HOGYAN ENGEDÉLYEZZÜK A GREENRADIUS KÉT FAKTOROS AZONOSÍTÁSÁT SSH SZOLGÁLTATÁSHOZ UBUNTU RENDSZEREN

BEVEZETŐ

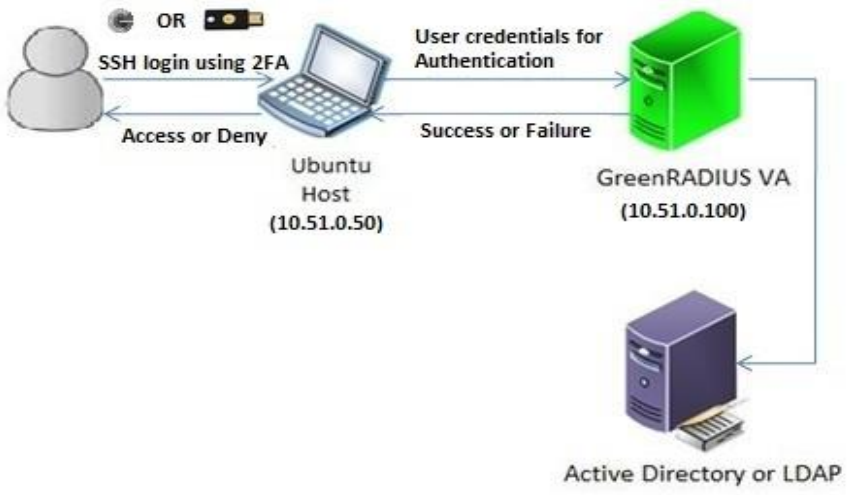
Ez a dokumentum bemutatja, hogy hogyan engedélyezhetjük a kétfaktoros azonosítást (2FA) SSH fehasználóknak Ubuntuban a GreenRADIUS rendszert használva.

ELŐFELTÉTELEK

- Ez a dokumentum feltételezi, hogy a GreenRADIUS már be van állítva ActiveDirectory/LDAP-ból importált felhasználókkal és a tokenek is hozzá vannak rendelve a felhasználókhoz

- Ubuntu rendszer (32/64 bites)

TELEPÍTÉSI ÁBRA



AZ UBUNTU-N VÉGREHAJTANDÓ LÉPÉSEK

1. Lépjünk be az Ubuntu-ban bármilyen SSH kliens programot használva pl. PUTTY
2. Váltsunk át a "/tmp" könyvtárba a következő parancs kiadásával:

```
cd /tmp/
```

3. Töltsük le a "pam_radius_auth.so" fájlt a következő paranccsal::

```
sudo wget -O "pam_radius_auth.so"
"https://files.greenrocketsecurity.com/pamradiusubuntu"
```

KImenete:

```
……

Saving to: ‘pam_radius_auth.so’

100%[==================================================
==================================================>]
40,750       140KB/s   in 0.3s

2016-06-17 14:00:37 (140 KB/s) - ‘pam_radius_auth.so’
saved [40750/40750]
```

4. 32 bites Ubuntu esetében másoljuk a 'pam_radius_auth.so' fájlt a ‘/lib/security/’ könyvtárba a következő parancsot használva:

```
sudo cp pam_radius_auth.so /lib/security/
```

5. 64 bites Ubuntu esetében másoljuk a 'pam_radius_auth.so' fájlt a ‘/lib/x86_64-linux-gnu/security/’ könyvtárba a következő parancsot használva:

```
sudo cp pam_radius_auth.so /lib/x86_64-linux-
gnu/security/
```

6. Szerkesszük a ‘/etc/pam.d/sshd’-t és írjuk be a következő sort a fájl első sorába:

```
auth required pam_radius_auth.so
```

7. Kommenteljük ki a következő sort az alábbi módon és mentsük el a fájt:

```
#@include common-auth
```

8. Készítsünk egy "raddb" könyvtárat az a "/etc/" mappába a következő parancsot használva:

```
sudo mkdir /etc/raddb/
```

9. Váltsunk át erre a "raddb" könyvtárra és hozzunk létre egy "server" nevű fájlt a következő parancsot használva:

```
cd /etc/raddb/

sudo touch server
```

