AVG Anti-vírus 7.0 verzió

(Linux operációs rendszerre)

Leírás és telepítés útmutató

Tartalomjegyzék

Bevezető és követelmények

Az AVG Linux operációs rendszeren való futtatása, nincs kötve egyetlen Linux kiadáshoz sem. Minden Linux változat alkalmas, vagy frissítések letöltésével és a beállítások módosításával alkalmassá tehető a GRISOFT AVG Anti-vírus 7.0 futtatására.
Egyetlen előírás, hogy a

- glibc-2.2.4-13
- libstdc++-libc6.2-2

könyvtáraknak legalább az itt megadott vagy frissebb változata legyen telepítve a számítógépre.
Az AVG Anti-vírus három fő feladat ellátásra képes a Linux-os számítógépeken:

1. Elektronikus levelek ellenőrzése a levelező szerver szoftverrel együttműködve
2. A fájlrendszer rendszeres ellenőrzése
3. Fájlok ellenőrzése azok megnyitásakor (a Windows verziók rezidens pajzsának megfelelő funkció)

Ahhoz, hogy ezek a funkciók megfelelően működjenek, az alábbi segédprogramok telepítésére van szükség:

1. Elektronikus levelezés ellenőrzéséhez: az amavis nevű programra (letölthető: http://www.amavis.org/)
2. A fájlrendszer ellenőrzése nem igényli más alkalmazás jelenlétét
3. A fájlok megnyitásukkor történő ellenőrzéséhez a Dazuko (letölthető: http://www.dazuko.org/) telepítése szükséges

Az a fájlrendszer és az elektronikus levelezés védelmének telepítése

Az AVG Anti-vírus telepítése

Legfontosabb, hogy a minden telepítési feladat elvégzéséhez rendszergazdai (root) jogosultságokkal kell rendelkeznie. Ehhez a root felhasználói névvel kell bejelentkezni, illetve megfelelő jogosultságok esetében a saját felhasználói neve alól használhatja a sudo vagy su parancsokat.
Elsőként telepíteni kell az AVG Linux-os verzióját. Itt több lehetőség áll rendelkezésre. Amennyiben valamilyen csomagkezelő rendszert használ az Ön által telepített Linux kiadás, úgy a telepítés elvégezhető ezen csomagok segítségével, az adott Linux verzió csomagkezelő leírásában megadott módon. Pillanatnyilag RPM telepítő csomag érhető el RedHat, Mandrake és SUSE rendszerekhez. Itt a telepítés a

rpm –ih <csomagnév>

parancs használatával elvégezhető

A többi rendszeren (természetesen az imént említetteken is!) használható a **.tar.gz**. formátumú telepítő készlet. Ebben az esetben először egy Ön által meghatározott helyre ki kell csomagolnia a telepítőkészletet a

tar zxvf <csomagnév>

parancs kiadásával. Ezt követően lépjen be létrejött alkönyvtárba, majd adja ki a

./install.sh

parancsot.

Telepítés után a terméket aktiválhatja a regisztrációs kulcs megadásával. Ehhez a

avgscan -register <licenc kulcs>

parancsot kell kiadnia. Amennyiben még nem vásárolta meg a terméket, úgy a kipróbáláshoz a **70LINUX-TTS05-PZ-C01-S1-J18-IHAR** kulcsot tudja használni.

Az AVGSCAN használata és beállításai

Az előbbi lépések sikeres elvégzése után a parancssori víruskereső motor már működőképes. Indítása az

avgscan [opciók] <könyvtár vagy fájl útvonal>

parancs kiadásával lehetséges.
Az **opciók** segítségével befolyásolhatja a víruskereső működését. Itt a következő módosítók használatára van lehetősége:

- **-asc** Ellenőrzi az archívumokat, tömörített állományokat is.
- **-rt** Ellenőriz a menet közben tömörített adatok is
- **-heur** Heurisztikus, alapos elemzést végez
- **-repok** A nem fertőzött fájlokat OK állapottal riportolja (enélkül csak a fertőzött fájlokról ad információt.
- **-ext** A megadott kiterjesztésű fájlokat ellenőrzi.
- **-noext** A megadott kiterjesztésű fájlokat nem ellenőrzi.
- **-h** A súgó megjelenítése
- **-d** daemon mód

Daemon módban is indítva a program betöltődik a memóriába és ott egy TCP (alapértelmezés szerint az 55555-ön) porton figyelve várja a hozzá érkező kéréseket. Ebben az üzemmódban a **/etc/avg.conf** fájlból olvassa be működési paramétereket.

