

# AVG 7.1 for Linux E-mail Server

## User Manual

Document revision 71.7 (15.6.2006)

**Copyright (c) 1992-2006 GRISOFT, s.r.o. All rights reserved.**

This product uses RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.

This product uses code from C-SaCzech library, Copyright (c) 1996-2001 Jaromir Dolecek <dolecek@ics.muni.cz>

This product uses compression library zlib, Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler

This product uses libtar library, Copyright (c) 1998-2003 University of Illinois Board of Trustees, Copyright (c) 1998-2003 Mark D. Roth

This product uses compression library libbzip2, Copyright (C) 1996-2002 Julian R Seward

This product uses XML parser library expat, Copyright (C) 1998, 1999 James Clark

This product uses library libcurl, Copyright (c) 1996 - 2003, Daniel Stenberg, <daniel@haxx.se>

This product includes Flex software developed by the University of California, Berkeley and its contributors, Copyright (c) 1993 The Regents of the University of California

All other trademarks are property of their respective owners.

## Contents

<b>1. Introduction.....</b>	<b>3</b>
<b>2. Before Installation .....</b>	<b>4</b>
2.1. Prerequisites .....	4
2.2. Installation Package .....	5
<b>3. Installation and Launch .....</b>	<b>6</b>
<b>4. Third Party Products .....</b>	<b>10</b>
4.1. AVG Anti-Virus Vendor Patches .....	10
4.2. AMaViS.....	11
4.3. Qmail-Scanner.....	13
4.4. Testing the Installation .....	18
<b>5. E-mail Scanning .....</b>	<b>19</b>
5.1. General Principles .....	19
5.2. Performance and Resource Usage.....	19
5.3. Using Unix Socket for an Extra Security.....	20
<b>6. Commercial E-mail Servers .....</b>	<b>21</b>
6.1. AVG for Lotus Notes/Domino Server Installation and Maintenance .....	21
6.2. AVG for Kerio MailServer Maintenance.....	29
<b>7. Standalone Command Line Modules.....</b>	<b>33</b>
7.1. AVGSCAN Command.....	33
7.2. AVGUPDATE Command .....	36
7.3. On-access Scanner .....	40
7.4. Service Signals .....	42
<b>8. Configuration File.....</b>	<b>43</b>
8.1. AvgCommon.....	43
8.2. OnAccessScanner .....	44
8.3. AvgDaemon .....	44
8.4. AvgUpdate .....	45
<b>9. FAQ and Technical Support .....</b>	<b>47</b>

## 1. Introduction

This User Manual is the full documentation describing **AVG for Linux E-mail Server**.

### a) **AVG for Linux E-mail Server Kernel Features**

**AVG for Linux E-mail Server** is a product based on the **AVG for Linux** scanning kernel. The **AVG for Linux** kernel provides comprehensive and reliable protection against viruses for Linux powered machines. It offers many features, such as scheduled and on-demand scanning of folders, files, and common archive types for possible virus infection. You can also perform a scheduled or on-demand update of your **AVG Anti-Virus** either from the Internet or from local update sources.

### b) **AVG for Linux E-mail Server E-mail Scanning Features**

The incoming and outgoing e-mail messages processed by the supported mail transport agents (MTA) are watched by constantly running **AVG Anti-Virus** process (memory resident scanning daemon). This means the e-mail spooling queues are protected and scanned regularly by **AVG for Linux E-mail Server**. The **AVG Anti-Virus** e-mail scanning performance can be easily controlled and configured using **AVG for Linux** daemon signals and comprehensive configuration file parameters.

### c) **AVG for Linux E-mail Server – Command Line Modules**

Powerful standalone command line modules are also included in the **AVG for Linux E-mail Server** installation. You can perform all possible on-demand file system tests and updates using these modules. They can be also utilized within for example the *cron* utility in order to schedule a regular automatic test or update.

## 2. Before Installation

### 2.1. Prerequisites

Before installing **AVG for Linux E-mail Server** you must verify that your system meets the following requirements:

#### a) Libraries

The following libraries are required in order to ensure the **AVG for Linux** kernel can be installed and run properly:

- o *libc.so.6*

#### b) Open Source E-mail Servers Supported

- o **sendmail**

The traditional *sendmail* mail transport agent (MTA, Linux synonym for lightweight e-mail server) is included in most modern Linux distributions. The latest version is also available for free at <http://www.sendmail.org>.

- o **qmail**

The latest version is available for free at <http://cr.yp.to/qmail.html>; an extensive description of download, installation, and maintenance issues related to *qmail* is also provided at <http://www.lifewithqmail.org>.

- o **postfix**

The *postfix* MTA is a popular alternative to the widely used *sendmail* e-mail server; the latest version is available for free at <http://www.postfix.org/>.

- o **exim**

This MTA can be also used as replacement for the common *sendmail* e-mail server, although its configuration and maintenance principles differ; the latest version of the *exim* e-mail server is available for free at <http://www.exim.org>.

#### c) Commercial E-mail Servers Supported

- o *Lotus Notes/Domino Server for Linux*
- o *Kerio MailServer for Linux*

#### d) AMaViS – A Mail Virus Scanner

One of the varieties of **AMaViS** (*amavis*, *amavisd*, *amavisd-new* or *amavis-ng*) is needed for the *sendmail*, *postfix*, *exim* and *qmail* mail transport agents in order to enable e-mail scanning with the use of **AVG for Linux E-mail Server**. **AMaViS** is available for free at <http://www.amavis.org>.

**Note:** We recommend using the *amavisd-new* scanner which offers the best compatibility with **AVG for Linux E-mail Server** and better overall performance for all supported mail transport agents.

Refer to chapter [4.2 Third Party Products/AMaViS](#) to see how to install the **AMaViS** scanner, and how to integrate it with **AVG for Linux E-mail Server**.

e) **Qmail-Scanner**

If you use the *qmail* MTA, an alternative solution to **AMaViS** mail virus scanner is

**Qmail-Scanner** – the e-mail content scanner designed to be used exclusively with *qmail*. **Qmail-Scanner** is available for free at <http://qmail-scanner.sourceforge.net/>.

Refer to section [4.3 Third Party Products/Qmail-Scanner](#) to see how to install the Qmail-Scanner mail virus scanner and how to integrate it with **AVG for Linux E-mail Server**.

f) **DAZUKO Kernel Module**

The DAZUKO kernel module is necessary for the proper function of the **AVG for Linux E-mail Server** on-access scanner. DAZUKO is available for free at <http://www.dazuko.org>.

Refer to section [7.3 Standalone Command Line Modules/On-access Scanner](#) for detailed information on this topic.

## 2.2. Installation Package

**AVG for Linux E-mail Server** installation packages are available on the installation CD in the form of RPM packages for various Linux distributions, or in the form of a precompiled .tar.gz package. You can also download the latest appropriate package version from <http://www.grisoft.com>, *Download/Programs* section.

### 3. Installation and Launch

AVG for Linux E-mail Server installation packages are provided as RPM files or .tar.gz package.

- For the installation from the RPM file, use the

```
$ rpm -i avg71{edition}-r{version}-a{version of avi}.i386.rpm
```

command in your shell (accessible for example using the *xterm* application within your X window system).

For the installation from the .tar.gz package, use the

- **\$ tar -xvzf avg71{edition}-r{version}-a{version of avi}.i386.tar.gz**

command in the directory where the package is located to unpack its content.

Switch to the unpacked **avg7-linux** directory then and run the

```
$ ./install.sh
```

installation script.

**Note:** The program files of the **AVG for Linux E-mail Server** versions 11 and older are installed into the **/usr/local/lib/avg7** directory. Even if you perform the full update of older version of your **AVG Anti-Virus**, the directory structure remains the same (ensuring the backwards compatibility). However, all essential components of **AVG for Linux E-mail Server** are always updated properly to offer you the maximum security and reliability.

The versions 12 and newer are comprehensively installed into the **/opt/grisoft** directory. Symbolic links are created in various system directories, leading to the **/opt/grisoft** directory subtree. If you want to upgrade the old directory structure, you must completely reinstall your **AVG for Linux E-mail Server**. Note that in this documentation is always described the preferred newer location of **AVG for Linux E-mail Server** installation!

In the installation packages' names:

- the **version** stands for the minor version number of **AVG for Linux E-mail Server**,
- the **distribution** string stands for the specification of Linux distribution (if necessary to distinguish it) which is the package intended for,
- the **specification** string stands for the **AVG Anti-Virus** internal virus database specification number.

#### Installation of GUI from a Specific Package:

Graphical user interface (GUI) can be installed from specific packages, found at <http://www.grisoft.com>, **Download/Programs** section.

- You can install GUI from a .tar.gz package as follows (for distributions that do not support RPM installation):

Download latest .tar.gz and unpack it:

```
# tar xzvf avggui-1.0-{release}.i386.tar.gz
```

Change directory to avggui:

```
# cd avggui1
```

Run the installation script as root then:

```
$ ./install.sh
```

- If your distribution supports it, you can install GUI from RPM package:  
Download latest rpm and install it:

```
# rpm -i avggui-1.0-{release}.i386.rpm
```

Launch the `/opt/grisoft/avggui/bin/avggui_update_licinfo.sh` script as root for updating license information after installation.

**Note:** You can configure PAM authentication (used in avggui run by a non-root user when changing license information) in the file `/etc/pam.d/avggui`.

## a) Distributions Currently Supported

Distribution	Installation package
Mandrake Linux, Red Hat, Red Flag, Fedora Core and other systems supporting the RPM packager utility	avg71{edition}-r{version}-a{version of avi}. <b>i386.rpm</b>
Any other Linux distribution (e. g. Debian, Slackware, Gentoo etc.)	avg71{edition}-r{version}-a{version of avi}. <b>i386.tar.gz</b>

## b) The Installation Process

The installation process will automatically determine all features of your system and will perform the proper installation of **AVG for Linux E-mail Server** on your computer. Perform installation from the packages mentioned in the table above to also install the **AVG for Linux E-mail Server** command line modules (besides the e-mail scanning daemons).

