A **RADIUS (Remote Authentication Dial-In User Service)** egy hálózati protokoll, amelyet hitelesítésre, jogosultságkezelésre és naplózásra (AAA – Authentication, Authorization, Accounting) használnak. **FreeRADIUS** az egyik legnépszerűbb RADIUS szerver, amelyet Debian 12-n használhatunk.

---

1. FreeRADIUS telepítése

Frissítsük a csomaglistát és telepítsük a FreeRADIUS szervert:

```
sudo apt update
sudo apt install freeradius freeradius-utils
```

Ellenőrizzük a verziót:

```
freeradius -v
```

Általában a **FreeRADIUS 3.x** verzió kerül telepítésre.

---

2. Felhasználó létrehozása és konfigurálása

A FreeRADIUS alapértelmezett konfigurációs könyvtára: `/etc/freeradius/3.0/`

Felhasználók hozzáadása

Nyissuk meg szerkesztésre a **users** fájlt:

```
sudo nano /etc/freeradius/3.0/users
```

Adjuk hozzá az alábbi sort a fájl végéhez:

```
testuser Cleartext-Password := "mypassword"
```

Ezzel egy **"testuser"** nevű felhasználót hozunk létre a mypassword jelszóval.

---

3. Titkos kulcs beállítása (RADIUS klienshez)

A RADIUS kliensnek (pl. Wi-Fi hozzáférési pont, VPN szerver, Cisco router) az **etc/freeradius/3.0/clients.conf** fájlban kell szerepelnie.

Nyissuk meg szerkesztésre a fájlt:

```
sudo nano /etc/freeradius/3.0/clients.conf
```

Példa beállítás:

```
client myrouter {
    ipaddr = 192.168.1.1
    secret = mysharedsecret
}
```

- **myrouter** – A kliens neve.
- **ipaddr = 192.168.1.1** – A RADIUS kéréseket küldő eszköz IP-címe.
- **secret = mysharedsecret** – A kliens és a RADIUS szerver közötti megosztott kulcs.

---

4. FreeRADIUS újraindítása és engedélyezése

Mentsük a módosításokat, majd indítsuk újra a szolgáltatást:

```
sudo systemctl restart freeradius
```

Ellenőrizzük, hogy fut-e a szolgáltatás:

```
sudo systemctl status freeradius
```

---

5. FreeRADIUS tesztelése

Használhatjuk a radtest parancsot a teszteléshez:

```
radtest testuser mypassword localhost 0 mysharedsecret
```

- **testuser:** tesztelni kívánt felhasználónév
- **mypassword:** a felhasználóhoz tartozó jelszó
- **localhost:** a RADIUS szerver IP-címe vagy hosztneve
- **0:** RADIUS NAS (Network Access Server) portazonosítója. Ez általában 0, ha nincs konkrét NAS azonosító.
- **mysharedsecret:** A RADIUS megosztott titkos kulcsa, amely a clients.conf fájlban van beállítva a megfelelő klienshez.

Ha minden helyesen van beállítva, ezt kell látnunk:

```
Received Access-Accept packet
```

Hibaelhárítás:

Ha hibaüzenetet kapunk, ellenőrizzük a FreeRADIUS naplókat:

```
sudo journalctl -u freeradius --no-pager | tail -n 20
```

Vagy futtassuk **debug módban**:

```
sudo freeradius -X
```

---

6. Tűzfal beállítása

A FreeRADIUS az **1812 (authentication) és 1813 (accounting)** UDP portokat használja.

Nyissuk meg ezeket a portokat:

```
sudo ufw allow 1812/udp
sudo ufw allow 1813/udp
sudo ufw reload
```

Ellenőrizzük a szabályokat:

```
sudo ufw status
```

---

7. Kliensek konfigurálása

Wi-Fi router esetén

1. Nyissuk meg a router adminisztrációs felületét böngészőben.
2. Navigáljunk a **802.1X RADIUS** vagy **WPA2-Enterprise** beállításokhoz.
3. Adjuk meg a RADIUS szerver IP-címét (Debian 12 szerver IP-je).
4. Adjuk meg a **1812-es portot**.
5. Állítsuk be a **megadott "secret" kulcsot** (mysharedsecret).