A /etc/avg.conf beállítása

Ebben a fájlban állíthatók be az alapértelmezett valamint a daemon módú futtatáshoz a működési paraméterek. A fájl egyszerű szövegfájl, amely bármely ismert Linux alatt is megtalálható szövegszerkesztővel módosítható.

Ezt a fájlt az avgscan mindig induláskor olvassa be, ezért a módosítás a következő indításkor (illetve a daemon újraindításakor) lépnek érvénybe.
Az avg.conf fájl négy szakaszt tartalmaz, ezek:

[AvgCommon]
Az általános, minden üzemmódra érvényes beállításokat tartalmazza
Paraméterei:

Paraméter	Értékei	Leírás
runtimeCompression	0, 1	A „röptében” tömörített fájlok ellenőrzésének engedélyezése (0=nem, 1=igen)
heuristicAnalysis	0, 1	Heurisztikus (alapos) elemzés (0=nem, 1=igen)
processesArchives	0, 1	Tömörített/csomagolt állományok ellenőrzése (0=nem, 1=igen)
syslogFacility	ld. Linux syslog	Beállítja, hogy a hiba/működési üzeneteket milyen jelöléssel küldje a Linux syslog daemon részére. Ez alapján az üzenetek a syslogban csoportosíthatók és szűrhetők lesznek. Alapértelmezett: daemon

[OnAccessScanner]
A „rezidens pajzs” funkcióhoz szükséges beállításokat tartalmazza
Paraméterei:

Paraméter	Értékei	Leírás
includePath	útvonal	megadhatja, hogy a mely könyvtárak legyenek bevonva az ellenőrzésbe. A paraméter egymás utáni sorokban többször is használható (több könyvtár is megadható).
excludePath	útvonal	megadhatja, hogy a mely könyvtárak **NE** legyenek bevonva az ellenőrzésbe. A paraméter egymás utáni sorokban többször is használható (több könyvtár is megadható).
numOfDaemons	0-10	A várakozási idő csökkentése érdekében előre is elindíthatóak daemonok, amelyek igény esetén azonnal rendelkezésre állnak és a betöltődési időt nem kell kivárni. Alapértelmezés: 3 db
scanOnOpen	0, 1	Ellenőrizze-e megnyitáskor a fájlokat (0=nem, 1=igen) Alapértelmezés: 1
scanOnExec	0, 1	Ellenőrizze-e futtatáskor a programokat (0=nem, 1=igen) Alapértelmezés: 0
scanOnClose	0, 1	Ellenőrizze-e lezáráskor a fájlokat (0=nem, 1=igen) Alapértelmezés: 0
scanOnCloseModified	0, 1	Ellenőrizze-e lezáráskor a MÓDOSÍTOTT fájlokat (0=nem, 1=igen) Alapértelmezés: 1
excludeFileSuffix	kiterjesztés	Megadhatja, hogy milyen kiterjesztésű fájlokat NE ellenőrizzen a rendszer (amelyek formátumuknál fogva elméletileg nem tartalmazhatnak vírust). Alapértelmezés: .jpg

[AvgDaemon]
A daemon módú futtatás paraméterei

Paraméter	Értékei	Leírás
port	TCP Port	Megadhatja, hogy mely porton várja a kapcsolatokat daemon módú szkenner.

		Alapértelmezés: 55555
address	IP Cím	Megadhatja, hogy mely IP Címen várja a kapcsolatokat daemon módú szkenner. Alapértelmezés: 127.0.0.1 , vagyis más gépről nem érhető el.
numOfDaemons	0-10	A várakozási idő csökkentése érdekében előre is elindíthatóak daemonok, amelyek igény esetén azonnal rendelkezésre állnak és a betöltődési időt nem kell kivárni. Alapértelmezés: 5 db

[AvgUpdate]

