

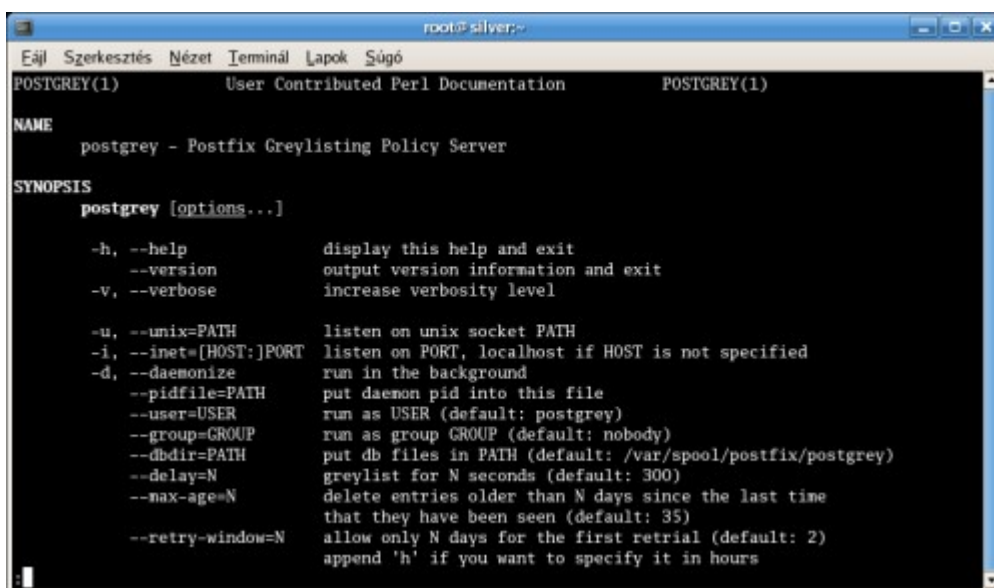
Spamszűrés hatékonyabban I. - Postgrey

A beérkező spamek és vírusok számát egy pofonegyszerű, ámde hatékony módszerrel csökkenthetjük.

A spamek elleni harcban eddig elsősorban olyan eszközöket használtunk, amelyek segítségével a már beérkezett levelekről próbáltuk megállapítani, hogy kéretlen reklámlevelek-e avagy sem. Léteznek ugyan RBL listák, amelyek révén már az SMTP kapcsolat egy korai fázisában elutasíthatjuk a levél beérkezését, de ezek közel nem jelentenek százszázalékos biztonságot, ráadásul nagy a veszélye annak, hogy ártatlan hostok is feketelistára kerülnek. Egy pofonegyszerű, ámde hatékony megoldással azonban jelentősen csökkenthetjük a kéretlen levelek és vírusok számát - ez lesz a greylisting.

A módszer nem véletlenül kapta a *szürkelista* elnevezést. Lényege, hogy mindaddig fenntartással kezelünk egyes leveleket, amíg meg nem bizonyosodunk azokról, hogy ártatlan, hagyományos küldeményekről van szó. De hogyan is működik mindez? A greylisting során egy olyan alkalmazást (a **postgrey**, illetve az **sqlgrey** nevűt) fogunk használni, amely minden egyes beérkező e-mail küldője, címzettje és a küldő host adatai alapján egy ún. **tripletet** generál. A triplet a keletkezésekor bekerül egy adatbázisba, amelyben rövidebb-hosszabb ideig eltároljuk annak "születési idejét" és előfordulásainak számát is. Ha a postgrey/sqlgrey első alkalommal találkozik ezzel a triplettel, akkor meghívóját - esetünkben a Postfixet - értesíteni fogja erről, amely 450-es (ideiglenes hiba) SMTP üzenettel visszautasítja a levél kézbesítését beállított ideig (alapértelmezésben 300 másodpercig). És itt jön a nagy ötlet: a normálisan működő SMTP kiszolgálók a hiba fellépésekor egy bizonyos idő eltelte után ismét meg fogják próbálni a levél kézbesítését, ekkor viszont már a postgrey/sqlgrey felismeri a tripletet és engedélyezni fogja a levél beérkezését. A spam- és vírusmotorok azonban nincsenek ilyen hibák lekezelésére felkészítve, így nem foglalkoznak a kéretlen levél további feladásával. Ügyes, nem? :)

