

AKO POVOLÍŤ DVOJFAKTOROVÉ OVEROVANIE GREENRADIUS PRE SSH V UBUNTU

ÚVOD

Tento dokument opisuje, ako povoliť dvojfaktorové overovanie (2FA) pre používateľov SSH v Ubuntu pomocou systému GreenRADIUS.

PREDPOKLADY

- Tento dokument predpokladá, že GreenRADIUS je už nakonfigurovaný s používateľmi importovanými z ActiveDirectory/LDAP a že používateľom sú pridelené tokeny.
- Systém Ubuntu (32/64 bitov)

SCHÉMA INŠTALÁCIE



KROKY, KTORÉ TREBA VYKONAŤ V UBUNTU

1. Prihláste sa do Ubuntu pomocou ľubovoľného klientskeho programu SSH, napr. PUTTY
2. Prejdite do adresára "/tmp" zadaním nasledujúceho príkazu:

```
cd /tmp/
```

3. Stiahnite si súbor "pam_radius_auth.so" pomocou nasledujúceho príkazu:

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

Výstup:

```
.....  
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. Pre 32-bitové Ubuntu skopírujte súbor 'pam_radius_auth.so' do '/lib/security/' pomocou nasledujúceho príkazu:

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

5. Pre 64-bitové Ubuntu skopírujte súbor 'pam_radius_auth.so' do '/lib/x86_64-linux-gnu/security/' pomocou nasledujúceho príkazu:

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

6. Upravte súbor '/etc/pam.d/sshd' a pridajte nasledujúci riadok na prvý riadok súboru:

```
auth required pam_radius_auth.so
```

7. Ďalší riadok zakomentujte takto a súbor uložte:

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

8. Vytvorte adresár "raddb" v priečinku "/etc/" pomocou nasledujúceho príkazu:

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

9. Prepnite sa do tohto adresára "raddb" a vytvorte súbor s názvom "server" pomocou nasledujúceho príkazu:

```
cd /etc/raddb/  
sudo touch server
```

10. Upravte súbor `/etc/raddb/server` a pridajte doň nasledujúce informácie (všetky oddelené medzerami):

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

Ak je napríklad IP adresa virtuálneho zariadenia GreenRADIUS "10.51.0.100" a zdieľané tajomstvo je "test", potom pridajte nasledujúci riadok:

```
10.51.0.100 test 3
```

11. Pridajte na server nového používateľa bez hesla pomocou nasledujúceho príkazu:

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

Ak chcete napríklad pridať používateľa "john", použijete nasledujúci príkaz:

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

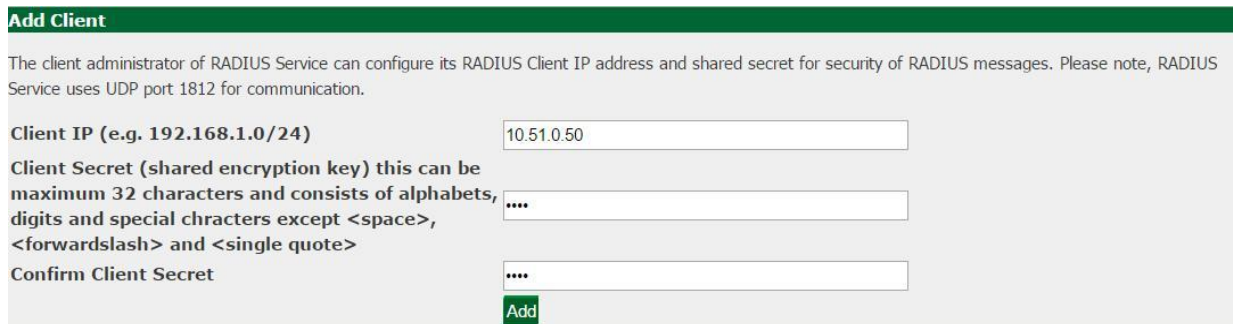
Poznámka: pridané používateľské meno musí byť prítomné aspoň v jednej z domén vytvorených vo virtuálnom počítači GreenRADIUS.

12. Reštartujte službu SSH pomocou nasledujúceho príkazu:

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

KROKY, KTORÉ TREBA VYKONAŤ NA VIRTUÁLNO M POČÍTAČI GREENRADIUS

1. Vstúpte do rozhrania správcu GreenRADIUS z ľubovoľného prehliadača
2. Prejdite na kartu "Domain" a vyberte doménu, v ktorej sa používateľ nachádza (v našom prípade "John")
3. Prejdite na kartu "Configuration"
4. V časti "Add Client" zadajte údaje o počítači Ubuntu:
 - Ak je IP adresa počítača Ubuntu "10.51.0.50" a zdieľané tajomstvo je rovnaké ako to, ktoré už bolo uvedené v kroku 10 (v našom prípade "test"), potom pridajte klienta RADIUS ako je znázornené na obrázku nižšie, a kliknite na "Add":



Add Client

The client administrator of RADIUS Service can configure its RADIUS Client IP address and shared secret for security of RADIUS messages. Please note, RADIUS Service uses UDP port 1812 for communication.

Client IP (e.g. 192.168.1.0/24)

Client Secret (shared encryption key) this can be maximum 32 characters and consists of alphabets, digits and special characters except <space>, <forwardslash> and <single quote>

Confirm Client Secret

TESTOVANIE PRIHLÁSENIA CEZ SSH NA POČÍTAČI UBUNTU POMOCOU DVOJFAKTOROVÉHO OVEROVANIA

1. Prihláste sa do počítača Ubuntu pomocou ľubovoľného klienta SSH, napríklad PuTTY
2. Zadáajte používateľské meno a stlačte ENTER
3. Potom môžete zadať heslo. Pri zadávaní hesla zadajte heslo používateľa nastavené v ActiveDirectory/LDAP a hneď za ním jednorazové heslo vygenerované tokenom prideleným používateľovi (v našom prípade "John").
 - Ak je napr. používateľské meno "John", otestujte prihlásenie podľa nasledujúceho obrázka:

