Postfix kiszolgáló bővítése Clam Antivirussal

Linuxos levélkiszolgálónkat nagyteljesítményű védelmi vonallal felszerelve megvédhetjük a bajtól a sérülékeny rendszereket.

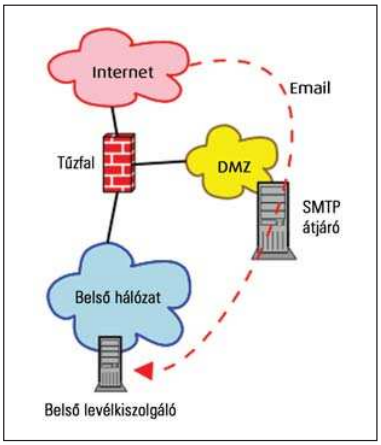
A *Linux Journal* 2004-es *Szerkesztői Díját* a biztonsági eszközök között a *ClamAV*, egy teljes mértékben szabad és nyílt forrású víruskereső kapta, amely ugyan jellemzően Linuxon fut, ám számos különböző géptípus vírusait képes felismerni. (Lásd: ***Linuxvilág,*** 2004. szeptemberi szám) Mint ***Reuven Lerner*** a díjakról szóló cikkben megjegyezte, a ***„ClamAV miatt az üzleti víruskereső programok tényleg futhatnak a pénzük után”***.
Ez alkalommal szeretném megmutatni, hogy ***Postfix*** alapú elektronikus levél átjárónkon hogyan használhatjuk ki a *ClamAV* tudását. Eközben szó esik majd az ***Amavisd-new***-ről, erről a sokoldalú, elektronikus levelek feldolgozására használható démonról, amely létfontosságú összekötőként szolgál a levélkiszolgálók, mint a ***Postfix*** és a ***Sendmail***, valamint a leveleket ellenőrző eszközök, mint a *ClamAV* és a ***SpamAssassin*** között.

A rendszer felépítése

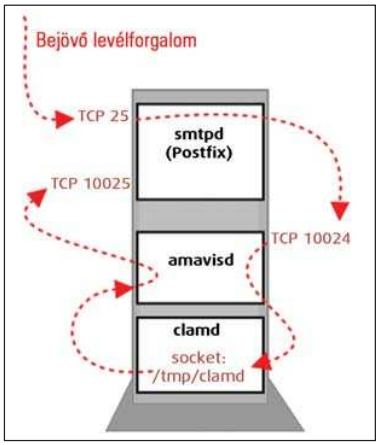
A továbbiakban ismertetendő összeállítás természetesen nem az egyetlen lehetséges vagy jó lehetőség a *ClamAV* használatára. Ez ugyanakkor a legelterjedtebb megoldás – mondjuk úgy, jellegzetesnek nevezhető. Tegyük fel, van egy ***SMTP*** átjárónk, az internet felől ez fogadja a saját cégünk, szervezetünk számára címzett elektronikus leveleket, a célunk pedig az, hogy az ***SMTP*** átjáró előzetesen ellenőrizze, a levelek nem tartalmaznak-e vírust. (*1. ábra*) Az átjáró feladata lehet az, hogy a leveleket a helyi postaládákban helyezze el, de belső levélkiszolgálónak való továbbításra is beállíthatjuk. A következőkben foglaltak függetlenek a tényleges levéltovábbítási módszertől.
Ha nagy forgalmú rendszert üzemeltetünk, akkor lehetséges, hogy az ***SMTP*** átjáró helyett a víruskeresést inkább egy különálló géppel érdemes elvégeztetnünk – az itt ismertetett eszközök ekkor is működni fognak. Az egyszerűség kedvéért azonban, illetve igazodva a szokásokhoz, most tegyük fel, hogy a víruskereső magán az ***SMTP*** átjárón fut. ***Levéltovábbító ügynökként (Mail Transfer Agent, MTA)*** ***Postfixet*** használunk, ez ugyanis egy népszerű és biztonságosan futtatható program, továbbá a *ClamAV*-vel is gond nélkül képes együttműködni. Csakhogy a ***Postfix*** nem tud közvetlenül kapcsolatba lépni a *ClamAV*-vel, vagy legalábbis ez a kapcsolat nem megbízható. A *ClamAV* sem jeleskedik az elektronikus levelek elemzésében, inkább adatfolyamokkal tud dolgozni. Ezért van szükségünk a kisegítő démonra, az ***Amavisd-new***-ra. Az ***Amavisd-new*** szintén ingyenes és nyílt forrású eszköz, létének egyetlen célja az ***MTA***-k, mint a ***Postfix*** és a ***Sendmail***, valamint a víruskereső és a szemétszűrő programok, mint a *ClamAV* és a ***SpamAssassin*** közötti tranzakciók közvetítése. Az ***Amavisd-new*** egyebek mellett kiválóan teljesít az elektronikus levelek ***MIME*** mellékleteinek hagyományos, a keresők által is érhető adatfájlokká alakításában.
Az ***Amavisd-new*** démonja, az ***amavisd*** számos protokollon keresztül képes kommunikálni, ide értendő az ***SMTP*** és az ***LMTP*** elektronikus levéltovábbító protokoll mellett a ***UNIX*** foglalatok rendszere is. Ebben az esetben az ***amavisd***-t úgy állítjuk be, hogy a leveleket ***SMTP***-n keresztül, a 10024-es számú ***TCP*** kapun át fogadja, annak helyi ***UNIX*** foglalatán keresztül lépjen kapcsolatba a *ClamAV*-vel, majd a levelet és a víruskeresés eredményét a 10025-ös ***TCP*** kapun adja tovább a ***Postfixnek***. A leveleknek az ***SMTP*** átjárón keresztüli mozgását a *2. ábra* szemlélteti.

