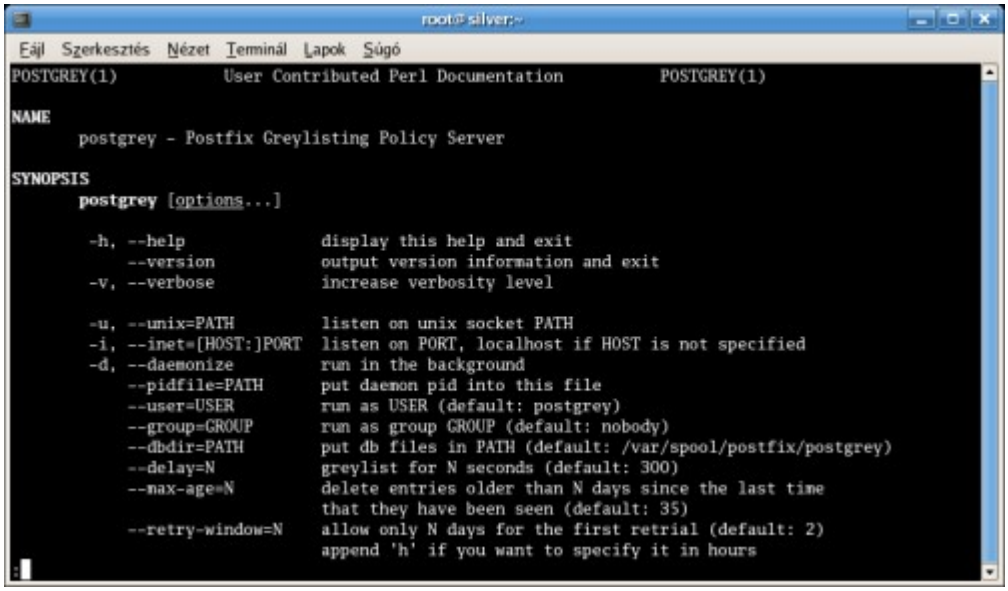
Spamszűrés hatékonyabban I. - Postgrey

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 eltáruljuk 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 másodprecig). 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 címzetthez (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.



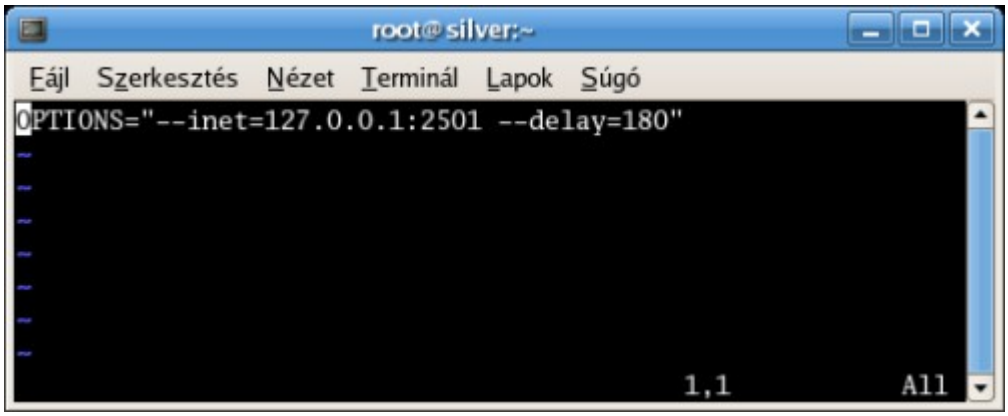
ábra 1. A postgrey dokumentációja

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:



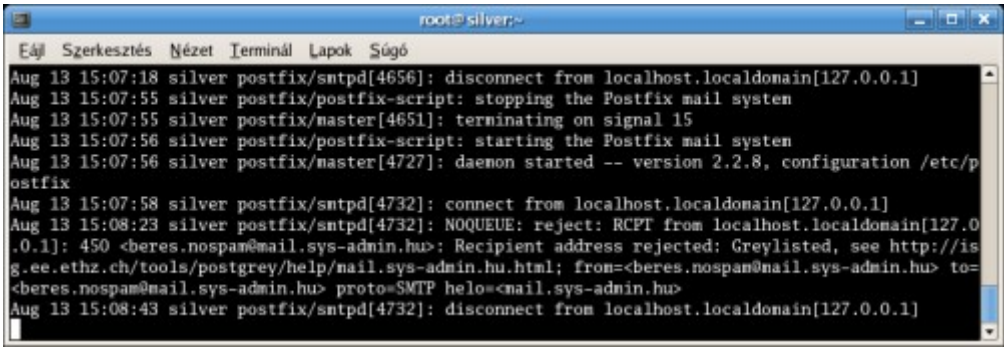
ábra 2. /etc/sysconfig/postgrey

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:



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 levéltranzakció lebonyolódásáig a felhasználóink panaszkodhatnak a levélforgalom lelassulására, azután viszont azt fogják látni, hogy a kéretlen üzeneteke száma drasztikusan csökken.