```
login as: John
John@10.51.0.50's password: Password+OTP
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 3.13.0-24-generic x86_64)

* Documentation:  https://help.ubuntu.com/

$ █
```

PRIHLÁSENIE SSH s OTP (one-time password) POŽIADAVKOU

Ak chcete povoliť prihlásenie SSH s požiadavkou OTP, postupujte podľa nasledujúcich krokov.

ĎALŠIE KROKY, KTORÉ TREBA VYKONAŤ NA POČÍTAČI S UBUNTU

1. Postupujte podľa krokov opísaných v časti "Kroky v Ubuntu" nižšie
2. Szerkesszük az "/etc/ssh/sshd_config" fájl..
3. Nájďte riadok obsahujúci "ChallengeResponseAuthentication no" a nahraďte ho riadkom "ChallengeResponseAuthentication yes".
4. Reštartujte službu SSH pomocou nasledujúceho príkazu:
`sudo /etc/init.d/ssh restart`

KROKY NA VYKONANIE NA GREENRADIUS

1. Prihláste sa do webového administrátorského rozhrania GreenRADIUS
2. Prejdite na kartu "Global Configuration" a kliknite na ikonu "General".



3. v časti "General Configuration" vyberte v časti "OTP Input Method" možnosť "Prompt for OTP (RADIUS only)" a uložte ju.

General Configuration

General Configuration

OTP Input Method

Append OTP To Username
 Append OTP To Password
 Promot For OTP (RADIUS only)
 Yes No

Enable Password Authentication Through GreenRADIUS

Temporary Token Length: 8

Max Number of Tokens Per User: 5

On Service Fail, Send Email Alert

Yes No
Selecting "Yes" will send an email alert if OTP validation server is unavailable.

Email Address(es):

Email Sent From: GreenRADIUS@grva2000.example.com

YubiKey (Yubico OTP Mode) Configuration

Enable Auto-provisioning For YubiKey Tokens# Yes No

Enable Auto-provisioning For Multiple YubiKey Tokens Per User# Yes No

Allow Multiple Users To Share a YubiKey Token# Yes No

YubiKey OTP Public ID Length (1-8 bytes): 6

On Service Fail, Fallback To Single Factor Yes No

YubiKey (OATH-HOTP Mode) Configuration

Enable Auto-provisioning For OATH Tokens# Yes No

Enable Auto-provisioning For Multiple OATH Tokens Per User# Yes No

You also need to enable Auto-provisioning for respective domains under Domain Configuration

Save

TESTOVANIE SSH PRIHLÁSENIA NA POČÍTAČI UBUNTU POMOCOU DVOJFAKTOROVÉHO OVEROVANIA (POŽIADAVKA OTP)

1. Prihláste sa do počítača Ubuntu pomocou ľubovoľného klienta SSH, napríklad PuTTY
2. Zadáte používateľské meno a stlačte tlačidlo Enter
3. Potom bude požadované heslo. Zadáte heslo používateľa nastavené v ActiveDirectory/LDAP a stlačte kláves Enter.
4. Vyžiada sa jednorazové heslo (OTP). Vygenerujte OTP s ľubovoľným kľúčom priradeným používateľovi.
 - Napr. ak je používateľ "John", otestujte prihlásenie podľa nasledujúceho obrázka:

```
login as: John
Using keyboard-interactive authentication.
Password: Password
Using keyboard-interactive authentication.
Please provide OTP: OTP

Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

* Documentation:  https://help.ubuntu.com/

$
```

VYHĽADÁVANIE CHÝB:

Pre vyhľadávanie chýb, použite nasledujúci príkaz v systéme Ubuntu.

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