Első hallásra bonyolultnak tűnik a folyamat, a valóságban azonban néhány apró kiegészítő telepítésével és pár sornyi konfigurációval hadrendbe állíthatjuk ezt a remek kis szűrőrendszert. Előtte azonban említsük meg a módszer két hátulütőjét: a levelek első alkalommal némi késéssel érhetnek el a címzethez (ez függ a küldő szerver működésétől), illetve ha a végső kézbesítést végző szerver nem az RFC-knek megfelelően működik, akkor bizony levelünk elveszhet a nihilben. Mindkettőre van azonban némi megoldás, de erről később.



```
root@silver:~
Ejrl Szerkesztés Nézet Terminál Lapok Súgó
POSTGREY(1)      User Contributed Perl Documentation  POSTGREY(1)

NAME
  postgrey - Postfix Greylisting Policy Server

SYNOPSIS
  postgrey [options...]

  -h, --help           display this help and exit
  --version           output version information and exit
  -v, --verbose       increase verbosity level

  -u, --unix=PATH     listen on unix socket PATH
  -i, --inet=[HOST:]PORT listen on PORT, localhost if HOST is not specified
  -d, --daemonize     run in the background
  --pidfile=PATH     put daemon pid into this file
  --user=USER        run as USER (default: postgrey)
  --group=GROUP      run as group GROUP (default: nobody)
  --dbdir=PATH       put db files in PATH (default: /var/spool/postfix/postgrey)
  --delay=N          greylist for N seconds (default: 300)
  --max-age=N        delete entries older than N days since the last time
                    that they have been seen (default: 35)
  --retry-window=N   allow only N days for the first retrial (default: 2)
                    append 'h' if you want to specify it in hours
```

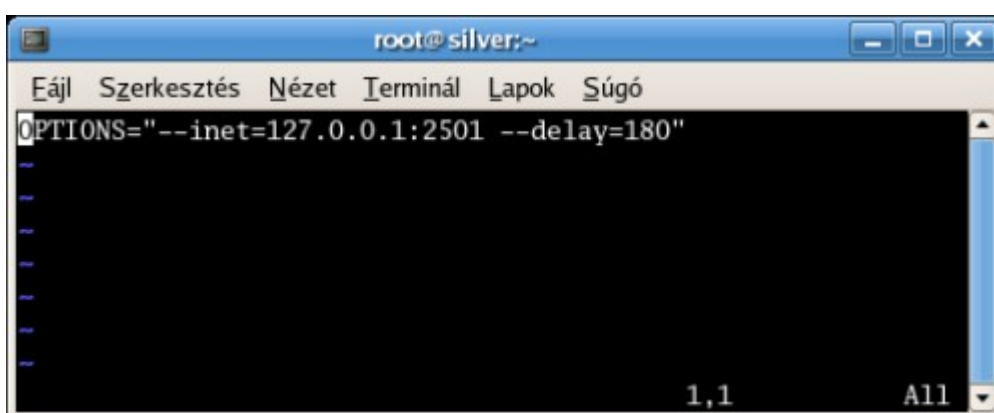
ábra 1. A postgrey dokumentációja

A postgrey (<http://isg.ee.ethz.ch/tools/postgrey/>) a Postfixszel együttműködő alkalmazás. A tripleteket BerkeleyDB adatbázisban tárolja, így megoldott azok konzisztens tárolása. Figyeli a tripletek utolsó előfordulásának idejét, ez alapján egy adott idő letelte után törli azokat az adatbázisból, de képes a lista automatikus bővítésére és ún. *whitelist* használatára is. A Debian disztribúció már tartalmazza a szükséges csomagot, de természetesen más környezethez is elérhető.

Telepítsük fel a postgrey-t! Fedora alatt installáljuk a yum segítségével az alábbi csomagokat:

- **perl-Net-Server**
- **perl-IO-Multiple**
- **perl-BerkeleyDB**

Töltsük le az RPM-csomagot a <http://www.lfarkas.org/linux/packages/> címről és tegyük fel: **rpm -Uvh postgrey-1.27-0.noarch.rpm**. A csomagban található daemon alapértelmezett beállításait a `/etc/sysconfig/postgrey` állományban tudjuk módosítani, melyekről információt a **perldoc postgrey** paranccsal kaphatunk. A legszükségesebbek:



```
root@silver:~
Éjl Szerkesztés Nézet Terminál Lapok Súgó
OPTIONS="--inet=127.0.0.1:2501 --delay=180"
1,1 All
```