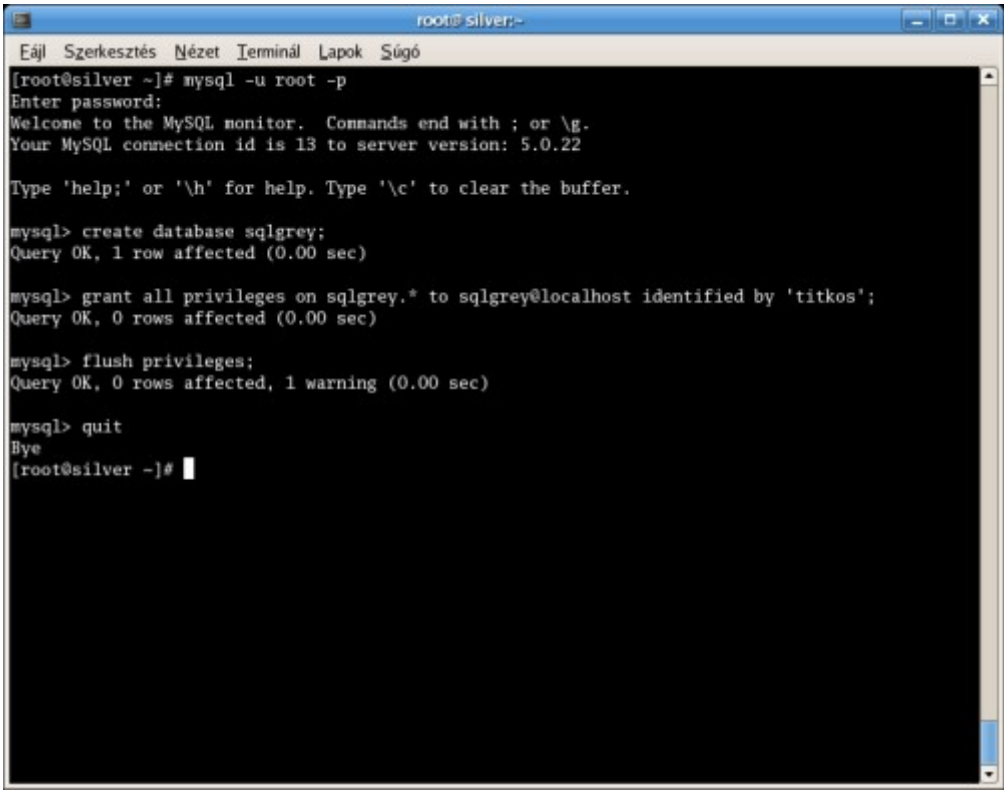
Spamszűrés hatékonyabban II. - SQLgrey

Jelen cikkünkben a postgrey SQL-alapú változatát mutatjuk be.

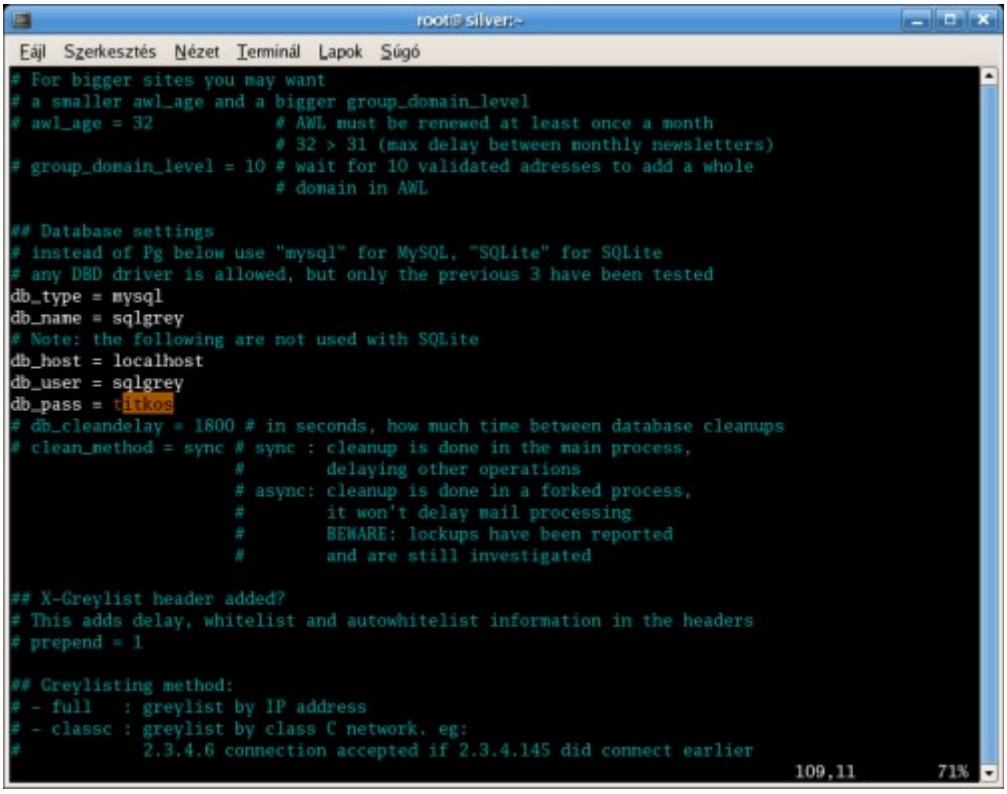
Az előző cikkünkben bemutatott **postgrey** önálló BerkeleyDB adatbázisban helyezi el a tripleteket. Előfordul azonban, hogy szeretnénk ezt az adatbázist megosztani több levelezőszerver között vagy gondoskodni szeretnénk arról, hogy az adatbázis meghibásodásakor is elérhető legyen a szolgáltatás. Minderre (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:



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:



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