(See chapter [7. Standalone Command Line Modules](#) for detailed information on this topic).

### c) Product Registration

After the installation process you need to register your **AVG for Linux E-mail Server** unless it has been registered already during the installation process; this applies to special packages for **AVG Anti-Virus** vendor partners.

The registration can be performed by launching the

```
$ avgscan -register
```

command in your shell.

(See chapter [7.1 Standalone Command Line Modules/AVGSCAN Command](#) for details).

### d) Launching the E-mail Scanning Daemon

Having installed and registered your **AVG for Linux E-mail Server** you must start the **AVG for Linux** services. These services completely cover both e-mail and on-access scanning modules that run as memory resident daemons. The daemons can be controlled using the signal mechanism and **AVG for Linux E-mail Server** configuration file.

(See chapters [7.4 Standalone Command Line Modules/Service Signals](#) and [8. Configuration File](#) for detailed information).

Launch the services as root (only root can send signals to daemons):

```
# /etc/init.d/avgd start
```

If you are not logged in as root, the command responds with respective warning.

You can use the

```
$ su
```

command and apply the superuser password to change your identity to the root.

**Note:** The fact you are logged in as root is usually indicated by the '#' character at the beginning of your prompt. The normal user identity is indicated by the '\$' character.

See chapter [5. E-mail Scanning](#) for detailed information on the e-mail scanning daemon.

**Note:** The e-mail scanning daemon serves its purpose only when a mail transport agent and possibly the necessary third party software are present and properly configured! See chapter [4. Third Party Products](#) for basic information on how to install and setup additional tools needed to enable the e-mail anti-virus protection with **AVG for Linux E-mail Server**.





For proper function of the on-access scanning daemon the DAZUKO kernel module is required. Refer to section [7.3 Standalone Command Line Modules/On-access Scanner](#) for detailed information on this topic.

The included command line modules can be operated as described in chapter [7. Standalone Command Line Modules](#).

## 4. Third Party Products

Third party software is needed to preprocess incoming and outgoing e-mail messages content before they can be scanned by **AVG for Linux E-mail Server**. Two solutions are available for particular e-mail servers – the **AMaViS** and the **Qmail-Scanner** security packages.

Both of these packages require **AVG for Linux E-mail Server** and optionally some **AVG Anti-Virus** vendor patches to be installed before attempting to install and configure them properly on your system. The **AMaViS** e-mail content scanner can be used with the *sendmail*, *postfix*, *qmail* and *exim* mail transport agents; the **Qmail-Scanner** can be used with *qmail* only.

Supported commercial e-mail servers (**Lotus Notes/Domino** and **Kerio MailServer**) do not require such tools. See chapter [6. Commercial E-mail Servers](#) for more information on this topic.

### 4.1. AVG Anti-Virus Vendor Patches

Before installing the **AMaViS** package *amavis* (various versions supported) you must apply the **AVG Anti-Virus** patch. Supposing you have unpacked the installation file, switch to the unpacked directory, copy the *amavis-{version}-avg.patch* file there (included in the **AVG for Linux**

**E-mail Server** installation package), and apply the patch using the

```
$ patch -p1 < amavis-{version}-avg.patch
```

command.

Run *autoconf* with the

```
$ autoconf
```

command.

Then create the *aclocal.m4* file using the

```
$ touch aclocal.m4
```

command and continue with the installation as described in chapter [4.2 Third Party Products/AMaViS](#).

**Note:** The patch is needed only for the *amavis* variant of **AMaViS**. For the version 'p7' and higher of the recommended *amavisd-new* you just have to uncomment the **AVG Anti-Virus** related lines in the *amavisd.conf* file. For older versions, use the respective *amavisd-new* patch

Besides the *amavis* patch, the **Qmail-Scanner** (versions 1.20, 1.22) patch is also needed when you are planning to install this tool. Switch to the unpacked **Qmail-Scanner** installation directory and copy the *qmail-scanner-{version}-avg.patch* file (included in the **AVG for Linux E-mail Server** installation package) there.

Apply the patch using the

```
$ patch -p1 < qmail-scanner-{version}-avg.patch
```

command, and follow the installation instructions as described in chapter [4.3 Third Party Products/Qmail-Scanner](#).

## 4.2. AMaViS

You can download the package from the <http://www.amavis.org/download/> page. Four separate packages are available:

- **amavis** for low and medium mail volume (home or small office use with up to ten accounts)
- **amavisd** for higher mail volume
- **amavisd-new** for higher mail volume with various add-ons included (such as anti-spam or ISP features)

**Note:** *We strongly recommend the **amavisd-new** variant to be used with AVG for Linux E-mail Server!*

- **amavis-ng**, a modular rewrite of amavis (intended for experienced administrators and/or **AMaViS** developers); this project is not being developed any longer, although its source code can be obtained via the **AMaViS** CVS repository.

### a) Prerequisites

The C language compiler and also the **make** and **autconf / automake** utilities are needed to build the **AMaViS** tools.

The essential modules responsible for extracting e-mail content and passing it to the **AVG for Linux E-mail Server** scanning engine are implemented in Perl. This is why the Perl language interpreter has to be installed on your system. The following Perl modules are required:

- Archive::Tar (Archive-Tar-x.xx)
- Archive::Zip (Archive-Zip-x.xx, version 1.09 or later is recommended!)
- Compress::Zlib (Compress-Zlib-x.xx)
- Convert::TNEF (Convert-TNEF-x.xx)
- Convert::UUlib (Convert-UUlib-x.xxx, stick to the newest version)
- MIME::Base64 (MIME-Base64-x.xx)
- MIME::Parser (MIME-Tools-x.xxxx)
- Mail::Internet (MailTools-1.58 or later have workarounds for Perl 5.8.0 bugs)
- Net::Server (Net-Server-x.xx)
- Net::SMTP (libnet-x.xx, use libnet-1.16 or later for better performance)
- Digest::MD5 (Digest-MD5-x.xx)
- IO::Stringy (IO-stringy-x.xxx)

- o Time::HiRes (Time-HiRes-x.xx, use 1.49 or later, older versions can cause problems)
- o Unix::Syslog (Unix-Syslog-x.xxx)
- o BerkeleyDB with bdb library 3.2 or later (4.2 or later preferred)

All of these modules are available for free at <http://www.cpan.org/>. The usual way of installing a new Perl module consists of unpacking the downloaded file, switching into the unpacked directory, and running the following sequence of commands as root:

```
# perl Makefile.PL
```

```
...
```

```
# make test
```

```
...
```

```
# make install
```

Make sure **AVG for Linux E-mail Server** is installed and operational before starting the **AMaViS** installation.

## b) Installation

To install **AMaViS** from the source code, unpack the selected downloaded package (the **amavis** package is given in the following example):

```
$ tar -xvzf amavis-{version}.tar.gz
```

Switch to the unpacked directory. It is recommended to read the detailed instructions in the INSTALL and/or README file located in this directory. The easiest way of performing the installation is to run the following sequence of commands as root (although the installation steps may slightly differ according to the particular **AMaViS** package):

```
# ./configure
```

```
...
```

```
# make
```

```
...
```

```
# make install
```

```
...
```

## c) Configuration

Most configuration options should have been resolved by automatic configuration. Of course, it is also possible to perform manual changes to the generated **amavis** script (note that the exact name of the script may depend on which **AMaViS** package you have decided to install). If you switch to a

different MTA, you must re-run **AMaViS** configuration, because the script contains only the code for the MTA it was initially configured for.

The configuration steps to be taken for particular mail transport agent consist of making small subtle changes in the related configuration files in order to ensure **AMaViS** can access the messages in the mail transport agent's queue before they are processed further. As MTA configuration is specific for each agent as well as for the particular administrator options and policies, it is not covered in detail in this documentation.

If you experience any problems with integrating your mail transport agent and **AMaViS**, refer to your mail transport agent documentation, and also to the *README.{MTA\_name}* file in the **README\_FILES** subdirectory of the **AMaViS** installation directory (the *MTA\_name* stands for the name of your mail transport agent). These README files contain detailed information and configuration examples for all supported mail transport agents.

### 4.3. Qmail-Scanner

#### a) Prerequisites

The *qmail* version 1.03 or higher is needed.

Make sure the *reformmime* tool for reformatting the MIME e-mail format is installed on your computer. The *reformmime* package can be obtained for free at <http://prdownloads.sourceforge.net/courier/>.