10. Szerkesszük az /etc/raddb/server" fájlt és adjuk hozzá a következő adatokat a fájlhoz (mindet szóközzel elválasztva):

```
<<GreenRADIUS Virtual Appliance IP>><<Shared
Secret>><<Timeout(seconds)>>

Például, ha a GreenRADIUS Virtual Appliance IP címe
"10.51.0.100" és a közös titok a "test", akkor a
következő sort adjuk hozzá:

     10.51.0.100 test 3
```

11. Adjunk hozzá egy jelszó nélküli új felhasználót a szerverhez a következő parancs használatával:

```
useradd –d /home/<<user name>> –m <<user name>>

Például, ha a "john" felhasználót akarjuk hozzáadni,
akkor a követező parancs használható:

     useradd -d /home/john -m john
```

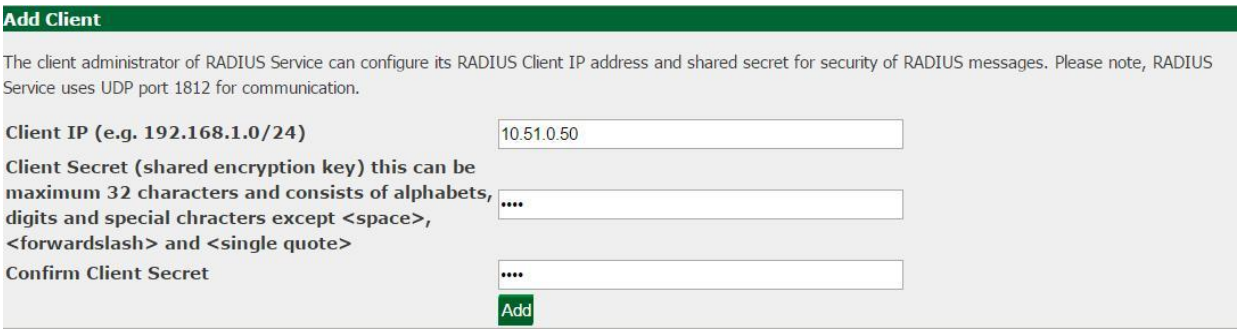
Megjegyzés: a hozzáadott felhasználónévnek a GreenRADIUS Virtuális gépben létrehozott tartományok egyikében legalább jelen kell lennie

12. Indítsuk újra az SSH szolgáltatást a következő parancs használatával:

```
sudo /etc/init.d/ssh restart
```

A GREENRADIUS VIRTUÁLIS ESZKÖZÖN VÉGREHAJTANDÓ LÉPÉSEK

1. Lépjünk be a GreenRADIUS admin felületre bármilyen böngészőből
2. Menjünk a "Domain" fülre és válasszuk ki azt a tartományt amiben a felhasználó megtalálható (esetünkben "John")
3. Menjünk a "Configuration" fülre
4. Adjuk meg az Ubuntu gép adatait az "Add Client" részben:
   - pl. Ha az Ubuntu gép IP címe "10.51.0.50" és a közös titok megegyezik a 10-es lépésben már bemutatott titokkal (esetünkben "test"), ezért adjuk hozzá a RADIUS klienst az alábbi képen látható módon és kattintsünk az "Add" gombra:



TESZTELJÜK AZ SSH BELÉPÉST AZ UBUNTU GÉPEN A KÉTFAKTOROS AZONOSÍTÁST HASZNÁLVA

1. Lépjünk be az Ubuntu gépre bármilyen SSH klienst használva, mint pl. PuTTY
2. Adjuk meg a felhasználónevet és nyomjunk ENTER-t
3. Ekkor megadhatjuk a jelszót. A jelszó megadásakor adjuk meg a felhasználó ActiveDirectory/LDAP-ban beállított jelszavát, ezt közvetlenül követi a felhasználóhoz (esetünkben "John") rendelt token által generált egyszer használatos jelszó
   - pl. ha a felhasználónév "John", teszteljük le a belépést ahogy a lenti képen látható módon:

SSH BELÉPÉS OTP (one-time password) KÉRÉSSEL

Ha szeretnénk engedélyezni az SSH belépéshez az OTP kérést akkor kövessük az alábbi lépéseket.