A frissítési beállítások paraméterei tartalmazza

Paraméter	Értékei	Leírás
location	URL	Megadhatja, hogy honnan töltse le a program és adatbázis frissítéseket az AVG. Alapértelmezés: http://www.grisoft.cz/softw/70/update
proxy	off, vagy cím:port	Megadhatja, hogy az Önök lokális hálózat proxy szerveren keresztül kapcsolódik-e a külvilághoz. Ha nem az értéke legyen **off** (alapértelmezés), egyébként pedig: **ipcim:port**
proxyLogin	off vagy login:jelszó	Amennyiben Önök proxy szervert használnak, itt megadhatja, hogy a szerver kér-e bejelentkezést. Ha nem, akkor állítsa off-ra (alapértelmezés), egyébként pedig adja meg a megfelelő **felhasználó:jelszó** párost
backupDir	útvonal	Mielőtt az avgupdate elvégzi a frissítést, biztonsági másolatot készít a jelenlegi telepített vezrzióról. Itt a biztonsági másolat helyét (hová szeretné lementeni) adhatja meg. Alapértelmezés: /tmp/avg7/backup
preinstallDir	útvonal	A frissítés során átmeneti fájlok jönnek létre. Ezeknek a helyét adhatja itt meg. Az átmeneti fájlok a telepítés után törlődnek, így nem fognak tartósan helyet foglalni. Alapértelmezés: /tmp/avg7/preinstall
downloadDir	útvonal	Megadhatja, hogy a frissítések mely könyvtárba töltődjenek le. Ezek a fájlok törlődnek a frissítés telepítése után, kivéve ha az **avgupdate** parancsot a **- -download** paraméterrel futtatja, mivel akkor a letölttött fájlok megőrződnek.
logFile	fájl	Megadhatja, hogy frissítések naplózása hová történjen. Ezzel megkönnyítheti az esetleges hibák feltárását. Alapértelmezés: /tmp/avg7/avg7upd.log
logLevel	1-3	Megadhatja a frissítési naplózás részletességét. Értékei: 1: csak a frissítés indulását és befejeződését naplózza, 2: jelzi a frissítés folyamatát is, 3: a telepítés előkészítési fázisról is ad információkat. Alapértelmezés: 1

Az AVG Linuxos változatának indítása és leállítása

Amennyiben az AVG-t szerverként (daemon) szeretné futtatni, akkor azt az **avgscan –d** parancs segítségével teheti meg. Ezen kívül a program telepítésekor létrejött a SystemV típusú rendszereknél szokásos init parancsállományt (avgd), amely a Linux változattól függően a **/etc/init.d** vagy a **/etc/rc.d/init.d** könyvtárak valamelyikében található meg, használhatja a daemon módú indításhoz a **/etc/rc.d/init.d/avgd start** parancs begépelésével. Ugyancsak ezt a fájlt kell belinkelni a megfelelő indítási szint könyvtárába egy Snn (nn egy a kívánt sorrendnek szám), ha a szerver indulásakor szertné az AVG-t is automatikusan elindítani.

A leállításhoz hasonlóképpen kell eljárni ha az AVG szervert le szeretné álláítani. Erre ugyan csak több alternatíva kínálkozik.
Legegyszerűbb a **/etc/rc.d/init.d/avgd stop** parancsot használni, de leállítás végrehajtható a **kill -TERM -- -`cat /var/run/avgd.pgrp`** parancs segítségével is.

A program futását a **telnet 127.0.0.1 portszám** (a portszám alapesetben 55555) parancs beírásával ellenőrizheti. Ekkor a
220-AVG7 Anti-Virus daemon mode scanner
220-Program version 7.0, engine 718
220-Virus Database: Version 258.13.2 10-06-2003
220 Ready
üzenetet kell látnia a képernyőn.

Illesztés a levelező szerverhez

Az AVG a legkülönbözőbb levelező szervekkel képes együttműködni (Sendmail, Postfix, Exim, Qmail, stb.). Ebben nagy segítséget nyújt az **AMaViS** (A Mail Virus Scanner) nyílt forráskódú modul. Ez a kiegészítés lehetővé teszi, hogy szinte tetszőleges szűrési feladatokat valósíthassunk igen egyszerűen az **AMaViS** által támogatott levelező szervereken.
Az **AMaViS** két verziója is megfelelő az AVG illesztéséhez, ezek a

- AMaViS version 0.3.12 (http://www.amavis.org/)
- amavisd-new-20030616 (http://www.ijs.si/software/amavisd/)

Mindkét AMAViS verzió igényli a legalább 5.005 verziójú (Ha UniCode használatra is szükség van, akkor 5.8.1 vagy frisebb verzióra van szükség!) perl interpreter jelenlétét! Ennek meglétét előfeltételként kezeljük!