Also the Perl language interpreter (version 5.005\_03 or higher) and the following Perl modules are needed:

- o Time::HiRes
- o DB\_File
- o Sys::Syslog

All of these modules are available for free at <http://www.cpan.org/>. The usual way of installing a new Perl module consists of unpacking the downloaded file, switching into the unpacked directory, and running the following sequence of commands as root:

```
# perl Makefile.PL
```

```
...
```

```
# make test
```

```
...
```

```
# make install
```

The *qmailqueue* patch is needed in order to enable *qmail* to call a different *qmail-queue* program than the one compiled by default. The patch instructions and also the patching process details are presented at <http://www.qmail.org/qmailqueue-patch>. Here is a direct example transcript (according to the previous website) of the differences that have to be performed:

```

diff -u qmail-1.03-orig/Makefile qmail-1.03/Makefile
--- qmail-1.03-orig/Makefile   Mon Jun 15 04:53:16 1998
+++ qmail-1.03/Makefile      Tue Jan 19 10:52:24 1999
@@ -1483,12 +1483,12 @@
trigger.o fmqfn.o quote.o now.o readsubdir.o qmail.o date822fmt.o \
datetime.a case.a ndelay.a getln.a wait.a seek.a fd.a sig.a open.a \
lock.a stralloc.a alloc.a substdio.a error.a str.a fs.a auto_qmail.o \
-auto_split.o
+auto_split.o env.a
    ./load qmail-send qutil.o control.o constmap.o newfield.o \
prioq.o trigger.o fmqfn.o quote.o now.o readsubdir.o \
qmail.o date822fmt.o datetime.a case.a ndelay.a getln.a \
wait.a seek.a fd.a sig.a open.a lock.a stralloc.a alloc.a \
-   substdio.a error.a str.a fs.a auto_qmail.o auto_split.o
+   substdio.a error.a str.a fs.a auto_qmail.o auto_split.o env.a

qmail-send.0: \
qmail-send.8
diff -u qmail-1.03-orig/qmail.c qmail-1.03/qmail.c
--- qmail-1.03-orig/qmail.c   Mon Jun 15 04:53:16 1998
+++ qmail-1.03/qmail.c      Tue Jan 19 09:57:36 1999
@@ -6,14 +6,25 @@
#include "fd.h"
#include "qmail.h"
#include "auto_qmail.h"
+#include "env.h"

-static char *binqqargs[2] = { "bin/qmail-queue", 0 } ;

```

```
+static char *binqqargs[2] = { 0, 0 } ;  
  
+  
  
+static void setup_qqargs()  
  
+{  
+ if(!binqqargs[0])  
+  binqqargs[0] = env_get("QMAILQUEUE");  
+ if(!binqqargs[0])  
+  binqqargs[0] = "bin/qmail-queue";  
+}  
  
int qmail_open(qq)  
  
struct qmail *qq;  
  
{  
  int pim[2];  
  int pie[2];  
  
+  
+ setup_qqargs();  
  
  if (pipe(pim) == -1) return -1;  
  if (pipe(pie) == -1) { close(pim[0]); close(pim[1]); return -1; }
```

Before installing the software a special account must be created, which the **Qmail-Scanner** processes will run under. By default, the user/group name for this account is **qscand**. For extra security, create it with a normal home directory (e.g. **/home/qscand**), but with a "fake" shell (e.g. **/bin/false**), as **Qmail-Scanner** never logs in directly.

Make sure **AVG for Linux E-mail Server** is installed and operational before attempting to install **Qmail-Scanner**.

## b) Installation

Unpack the **Qmail-Scanner** package using the

```
$ tar -xvzf qmail-scanner-{version}.tgz
```

command (the **version** stands for the downloaded package version).

Switch to the unpacked directory and run the

```
$ ./configure --help
```

command if you want to get an overview of possible configuration options.

Run the

```
$ ./configure
```

command (possibly with selected options). This determines all the features and recognizes the **AVG for Linux E-mail Server** virus scanning software on your computer.

Run the

```
# ./configure --install
```

command as root this time (again, possibly with other options you have selected before). This updates the **qmail** directory structure on your system and also installs the

**qmail-scanner-queue.pl** script.

You can test the installation using the

```
$ ./contrib/test_installation.sh
```

command in the installation directory. This will send four e-mails: one normal, two infected with the EICAR anti-virus test file, and one obvious spam to the root's address. Ideally

**Qmail-Scanner** should let one through, catch the viruses, and tag the spam as "spammy" (if **SpamAssassin** is installed of course). As **Qmail-Scanner** initially defaults not to notifying anyone when a virus is caught, you may have to view the logs (e.g. *syslog*) to see what **Qmail-Scanner** exactly did.

### c) Configuration

To enable **Qmail-Scanner** to access the e-mail queue contents the **qmail-smtpd** daemon has to be told that **qmail** knows to use the **qmail-scanner-queue.pl** script instead of the default **qmail-queue** binary executable. This is done via the TCP server control files for SMTP. See where the TCP server for **qmail-smtpd** gets its rules from according to your installation options of **qmail** mail transport agent. Edit the rule file and tell **qmail-smtpd** what IP address range (corresponding to SMTP client IP addresses) you want **Qmail-Scanner** to be invoked on. You should select all the addresses to be scanned. A typical example of changing the rule file for the **qmail-smtpd** daemon follows:

```
#/etc/tcpserver/smtp.rules
```

```
#
```



```
# No Qmail-Scanner at all for mail from 127.0.0.1

127.:allow,RELAYCLIENT="",RBLSMTPD="",QMAILQUEUE="/var/qmail/bin/qmail-queue"

# Use Qmail-Scanner without SpamAssassin on any mail from the local network

# [it triggers SpamAssassin via the presence of the RELAYCLIENT var]

10.:allow,RELAYCLIENT="",RBLSMTPD="",QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"

#

# Use Qmail-Scanner with SpamAssassin on any mail from the rest of the world

:allow,QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"
```

The above example means that all SMTP e-mails will be scanned, but each in a different manner according to the address classification. E-mail from the LAN (the 10. prefixed network) will be scanned by the **AVG for Linux E-mail Server** whereas e-mail from the Internet will be scanned for viruses (and also tagged by **SpamAssassin** if present). This control philosophy provides you with a lot of versatility – virus scanning can be only performed for example on mail coming from your Exchange server and not on mail from your Unix servers.

**Note:** You must increase the amount of memory your system allows **qmail-smtpd** to run with because it is now running the entire Perl language interpreter and also the **AVG for Linux E-mail Server**. Typical installations of **qmail** are provided with the system `rc/startup` scripts (e.g. `/etc/rc.d/init.d/qmail` or `/service/smtp/run`). These scripts limit the amount of RAM the **qmail-smtpd** daemon can use (via **ulimit** or **softlimit** shell commands). You must increase the limit to approximately 5-11MB (the exact range depends on your system parameters and load).

If you want to enable **AVG for Linux E-mail Server** to scan all mail sent by local shell users, the **qmailqueue** must be defined in `/etc/profile` file.

If the "`$DEBUG=1`" (the default) variable is set within **qmail-scanner-queue.pl** script, then every transaction will be logged to the `/var/spool/qmailscan/qmail-queue.log` file. Regardless of debugging, errors (and attachment info if enabled) should also be recorded in the **qmail** logs (probably via **syslog**). Note that the `/var/spool/qmailscan/qmail-queue.log` log file will grow in time unless you manage its regular cleanup (either manual or scheduled for example via the **cron** utility).

Any dropped SMTP session (for example due to network outages) may lead to files lying around in `/var/spool/qmailscan`. Running the

```
# /var/qmail/bin/qmail-scanner-queue.pl -z
```

command as root at least once a day will ensure such files are deleted when they are over 30 hours old (for example the **cron** utility can be employed to perform the regular cleanup).

**Note:** For details on the **Qmail-Scanner** please refer to the <http://qmail-scanner.sourceforge.net/> website.

#### 4.4. Testing the Installation

Successful installation of **AVG for Linux E-mail Server** and the appropriate mail content scanner (**AMAViS** or **Qmail-Scanner**) can be tested within any supported e-mail server by sending a message with the Eicar test file attachment. The attachment should be removed from the e-mail, and replaced by a virus infection notification. Refer to the [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm) website for detailed information and the test file itself.

## 5. E-mail Scanning

### 5.1. General Principles

The **AVG for Linux E-mail Server** service responsible for e-mail scanning runs as a set of memory resident daemons. These daemons are identical preforked processes bearing the **AVG Anti-Virus** scanning kernel and interface for scanning the e-mail content fetched by **AMaViS**, **Qmail-Scanner** or respective commercial e-mail server.

The number of e-mail scanning daemons can be specified in the **AVG for Linux E-mail Server** configuration file (see chapter [8.3 Configuration File/AvgDaemon](#) for detailed information on this issue). The default number of daemons is **2**, possible values range across all non-negative integers. Increase the number of daemons for very busy servers to accelerate the e-mail scanning by introducing a higher level of parallel processing. A general rule of how to regulate the number of daemons can not be formulated exactly because the scanning performance widely varies according to the particular system configuration, other services running and software installed.

***Note:** Be careful when changing the number of daemons; its excessive increase can cause temporary service failure problems after restarting or sending another signal to the **AVG for Linux** daemons (for example when the virus database is updated and being reloaded by scanning daemons)!*

The **AVG for Linux E-mail Server** e-mail scanning service is bound to the IP address that is also specified in the respective section of the configuration file (127.0.0.1 by default). The address must be the same as the one the mail transport agent is bound to. The default port which the daemons are listening on is 55555. If necessary, this value can be changed in the configuration file as well.

**AVG for Linux E-mail Server** does not support direct configuration of actions to be performed after virus detection and/or suspicion in the processed e-mail. These features are covered by the e-mail server agent and/or respective mail content scanner. Please refer to the documentation of your e-mail server and **AMaViS** or **Qmail-Scanner** for detailed information.

### 5.2. Performance and Resource Usage

Adding virus scanning to an e-mail server can slightly increase the resource usage of the server for the open source mail transport agents (these are **sendmail**, **postfix**, **qmail**, **exim**). As both of the e-mail scanner wrappers (**AMaViS** and **Qmail-Scanner**) are written in Perl instead of low-level C, some amount of memory and other system resources is required to make the scanning processes run in order to scan the e-mail server traffic efficiently. However, the real additional system load depends on many factors (such as the size of e-mail float, the number of memory resident processes and so on) that can be effectively optimized by the system administrator.

It is suggested that you look at how many simultaneous SMTP sessions you are willing to run on your system. Each SMTP session can claim a certain number of **AVG for Linux E-mail Server** virus scanning daemons. The estimated amount of memory to be used by all the scanning processes per SMTP session is about 5-6 MB. It is strictly recommended to take this into the account when planning a server policy and usage management strategies.

