

A kétfaktoros belépés engedélyezése a Greenradius webfelületéhez

A biztonság, valamint a konzisztencia miatt és hogy elkerüljük annak a szükségességét, hogy a GreenRadius adminisztrátoroknak további belépési adatokat kelljen megjegyezni, javasoljuk, hogy ugyanazt GreenRadius nyújtotta két faktoros azonosítást használják a webfelület elérésére is.

A dokumentum bemutatja a két faktoros hitelesítést engedélyezéséhez szükséges lépéseket a GreenRadius adminisztrációs felülethez történő belépésre.

ÚJ FELHASZNÁLÓ HOZZÁADÁSA A GREENRADIUS ADMIN KONZOLHOZ

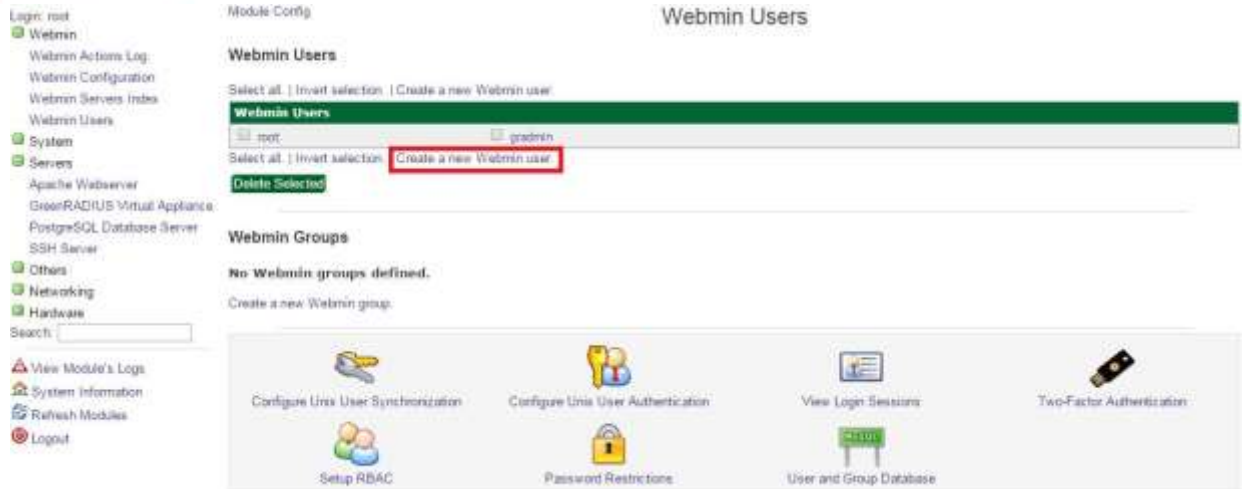
1. Lépjünk be a GreenRadius admin felületre a root/gradmin felhasználóval ahogy lentebb látható (alapesetben a jelszó mindkét felhasználónál GreenRocket!23):



2. A baloldali panelben kattintsunk a 'Webmin=> Webmin Users' menübe, ahogy a lenti képen látható:



3. Kattintsunk a "Create a new Webmin user" linkre, ahogy a lenti képen látható:



4. Adjuk meg a felhasználói nevet a "Username" mezőben és válasszuk ki a "Unix authentication"-t a jelszó opciónál, ahogy a lenti képen látható.:



MEGJEGYZÉSEK::

- A felhasználónévnek ("username") meg kell egyeznie a "Login Name"-mel, amit a felhasználó hitelesítésekor használunk a felkonfigurált AD/OpenLDAP-pal a standard felhasználónév-jelszó hitelesítéséhez a GreenRadiusban..
 - A hitelesítés működéséhez az új felhasználónévnek már kötelezően importálva kell lennie a GreenRadiusban a felkonfigurált AD/OpenLDAP-ból..
 - Ha a GreenRadiusban több tartomány van beállítva a felhasználónevet "felhasználónév@tartománynév" formátumban adjuk meg. A GreenRadius-ban létrehozott tartomány adjon meg.
5. Kattintsunk az "Available Webmin modules" szekció kibontására, ahogy a lenti képen látható. Az elérhető "Available Webmin modules" válasszuk ki az új felhasználó részére szükséges webmin modulokat. Javasoljuk, hogy legalább a "GreenRadius Virtual Appliance"-t válasszuk ki az új GreenRadius adminisztrátornak. Kattintsuk a "Create"-re, hogy elmentsük az új felhasználót.

Module Index Create Webmin User

Username:

Password: Force change at next login

Real name:

Select all | Invert selection

Webmin

- Scheduled Webmin Functions
- Webmin Configuration
- Webmin Users
- Webmin Actions Log
- Webmin Servers Index

System

- Bootup and Shutdown
- Running Processes
- System Documentation
- System Status
- Log File Rotation
- Scheduled Cron Jobs
- System Logs

Servers

- Apache Webserver
- PostgreSQL Database Server
- GreenRADIUS Virtual Appliance
- SSH Server

Networking

- Network Configuration

Hardware

- System Time

Others

- Upload and Download

Select all | Invert selection

[Return to user list](#)

6. Lépjünk ki a GreenRadius admin felületről és lépjünk be az előbbiekben létrehozott felhasználóval, ahogy a lenti képen látható:

Login to Webmin

You must enter a username and password to login to the Webmin server on 10.51.0.108.

Username:

Password:

Remember login permanently?

7. A "Password" mezőben elsőként adjuk meg az AD/OpenLDAP felhasználó jelszavát majd utána adjunk meg egy érvényes OTP-t (one time password) az adott felhasználóhoz rendelt biztonsági kulccsal.

MEGJEGYZÉSEK:

- Az új felhasználó kétfaktoros azonosítása a GreenRadiust használva történik meg. A felhasználónév és jelszó hitelesítése a felkonfigurált AD/OpenLDAP szervert használva a GreenRadiusban történik és egy érvényes egyszer használatos jelszó (OTP) egy a felhasználóhoz rendelt biztonsági tokenből származik.
- Az alap "root" és "gradmin" felhasználók hitelesítése a webmin saját felhasználói tárolójából történik. Arra az esetre, ha GreenRadius hitelesítés meghibásodna és el szeretnénk kerülni, hogy az összes GreenRadius admin felhasználót kizárjuk erősen javasolt, hogy a "Password" beállítást a "root" és "gradmin" felhasználóknál ne módosítsuk "Unix authentication"-ra, vagy "No password accepted"-re. Erre azért van szükségünk, hogy a GreenRadius alapú azonosítás meghibásodásának esetébe a "root" és "gradmin" felhasználókkal még képesek leszünk belépni a helyi jelszavakkal.