A telepítés lépéseit az **amavisd-new** segítségével mutatjuk be.

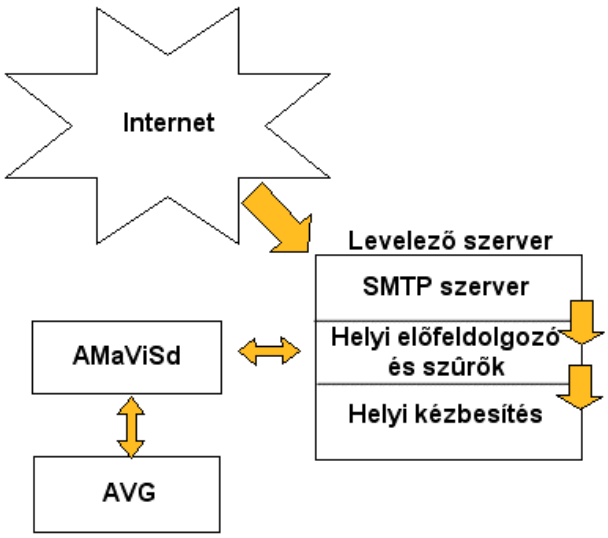
1. Töltse le az **amavisd-new-20030616-p4.tar.gz** fájlt a http://www.ijs.si/software/amavisd/ vagy a http://www.grisoft.hu/ címről.

2. Csomagolja ki a telepítő készletet egy tetszőleges helyen a **tar -xvzf amavisd-new-20030616-p4.tar.gz** parancs segítségével.
3. Lépjen be a kicsomagoláskor keletkezett könyvtárba: **cd amavisd-new-20030616**
4. Telepítse az AVG használatához szükséges patch-et (foltot) [Elérhető: http://www.grisoft.hu/] **patch < amavisd-new-20030616-avg.patch**
5. Amennyiben még nincs telepítve telepítse szükséges PERL modulokat, amelyek a következők (Letölthetők a http://www.cpan.org/ oldalról vagy összegyűjtve a http://www.grisoft.hu/ -ról):
   - Archive::Tar (Archive-Tar-x.xx)
   - Archive::Zip (Archive-Zip-x.xx)
   - Compress::Zlib (Compress-Zlib-x.xx)
   - Convert::TNEF (Convert-TNEF-x.xx)
   - Convert::UUlib (Convert-UUlib-x.xxx)
   - MIME::Base64 (MIME-Base64-x.xx)
   - MIME::Parser (MIME-Tools-x.xxxx) Legalább 6.2xx verzió! (http://search.cpan.org/dist/MIME-tools/)
   - Mail::Internet (MailTools-1.58 vagy újabb)
   - Net::Server (Net-Server-x.xx)
   - Net::SMTP (libnet-x.xx) (1.16 verzió vagy frissebb!)
   - Digest::MD5 (Digest-MD5-x.xx)
   - IO::Stringy (IO-stringy-x.xxx)
   - Time::HiRes (Time-HiRes-x.xx) (1.49 verzió vagy újabb!)
   - Unix::Syslog (Unix-Syslog-x.xxx)
6. Telepítse a PERL modulokat a csomagokban található leírás szerint.
7. Amennyiben a kezelendő levelek várhatóan tömörített állományokat is tartalmaznak, telepítenie kell a kibontáshoz szükséges tömörítő programokat is. Ha ez megtörtént, akkor az AMaViSd ezeket automatikusan felismerni és használni fogja. Az alábbi programok használatára van lehetőség: **compress, gzip, bzip2, nomarch (vagy arc), lha, arj (vagy unarj), rar (vagy unrar), zoo, cpio, lzop, freeze (vagy unfreeze, vagy melt).**
8. Ez után létre kell hoznia egy dedikált felhasználót és csoportot az amavis részére. Ez célszerűen amavis és amavis lehet. **Figyelem! a /etc/passwd, /etc/shadow, /etc/group állományokat elővigyázattal szerkessze!** Használjon olyan szövegszerkesztőt (pld. vipw), amely gondoskodik az adatok egységességéről!
9. Hozza létre a munkakönyvtárakat és állítsa be a jogosultságokat:
   - **mkdir /var/amavis**
   - **chown amavis:amavis /var/amavis**