### 5.3. Using Unix Socket for an Extra Security

You can take advantage of launching the **AVG Anti-Virus** e-mail scanning daemon within the same account as the e-mail content scanner (**AMaViS** or **Qmail-Scanner**). Moreover, the e-mail scanning daemon can create a Unix socket and listen on it then in order to increase the e-mail scanning security. The socket is created and also destroyed by the daemon automatically with the proper access rights and ownership (e. g. **amavis** when the daemon is running under the **amavis** account).

To enable the using of the socket, follow these steps (you must be logged in as root):

- Uncomment the line with the **unixSocketName** parameter in the **/ect/avg.conf** **AVG for Linux E-mail Server** configuration file. You can also change the parameter value if necessary (the default value is **/tmp/avg.sock**). See chapter [8. Configuration File](#) for detailed information on the configuration file.
- In the **/opt/grisoft/avg7/etc/init.d/avgdinit.conf** file, change the **SUSER** parameter value to the name of the user who is supposed to run the e-mail scanning **AVG Anti-Virus** daemon (for example **amavis**).
- Finally, you must change the configuration file of the respective e-mail content scanner (**AMaViS** or **Qmail-Scanner**). For example, in the case of the preferred **amavisd-new** scanner the **AVG Anti-Virus** related section of the **/etc/amavisd.conf** file should look like as follows:

```
['AVG Anti-Virus', \&ask_daemon, ["SCAN {} \n", '/tmp/avg.sock'], qr/^200/,  
qr/^403/, qr/^403 .*?: (.+)/ ]
```

**Note:** The on-access scanning must be running under the root account. So if you change the user who is running the daemons in the **/etc/init.d/avgd** file, you will disable the on-access scanning! You have to resolve the trade-off between the on-access scanning and increased e-mail scanning security.

## 6. Commercial E-mail Servers

**AVG for Linux E-mail Server** can also be used with commercial e-mail servers running under Linux. The main idea of such a solution is to protect the (possibly Windows powered) computers of users connected to these e-mail servers against the possible virus infection. The following server products are supported:

- **Lotus Notes/Domino Server**
- **Kerio MailServer**

For all servers the preceding installation of the **AVG for Linux E-mail Server** product is necessary. For **Lotus Notes/Domino Server** a special **AVG Anti-Virus** plugin is also needed. **Kerio MailServer** offers internal support of **AVG for Linux E-mail Server**, so no additional tools are required.

### 6.1. AVG for Lotus Notes/Domino Server Installation and Maintenance

The anti-virus protection of e-mail communication on **Lotus Notes/Domino Server** with **AVG for Linux E-mail Server** can be performed using the special **AVG for Lotus Notes/Domino** Linux plugin. You can obtain the plugin in the form of a precompiled *.tar.gz* package on the **AVG Anti-Virus** installation CD, or in the **Download/Programs** section at <http://www.grisoft.com>.

Before you can install the plugin, you need to:

- install and configure **Lotus Domino Server for Linux**
- install and configure **AVG for Linux E-mail Server**

Also, you have to verify these configuration details:

- **AVG for Linux E-mail Server** mail scanning daemon **must** be bound to the 127.0.0.1(localhost) address  
(See section [8.3 Configuration File/AvgDaemon](#) for details)
- For Linux distributions with default UTF-8 locales (these are Red Hat 8, Red Hat 9, Fedora Core 1, Fedora Core 2, etc.), set the *LANG* environment variable to *C* or *cs\_CZ* (for Czech users) for the account which the Domino server is running under. These changes can be made following this example (supposing the Domino server is running under the **notes** account):

The **notes** account profile file (e. g. *.bash\_profile*) must contain these lines:

```
...  
  
LANG=cs_CZ  
  
LC_TIME=POSIX  
  
LC_MONETARY=cs_CZ  
  
LC_NUMERIC=cs_CZ  
  
LC_COLLATE=cs_CZ  
  
...
```

```
export BASH_ENV PATH LANG LC_TIME LC_MONETARY LC_NUMERIC  
LC_COLLATE
```

...

Once all the prerequisites mentioned above are satisfied, you can install the plugin. Unpack the plugin installation package with the

```
# tar -xvzf avgln_linux-{version}.i386.tar.gz
```

command (the *version* stands for the number of the plugin version).

Switch to the unpacked *avgln\_linux* directory and run the installation script as root:

```
# ./install.sh
```

This will install the **AVG for Lotus Notes/Domino Server** Linux plugins in several steps. At the end of the installation the *notes.ini* Lotus Notes/Domino server configuration file is edited in order to enable launching the **AVG for Lotus Notes/Domino** services. Check your *notes.ini* file for changes.

The following lines should be present there:

...

```
NSF_HOOKS=avghook
```

...

```
servertasks=...,avgmail,avgscan
```

...

```
AVGLang=x
```

...

where *x* is 1, 2, or 3 depending on language you have selected. The server tasks (servertasks) configuration line tells the **Lotus Notes/Domino Server** to run the **AVG for Lotus Notes/Domino** server services.

In order to complete the installation, **Lotus Notes/Domino Server** must be restarted. This will automatically launch the **AVG for Lotus Notes/Domino Server** Linux plugin (server services AvgScan and AvgMail) and create the **AVG Anti-Virus** databases (*AVG Configuration*, *AVG Log* and *AVG Virus Vault*). All of these can be blocked in the appropriate configuration sections later if needed.

After correct installation of the **AVG for Lotus Notes/Domino Server** plugin and **Lotus Notes/Domino** server restart there are no further actions needed for efficient mail protection. The default settings are as follows:

- scan all e-mails with attachments
- a certification message will be added to any e-mail which is virus-free, does not include a signature attachment, and has not been encrypted

- incoming files which are considered infected are sent to the recipient with a message containing file and virus details
- outgoing e-mail containing infected attachments will be returned to the sender with information about the infected objects and corresponding viruses; the infected e-mail will not be delivered to the recipient

You can easily change the default configuration of **AVG for Lotus Notes/Domino Server** using the **Lotus Notes/Domino Server administration console** graphical user interface. After selecting the **Files** tab in the initial window, you will see various **AVG Anti-Virus** related files (server databases literally) among all the files to administer:

Three **AVG Anti-Virus** fields are present:

- AVG Log
- AVG for Lotus Notes
- AVG Virus Vault

#### a) **AVG for Lotus Notes**

Double click on the **AVG for Lotus Notes** field in the administrator utility domain window's **File** tab (see the previous screenshot) to open the **AVG for Lotus Notes – Configuration** window:

In this window, select the appropriate server on which you want to have the **AVG Anti-Virus** configuration database. Double click its field or simply press the **Edit** button which is right above the servers' list. A new untitled window will then be opened within the administrator utility environment (see the following two screenshots):

You can fully control the scanning and infected e-mail management behavior of **AVG for Lotus Notes/Domino Server**, and also schedule possibly multiple server database scans. To save the configuration changes performed press the **Save and close** button in the upper area of the window.

All the configuration options fully corresponding to the fields presented on the screenshots above are as follows:

- **Global Settings**
  - **Server name** – the current server specification
  - **Certify mail** – select if **AVG for Lotus Notes/Domino Server** should certify e-mails or not
  - **Certify text** – edit the certification text (e.g. "The message is virus-free...")
- **Mail Scan**
  - **Scan mail** – enable/disable automatic e-mail anti-virus scanning
- **Incoming Mail Settings**
  - **Attachments** – enables defining file extensions of e-mail attachments that should be automatically removed from the e-mail. Attachments with user-defined extensions will be automatically



removed from an incoming e-mail, no matter whether the identified file has been infected by a virus or not. The possible actions are:

**No action**, incoming attachments won't be filtered or removed

**Remove**, user-defined attachments will be removed from virus-detected e-mail and then deleted

**Remove and store in Virus Vault**, user-defined attachments will be deleted from virus-detected e-mail and moved to the Virus Vault

You will be allowed to choose the attachment file extensions from the list of keywords (or you can type a new one if the desired extension is not in the list) in a new **Extensions** field when the **Remove** or **Remove and store...** actions are selected.

- **Virus found action** – you can specify action to be taken if a virus is found in an incoming e-mail:
  - **Deliver mail to the recipient**, the infected e-mail will be delivered to the recipient with a warning about the virus and infected file added; additional settings will define whether the infected attachments are removed from the mail and/or moved to the *AVG Virus Vault* database. A field entitled **Infected files** allows you to specify the action to be taken for virus-infected files. Possible actions are:
    - **Remove** – the infected files are removed from the e-mail
    - **Remove and store in Virus Vault** – the infected files are removed from the e-mail and stored in local Virus Vault
    - **Store in Virus Vault and deliver to recipient** – the infected files are kept in the e-mail and copies are also stored in local Virus Vault
    - **Deliver to recipient** – the infected files will be kept in the e-mail and delivered to recipient
    - **Return mail to sender**, the infected e-mail will be returned to the sender as undeliverable with an option to add a warning about the virus found
  - **Send warning to recipient/sender** – you can check this field if you wish to warn the recipient/sender (depending on whether you choose *Deliver mail to the recipient* or *Return mail to the sender* action on virus found) of virus-infected e-mail.
  - **Text of warning** – here, you can edit the default message text, which is included in the virus-infected e-mail if you have the **Send warning to recipient/sender** field checked on.
  - **Send warning to administrator** – when this field is checked on, a warning will be sent to administrators specified in the **Administrators** field after an incoming e-mail is detected as virus-infected. You can edit the text of the warning message in the corresponding **Text of warning** field.
  - **Outgoing Mail Settings**
    - Virus found action** – you can specify, which action is to be taken if there is a virus found in an outgoing e-mail:



- **Deliver mail to the recipient**, the infected e-mail will be delivered to the recipient with a warning about the virus and infected file added; additional settings will define whether the infected attachments are removed from the mail and/or moved to the *AVG Virus Vault* database. A field entitled **Infected files** allows you to specify the action to be taken for virus-infected files. Possible actions are:

**Remove** – the infected files are removed from the e-mail

**Remove and store in Virus Vault** – the infected files are removed from the e-mail and stored in local Virus Vault

**Store in Virus Vault and deliver to recipient** – the infected files are kept in the e-mail and copies are also stored in local Virus Vault

**Deliver to recipient** – the infected files will be kept in the e-mail and delivered to recipient

- **Return mail to sender**, the infected e-mail will be returned to the sender as undeliverable with an option of adding a warning about the virus found

**Send warning to recipient/sender** – you can check this field if you wish to warn the recipient/sender (depending on whether you choose *Deliver mail to the recipient* or *Return mail to the sender* action on virus found) of virus-infected e-mail.