A program beszerzése és telepítése

A *ClamAV* és az ***Amavisd-new*** egyaránt ***Perlben*** íródott, és számos *Perl*-modultól függ. Mindenkinek javaslom tehát, hogy a két eszköz valamelyik újabb változatának saját terjesztéséhez készült bináris csomagját használja. Még egyszerűbb, ha az ***apt-get***, a ***Yum*** vagy az ***up2date*** szolgáltatásaira hagyatkozunk, így nem kell foglalkoznunk a függőségek kézi telepítések során felmerülő gondjával.
A *ClamAV* webhelye, amellett, hogy itt lelhető fel a legújabb *ClamAV* forráskód is, tartalmaz egy oldalt, amelyen a *ClamAV* különféle Linux-terjesztésekhez és egyéb operációs rendszerekhez készült bináris csomagjainak elérhetőségét gyűjtötték össze. A ***Red Hat*** vagy ***Fedora*** terjesztést használók ***Dag Wieers*** oldalán (lásd az internetes forrásokat) találnak ***Yum*** ágakat és ***up2date*** forrásokat, *ClamAV*-t és ***Amavisd-new***-t egyaránt. Az ***Amavisd-new*** weboldalon további ***Amavisd-new*** csomagok forrásaira mutató hivatkozásokat is találunk, illetve a legújabb ***Amavisd-new*** forráskódot is innen tölthetjük le. A *ClamAV* a ***sarge*** kiadása óta a ***Debian*** alapcsomagja, az ***Amavisd-new*** pedig például a ***SuSE*** rendszerekben a 9.1-es kiadás óta szerepel.
Ha bármelyik összetevőt forráskódból vagy önálló csomagból telepítjük, akkor a ***Yum***, ***up2date*** vagy ***apt-get*** alapú



1. ábra Példa levelezőrendszer



2. ábra A Postfix, az Amavisd-new és a ClamAV közötti adatáramlás

megoldással ellentétben nekünk kell ügyelnünk arra, hogy az ***Amavisd-new***-hoz tartozó telepítési leírás ***Prerequisites*** (előfeltételek) című részében foglaltakat teljesítsük. Sajnos a ***ClamAV*** telepítésének feltételeit eléggé hiányosan foglalták össze. Ha kétségeink támadtak, semmibe sem kerül saját ***ClamAV RPM***-ünk nevével kiadni az

```
rpm –test -iv clamav_csomagnév.rpm
```

parancsot, így láthatjuk, hogy mi hiányzik még a gépünkről. Ha van egy kis szerencsénk, akkor terjesztésünkhöz elérhetők a ***ClamAV*** és az ***Amavisd-new*** használatához szükséges ***Perl***-modulok csomagjai. Amit mégsem találunk, azt a ***CPAN***-ról vagy az egyéb, a saját terjesztésünkhöz készített csomagokkal foglalkozó weboldalak valamelyikéről tölthetjük le.

A ClamAV beállítása

A ***ClamAV*** és az ***Amavisd-new*** telepítése után nekiláthatunk a beállítások megadásának. A ***ClamAV***-vel kezdünk, ez az egyszerűbb. A ***ClamAV*** beállító fájlja a */etc/clamav.conf*. Nyissuk meg a kedvenc szövegszerkesztőnkkel. Az 1. ábrán azok a beállítások láthatók, amelyeket a legtöbbeknek azonnal meg kell változtatniuk.