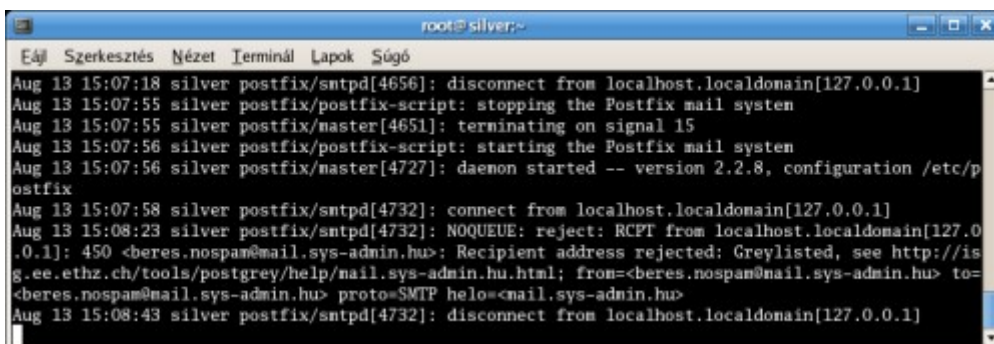
ábra 2. `/etc/sysconfig/postgrey`

Ha ezzel megvagyunk, akkor indíthatjuk a postgrey-t a **service postgrey start**-tal.

Következő lépésként a Postfix **main.cf** állományát kell módosítanunk. Keressük meg benne az **smtpd_recipient_restrictions** paramétert, és fűzzük hozzá az alábbiakat:

check_policy_service inet:127.0.0.1:60000

A portszám természetesen függ attól, hogy a konfigurációs fájlban mit határoztunk meg. A Postfix újraindításakor a szolgáltatás már él, ezt megfigyelhetjük a naplófájlok üzeneteiben:



```
root@silver:~
Éjl Szerkesztés Nézet Terminál Lapok Súgó
Aug 13 15:07:18 silver postfix/smtpd[4656]: disconnect from localhost.localdomain[127.0.0.1]
Aug 13 15:07:55 silver postfix/postfix-script: stopping the Postfix mail system
Aug 13 15:07:55 silver postfix/master[4651]: terminating on signal 15
Aug 13 15:07:56 silver postfix/postfix-script: starting the Postfix mail system
Aug 13 15:07:56 silver postfix/master[4727]: daemon started -- version 2.2.8, configuration /etc/postfix
Aug 13 15:07:58 silver postfix/smtpd[4732]: connect from localhost.localdomain[127.0.0.1]
Aug 13 15:08:23 silver postfix/smtpd[4732]: NOQUEUE: reject: RCPT from localhost.localdomain[127.0.0.1]: 450 <beres.nospam@mail.sys-admin.hu>; Recipient address rejected: Greylisted, see http://isg.ee.ethz.ch/tools/postgrey/help/mail.sys-admin.hu.html; from=<beres.nospam@mail.sys-admin.hu> to=<beres.nospam@mail.sys-admin.hu> proto=SMTP helo=<mail.sys-admin.hu>
Aug 13 15:08:43 silver postfix/smtpd[4732]: disconnect from localhost.localdomain[127.0.0.1]
```

Debian alatt adjuk ki az **apt-get install postgrey** parancsot, módosítsuk a `/etc/default/postgrey` állományt és a Postfix **main.cf**-jét, majd indítsuk el, illetve újra a postgrey-t és a Postfixet.

Mint említettük, néhány szabályos levéltranszakció lebonyolódásáig a felhasználóink panaszkodhatnak a levélforgalom lelassulására, azután viszont azt fogják látni, hogy a kéretlen üzenetek száma drasztikusan csökken.