**Text of warning** – here, you can edit the default message text, which is included in the virus-infected e-mail if you have the **Send warning to recipient/sender** field checked on.

**Send warning to administrator** – when this field is checked on, a warning will be sent to administrators specified in the **Administrators** field after an outgoing e-mail is detected as virus-infected. You can edit the text of the warning message in the corresponding **Text of warning** field.

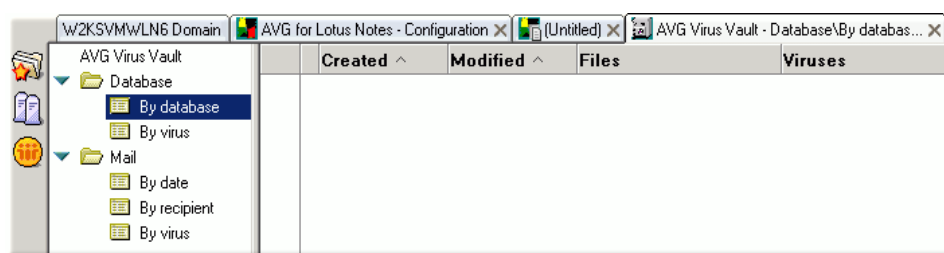
- o **Scheduled Database Scan**

You can plan the scanning of server databases in this area of the **AVG for Lotus Notes/Domino Server** configuration form. Various fields are available:

- **Scan at times** – a time interval and/or exact time data can be filled in to tell **AVG for Lotus Notes/Domino Server** when it should run the databases scanning (e. g. 8:00–22:00 or 8:00–22:00, 23:30, 05:00)
- **Repeat interval of** – the time in minutes, which defines the frequency of scans during the intervals specified in the Scan at times field
- **Days of the week** – you can select the days when database tests are run

- **Scan** – the attachments related field – you can define here whether to check all the attachments or only those with extensions specified in the **Extensions** field
- **Infected files** - allows you to specify the action to be taken for virus-infected files. Possible actions are:
  - Remove** – the infected files are removed from the document
  - Remove and store in Virus Vault** – the infected files are removed from the document and stored in local Virus Vault
  - Leave in the document** - the infected files are kept in the document
- **Scan** – the databases related field – you can define here, whether to scan all the server's databases or only those specified in the **List of databases** (files to scan) field
- **Send warning to administrator** – when this field is checked on, a warning will be sent to administrators specified in the **Administrators** field after a virus is detected during the database scan. You can edit the text of the warning message in the corresponding **Text of warning** field. The administrator is able to define the text of the subject line of an e-mail to be sent. In the warning e-mail body there a list of infected files (with links) and the viruses found.

## b) AVG Virus Vault



*AVG Virus Vault* is a special **Lotus Notes/Domino** server database, which the virus-infected files can be put into to treat (or delete or recover) them safely without risk of affecting the rest of your system resources.

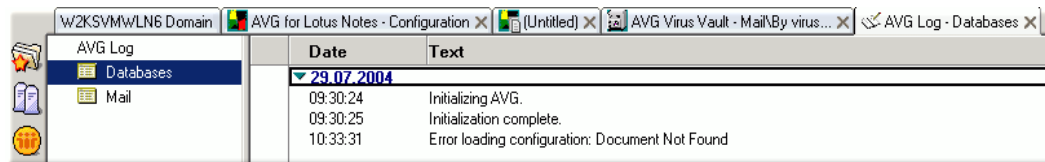
In the **Lotus Notes/Domino Server** administration environment you can access the Virus Vault via the *AVG Virus Vault* database. It is a special server database as mentioned in the previous paragraph. Double click the corresponding field in the Lotus administrator utility domain window's **File** tab and a new window will be opened:

You can examine the viruses put into Virus Vault in various ways of grouping the fields:

- o fields grouped by virus-infected database files detected during database scans
- o fields grouped by viruses found in databases during database scans
- o fields grouped by the date of infected message detected in e-mail scan

- o fields grouped by the recipient of infected message detected in e-mail scan:
- o fields grouped by the virus in infected message detected in e-mail scan

## c) AVG Log



Date	Text
29.07.2004	
09:30:24	Initializing AVG.
09:30:25	Initialization complete.
10:33:31	Error loading configuration: Document Not Found

In the *AVG Log* database information is stored on **AVG for Lotus Notes/Domino Server** events

recorded during the server's run. You can check and further examine various events such as initialization progress, viruses found and so on.

In the **Lotus Notes/Domino Server** administration environment you can access the log information via the *AVG Log* database. Double click the corresponding field in the administrator utility domain window's **Files** tab and a new window will be opened:

There are two fields present for both the Databases and Mail folders. Those are:

- o **Date** – the timestamp of the logged record
- o **Text** – the text of the log information

## d) Uninstalling the AVG for Lotus Notes Linux Plugin

If you want to install newer version of AVG for Lotus Notes Linux plugin, you must uninstall the older version first. You can perform the uninstallation manually as root. Follow these steps:

- o Check whether the Lotus Notes/Domino Server is running or not using the

```
# ps -A | grep server
```

command. If the server is running, the output should be something like this:

```
17064 pts/1 00:00:01 server
```

```
17068 pts/1 00:00:00 server
```

```
17069 pts/1 00:00:00 server
```

```
17076 pts/1 00:00:00 server
```

```
17077 pts/1 00:00:00 server
```

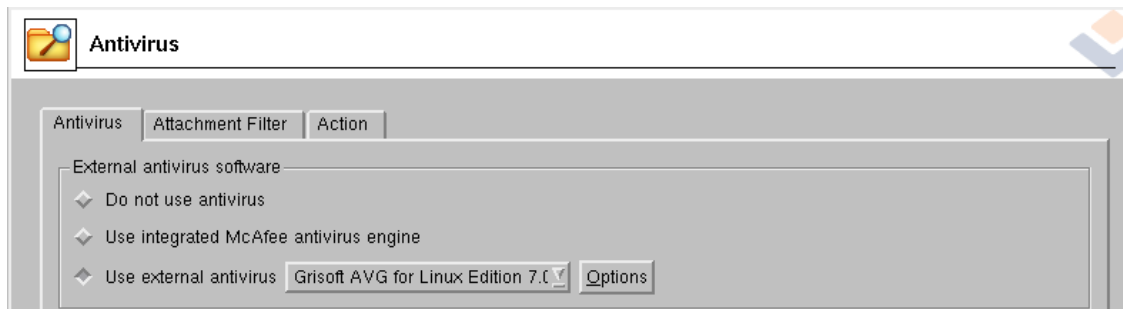
If the server is running, search all consoles (using the ALT+F1 – ALT+F6 keys). When you find the console which is the server running on, shut it down with the **exit** command.

- o Delete the following files from the ***/usr/local/lotus/notesdata*** directory:
  - avgln.pdf*
  - avglog.ntf*
  - avglog.nsf*
  - avgsetup.ntf*
  - avgsetup.nsf*
  - avgvirus.ntf*
  - avgvirus.nsf*
- o Open the ***/usr/local/lotus/notesdata/notes.ini*** in a text editor and delete the ***avgmail*** and ***avgscan*** strings from the line beginning with ***ServerTasks*** identifier.  
Delete also the whole lines
  - NSF\_HOOKS=AVGHOOK*
  - AVGLang=x*The 'x' depends on the language installed (1 for Czech, 2 for English and 3 for German).
- o From the ***/usr/local/lotus/notes/~latest/linux*** directory delete the files:
  - avgscan*
  - avgmail*
  - libavghook.so*

After performing the manual uninstallation you can install a new version of the AVG for Lotus Notes Linux plugin.

## 6.2. AVG for Kerio MailServer Maintenance

The anti-virus protection mechanism is integrated directly into the **Kerio MailServer** application. In order to activate e-mail protection of **Kerio MailServer** by the **AVG Anti-Virus** scanning engine, launch the **Kerio Administration Console** application (using the *kerioadmin* command in your shell). In the control tree on the left side of the application window choose the **Antivirus** sub-branch in the **Configuration** branch:



Click the **Antivirus** item to open the **Antivirus** dialog window. There are three tabs in the window:

- Antivirus
- Attachment Filter
- Action

To save the changes press the **Apply** button in the bottom area of the configuration window. You can also return to the previously saved state by pressing the **Reset** button.