Az első sor ártatlannak tűnik, de mindenképpen tegyük megjegyzésbe. Ha ezt elmulasztjuk, a ***clamd*** nem fog futni. A két `LogFile...` beállítás alapesetben megjegyzésként szerepel. Ha engedélyezni akarjuk a naplózást, vegyük ki őket megjegyzésből. A naplófájlt mi választjuk ki, maximális mérete `LogFileMaxSize`, ennek elérésekor a fájl felülírásra kerül. A `DatabaseDirectory` kulcsfontosságú beállítás. A ***ClamAV*** itt tárolja a vírusaláírások adatbázisait, mondhatnánk, az agyát. Az általam telepített ***ClamAV RPM***-ben található ***clamd*** démon úgy volt lefordítva, hogy a */usr/share/clamav* könyvtárat használta erre a célra, miközben a hozzá mellékelt példa ***clamav.conf*** fájlban a */var/lib/clamav* érték szerepelt, igaz, megjegyzésbe téve. Úgy döntöttem, kiveszem megjegyzésből a sort, és */usr/share/clamav* értékre módosítom, kerülendő a félreértéseket.

A `LocalSocket` beállítás azt határozza meg, hogy a ***clamd*** melyik foglalaton keresztül tartja a kapcsolatot a külvilággal, jelen esetben az ***Amavisd-new***-val. Ha használjuk ezt a beállítást, márpedig én ezt javaslom, akkor ügyeljünk arra, hogy a `TCPSocket` és a ***TCPAddr*** beállítás megjegyzésben maradjon. Saját ***Genco*** csomagomnál a `LocalSocket` elérési út alapértéke `/tmp/clamd` volt, amivel az a baj, hogy a /tmp bárki által írható-olvasható. Helyette javaslom a `/usr/share/clamav/clamd.sock` elérési út választását, a */usr/share/clamav* engedélyeit pedig állítsuk `rwxrwx` értékre, vagyis vonjuk meg az egyéb felhasználók olvasási, írási és futtatási jogát. Az *1. kódrészlet* utolsó beállítása a `User`, ez annak a felhasználónak a neve, amelynek fiókjával a ***clamd***-nek indulása után futnia kell. A ***clamd***-t a rootnak kell elindítania, de ha ezt a beállítást kivesszük megjegyzésből, majd értéket adunk neki, akkor a ***clamd*** indulás után lefokozza önmagát.

A legtöbbünk számára elég ennyit ismerni a */etc/clamav.conf* fájlból. A ***clamd*** indítása előtt ellenőrizzük, hogy van-e rendszerünkben fiókja a ***clamav***-nek, és a */etc/clamav.conf* fájlban szereplő elérési utakra vonatkozó engedélyeket megfelelően beállítottuk-e. A fiók csoportjaként szintén érdemes a ***clamav***-t választani. Amint a következő részben látni fogjuk, így könnyebben meg tudunk osztani bizonyos erőforrásokat a ***clamd*** és az ***amavisd*** között.

A */etc/passwd* bejegyzése a ***clamav*** fiókhoz a következő:

```
clamav:x:52:52:ClamAV Daemon:/:/bin/false
A /etc/group fájl clamav csoportfiókja pedig a következő:
clamav:x:52:
```

Ha a ***clamd*** beállításán is túlestünk, elindításához csupán a ***clamd*** parancsot kell kiadnunk. Ha a ***ClamAV***-t bináris csomagból telepítettük, */etc/init.d* névvel valószínűleg bekerült rendszerükbe a ***clamd*** indító parancsfájlja is. Ha így van, akkor ne feledkezzünk el az engedélyezéséről, így a ***clamd*** már a rendszer betöltésekor elindul. Ha a fájl hiányzik, akkor magunknak kell gondoskodnunk a létrehozásáról.

Az Amavisd-new beállítása

Ahogy a ***clamd***, úgy az ***amavisd*** beállításait is egyetlen fájl tárolja, ez a */etc/amavisd.conf*. Ezzel azonban egy kicsit több munkánk lesz. A *2. kódrészlet* saját */etc/amavisd.conf* fájlom legfontosabb elemeit tartalmazza.