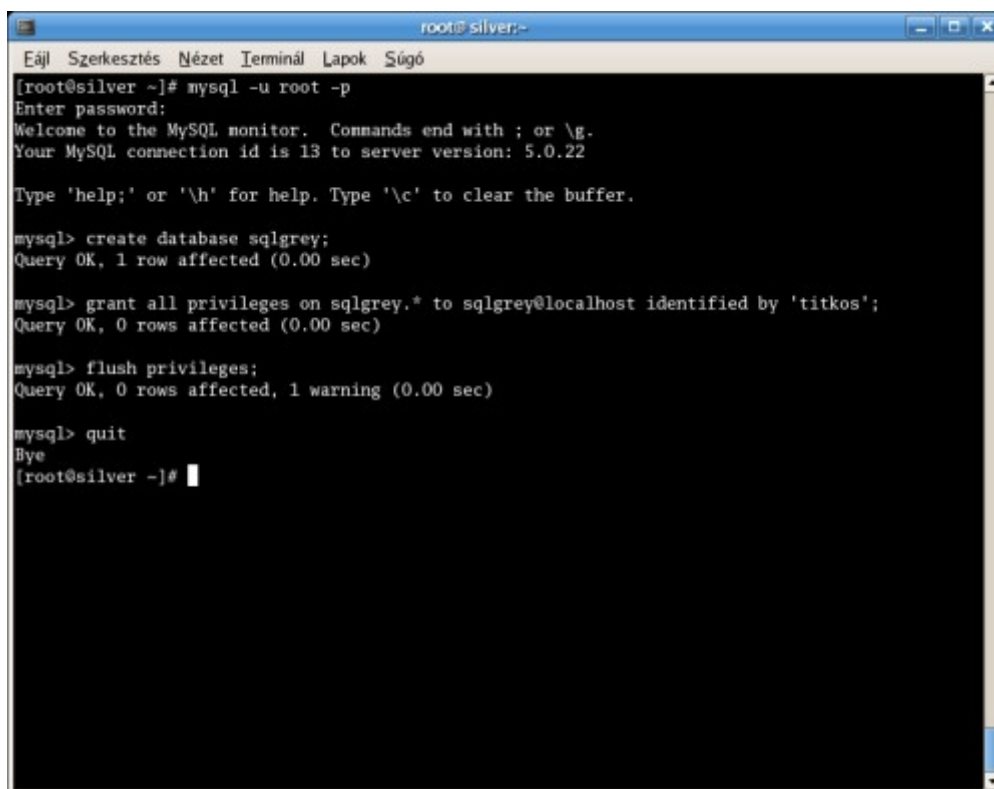
Spamszűrés hatékonyabban II. - SQLgrey

Jelen cikkünkben a postgres SQL-alapú változatát mutatjuk be.

Az előző cikkünkben bemutatott **postgrey** önálló BerkeleyDB adatbázisban helyezi el a tripleteket. Előfordul azonban, hogy szeretnénk ezt az adatbázist megosztani több levelezőszerver között vagy gondoskodni szeretnénk arról, hogy az adatbázis meghibásodásakor is elérhető legyen a szolgáltatás. Minderre (is) megoldást jelenthet az **SQLgrey**, amelyben a DBD-t felválthatjuk a MySQL, PostgreSQL, SQLite triumvirátus bármely tagjával.

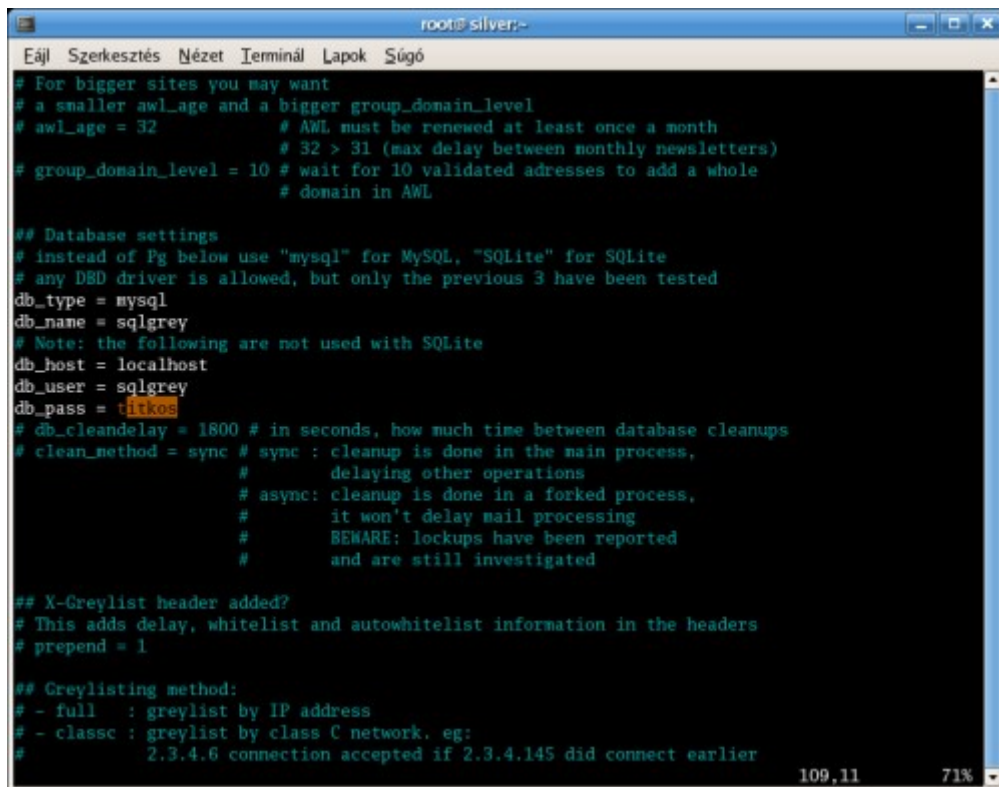
Kis nehezítés, hogy az SQLgrey jelenleg egyetlen disztribúcióban sem található meg, így kézzel kell gondoskodnunk a teljes telepítésről. Nem jelenthet problémát, ugyanis a <http://sqlgrey.sourceforge.net/> címről letölthető forrás-RPM, noarch-RPM, illetve forrás formában. Nézzük végig, hogyan telepíthetjük őt Fedora Core 5 alá! Példáink MySQL mellé szólnak, de minimális változtatással működnek a másik kettőn is.

