



Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET



Vilniaus universitetas

# Ankstyvo perspėjimo apie grėsmes paslauga

## Paslaugos administravimo instrukcija

Paslauga sukurta vykdant Europos socialinio fondo finansuojamą projektą „Mokslo ir studijų institucijoms LITNET teikiamų IT paslaugų plėtra“ Nr. 09.3.3-ESFA-V-711-01-0003



Kuriame  
Lietuvos ateitį

2014–2020 metų  
Europos Sąjungos  
fondų investicijų  
veiksmų programa

Vilnius  
2018 m.

## Centrinis serveris

Naudojama operacinė sistema – Ubuntu 16.04 LTS

Operacinės sistemos diegimo metu IP adresas nustatytomas statišškai, papildomai įrašoma programinė įranga: LAMP server, PostgreSQL database, OpenSSH server.

Naujai įdiegtame serveryje įdiegti pagrindines reikalingas programas:

```
apt-get install git supervisor postgresql-contrib php-mcrypt  
phpenmod mcrypt
```

```
curl -s https://deb.nodesource.com/gpgkey/nodesource.gpg.key | apt-key add -
```

```
$ sudo sh -c "echo deb https://deb.nodesource.com/node_10.x cosmic main \  
> /etc/apt/sources.list.d/nodesource.list"
```

```
$ sudo apt-get update
```

```
$ sudo apt-get install nodejs
```

### APGS kodo atsisiuntimas ir duomenų bazės paruošimas:

Sukurti sistemos naudotoją:

```
sudo -u postgres createuser apgs_server
```

Pakeisti jo slaptažodį:

```
sudo -u postgres psql
```

```
psql=# alter user apgs_server with encrypted password '<slaptazodis>';
```

Sukurti apgs duomenų bazę:

```
sudo -u postgres createdb apgs
```

Suteikti teises prie naujai sukurtos duomenų bazės

```
psql=# grant all privileges on database apgs to apgs_server;
```

Sukurti centrinės sistemos aplanką:

```
mkdir /etc/apgs
```

Atsiūsti apgs kodą:

```
cd /etc
```

```
git clone https://gitlab.ittc.vu.lt/vu13318/apgs.git
```

Importuoti duomenų bazės schema:

```
sudo -u postgres psql apgs < /etc/apgs/db_schema/schema.sql
```

Sukurti vietinį naudotoją sistemoje, su kuriuo bus galima prisijungti per WEB:

```
sudo -u postgres psql -d apgs
```

```
apgs=# CREATE EXTENSION pgcrypto schema users;
```

```
apgs=# SET SCHEMA 'users';
```

```
apgs=# INSERT INTO users.users (email, username, password, role, institution) VALUES  
( 'admin@admin.vu.lt', 'admin', CRYPT('slaptazodis', GEN_SALT('md5')), 'admin', 'VU');
```

Nukopijuoti duomenų bazės prisijungimo duomenų konfigūracijos pavyzdinį failą:

```
cd /etc/apgs
cp config.js.template config.js
```

*config.js* faile pakeiskite duomenų bazės konfigūracijoje reikalingus laukus į prieš tai sukurtus naudotojo duomenis:

```
//duomenų bazės konfigūracija
var config = {
  user: 'apgs_server',
  database: 'apgs',
  password: 'slaptažodis',
  host: '127.0.0.1',
  port: 5432,
  max: 10,
  idleTimeoutMillis: 30000,
};
```

### **Sugeneruoti serverio raktą ir sertifikatą:**

```
cd /etc/apgs
mkdir cert
cd cert
Sugeneruoti raktą su slaptažodžiu:
openssl genrsa -des3 -out rsa.pem 2048
```

Sugeneruoti prašymą su serverio duomenimis:  
`openssl req -new -key rsa.pem -out server.csr`

Ištrinti slaptažodį iš rakto, kad nereikėtų suvedinėti kiekvieną kartą startavus serveriui:  
`cp rsa.pem rsa.pem.org`  
`openssl rsa -in rsa.pem.org -out rsa.pem`

Šį sertifikato pasirašymo failą reikia nusiųsti pasirašyti. Jei naudojamas savo paties pasirašytas sertifikatas, tada:  
`openssl x509 -req -days 365 -in server.csr -signkey rsa.pem -out server.crt`

Konfigūracijose nurodyti failų pavadinimai raktui **rsa.pem**, sertifikatui **server.crt**, esantys `/etc/apgs`.