A 2. kódrészlet első két beállítása a `$daemon_user` és a `$daemon_group`, ezek az ***amavisd*** futtatásához használt felhasználói és csoportfiókot adják meg. Értéküket rendre legyen ***amavis*** és ***clamav***. Mint korábban említettem, szerintem érdemes közös csoportba rendelni az ***amavisd*** és a ***clamd*** fájljait, így tehát van értelme az amavisd-t is ezzel a csoporttal futtatni. Az ***amavishoz*** tartozó */etc/passwd* bejegyzés így néz ki:

```
amavis:x:53:52:Amavisd-new
Daemon:/var/amavis:/bin/false
```

A `$mydomain` szervezetünk tartománynevét adja meg. A `$MYHOME`, amelyet az ***amavis*** fiókjának kezdőkönyvtárára

kell állítani, az *Amavisd*-new fájljainak gyökérkönyvtárát határozza meg, ez általában a */var/amavis*. Erre a könyvtárra csak a root kapjon írási jogot, és a tulajdonjogot is neki adjuk. A `$QUARANTINEDIR` annak a könyvtárnak az elérési útja, amelybe az *amavisd*-vel a karanténba helyezett elektronikus leveleket el szeretnénk helyeztetni. A könyvtár tulajdonosa az *amavis* felhasználói fiókja legyen, és kizárólag ez kapjon írási jogot hozzá.
A `$db_home`, melyet lehetséges, hogy ki kell vennünk megjegyzésből, azt határozza meg, hogy az *amavisd* hol tárolja adatbázisait, például a gyorstárazott keresési eredményeket.
A `$helpers_home` az a könyvtár, amelybe az *amavisd* saját `SpamAssassin` beállításait írja, és néhány további apróságot helyez el. Lehetséges, hogy alapesetben a `$helpers_home` megjegyzésként szerepel. A `$db_home` és a `$helpers_home` könyvtárat az *amavis* felhasználói fiókja birtokolja, és kizárólag általa legyen írható.
A `$pid_file` és a `$lock_file`, melyek szintén megjegyzésként kerülhetnek a kezünk alá, az *amavisd* folyamatazonosító és zárolási fájljának helyét adják meg.
A `$log_level` szabja meg, hogy az *amavisd* naplóüzenetei mennyire legyenek részletesek. Itt 0 - 5 közötti értéket adhatunk meg, ahol az 5 jelenti a legrészletesebb naplózást. Az alapérték 0, személyes tapasztalatom szerint a 2-es szint elegendő adatot szolgáltat, de a naplófájl sem hízik kezelhetetlen méretűre. Alapesetben az *amavisd* naplóüzeneteit `mail` erőforrásként a *syslog*-nak küldi el, vagyis az *amavisd* és a *Postfix* naplóüzenetei ugyanarra a helyre kerülnek.
A következő négy beállítás az *amavisd* által vírus vagy levélszemét felismerésekor küldött levelekre vonatkozik.
A `$virus_admin` az az elektronikus levélcím, amelyre a vírusokról szóló értesítőket kapni fogjuk. Érvényes címnek kell lennie, ha az itt szereplő érték még nem szerepelne benne, akkor gondoskodjunk a helyi `aliases` fájl frissítéséről. A gyakorlatban itt jellemzően a rendszergazda, vagyis a saját címünk szerepel.
Arra is van lehetőség, hogy az *amavisd* az egyes levelek eredeti címzettjeinek vagy küldőjének küldjön értesítést, ám ezzel csak bosszúságot fogunk okozni másoknak, hiszen a levélszemetek és a vírusos levelek feladójának címe szinte mindig hamis. Jobb tehát, ha lemondunk erről a lehetőségről.
A `$mailfrom_notify_admin` és a `$mailfrom_notify_spamadmin` rendre azt a feladócímet adja meg, amellyel az *amavisd* a vírusokról és a levélszemetekről szóló értesítő leveleket feladja.
Ezen a ponton végre elérkeztünk az *amavisd.conf* lényegéhez: a *ClamAV*-hez tartozó víruskereső beállításokhoz. Nálam az alapértelmezett */etc/amavisd.conf* fájl a teljes részt megjegyzésbe téve tartalmazta, tehát azzal kezdtem, hogy töröltem a # karaktereket a sorok elejéről. Szükség esetén tehát ne feledkezzünk meg erről a lépésről.
Mindenképpen ellenőrizzük a *clamd* foglalatának ebben a részben megadott elérési útját. A 2. kódrészletben az alapértelmezett */var/run/clamav/clamd* helyett a */usr/share/clamav/clamd.sock* elérési út szerepel, ugyanaz, mint amit a */etc/clamav.conf* fájlban adtunk meg.
Ha megfelelően átírtuk a */etc/amavisd.conf* fájlt, és beállítottuk az *amavisd* könyvtáraira vonatkozó engedélyeket, akkor az *amavisd* parancsot – kapcsolók nélkül – kiadva indíthatjuk el a programot. Ahogy a *clamd*, úgy lehetséges, hogy