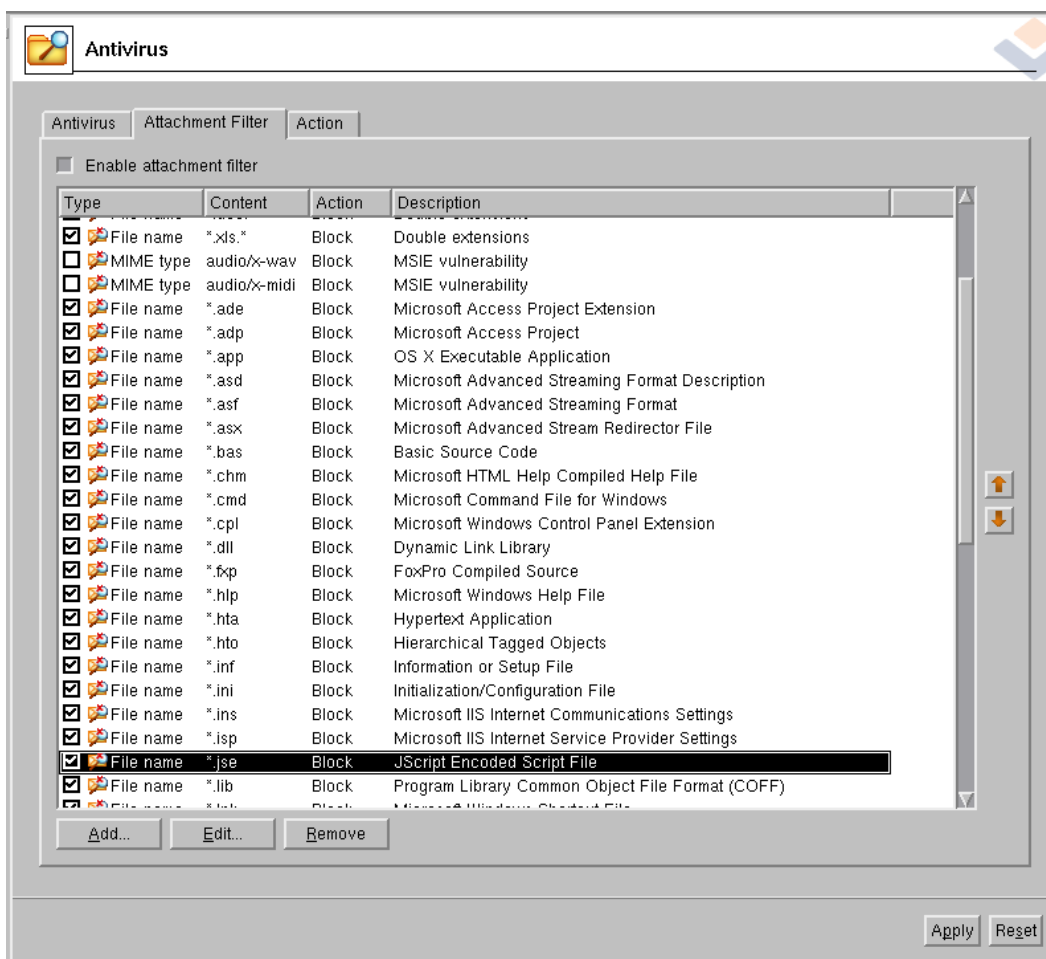
### a) Antivirus Tab

To activate **AVG for Kerio MailServer**, select the **Use external antivirus** radio button and choose the **Grisoft AVG for Linux Edition 7.1** item from the external software menu on the **Antivirus** tab of the configuration window:

You can press the **Options** button to open the following window:

In this window you can change the values of the address and port the **AVG for Linux** e-mail scanning daemon is listening on.

**Note:** You must set the appropriate values here, if you changed the address and port default settings in the **AVG for Linux E-mail Server** configuration file (refer to section [8.3 Configuration File/AvgDaemon](#) for detailed information on the configuration file)!



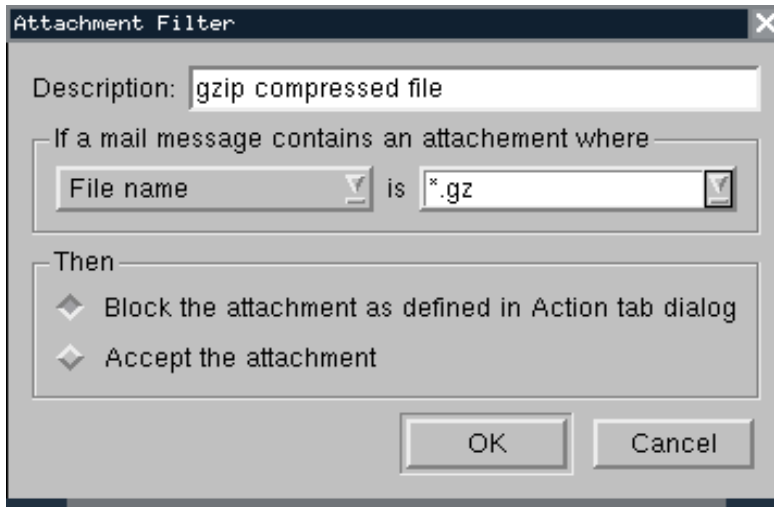
## b) Attachment Filter Tab

On the **Attachment Filter** tab there is a list of various attachment definitions:

You can enable/disable filtering of mail attachments by selecting the **Enable attachment filter** field. Each item in the list has four fields:

- **Type** – specification of the kind of attachment determined by the extension given in the **Content** field. Possible types are *File name* or *MIME type*. You can select the respective box in this field to include/exclude the item in/from attachment filtering.
- **Content** – an extension to be filtered can be specified here. You can use operation system wildcards here (for example the string *\*.doc.\** stands for any file with the .doc extension, and any other extension following).
- **Action** – define action to be performed with the particular attachment. Possible actions are *Accept* (accept the attachment), and *Block* (block the attachment as defined in the **Action** tab dialog).
- **Description** – description of the attachment defined in this item.

An item is removed from the list by pressing the **Remove** button. You can add another item to the list by pressing the **Add...** button. Or, you can edit an existing record by pressing the **Edit...** button. This window then appears:



- In the **Description** field you can write a short description of the attachment to be filtered.
- In the **If a mail message contains an attachment where** field you can select the type of attachment (*File name* or *MIME type*). You can also choose a particular extension from the offered extensions list, or you can type the extension wildcard directly.
- In the **Then** field you can decide whether to block the defined attachment or accept it.

**c) Action Tab**

You can specify what to do with a virus-infected or filtered message on the **Action** tab:



There are two sections:

o **Action**

This section specifies an action to be carried out when a virus is detected in a message, or when a message is filtered by an attachment filter:

- **Forward the message to administrator address** - when selected, the virus-infected message is forwarded to the address specified in address text field
- **Forward the filtered message to administrator address** - when selected, the filtered message is forwarded to the address specified in address text field
- **Deliver the message with the attachment removed** - when selected, the message with the possibly harmful attachment removed is delivered to the recipient
- **Also send warning to sender** - when selected, a warning is sent back to the message sender that his/her message was virus-infected and/or filtered. Having selected this item, the **Only if sender is local** checkbox will be active. You can specify whether to send the warning to all senders or to the local ones only (your domain users).
- **Bounce the message to sender** - when selected, the infected or filtered message is returned to its sender.
- **Discard the message** - when selected, the infected or filtered message is discarded.

o **If the attachment cannot be scanned**

This section specifies an action to be taken with unreadable attachments:

- **Perform action defined in the action frame** - message is treated as virus-infected and/or filtered and the action defined in the action frame is performed.
- **Allow the attachment to be delivered** - when checked, the message will be delivered. Also, the **Append a warning to the message** checkbox will be active then, so you can define whether to append a warning to the message to let the users be informed of a possible threat or not.



## 7. Standalone Command Line Modules

As a part of the **AVG for Linux E-mail Server** internal structure, several command line configurable and executable modules are included in the installation package.

### 7.1. AVGSCAN Command

The **avgscan** command is intended to perform various on-demand tests. Its performance is comprehensively controlled by the command line parameters. The general syntax of the command is

**\$ avgscan [options] [path|paths]**

The **[path|paths]** string stands for a single path or multiple paths to be scanned. The multiple paths are given in a list separated by the space character; a single object can be also given to be processed by the scanner. When no options are specified, a generic scan is performed for the given path(s).

**Note:** Although the **avgscan** command itself can manage only the on-demand test, you can also use it to create scheduled tests by incorporating the **cron** Linux system utility. See the manual pages (`man [cron/crontab]`) or the respective documentation for detailed information.

The options for the **avgscan** command and their descriptions are given in the following table:

Parameter	Description
-scan	Simple generic scan of the given objects and/or locations.
-heur	Switches on the heuristic analysis.
-exclude [PATH PATHS]	Excludes a particular path or paths from the scan; the path(s) to be excluded must be given right after this option, and separated by the space character.
-@ FILE	Specifies the command file with parameters to be processed by the <b>avgscan</b> program; the file name must be given right after this option, and separated by the space character.
-ext=<ext_mask>	Explicit specification of file extensions to be scanned in the form of  -ext=<ext_mask>, where the <ext_mask> string stands for the extension definition (for example "*", "jpg" , etc.). When entering multiple file extensions, they should be separated by a semicolon.

Parameter	Description
-noext=<ext_mask>	Explicit specification of file extensions not to be scanned in the form of  <i>-noext=&lt;ext_mask&gt;</i> , where the <i>&lt;ext_mask&gt;</i> string stands for the extension definition (for example <i>"*"</i> , <i>"jpg"</i> , etc.).
-smart	Switches on the smart scan testing feature.
-arc	Switches on scanning of archives (common archive file types like ZIP, GZIP, BZIP2 and others are supported).
-rt	Switches on scanning of run-time compressed objects.
-clean	Switches on the automatic healing of infected files.
-arcw	Reports archives encountered during scanning.
-rtw	Reports run-time compressions encountered during scanning.
-macrow	Reports macros encountered during scanning.
-pwdw	Reports password-protected files encountered during scanning.
-changew	Reports changes encountered during scanning.
-ignlocked	Makes the scanner ignore locked files.
-register [LICENSE]	Registers the <b>AVG for Linux E-mail Server</b> ; it is necessary to enter the valid license number either on the command line right after the <i>-register</i> option (separated by the space character), or later when prompted after the command execution without license given on the command line.
-report FILE	Reports messages about the test progress and results to the specified file; the file name must be given right after this option, and separated by the space character; when the specified file already exists, it will be overwritten.