Jei viską atlikote teisingai, galima pabandyti paleisti serverį ir prisijungti:  
`cd /etc/apgs`  
`nodejs server.js`

Jei serveris sėkmingai startavo, patikrinkite prisijungimą prie naudotojo sąsajos -  
[https://serverio\\_ip:3000](https://serverio_ip:3000)

Jei galite prisijungti su vietiniu naudotoju, sekite tolimesnes instrukcijas.

### **Apache konfigūracija**

Su standartiniais parametrais serveris pasiekiamas 3000 portu. Jei norima taip pat naudoti 443, reikia sukonfigūruoti apache proxy:

```
cp /etc/apgs/apache-site_ssl.conf /etc/apache2/sites-available/default-ssl.conf
```

Jei nenaudojamas DNS adresas [apgs.litnet.vu.lt](https://apgs.litnet.vu.lt), `default-ssl.conf` faile pakeisti šį adresą į atitinkamą

arba naudojamą IP. Taip pat su savo paties pasirašytais sertifikatais gali prisiųsti papildomų eilučių po `SSLProxyEngine On` parametro:

```
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off
```

Tada vykdomos komandos:

```
a2ensite default-ssl.conf
a2enmod ssl proxy proxy_wstunnel proxy_http
service apache2 restart
```

Jei viskas gerai, paleidus serverį, naudotojo sąsają galima pasiekti ir adresu [https://serverio\\_ip](https://serverio_ip).

### **APGS kaip tarnybos paleidimas**

Sukurti supervisor konfigūracinį failą:

```
vim /etc/supervisor/conf.d/apgs.conf
```

Jame įrašyti:

```
[program:apgs]
command=nodejs /etc/apgs/server.js
directory=/etc/apgs
stdout_logfile=/var/log/apgs.out
stderr_logfile=/var/log/apgs.err
autostart=true
autorestart=true
stopasgroup=true
killasgroup=true
user=root
```

Išsaugoti ir suvesti komandas:

```
supervisorctl reread
supervisorctl update
supervisorctl start apgs
```

Paslauga startuos operacinės sistemos paleidimo metu, tai pat bus paleista iš naujo dėl kokių nors klaidų. Žurnalų įrašai saugomi `/var/log/apgs.out` ir `/var/log/apgs.err`.

### **SSO**

SSO nustatymai yra `/etc/apgs/sso.js` faile. Paslaugos tiekėjo (SP) duomenys, kuriuos reikia perduoti Tapatybės tiekėjui (IdP) yra – `https://serverio_ip_ar_dns/metadata.xml`

Konfigūracijos faile pagrindiniai IdP nustatymai:

```
var cert = "IdP sertifikato tekstas ";
var idp_options = {
  sso_login_url: " prisijungimo per SSO nuoroda ",
  sso_logout_url: " atsijungimo nuoroda ",
  certificates: [cert]
};
```

Taip pat faile `metadata-apgs` pakeisti `<ds:X509Certificate>` duomenis į savo `server.crt` sertifikatą.

Automatinis kitų paslaugų tiekėjų (SP) aptikimas (Discovery) negalimas, IdP turi pateikti visus SP pats.

## **Sensorius**

Įdėjus SD kortelę į kortelių skaitytuvą ir prijungus prie kompiuterio tereikia įkelti sensoriaus atvaizdą (image).

Atsisiųskite naujausią atvaizdo versiją (rašymo metu *sensor\_1.0.iso*) iš sistemos administratoriaus. Įrašykite atvaizdą į SD kortelę jums patogiu būdu, pvz. Linux komanda šiam veiksmui atlikti:

```
dd bs=1M if=/vieta_iki_atvaizdo/sensor_1.0.img of=/dev/sdX
```

kur sdX yr SD kortos vieta.

Nustačius pagrindinius parametrus (APGS naudotojo sąsaja → Nustatymai → Instrukcijos → Sensorių diegimas), sensorių galima jungti į tinklą ir jis pradės pilnai veikti.