1. kódrészlet Nem alapértelmezett beállítások a /etc/clamav.conf fájban

```
# Példa
LogFile /var/log/clamd.log
LogFileMaxSize 5M
DatabaseDirectory /usr/share/clamav
LocalSocket /usr/share/clamav/clamd.sock
User clamav
```

az *amavisd* számára is létre kell hoznunk egy indító parancsfájlt. Javaslom, hogy elsőként a *clamd*-t indítsuk. Így elérhetjük, hogy mire az *amavisd* elindul, addigra a *clamd* foglalata már jelen legyen.
A clamd-hez hasonlóan az amavisd-t is a rootnak kell indítania. A program ezt követően az amavisd.conf fájlban megadott felhasználó és csoport jogosultságaival fut tovább.

A Postfix beállításai

ClamAV és *Amavisd-new* démonunk megkapta a kellő beállításokat, és el is indult. Még ne dőljünk hátra, némi tennivalónk még akad, ugyanis be kell állítanunk a *Postfixet* a tartalomszűrésre, továbbá frissítenünk kell a *ClamAV* vírusadatbázisát.
Egy fontos megjegyzés: a továbbiakban feltételezem, hogy a *Postfix* már be van üzemelve, és képes ellátni normál fogadó/továbbító feladatait.
Először nyissuk meg kedvenc szövegszerkesztőnkkel a */etc/postfix/master.cf* fájlt, majd – amennyiben még nem szerepelnek ott – fűzzük a *3. kódrészletben* látható sorokat a fájl végére.
Az *smtp-amavis* rész a *Postfix* kimenő, az *amavisd*-vel *SMTP*-n keresztül létesített kapcsolataira vonatkozik.
Ide a következő sor tartozik, ezt kell hozzáadnunk a */etc/postfix/main.cf* fájlhoz, illetve átírnunk, ha már szerepel benne:

```
content_filter = smtp-amavis:[127.0.0.1]:10024
```

Ezzel a sorral arra utasítjuk a *Postfixet*, hogy a *master.cf* fájlban megadott *smtp-amavis* felületen keresztül minden bejövő levelet küldjön ki a `127.0.0.1` címre, vagyis a helyi rendszernek, mégpedig a 10024-es *TCP* kapun, az *amavisd* alapértelmezett *SMTP* figyelő kapuján át. Az *amavisd* figyelő kapuját a */etc/amavisd.conf* fájl `$inet_socket_port` beállításának átírásával változtathatjuk meg.
A 3. kódrészlet második szakasza azt a bejövő felületet adja meg, amelyen keresztül a *Postfixnek* fogadnia kell az *amavisd* által visszaadott üzeneteket. A *Postfix* tehát a helyi hurokfelület, a `127.0.0.1`-es IP-cím 10025-ös TCP kapuján hallgatózik, ez az a kapu, amelyre alapesetben az *amavisd* az értesítéseket és a továbbított üzeneteket küldi. Az *amavisd* értesítési és továbbítási címét és kapuját rendre a */etc/amavisd.conf* fájlban szereplő `$notify_method` és a `$forward_method` beállítások átírásával változtathatjuk meg. A *master.cf* és a *main.cf* módosítása után a *Postfixet* újra kell indítani.

2. kódrészlet A /etc/amavisd.conf fontosabb beállításai

```
$daemon_user  = ´amavis´;
$daemon_group = ´clamav´;
$mydomain = ´pelda.org´;
$MYHOME   = ´/var/amavis´;
$QUARANTINEDIR = ´/var/virusoslevelek´;
$db_home   = "$MYHOME/db";
$helpers_home = "$MYHOME/var";
$pid_file  = "$MYHOME/var/amavisd.pid";
$lock_file = "$MYHOME/var/amavisd.lock";
$log_level = 2;
$virus_admin = "mick@$mydomain";
$mailfrom_notify_admin = "antivirus@$mydomain";
$mailfrom_notify_spamadmin = "antivirus
➥@$mydomain";

### http://www.clamav.net/
[´ClamAV-clamd´,
  \ &ask_daemon, ["CONTSCAN { } \ n",
"/usr/share/clamav/clamd.sock"],
  qr/\ bOK$/, qr/\ bFOUND$/,
  qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
```