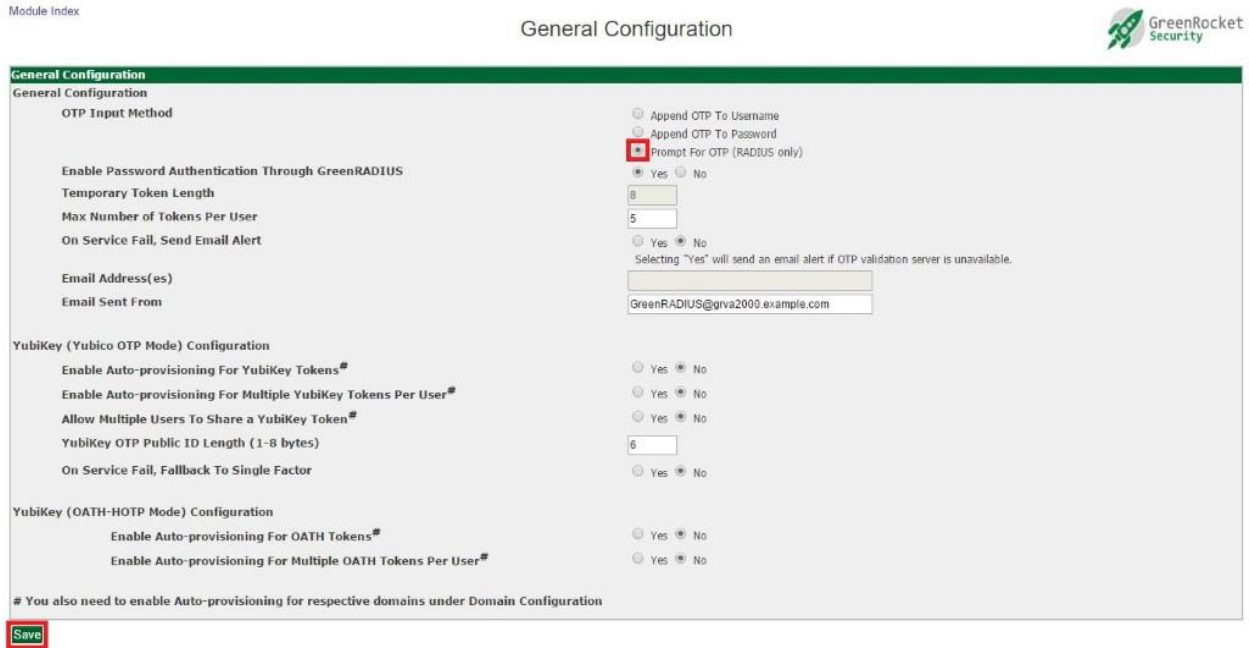
TOVÁBBI VÉGREHAJTANDÓ LÉPÉSEK AZ UBUNTU GÉPEN

1. Kövessük a lenti "Ubuntu-n végrehajtandó lépések" szekcióban leírt lépéseket
2. Szerkesszük az "/etc/ssh/sshd_config" fájlt..
3. Keressük meg a "ChallengeResponseAuthentication no" tartalmazó sort és cseréljük le "ChallengeResponseAuthentication yes"-re
4. Indítsuk újra az SSH szolgáltatást a következő paranccsal:
   sudo /etc/init.d/ssh restart

A GREENRADIUSON VÉGREHAJTANDÓ LÉPÉSEK

1. Lépjünk be a GreenRADIUS webes admin felületére
2. Menjünk a "Global Configuration" fülre és kattintsünk a "General" ikonra

3. A "General Configuration" alatt válasszuk ki az "OTP Input Method"-nál a "Prompt for OTP (RADIUS only)"-t és mentsük el.



TESZTELJÜK AZ SSH BELÉPÉST AZ UBUNTU GÉPEN A KÉTFAKTOROS AZONOSÍTÁST HASZNÁLVA (OTP KÉRÉS)

1. Lépjünk be az Ubuntu gépre bármilyen SSH klienst használva, mint pl. PuTTY
2. Adjuk meg a felhasználónevet és nyomjuk Enter-t
3. Ekkor a jelszó békérésre kerül. Adjuk meg a felhasználó jelszavát ami az ActiveDirectory/LDAP-ban van beállítva, majd nyomjunk Enter-t.
4. Ekkor az egyszer használatos jelszó (OTP) bekérésre kerül. Generáljunk egy OTP-t bármelyik kulccsal ami az adott felhasználóhoz van rendelve.

    - pl. Ha a felhasználó "John" teszteljük a belépést a következő képen látható módon:

HIBAKERESÉS:

Hibakereséshez használjuk a következő parancsot az Ubuntu-n

```
tail -f /var/log/auth.log
```