Első lépésként győződjünk meg arról, hogy rendszerünkön működőképes állapotban van-e bármelyik fent említett SQL kiszolgáló. Ha ezzel végeztünk, akkor hozzunk létre egy adatbázist és egy felhasználót az sqlgrey számára:



```
root@silver:~  
Ejrl Szerkesztés Nézet Terminál Lapok Sűgő  
[root@silver ~]# mysql -u root -p  
Enter password:  
Welcome to the MySQL monitor. Commands end with ; or \g.  
Your MySQL connection id is 13 to server version: 5.0.22  
  
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.  
  
mysql> create database sqlgrey;  
Query OK, 1 row affected (0.00 sec)  
  
mysql> grant all privileges on sqlgrey.* to sqlgrey@localhost identified by 'titkos';  
Query OK, 0 rows affected (0.00 sec)  
  
mysql> flush privileges;  
Query OK, 0 rows affected, 1 warning (0.00 sec)  
  
mysql> quit  
Bye  
[root@silver ~]#
```

Szükség lesz még a perl(Date::Calc) modulra is, ezért telepítsük a **yum install perl-Date-Calc.i386** utasítással, ezután töltsük le és installáljuk az előbbi címen található sqlgrey-1.6.7-1.noarch.rpm csomagot is. Ha sikeresen lezajlott, akkor az sqlgrey beállításait a `/etc/sqlgrey/sqlgrey.conf` fájlban kell módosítanunk. Számos beállítás gyári értékekkel is működik, azonban az adatbázis nevét, a felhasználó nevét és jelszavát mindenképpen meg kell adnunk:

A terminal window titled 'root@silver:-' showing the configuration of the SQLgrey service. The window has a menu bar with 'Ejél Szerkesztés Nézet Terminál Lapok Súgó'. The terminal content includes comments and configuration parameters for SQLgrey, such as 'db_type = mysql', 'db_name = sqlgrey', and 'db_pass = titkos'. The window's status bar at the bottom right shows '109,11' and '71%'.

```
root@silver:-
Ejél Szerkesztés Nézet Terminál Lapok Súgó
# For bigger sites you may want
# a smaller awl_age and a bigger group_domain_level
# awl_age = 32 # AWL must be renewed at least once a month
# # 32 > 31 (max delay between monthly newsletters)
# group_domain_level = 10 # wait for 10 validated addresses to add a whole
# # domain in AWL

## Database settings
# instead of Pg below use "mysql" for MySQL, "SQLite" for SQLite
# any DBD driver is allowed, but only the previous 3 have been tested
db_type = mysql
db_name = sqlgrey
# Note: the following are not used with SQLite
db_host = localhost
db_user = sqlgrey
db_pass = titkos
# db_cleandelay = 1800 # in seconds, how much time between database cleanups
# clean_method = sync # sync : cleanup is done in the main process,
# # delaying other operations
# # async: cleanup is done in a forked process,
# # it won't delay mail processing
# # BEWARE: lockups have been reported
# # and are still investigated

## X-Greylist header added?
# This adds delay, whitelist and autowhitelist information in the headers
# prepend = 1

## Greylisting method:
# - full : greylist by IP address
# - classc : greylist by class C network. eg:
# # 2.3.4.6 connection accepted if 2.3.4.145 did connect earlier
109,11 71%
```

Ha ezzel megvagyunk, akkor indítsuk el a szolgáltatást (**service sqlgrey start**), illetve állítsuk be a Postfix konfigurációjában a *check_policy_service* direktívát az előző cikkben említett módon. Ha a Postfixet újraindítjuk, akkor máris üzemel a megoldásunk.

Ha több host között szeretnénk megosztani az SQLgrey adatbázisát, gondoskodnunk kell a mysql távoli elérhetőségéről, illetve a felhasználó jogosultságairól is!

Béres László
rendszermérnök, RHCE
beres.laszlo@sys-admin.hu