Parameter	Description
-repappend FILE	Reports messages about the test progress and results to the specified file; the file name must be given right after this option, and separated by the space character; in reverse to the previous option, an existing file can be used to append the information to the end of the file; when a new file is specified, it will be created.
-repok	Switches on reporting of uninfected files 'is OK'.
-stoplevel N	Pauses when an erroneous state is encountered during scanning. Requires the integer argument N defining the internal code of a state in which the scan shall be paused.
-h, --help	Prints a brief overview of the program's options and usage.
-pup	Results in the detection of "potentially unwanted programs" within the scanning. Potentially unwanted program can be for example spy-ware or other possibly insecure programs.

**Note:** If you launch the **avgscan** command with the **-clean** parameter, **AVG Anti-Virus** will attempt to heal all infected files automatically. When the healing is successful, a **\$VAULT\$.AVG** folder is created (unless it exists already) in the home directory of the user who performed the test. The infected files are moved into this directory then, whereas the cleaned files remain in their original locations. Note the infected files are stored in a special **AVG Anti-Virus** format, ensuring they are absolutely harmless for your system!

Return values of **avgscan** program are:

- 0 – no errors
- 1 – the test was interrupted by user
- 2 – an error occurred during the test (e.g. cannot open file event)
- 3 – file system changes detected
- 4 – a suspect object found by heuristic analysis
- 5 – a virus found by heuristic analysis
- 6 – a particular virus was found
- 7 – an active virus found in memory
- 8 – corruption of some of the **AVG for Linux E-mail Server** command line components
- 10 – an archive contains password protected files

Some typical examples of **avgscan** use with brief explanations follow:

- **\$ avgscan /home/user**

scans the *user's* home directory

- **\$ avgscan -heur /home/user**  
scans the *user's* home directory using heuristic analysis
- **\$ avgscan /home/user/bin/run\_something.sh**  
scans the single file *run\_something.sh* in the *bin* directory of *user's* home
- **\$ avgscan -repok /home/user**  
scans *user's* home directory, reporting uninfected files as OK
- **\$ avgscan -report ~/reports/report001.avg /home/user**  
scans the *user's* home directory and reports the test results into the file *report001.avg* in the *reports* directory in the actual user's home
- **\$ avgscan -repappend ~/reports/report001.avg /home/user**  
scans the *user's* home directory and appends the test results to the file *report001.avg* in the *reports* directory in the actual user's home
- **\$ avgscan -arc -repok /home/user**  
scans the *user's* home directory including archives, reporting uninfected files as OK
- **\$ avgscan -ext=\* -rt -arc -heur /home**  
scans the files with any extension in the */home* directory, including the run time compressions and archives

**Note:** For online help on the *avgscan* command type

**\$ man -l /opt/grisoft/avg7/man/man1/avgscan.1.gz**

*in your shell.*

## 7.2. AVGUPDATE Command

Anti-virus systems can guarantee reliable protection only if they are updated regularly. **AVG for Linux E-mail Server** provides a reliable and fast update service with quick response times via the *avgupdate* command line utility.

**AVG Anti-Virus** offers three different update levels (update levels of lower importance automatically include more critical ones):

- **Priority update**  
The priority update contains changes necessary for reliable anti-virus protection. Typically, these are important virus definition updates. These updates should be applied as soon as they are available.
- **Recommended update**  
The recommended update contains various program changes, fixes and improvements.

- **Optional update**

The optional update reflects changes that are not necessary for program functionality – texts, updates of the setup component, etc. Optional updates can be downloaded and applied together with recommended updates but the timeliness of implementing them is not urgent.

**Note:** For e-mail servers in general it is **strictly recommended** to perform the priority update approximately every two hours! The recommended update should be performed at least once a day or on-demand.

You can review the performed update information in the update log file **avg7upd.log** that is to be found in the

**/opt/grisoft/avg7/var/update/log**

directory.

The **avgupdate** command is a tool for complex control over the on-demand update process. The update in general can be performed by launching this command. The update properties are controlled using the command options, which are listed in the table below. General syntax of the command is:

**\$ avgupdate [options] [path/list]**

The **[path/list]** string stands for the path of the explicitly given update files (or for the list of these update files separated by the space character).

**Note:** Although the **avgupdate** command itself can manage only the on-demand update, you can also use it to create scheduled updates by incorporating the **cron** Linux system utility. See the manual pages (`man [cron|crontab]`) or the respective documentation for detailed information.

The options for the **avgupdate** command are described in the following table:

Parameter	Description
-o, --online	Performs an online update from the Internet; the location where the update files are downloaded from is specified in the <b>AVG Anti-Virus</b> configuration file.  (See section <a href="#">8. Configuration File</a> for detailed information.)
-f, --offline	Performs an offline update from the location specified in the given <b>path</b> or <b>list</b> (as described in the beginning of this paragraph).
-d, --download	Only downloads update files without applying them; the download directory is specified in the <b>AVG Anti-Virus</b> configuration file.  (See section <a href="#">8. Configuration File</a> for detailed information.)
-p, --priority NUM	Specifies the priority of an update explicitly; the possible priority numbers are:  2 – priority update  3 – recommended update  4 – optional update
-c, --config FILE	Forces use of a configuration file other than the default one ( <b>/etc/avg.conf</b> ). The filename (with the specified path if necessary) is given by the FILE argument.
-i, --no-diff	Even when smaller binary diff files are available, only the full update files will be downloaded; this option can be useful when some parts of your <b>AVG for Linux E-mail Server</b> installation are corrupted or missing.
-b, --no-backup	When this option is selected the update process will not create backups of older files.
-n, --no-progress	<b>avgupdate</b> does not display update progress information after selecting this option.
-l, --no-log	No log file describing the update process will be created when this option is selected (by default, the log file is stored as <b>/opt/grisoft/avg7/var/update/log/avg7upd.log</b> ).

Parameter	Description
-a, --no-daemons	When this option is selected, the <b>AVG for Linux E-mail Server</b> daemons will not be restarted following the update; for some server systems this option can help in avoiding problems with the incorrect restart of daemons.
-m, --complete	Select this option when your <b>AVG for Linux E-mail Server</b> installation is seriously damaged to repair it.
-r, --restore	Restores the previous version of the whole <b>AVG for Linux E-mail Server</b> (before the last update was performed).
-v, --version	Displays the program version.
-h, --help	Prints a brief overview of the program's options and usage.

Return values of *avgupdate* program are:

- 0 – no errors occurred during the update
- 1 – nothing new to update
- 2 – an error occurred during the update

Some typical examples of *avgupdate* use with brief explanations follow:

- ***\$ avgupdate -o***  
the simple online update
- ***\$ avgupdate -f /tmp/avg/updfiles***  
performs the update from the files in the */tmp/avg/updfiles* local directory
- ***\$ avgupdate -o -p 4***  
performs the optional online update
- ***\$ avgupdate -o -c /home/user/conf/avg/avg.conf***  
performs the online update according to the configuration file *avg.conf* located in the */home/user/conf/avg/* local directory
- ***\$ avgupdate -o -l -m***  
performs the online update: downloads and applies the complete update file, and writes no information into the log file

**Note:** For online help on the *avgupdate* command type

***\$ man -l /opt/grisoft/avg7/man/man1/avgupdate.1.gz***

*in your shell.*

### 7.3. On-access Scanner

The DAZUKO kernel interface for file access control must be inserted as a module into your kernel in order to enable the on-access scanning using the **AVG for Linux E-mail Server** engine. You can download the latest version of DAZUKO at <http://www.dazuko.org>. It is recommended to download the latest version available especially if you are running the kernel of major version 2.6 (or higher)!

To install the DAZUKO kernel module, follow these instructions:

#### a) Get your Kernel Source Code

It is highly recommended to build and install a kernel from the actual kernel sources first. Then it is certain that the kernel source code you use to build DAZUKO matches the running kernel. Many Linux distributions provide packages with the kernel source code. If you do not plan building a completely new customized kernel, make sure you install the proper kernel source packages for your distribution.

***Note:** If you do not have any experience with building the Linux kernel, you should not attempt to install DAZUKO unless you get some information and practice in hacking the Linux kernel internals!*

#### b) Compile DAZUKO

Once the source code for your running kernel is available, you can build DAZUKO. You can download the latest version of DAZUKO at <http://www.dazuko.org>. Unpack the downloaded file using the

```
$ tar -xvzf dazuko-{version}.tar.gz
```

command and switch to the unpacked directory.

Edit the *configure* file and change the 0 value to 1 for the ON\_CLOSE\_MODIFIED parameter in the MAIN section. Generate a *Makefile* by running the

```
$ ./configure
```

command in the directory with the DAZUKO source files. This will determine the features of your system needing to be specified in the generated Makefile.

Then you can compile DAZUKO with the

```
$ make
```

command. This will create the device driver as well as a couple of example programs. Under Linux 2.2-2.4 the device driver is named *dazuko.o*. Under Linux 2.6 it is named *dazuko.ko*.

#### c) Insert DAZUKO

Having compiled DAZUKO successfully, the final step is to insert the module into the kernel.



**Note:** The process of inserting a kernel module may vary according to the particular Linux distribution. Refer to your distribution documentation to resolve possible problems. Also, there can be some differences according to various versions of DAZUKO. Refer to the detailed DAZUKO documentation at <http://www.dazuko.org>.

Create the device node for DAZUKO. This can be done executing the command (supposing the device major number is 254 for example reasons)

```
# mknod -m 600 /dev/dazuko c 254 0
```

```
# chown root:root /dev/dazuko
```

as the root.

Also, you have to copy the module (the **dazuko.o** or **dazuko.ko** file) to the **/lib/modules/src/kernel/char** directory.

Create a link to module by adding the line

```
alias char-major-254 dazuko
```

to the **/etc/modules.conf** file.

Insert the module as the root by executing the command

```
# /sbin/insmod/ dazuko.o or #/sbin/insmod dazuko.ko
```

for Linux 2.2-2.4 or Linux 2.6 kernels respectively.

