőbb szintű időforrásokat (NTP szervereket)

Keressük meg az alábbi sort:

```
pool 0.debian.pool.ntp.org iburst
```

Ha másik időforrást szeretnénk használni (pl. a pool.ntp.org globális szervereket vagy egy vállalati időforrást), szerkesszük át például erre: (Ezek az alapértelmezett Debian NTP szerverek)

```
pool 0.pool.ntp.org iburst
pool 1.pool.ntp.org iburst
pool 2.pool.ntp.org iburst
pool 3.pool.ntp.org iburst
```

Az iburst opció gyorsabb szinkronizációt biztosít.

Helyi hardveróra használata (ha nincs külső időforrás)

Ha azt akarjuk, hogy a szerver offline is működjön, engedélyezzük az önálló időforrást:

```
local stratum 10
```

Ez azt jelenti, hogy ha a szerver nem éri el az internetes NTP szervereket, akkor a saját órája lesz az időforrás (stratum 10-es prioritással).

Az NTP szerver engedélyezése kliensek számára

Alapértelmezés szerint a Chrony nem engedi más gépek számára az idő lekérdezést, ugyanis kliensként működik. Engedélyezzük szerverként a saját hálózatunkon. Adjuk hozzá ezt a sort a konfigurációhoz:

```
allow 192.168.1.0/24
```

Ez azt jelenti, hogy a 192.168.1.0 tartományban lévő eszközök kérhetnek időszinkronizációt.

NTP engedélyezése bármely kliens számára:

```
allow all
```

Ez azt jelenti, hogy bármilyen IP-címről érkező kliens csatlakozhat, és használhatja az NTP szervert időszinkronizálásra.

---

3. Indítsuk újra az NTP szervert

Miután elvégeztük a módosításokat indítsuk újra a chrony szolgáltatást:

```
sudo systemctl restart chronyd
```

Ellenőrizzük, hogy a szolgáltatás fut-e és működik-e:

```
sudo systemctl status chronyd
```

4. Nyissuk meg az NTP portot a tűzfalon (ha szükséges)

Ha használunk ufw tűzfalat, akkor engedélyezzük az NTP forgalmat:

```
sudo ufw allow 123/udp
sudo ufw reload
```

Ha iptables-t használunk, akkor:

```
sudo iptables -A INPUT -p udp --dport 123 -j ACCEPT
```

Ha firewalld-t használunk, akkor:

```
sudo firewall-cmd --add-service=ntp --permanent
sudo firewall-cmd --reload
```

---

5. Teszteljük az NTP szervert
Ellenőrizd a csatlakozott időforrásokat:

```
chronyc sources -v
```

Ellenőrizzük, hogy a szerver szolgáltat-e időt más gépeknek:
Linux rendszer esetén futtassuk az alábbi parancsot:

```
ntpdate -q 192.168.1.100  #a szerver IP-címe
```

Windows számítógépről futtassuk ezt a parancsot (rendszergazdai parancssorban):

```
w32tm /stripchart /computer:192.168.1.100 /samples:5 /dataonly
```

Ha a teszt sikeres, az NTP szervered megfelelően működik!

---

6. (Opcionális) Automatikus szinkronizáció beállítása a klienseken
A kliensek beállíthatók úgy, hogy az NTP szerverről vegyék az időt.
Linux rendszereken a /etc/systemd/timesyncd.conf fájlt kell szerkeszteni:

```
sudo nano /etc/systemd/timesyncd.conf
```

Keressünk egy ilyen sort:

```
#NTP=
```

és módosítsuk a szerver IP-címére:

```
NTP=192.168.1.100
```

Mentsük el, majd indítsuk újra az időszinkronizálást:

```
sudo systemctl restart systemd-timesyncd
```

Windows klienseken így állítható be az NTP szerver:

```
w32tm /config /manualpeerlist:"192.168.1.1" /syncfromflags:manual /update
```

Cisco kliens beállítása:
Adjuk meg egy NTP szerver IP-címét:

```
ntp server 192.168.1.100
```

Jelszavas hitelesítés konfigurálása Cisco NTP kliens és Debian 12 NTP szerver között (Chrony)
A Cisco eszköz és a Debian 12 rendszeren futó Chrony közötti NTP hitelesítést a NTP autentikációs kulcsokkal (MD5/SHA1) lehet megvalósítani.

---

7. NTP hitelesítés engedélyezése a Debian 12 szerveren (Chrony)

Először be kell állítani a hitelesítést a **Chrony szerveren**.
Lépések:
7.1 Nyissuk meg a Chrony konfigurációs fájlt:

```
sudo nano /etc/chrony/chrony.conf
```

7.2 Adjunk hozzá egy NTP kulcsfájlt:

```
keyfile /etc/chrony/chrony.keys
```

Ez megadja a kulcsok helyét.

7.3 Hozzuk létre a kulcsfájlt és adjunk hozzá egy hitelesítési kulcsot:

```
sudo nano /etc/chrony/chrony.keys
```
Adjunk hozzá például egy **MD5** kulcsot:
```
1 M mysecretpassword
```
Magyarázat:
- 1 → Kulcs azonosító (ID).
- M → MD5 titkosítás (Chrony támogatja az M és SHA1 típusokat is).
- mysecretpassword → Használandó jelszó.

7.4 A szerver konfigurációjában engedélyezzük a hitelesítést:
A chrony.conf fájl végére írjuk be:
```
allow 192.168.1.0/24
authselect 1-10
```
Magyarázat:
- A 192.168.1.0 hálózat eszközei csatlakozhatnak.
- Az 1 és 10 közötti azonosítójú kulcsok vannak engedélyezve.

7.5 Mentés és kilépés (CTRL+X, Y, Enter), majd a **Chrony újraindítása:**
```
sudo systemctl restart chronyd
```

---

8. Cisco eszköz konfigurálása hitelesített NTP kliensként

8.1 Lépjünk be a konfigurációs módba:
```
configure terminal
```

8.2 Adjunk meg egy hitelesítési kulcsot:
A kulcs **ID és jelszó** meg kell, hogy egyezzen a Debian szerver beállításaival:
```
ntp authentication-key 1 md5 mysecretpassword
```

8.3 Engedélyezzük az NTP hitelesítést a Cisco eszközön:
```
ntp authenticate
```

8.4 Állítsuk be az NTP szervert hitelesítéssel:
```
ntp server 192.168.1.100 key 1
```

---

9. Ellenőrzés
Cisco eszközön:
Ellenőrizhetjük az NTP státuszát és a hitelesítést:
```
show ntp status
show ntp associations detail
```
Ha minden megfelelően működik, akkor az **NTP szerver szinkronizált állapotban lesz**.
Debian szerveren:
Listázzuk az aktív NTP kapcsolatokat:
```
chronyc sources -v
```