3. kódrészlet A /etc/postfix/master.cf fájlhoz hozzáadandó sorok

```
smtp-amavis unix -    -     y     -     2  smtp
     -o smtp_data_done_timeout=1200
     -o disable_dns_lookups=yes

127.0.0.1:10025 inet n  -     n     -     -  smtpd
     -o content_filter=
     -o local_recipient_maps=
     -o smtpd_client_restrictions=
     -o smtpd_helo_restrictions=
     -o smtpd_sender_restrictions=
     -o
smtpd_recipient_restrictions=permit_mynetworks,
        ➥reject_unauth_destination
     -o mynetworks=127.0.0.0/8
     -o strict_rfc821_envelopes=yes
     -o smtpd_error_sleep_time=0
     -o smtpd_soft_error_limit=1001
     -o smtpd_hard_error_limit=1000
```

A rendszer ellenőrzése

Mielőtt bármilyen további műveletnek nekifognánk, ellenőrizzük a rendszert. A legegyszerűbb módszer az ellenőrzésre az, hogy küldünk magunknak egy levelet, amelybe az alábbi karakterláncot helyezzük el. Ez nem egy valódi vírus, hanem az *Eicar* tesztaláírásnak nevezett karakterlánc:

```
X5O!P%@AP[4\ PZX54(P^)7CC)7} $EICAR-STANDARD-
ANTIVIRUS-TEST-FILE!$H+H*
```

Ha minden rendben működik, az *amavisd* küldött az *amavisd.conf* `$virus_admin` beállításában megadott címünkre egy levelet, eredeti üzenetünk pedig az *amavisd.conf* `$QUARANTINEDIR` beállításában megadott karanténkönyvtárba került.
Az ellenőrzés idejére erősen ajánlott a levelezési naplófájl végének elkülönítése. Adjuk ki tehát a

```
tail -f /var/log/mail
```

parancsot, így elkülöníthetjük a *Postfix* és az *amavisd* naplóüzeneteit. Tapasztalatom szerint ez a leggyorsabb megoldás az esetleges hibák felismerésére, főleg akkor, ha a korábban javasolt módon növeltük az *amavisd* naplójának részletességét.
Ne feledjünk legalább egy tiszta próbalevelet küldeni, ezzel ellenőrizhetjük, hogy a *Postfix* továbbra is képes-e a szűretlen levelek fogadására és továbbítására.

A ClamAV adatbázisainak frissítése

Már csak egyetlen, de nem kevésbé fontos dolog van hátra, mégpedig a *ClamAV* vírusaláírásokat tartalmazó adatbázisainak frissítése, illetve az ezt a műveletet napi rendszerességgel végrehajtó *cron* munka megadása. A *ClamAV*-hez tartozik egy pontosan ilyen célra készült, *freshclam* nevű segédprogram.
Mivel a *freshclam* az egész rendszer legegyszerűbb eleme, és gyakorlatilag a helyből is kifutottam, mindenkinek meghagyom az élményt, hogy maga fedezze fel a *freshclam(1)* és a *freshclam.conf(5)* súgóoldalakat. Annyit azért gyorsan elmondanék, hogy a hétköznapok során csupán a

```
freshclam -l /naplófájl/elérési/útja
```

parancsot kell használnunk, ahol a `/naplófájl/elérési/útja` azt a fájlt adja meg, amelybe a *freshclam* a naplóüzeneteit írja.
A *freshclamet* néhány óránként érdemes lefuttatni. A legegyszerűbb az, ha a *freshclamet* a -c és a -d kapcsolók segítségével démon módban használjuk. További tudnivalókat a *freshclam(1)* súgóoldalon találni.

Összefoglalás

Munkánk eredményeként egy *ClamAV* alapú védelemmel felszerelt *SMTP* átjárót kaptunk, vagy legalábbis elindultunk az úton ennek megvalósítása felé. Akinek további kérdése maradtak, az az internetes források között *Postfix* és *Amavisd-new* oktatóanyagot egyaránt talál. Sok szerencsét!

Linux Journal 2004. december, 128. szám

Mick Bauer biztonsági szakember, a Linux Journal biztonsági témákkal foglalkozó szerkesztője, biztonsági tanácsadó a Minnesota állambeli Minneapolisban. A Building Secure Servers With Linux című kötet szerzője (O'Reilly & Associates, 2002).