To check if the module has been loaded use the

```
$ cat /proc/modules or $ lsmod | grep dazuko
```

command. If you see 'dazuko' string along with its device major number (usually 254) in the list of modules, it is successfully installed and inserted.

**Note:** If you get any warnings or error messages during the above described process, something may be wrong with your kernel source code or configuration. Please refer to the DAZUKO FAQ page at <http://www.dazuko.org> for detailed information on what may have happened, and how to fix the problem.

Once the DAZUKO module is installed and inserted, the **AVG for Linux E-mail Server** daemons responsible for the on-access scanning will be fully functional. You need to make sure the daemons are running and restart them if they have been stopped (refer to the following paragraph to see how to do this).

#### 7.4. Service Signals

Both on-access and e-mail scanning daemons are controlled within common **AVG for Linux E-mail Server** services. The services can be comprehensively managed by sending them a signal at once via the

```
# /etc/init.d/avgd [start/stop/restart/reload/status/condrestart]
```

command on most systems, or directly, using the

```
# /opt/grisoft/avg7/etc/init.d/avgd  
[start/stop/restart/reload/status/condrestart]
```

command.

The options in the square brackets represent the possible signals that can be sent to the **AVG for Linux E-mail Server** daemons:

- **start** – starts the daemons
- **stop** – stops the daemons
- **restart** – restarts the daemons
- **reload** – forces the daemons to reload the internal virus database
- **status** – shows the status of the daemons
- **condrestart** – conditionally restarts the daemons

*Note: You can only control the **AVG for Linux E-mail Server** daemons as root this way!*

The on-access scanning performance can be configured using the common **AVG for Linux E-mail Server** configuration file. (See chapter [8. Configuration File](#) for detailed information.)

## 8. Configuration File

The common configuration of **AVG for Linux E-mail Server** command line modules is covered in the **avg.conf** file, usually located in the **/opt/grisoft/avg7/etc** directory. The general syntax of the configuration file is described as follows:

```
...  
  
# comments  
  
[<section_name>]  
  
<parameter_name> = <value1> <value2>  
  
<parameter_name> = <value3> # comments  
  
...  
  
[<yet_another_section>]  
  
<parameter_for_this_section> = <its_value>  
  
...
```

The '#' character indicates a comment – the rest of the line following this character is ignored and will not be processed.

The square brackets ('[' and ']' characters) enclose a section name. All entries following the section specification until another section specification (or end of file) are considered as configuration options related to the respective section.

The entries for each section consist of the **parameter name** and its **value** (or **values**) specified after the '=' character. The values can be either numeric (integer) or strings. The numeric 1/0 values usually represent enabling/disabling of the respective feature specified by the parameter name.

Multiple values for one parameter can be separated by white space characters (for example space, tabulator, etc.) or by a new line (the parameter name must be given again in this case).

If you are logged in as root, you can change the parameter values directly in the configuration file **avg.conf** using any plain text editor (e.g. vi, vim, pico, joe, gedit, emacs, jed, jedit, ed, ...).

The configuration file consists of four sections.

### 8.1. AvgCommon

Configuration of the common features of **AVG for Linux E-mail Server** memory resident services (daemons) in general:

- **runtimeCompression** – scanning of files with runtime compression; possible values are 0 or 1; the default value is **1** (runtime compression scanning enabled)

- **heuristicAnalysis** – using of heuristic analysis scanning; possible values are 0 or 1, the default value is **0** (heuristic analysis disabled)
- **processesArchives** – scanning of archives; possible values are 0 or 1; the default value is **0** (archives scanning disabled)
- **syslogFacility** – specification of facility used by syslog daemon (refer to the syslog.conf manual pages for detailed information on the syslog features); possible values are literal string types; the default value is **daemon**
- **reportPasswordProtectedFiles** – reporting of password protected files; possible values are 0 or 1, the default value is **0** (reporting disabled)
- **reportMacros** – reporting of macro structures in the scanned files; possible values are 0 or 1, the default value is **0** (reporting disabled)
- **reportLockedFiles** – reporting of locked files; possible values are 0 or 1, the default value is **0** (reporting disabled)
- **pupAnalysis** – when set to **1**, “potentially unwanted programs” are detected within the on-access scanning; the default is **0** (no detection)

## 8.2. OnAccessScanner

Configuration of the on-access scanning daemon(s):

- **includePath** – the list of paths scanned by the on-access scanner (at least one path is required); possible values are strings according to the path specification syntax; the default value is **/mnt**
- **excludePath** – the list of paths ignored by the on-access scanner; possible values are strings according to the path specification syntax; the default value is **/proc**
- **numOfDaemons** – the number of on-access scanning daemons; possible values are non-negative integers from 0 to 10; the default value is **2**; specifying the number as 0 will disable the on-access scanning
- **scanOnOpen** – scanning of the files when being opened; possible values are 0 or 1; the default value is **1** (on open scan enabled)
- **scanOnExec** – scanning of the files when being executed; possible values are 0 or 1; the default value is **0** (on execute scan disabled)
- **scanOnClose** – scanning of the files when being closed; possible values are 0 or 1; the default value is **0** (on close scan disabled)
- **scanOnCloseModified** – scanning of the files when being closed after modification; possible values are 0 or 1; the default value is **1** (on close modified files scan enabled)
- **excludeFileSuffix** – the list of file suffixes ignored by the on-access scanner; possible values are strings according to suffix specification syntax, example values: **.jpg .gif**; the default value is none

## 8.3. AvgDaemon

Configuration of the **AVG for Linux E-mail Server** e-mail scanning daemon(s):

- **port** – port number the daemon listens on; possible values are positive integers (preferably assigned to unused ports); the default value is **55555**

- **unixSocketName** – the name of the Unix socket used for the e-mail scanning daemon communication purposes; the default value is ***/tmp/avg.sock***
- **address** – local IP address the daemon is bound to – should be the same as the local address of your e-mail server; possible values are numerical strings according to the IP address decimal representation syntax; the default value is ***127.0.0.1***
- **numOfDaemons** – the number of daemons; possible values are non-negative integers, the default value is ***2***; specifying the number to 0 will disable the daemon

#### 8.4. AvgUpdate

Configuration of the **avgupdate** module:

- **location** – the location where the update will be performed from; possible values are strings according to the general URL; the default value is ***http://www.grisoft.cz/softw/70/update***
- **proxy** – specification of the proxy server; possible values are strings in the form of *host:port*, where *host* is the address of a proxy server (decimal or alphanumeric address notation, e.g. *192.168.100.99* or *proxy.myserver.com*) and *port* is the numeric specification of respective port; to disable the proxy server leave the default ***off*** value
- **proxyLogin** – specification of the proxy user, enabled only when the *proxy* option is enabled as well; possible values are strings in the form of *user:password*, for example *frog:swamp*; to disable this feature leave the default ***off*** value
- **backupDir** – the location of the backup directory that is used for storing the backup data before performing the update itself; possible values are strings according to the path specification syntax; the default value is ***/opt/grisoft/avg7/var/update/backup***
- **preinstallDir** – the location of the directory that is used for storing the update data before installing them (the directory is cleared after completing the update); possible values are strings according to the path specification syntax, the default value is ***/opt/grisoft/avg7/var/update/preinstall***
- **downloadDir** – the location of the directory that is used for storing the downloaded update files (unless the **avgupdate -d** command line option is specified, the directory is cleared after finishing the update); possible values are strings according to the path specification syntax; the default value is ***/opt/grisoft/avg7/var/update/download***
- **logFile** – the location of the update log file; possible values are strings according to the path specification syntax; by default ***/opt/grisoft/avg7/var/update/log/avg7upd.log***
- **logLevel** – the update logging level; possible values are integer numbers from 1 to 3 (the default value is ***1***):
  - 1 – lowest logging level, only the update start/finish information is recorded
  - 2 – medium logging level, some more information on various update phases is recorded

- 3 – maximum logging level, detailed information on all update phases is recorded (useful when an update fails for some unknown reason)
- ***timeout*** – specification of the maximum time the download can take (in seconds); possible values are non-negative integers; the default value is **0** (no limitation posed upon the downloading time)

## 9. FAQ and Technical Support

The FAQ section of the **Grisoft** website (<http://www.grisoft.com>) provides answers to most issues that you may encounter while using **AVG for Linux E-mail Server**.

If you do not find the solution of your problem in the **FAQ section** or **documentation**, contact the **GRI SOFT** technical support department via e-mail at [technicalsupport@grisoft.com](mailto:technicalsupport@grisoft.com).

Providing the following information in the e-mail will help our technical support to give you a quick and comprehensive response:

- **Basic information (should be included always):**
  - version of your **AVG for Linux E-mail Server** (the version can be found out using the *avgscan* command)
  - your distribution of Linux (or other UNIX based system version)
  - your **AVG Anti-Virus** license number
- **Situation dependent information (according to the particular problem):**
  - If there is a problem with e-mail processing in general, we need to know which e-mail server and e-mail content scanner (**AMaViS** or **Qmail-scanner** version) you use.
  - If some viruses are coming through the e-mail server, send the virus samples and also the information required in the previous point.
  - If there is a problem with updates, set the logging level to 3 in the */etc/avg.conf* file and send us the */etc/avg.conf* and */opt/grisoft/avg7/var/update/log/avg7upd.log* files. See section [8.4 Configuration File/AvgUpdate](#) for details on the logging level settings.
  - If you have some problem with on-access scanner, we need you to tell us which version of DAZUKO you use. You should also send the */etc/avg.conf* file.
  - For problems with the system libraries, please refer to section [2.1 Before Installation/Prerequisites](#) in this document.
  - If you experience license number and/or registration problems, send us your license number and the exact transcript of the command you used for the registration.
  - If there is some problem with file system scanning, send us the exact transcript of the scanning command you have used.