Cisco IOS router esetén

A következő parancsokkal adhatjuk hozzá a RADIUS szervert:

```
configure terminal
aaa new-model
radius server radiusserver
address ipv4 192.168.1.100 auth-port 1812
key mysharedsecret
exit
aaa authentication login default group radius local
aaa authorization exec default group radius local
```

- **default:** alapértelmezett hitelesítési módszer lesz használva a bejelentkezéshez
- **group radius:** elsőként a RADIUS szervert próbálja meg hitelesítéshez használni
- **local:** ha a RADIUS szerver nem elérhető vagy sikertelen a hitelesítés, akkor a helyi felhasználói adatbázist fogja használni

---

FreeRADIUS szerver Active Directory (AD) alapú hitelesítéssel történő használata

Hitelesítést a Kerberos és az NTLM vagy az LDAP segítségével lehet végezni. Az egyik legjobb megoldás az Samba+Winbind+Kerberos integráció.

1. Alapvető csomagok telepítése

```
sudo apt install winbind libnss-winbind libpam-winbind krb5-user
```

Ezek a csomagok teszik lehetővé az AD integrációt és az NTLM-alapú hitelesítést.

2. Host csatlakoztatása az Active Directoryhoz

2.1 A Kerberos konfigurációs fájl szerkesztése: `sudo nano /etc/krb5.conf`

Példa beállítás:

```
[libdefaults]
    default_realm = EXAMPLE.COM
    dns_lookup_realm = false
    dns_lookup_kdc = true
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true

[realms]
    EXAMPLE.COM = {
        kdc = dc1.example.com
        admin_server = dc1.example.com
    }

[domain_realm]
    .example.com = EXAMPLE.COM
    example.com = EXAMPLE.COM
```

Az EXAMPLE.COM-ot a saját tartományra, és dc1.example.com-ot az AD szerver nevére szükséges kicserélni.

2.2 Csatlakozás az AD-hoz

A következő paranccsal ellenőrizhető, hogy sikeres-e a kapcsolat:

```
kinit Administrator@EXAMPLE.COM
```

Írjuk be az AD Administrator jelszavát. Ha sikeres, a következő paranccsal ellenőrizhetjük a jegyeket: `klist`

2.3 Samba beállítása

Szerkesszük a Samba konfigurációs fájlt:

```
sudo nano /etc/samba/smb.conf
```

Példa beállítás:

```
[global]
    workgroup = EXAMPLE
    security = ADS
    realm = EXAMPLE.COM
    encrypt passwords = yes
    idmap config * : backend = tdb
    idmap config * : range = 10000-20000
    template shell = /bin/bash
    winbind use default domain = yes
    winbind offline logon = false
```

Indítsuk újra a Samba és a Winbind szolgáltatásokat:

```
sudo systemctl restart smbd nmbd winbind
sudo systemctl enable winbind
```

Csatlakozás az AD tartományhoz: `sudo net ads join -U Administrator`

Ellenőrizzük a tartományi csatlakozást: `wbinfo -u`

Ha sikeres, a parancs kilistázza az AD felhasználókat.

3. FreeRADIUS beállítása AD autentikációhoz

3.1 Winbind hitelesítés engedélyezése:

Szerkesszük a modules/mschap fájlt:

```
sudo nano /etc/freeradius/3.0/mods-enabled/mschap
```

Keressük a következő a szakaszt: `with_ntdomain_hack = yes`

Győződjünk meg róla, hogy a "yes" értékre van állítva.

Az **ntlm_auth** használatának engedélyezése az AD hitelesítéshez a sites-enabled/default fájlban:

```
sudo nano /etc/freeradius/3.0/sites-enabled/default
```

Keressünk rá az authorize szakaszra, és adjuk hozzá az ntlm_auth-ot:

```
authorize {
    preprocess
    chap
    mschap
    suffix
    eap {
        ok = return
    }
    ntlm_auth
}
```

Engedélyezzük az **ntlm_auth** használatát az MSCHAP hitelesítésnél is:

```
sudo nano /etc/freeradius/3.0/mods-config/files/authorize
```

Adjuk hozzá a következőt:

```
ntlm_auth
```

Most be kell állítani az ntlm_auth parancsot a mods-config/ntlm_auth fájlban:

```
sudo nano /etc/freeradius/3.0/mods-enabled/ntlm_auth
```

Győződjünk meg róla, hogy az alábbi sor benne van:

```
exec ntlm_auth {
    wait = yes
    program = "/usr/bin/ntlm_auth --request-nt-key --
domain=EXAMPLE --username=%{mschap:User-Name} --
password=%{User-Password}"
}
```

4. FreeRADIUS újraindítása és tesztelése

```
sudo systemctl restart freeradius
```