- **chmod 750 /var/amavis**

10. Másolja az amavisd-t végleges helyére és állítsa be a jogosultságokat:
    - **cp amavisd /usr/local/sbin/**
    - **chown root /usr/local/sbin/amavisd**
    - **chmod 755 /usr/local/sbin/amavisd**
11. Másolja át az amavisd.conf konfigurációs állományt a végleges helyére és állítsa be a jogosultságokat
    - **cp amavisd.conf /etc/**
    - **chown root /etc/amavisd.conf**
    - **chmod 644 /etc/amavisd.conf**
12. Végezze el a konfigurációs állomány módosítását, saját szerverének megfelelően
    Fontosabb konfigurációs paramétereket a **/etc/amavisd.conf** szövegfájl szerkesztésével:
    - **$mydomain = 'pelda.hu'; #ide az Ön domain nevét kell írnia**
    - **$daemon_user = 'amavis'; #vagy amit megadott**
    - **$daemon_group = 'amavis'; #vagy amit megadott**
    - **$inet_socket_port = 10024; # az ön által választott TCP port szám, ahol az amavisd várja a kapcsolatokat.**

13. Ezzel, amennyiben mindent helyesen beállított és az összes előfeltételt teljesítette az amavisd használatra kész. Teszteléséhez adja ki a **/usr/local/sbin/amavisd debug** parancsot. Amennyiben itt nem kap hibaüzenetet a szerverhez kapcsolódhat is egy másik terminálról a **telnet 127.0.0.1 10024** parancs segítségével. Sikeres tesztelés után az indításhoz a **/usr/local/sbin/amavisd** parancsot kell kiadnia (debug nélkül). Gondoskodjón róla, hogy a rendszer indulásakor az amavisd elinduljon!
14. Az amavisd levelező programhoz illesztését a levelező szervertől függően más és más módon kell elvégezni. Ezeket a leírásokat az amavisd telepítő könyvtárának **README_FILES** alkönyvtárában találhatja meg. Az általános működési elv a következő ábrán látható:



A víruskereső program tesztelése

A levelező rendszerhez való illesztés után a rendszert legkönnyebben olyan módon tesztelheti, hogy vírusos próba levelet küld rajta keresztül. Ehhez egy teszt vírust tölthet le a http://www.grisoft.hu/ honlap letöltések oldaláról. Az itt található EICAR vírus egy ártalmatlan kódsor, amely a víruskereső programok gyártóinak együttműködése révén jött létre. Pusztán a víruskereső programok üzemképességének tesztelésére készítették, nem fertőz, nem terjed és kárt sem okoz. A tesztelést természetesen célszerű elvégeznie nem fertőzött levelekkel is!

Az AVG Linuxos verziójának frissítése

A megbízható működéshez elengedhetetlen hogy a program mindig a legfrissebb vírusminta adatbázis és keresési eljárások felhasználásával működjön. A GRISOFT mérnökei rendszeresen közzétesznek program és vírusminta frissítéseket, amelyek az gyártó honlapjáról letölthetőek. A frissítés letöltéséhez és telepítéséhez az **avgupdate –o** parancsot kell kiadnia. Mivel a frissítések gyakran, hetente több alkalommal letölthetőek, célszerű ezt a folyamatot automatizálnia. Ezt legkönnyebben úgy végezheti el, hogy az frissítésre szolgáló parancsot a kívánt gyakoriság beállításával elhelyezi a **/etc/crontab** fájlban. Amennyiben napi gyakorisággal szeretné a frissítéseket letölteni, úgy a /etc/cron.daily könyvtárban helyezzen el egy parancsfájlt a következő tartalommal:

#!/bin/sh
/usr/local/bin/avgupdate -o

A fájlnak ne felejtsen el futtatási jogosultságot adni a chmod 755 <fájlnév> paranccsal.

A cron funkció minden elterjedt Linux rendszernek része!